The Electronic Money Mill

Xavier I. Quennel

March 30, 1998

Chapter 1

Damn.
It still wouldn't work out. This must have been the third time I had worked it through from the start and I was beginning to realize that there was a good chance I would not be able to get it.

The chair let out a plaintive creak as I leaned over the table, pulling the chair up onto two legs. I mouthed my thoughts quietly to myself as I once again began at the top.

I had x_0 and x_1 available as inputs and knew that $h(x_0) \neq h(x_1)$. Well, I didn't *know* they were unequal but I could justifiably *assume* that they were unequal since both x_0 and x_1 were arbitrary and h represented a collision-free hash function. More specifically, h was a MAC with a fixed key. The chances of two arbitrarily chosen inputs hashing to the same output value were very slim indeed.

Damn it! The point on my pencil broke. Again. I was using a 0.5mm mechanical pencil as usual. And as usual I was going through the lead pretty quickly, breaking the point every few minutes.

I threw the pencil down in disgust and pushed the chair back. I got up and headed over to the window. I had to collect my thoughts and try a new approach. The old approach was getting nowhere and I was getting impatient. Justifiably so too, since it was already 2:30 in the morning, leaving only six more hours until my deadline. Not that I had an interest in resolving this mess quickly. Rather, because *she* had an interest in seeing this whole mess sorted out. My only involvement was that I was the one who created the mess. I suppose that meant that I had a certain responsibility to correct the situation. Yet even that wasn't quite it. I just felt compelled to help her... I had tried to convince myself, unsuccessfully, that it had nothing to do with her looks.

As I stood staring out the window, with the rain-soaked street glistening in the glow of the street-light below, a feeling of despair came over me. I'd been at it since late afternoon, taking only a short break to grab dinner at the fast-food place just around the corner. I had brought the food back to my small apartment and eaten it at the kitchen table. While wolfing down the greasy burger in large mouthfuls, I had stared at the formulas scrawled on the papers strewn across the cluttered table before me. My kitchen table is barely

large enough to accommodate two people, so it does not require many papers to entirely cover the surface. The papers were filled with dead ends. Every scenario I had tried had failed. Every avenue I had pursued had come up empty. I was unable to develop a chronology of events that would explain the few clues I had.

I wiped perspiration off my brow. The week before had been one of the hottest on record for Chicago and this week wasn't much better. The rain from earlier that night had done nothing to bring down the temperature; it had only made the air moist and muggy. I was grateful that my apartment, while lacking in nearly every other respect, does have adequate air-conditioning.

The sphere of light extending outward from the street-light was cloudy with moisture. The light was not strong enough to penetrate the hot haze, leaving the rest of the street dark and murky. It matched my mood.

I sighed heavily, unclasped my hands from behind my back, and folded them across my chest instead. I had to face the possibility that I would not be able to find the problem, nevermind the solution. I was still struggling to determine what had happened the afternoon of July 11th.

Chapter 2

I don't own a car. I know that sounds strange, and I suppose it is, but after my last car was beyond repair I discovered that I didn't really need one and never bothered to replace it. That was three years ago.

It seems to me that the two primary uses for a car are to commute to work and to run daily shopping errands. Neither apply to me; I live about two blocks from the small room I rent for office space, and I am not much of a shopper.

Using my usual mode of transportation, I took the bus the afternoon of Saturday, July 15th. After transferring near the Aquarium, I took another bus to the 52000 block of Michigan Avenue. I was still groggy from lack of sleep the night before when I stepped off the bus. I consulted the scrap of paper upon which I had scrawled the address. It was a small piece of paper, torn off the corner of a larger sheet, with only the number written on it. I had scribbled it down as I listened to the president of First Chicago Trust speaking on the phone to a member of the FBI. The FBI agent, a man who identified himself as Mr. Carter, had informed the bank president that Lisa Cryer, a customer of the bank, was the prime suspect in the July 11th "incident". It was Lisa Cryer I was now on my way to meet. My arrival at her doorstep would be unannounced and uninvited. After hearing the phone conversation between Mr. Carter and the president of First Chicago Trust, I came to realize that Lisa Cryer would bear the burden of a problem that I had helped create.

I hadn't heard all of that particular conversation, as it took me longer to set up the wire-tap that day than it usually does (the trunk line I usually use was down for maintenance). Nonetheless I had heard enough of the phone call to learn about an appointment between Lisa Cryer and the bank security officer. After spending very nearly all of Thursday night trying to unravel the mysterious events of the previous Tuesday, and making no progress, I had arranged to be at the bank at 9:00 AM Friday. I was standing in the lobby when Lisa Melinda Cryer kept her appointment. She appeared to be in her late twenties. An African-American with light-brown complexion, perhaps her most striking feature was her hair. It was extremely short, little more than a smooth fuzz that covered her head. It was just long enough to curl a bit, lending some texture. After her hair, her next most striking feature was her gate and general bearing. Her legs were long and shapely, and she walked with a slight bounce

or hop in her step. Her walk was care-free and confident, with a slight hint of a skip. Her whole manner exuded self-confidence and good humor. And this was on her way to a meeting with bank security to discuss irregularities in her account transactions. Hers was the sort of face that breaks into a smile at the slightest provocation. She was not overly athletic; she was physically fit yet still shapely in all the right places.

Now, a little over 24 hours after watching her at the bank, I was on my way to her apartment. I had been unable to gather much information from that meeting, as I had no way of knowing what transpired in the meeting itself. However, simply by being in the bank lobby at 9:00 when Lisa Cryer kept the appointment allowed me to put a face with the person being blamed for my tinkering.

As the bus coughed and wheezed away from the curb behind me, I checked the paper again. Number 49812, apartment 2E. I looked up. The first number I noticed, on the building just across the street, was 51081. I was on the correct side of the street at least, but it looked like I had a bit of walking to do.

It was a pleasant day, probably about 78 degrees, and sunny. It was the nicest day we had had in two weeks, with a cool breeze to keep me comfortable as I began walking south, noting the street numbers as I went. This was a residential area; the majority of the buildings were high-rise apartments. Still, there were occasional smaller buildings mixed in, particularly near the street corners.

After I passed number 50008 I began to pay close attention to my surroundings. I had suspicions that Ms. Cryer might be under surveillance.

There were several pedestrians on the sidewalks, and of course a steady stream of cars filled the street. There were also cars parked along the curb at metered spots, with very few empty spaces. I checked each parked car on both sides of the street as I walked. So far they were all empty. I had no idea what an undercover cop might look like but I dutifully studied each pedestrian I passed on the sidewalk. I wondered if the guy in the white T-shirt loitering in the door-frame of the party store across the street was a spook. More than likely he was the proprietor, lamenting the lack of business. What about the woman with the over-sized sunglasses walking down the sidewalk towards me? She seemed to be walking too fast to be conducting surveillance, unless she was one of several people and only had to cover a limited area in her immediate vicinity. I doubted there would be too many undercover cops on this assignment. More likely it would be less than three people (and quite probably zero). The woman approaching me wore a tight yellow skirt with a matching jacket (or blouse, she was still too far away to tell which). Her hair was about shoulder length, brunette.

I turned my attention to the cars running along Michigan Avenue. Would I be able to tell if the same car went by more than once? Not likely. I did try to make a mental note of the cars as they went by, but there were far too many to really remember any of them. At that moment one car in particular caught my attention. This car was different only because it was moving slowly enough that it was interfering with the otherwise unimpeded flow. Traffic was

heavy, but not heavy enough to cause congestion. The average speed appeared to be comfortably over the posted limit of 45 mph. But this particular car, a black Caprice with two men seated in the front, was moving considerably slower than the other cars. The result was that a long queue had formed behind it. A couple of the cars directly behind it were weaving left and right to catch a glimpse around it and honking occasionally. The two passengers in the Caprice were probably in their early forties and well dressed. Hmmm... FBI?

The Caprice traveled down the street for two blocks and then turned right. I decided to walk a bit more slowly to give them time to circle around... if that was in fact what they were up to.

As I slowly plodded along I was passed from behind by a man trotting at a light pace. He was not running for exercise but rather was in a hurry to get someplace. He was wearing a dark-blue work uniform; probably a plumber or repairman of some sort.

I stole a glance at the woman wearing the yellow skirt and the sunglasses as she swished past me. It was hard to determine where her eyes were directed, but she certainly didn't have the air of somebody paying much attention to her surroundings (and she showed no interest in me whatsoever (too bad too because she was quite attractive)).

I was down to number 49874. Number 49870 was a flower shop. There was a small table in front of the store with an elderly woman standing behind it unhurriedly cutting and arranging flowers. She smiled as I walked by.

I looked at my watch (3:30). I glanced at the street. Aha! The Caprice was back. There was no question that it was the same car. And it was behaving in the same way (the people stuck behind it this time were no happier about it than the last pack had been). I watched it as it once again crawled along and turned right at the same corner.

This time I reacted by quickening my pace. I wanted to be inside building 49812 before they came by again. Darn! Why hadn't I thought to time the interval? Then I would know how much time I had before they showed up again. I really should have timed them... why didn't I? I answered my own question: because I really had not expected them to circle around; I had been looking for undercover cops as a diversion to pass the time and amuse myself. I was quite surprised (and pleased with myself) to learn that my caution had paid off.

Not happy with my rate of progress, I broke into a trot. I was getting closer: 49860, 49856, 49854. Why are street addresses so unevenly distributed? 49852, 49848, 49840,... I quickened my pace. 49832, 49818. Huh? I did a double-take and then checked the next number carefully, slowing down to do so. It was 49816. Good, almost there.

I barely broke stride when I got to 49812. I made a quick left and ran up the steps. There was a set of outer glass doors, which I quickly entered.

"You are not out of view of the street yet," I thought to myself. I quickly scanned the street but saw no sign of the Caprice. Then, on impulse, I quickly looked up and down both sidewalks but did not notice any pedestrians watching the building. I suddenly realized that if anybody *had* been watching, or if

anybody was sitting in a parked car and watching me now, that my arrival had not been the most circumspect, racing up to the door-way as I had. Too late; I'd just have to hope that the Caprice was the full detail for this assignment.

There was a panel of buzzer buttons on the wall, with the apartment number associated with each button indicated by little strips of tape beside each one. I quickly scanned down the list of apartment numbers, absently noting that some numbers were missing. Did this mean that those apartments were empty or what? I went ahead and pushed 2E, still not sure exactly what I would say.

"Yeah?", came the curt, almost bored, reply.

"Hello, Ms. Cryer?"

"Yes, who is it?"

"My name is Carl Raymond. You don't know me but I would very much like to speak to you. If you are uncomfortable ringing me in, could you at least come down and speak to me for a moment. This concerns the confusion at First Chicago."

"OK, hold on a sec. I'll be down."

So far so good. At least she was willing to talk to me. I had been worried that she would dismiss me as either a nut or a pushy salesman. If I could just have a chance to explain the situation I felt that there was a good chance that she might be understanding. I had been dreading the coming conversation for several days now. How do you tell a total stranger that you are responsible for causing her to be the prime suspect in a bank heist?

I raked my fingers through my black curly hair as I waited. I straightened out the front of my shirt. I wanted to make a good first impression. I hoped that my appearance was professional but casual. I had chosen to wear dark blue pants with black loafers. My shirt, an Oxford, was neatly pressed and light blue in color. I had considered wearing a tie but thought better of it. It would only make me uncomfortable since I never wear them. Besides, I did not want to *appear* to be concerned with my appearance, even if I was.

Ms. Cryer didn't keep me waiting long. I could see the elevator doors open from where I was standing. They were along the wall perpendicular to the glass doors where I was standing. She immediately turned to look in my direction upon stepping out of the elevators. She approached without hesitation, but studied me as she walked. I of course studied her in return, although I had the advantage, having already seen her at the bank. This time she was dressed more casually. She was wearing a loose-fitting grey sweatshirt with the collar stretched out, exposing more of one shoulder than the other. Quite a bit more. This was due in part to the fact that she had the tip of one sleeve pinched in her fist. She was wearing black stretch-pants and short soft-leather boots, also black. I was struck by her seemingly effortless beauty, for it was clear that she was not dressed to impress anybody.

At the door there was an almost imperceptible pause as she quickly looked me over a final time before opening the door. She wasn't overtly hostile, nor overly friendly. She stood holding the door, saying nothing. I walked in, giving her what I hoped was a reassuring smile. I was glad to be out of view from the street and the black Caprice.

"We can talk here in the lobby," she said. "Go ahead and have a seat." There were two sofas in the center of the room, arranged in an 'L'. Between the sofas was a small end table with a lamp and a small glass dish filled with mints. The room lighting was dim, with the lamp on the end-table being the primary source of illumination for that part of the room. On the floor was a nice (imitation?) oriental rug of red and green. This was a far cry nicer than my own apartment building. Not only does my building lack a lobby, but the hallway downstairs is tiled with cracked linoleum and the air is stale due to poor ventilation. The lone window at the end of the hallway does not provide adequate movement in the air to rid it of the musty odor. The light-bulb overhead has long since burned out, and while that one window does allow a sharp beam of sunlight to fill the hallway in the late afternoon, it is always a bit of a struggle to navigate from the front door to the staircase late at night. Even regular residents, who travel that route daily, stumble in the dark.

Ms. Cryer's apartment building was considerably more pleasant. As we sat down in the comfortable sofas, I tried once more to figure out where to begin. I looked into her eyes and was met with a steady gaze. Her expression remained neutral; she wasn't going to make this easy for me. Apparently she had decided that she was going to let me have my say but she wasn't going to play her hand until she saw where things were heading. What was it about her that put me off-guard? Why did I suddenly feel so helpless? Wasn't she the one that was at a disadvantage, having the bank breathing down her neck and not knowing what was going on? So why did I feel she had the upper hand?

I let out a long breath and dove in. "I'm aware of the situation at First Chicago and I may be able to help you. I think I know what happened. Some funds have been improperly transfered out of several bank accounts at a number of banks around the country, including accounts at First Chicago. Apparently these funds have ended up in your account, which is why First Chicago has been auditing your account recently."

Not knowing how to continue I paused there. Thankfully, she filled the silence.

"Who do you work for? Are you with First Chicago Trust?"

OK, not exactly the question I wanted just then, but fair enough.

"No. At the moment I don't work for anybody. I am a self-employed computer scientist. I do consulting work. I was in the bank yesterday afternoon and overheard part of your conversation."

"Are you always this nosy," she asked. She wasn't angry, just annoyed.

"Well no. I had a special interest in this particular case... having been partly responsible."

Now she was angry. Those large dark eyes were piercing into me, with a sparkle that hadn't been there moments before. Her nostrils flared and her breathing came in shorter intervals. Her lips were drawn tight. Yet she said nothing, waiting. I felt thoroughly disarmed. Was this the same woman? Was this the woman that had appeared so uncaring yesterday on the way to her interrogation at the bank? Despite my best efforts to remain collected I found myself shrugging sheepishly.

"Look, I'm sorry," I said, "things didn't turn out quite the way I planned."

"PLANNED!?" She was on her feet now, facing me with her hands on her hips, her feet spread wide. I was still seated and this, combined with her own height, meant that her eyes bore down on me from above. "I don't know what your *plan* was, but I sure as hell hope it didn't turn out quite the way you planned! What were you trying to accomplish?"

She didn't give me a chance to reply as she continued to berate me. Her hands were on her hips and she was bent forward with her chin chutting outward. "The police say that thousands of dollars were stolen. Are you the one that was messing with the transmissions? Do you know that tampering with electronic banking is a serious federal offense?

"Did you just pick a person at random and decide you'd see if you could completely screw up her life?" Her eyes burned into me as she now waited for a response.

"No," I said, "I didn't pick a person at random. I didn't *pick* anybody. The fact that you were singled out is the part that I still don't understand. It wasn't my doing. Really.

"I don't even know you," I continued. "I never saw you before yesterday. I came here today because I want to help you. If I'm going to help you then I need to understand why only you were affected by the bad transfers." I was talking fast, on the defensive, and I could see that I wasn't helping my case. Her face was twisted in utter contempt.

"So tell me again why you want to help me. If you are the one behind all of this then that hardly gives me the impression that you are the most humanitarian person around," she jeered. She quickly added, "why shouldn't I call the police or the bank immediately? You can talk to them. And before you get any ideas, one scream from me and the landlord and his staff will be in here before you can get out of that seat."

I glanced around and could not help but notice that the place was deserted. I had no intention of harming her in any way, but that last comment was clearly a bluff and I began to worry that she would cut our conversation short unless I put her at ease.

"Look", I said. "I'm not going to do anything. You can call the police if you like. Or the bank for that matter. I'll tell them what I know, they'll ask some more questions of you, and together we can all try to work this out. But I don't think anything will be resolved if we try that." I needed to placate her, and do it quickly before she gave up on me.

"The situation is actually quite complicated," I continued. "I really don't know what is going on myself. One thing I *do* know however is that dragging First Chicago and the police into this matter at this time might not be the best way to proceed."

"And why not?"

"Because First Chicago's role in all of this is pretty suspicious." I raised my hand to cut-off her reply, having already realized that I'd left myself wide open to another barb about my own suspicious behavior.

"As near as I can tell," I explained, "you were singled out as a result of their actions... or at least their reactions to my actions. Yet, they are investigating you as if they don't realize this. They should know full well that you were not actively involved. This is the part that I don't understand," I said. She let out an exasperated sigh and shook her head, rolling her eyes slightly.

"Look," I said as I spread my arms wide imploringly, "if we are going to get anywhere with this, you'll have to let me explain everything from the top. But this isn't really the best place for that." I glanced across the room at a middle-aged couple that stepped out of the elevators and headed for the door.

She let out a short sigh, looked at the clock on the far wall, and said, "OK, you're right. But you're not coming up to my apartment. Do you have any suggestions? Would a restaurant be OK?"

"Perfect. I'll let you pick the place; I don't live around here."

"There is a small restaurant down the street. They have good seafood. Why don't we go there?" she suggested. I nodded and she continued, "It's still too early to eat now. Come back in about two hours. That'll be 6:15," she said, doing my math for me.

We agreed to meet again in the lobby at that time, as I wasn't exactly sure where the restaurant was and it seemed easier to walk over together. I got up and offered to shake her hand as I prepared to leave. She shook my hand lightly and we went our separate ways — she headed back for the elevators and I headed off to kill two hours.

Chapter 3

As I went back out the glass doors I checked the street in front of me for a black Caprice. No sign of it. Fully expecting the ominous car to show up at any moment I hurried away heading south, trying to put as much distance as possible between me and Ms. Cryer's apartment. After I had gone two blocks, I looked back up the street. Yup. There it was! Or at least there was a dark car moving slowly in my direction. It seemed a safe assumption that it was the Caprice. I turned my back to them and hoped that I was far enough away from the apartment that they wouldn't notice me. I made an effort to "act natural" as I continued to walk down the sidewalk.

As I sauntered down Michigan Avenue, I reflected on the odds that somebody had seen me leave. My exit had been only slightly less rushed than my arrival. That was a mistake; I really should have taken the time to check for surveillance when I left. I'm not good at the cloak-and-dagger game. I've got no experience at this sort of thing.

I would have to assume I had been spotted. Maybe even photographed. I had better keep on my toes. I looked behind me. Nobody was following me on foot, and all of the cars were moving more quickly than I was. The Caprice had turned off at an intersection behind me. I would have to do the best I could to note the cars as they went by and try to determine if any were using the circling trick.

As I walked (and watched cars) I reviewed my conversation with Lisa Cryer. It hadn't gone too badly. Sure she was annoyed with me, maybe even disgusted, but she was giving me a second chance to explain myself and she said she wouldn't call the police yet.

I was far enough from the building now that I began to relax. I jammed my fists into my pockets and let the tension leave my shoulders. The sun shone brightly and the pavement was hot beneath my feet. This was probably due to the thin soles on my sneakers as much as it was the warm sunshine. I tend to wear one pair of sneakers as walking shoes, using a separate pair for athletics. The result is that my walking sneakers wear out very slowly and the soles go before the rest of the shoe. As I walked along the street I tried to remember how long I'd had these shoes. I'd bought them the summer between college and graduate school, so that would make them about fifteen years old now. That

was the summer I started work at AT&T. I began as a part-time employee in the OS department. My first project involved reviewing source code and testing networking software for bugs. I had liked the work, and perhaps more importantly to me at the time, I liked the people. It was a care-free time for me. I had already decided to go on to grad school and had several more years ahead of me before I had to think seriously about a career. In the meantime I only needed a bit of spending money and a job I enjoyed. For their part AT&T was pleased with me and allowed me to maintain a position throughout my five years of graduate school at Princeton. The arrangement worked well for all involved. My dissertation was all I could handle and I didn't want a job that would distract from my research, so I continued to work in the software testing department. It wasn't hard work, nor especially exciting, but it served my purposes.

There was a time when I went through my sneakers more quickly than I do now. I don't even have a second pair for athletics anymore. I ran track while in college at Berkeley, but no more. I had joined the team Junior year. Originally, I had joined only to give myself a distraction from my studies and from Marsha Banniff. Marsha and I had just broken up, after a two-year relationship. Marsha was a German major with no interest whatsoever in math, engineering, science, or economics. Her interests were romance languages, sociology, and theology. We could not have been further apart academically, and I think we both found this refreshing (I know I did). My interests were computer languages, economics, and discrete mathematics. She claimed the reason for the breakup was that I spent too much time on my schoolwork and that I did not leave time for us. I suspect the real reason for the breakup was that I did not leave enough time for her course-work, as she was the more studious of the two of us. Still, she had a point; both of us seemed to be over-committed and anxious to blame somebody or something other than ourselves. We both dealt with it in the same way — using the other as a scapegoat.

Joining track proved to be a good idea. It gave me an outlet for my frustration. I spent many long hours circling the football field, thinking about whatever crossed my mind. I never did excel in the sport. After two years I reached a reasonably competitive level, but never was a top member of the team. Still, I enjoyed it. I should start jogging again I suppose; I have let myself slip out of shape of late.

A car horn and the squealing of brakes brought me back to the present. A large truck was making a right turn and the car behind it had made the mistake of not heeding the "this truck makes wide turns" sign on the back of the truck. The car had to back up slightly to make more room, thus upsetting the cars behind it. This had a small rippling affect, as the line of six or seven cars each had to back up a car-length, each driver showing his or her annoyance in turn, some more so than others. I slowly approached the corner and paused for a break in the traffic. Somewhere about two blocks earlier I had stopped watching for undercover cops that might be following me. I now quickly surveyed the situation.

Across the street, in the direction I was heading, was a gas station. Just

beyond it was a carpet store. It was one of those stores that runs a perpetual sale. The banner in the window warned that time was running out on the current sale (but neglected to say that the next sale would undoubtedly be starting within a week). On the corner diagonally across from where I stood was a residential apartment building. Two old men were sitting on the stoop passing the time. Neither one looked remotely like an undercover agent (it was at this point that I decided I was being paranoid and could stop viewing everybody I saw as a spy).

Beside me was a restaurant; the sign above the door read "Sid's Seafood Grill." I realized that this must be the seafood restaurant Lisa had suggested. Judging from the store-front, it looked like a nice place. On impulse I decided to explore further. The sign in the window said it was open; I walked in.

There was a dining room off to the left and the bar was to my right. Two middle-aged men were sitting together near the middle of the bar and a young blonde-haired woman was sitting alone at the far end. The bartender was busying himself wiping glasses with a dish-cloth that looked a bit too dirty to be useful. He glanced in my direction, nodded, and went back to work on another glass. The two men were engaged in an animated conversation and didn't notice my arrival. The woman was lost in thought, contemplating the cigarette in her hand. She wore a tight red dress and heavy make-up.

"May I help you?"

It was the maître d' coming up beside me. It would have been odd to reply with, "no thanks, I'm just looking." Accurate... but odd. Instead, I made a reservation for dinner for two. Why not? It might not occur to Lisa, and it would be a nuisance if we were unable to get a table.

As she took down my name I glanced into the dining room. It was early enough that all the tables were empty. The decor was pleasant, with fish netting and wooden models of fish and crabs on the walls. The tables, of which there were only a few, were covered with clean white table-clothes. The chairs had vinyl coverings. Not too formal but not too casual either. Good.

After making the reservation I headed back out the door and into the bright sunshine. I paused briefly to let my eyes adjust and then continued south on Michigan Avenue.

The sidewalks were filled with people walking this way and that. I passed a young couple walking a dog, an older couple walking a baby, and numerous individuals out for a stroll on their own. I let my mind wander as I walked. Somehow, while tinkering with electronic funds transfers between banks, I had caused a malfunction of some sort. For some reason, and this is the part that is most baffling, this caused the accusing finger to be pointed at Lisa Melinda Cryer. Why her? For four days that question had been haunting me. For four days I had monitored electronic banking messages. For four days I had eavesdropped on phone conversations. I had pursued every avenue in search of clues. Yet there was nothing extraordinary about Ms. Cryer. I had studied the electronic computer messages for funds transfers on her account until my eyes watered from staring at the computer monitor, yet I could not find anything the least bit unusual about her transactions, nothing that might suggest that

hers would be singled out and handled differently from other transfers.

As a protocol cryptanalyst, I was well-equipped to recognize subtle anomalies in electronic funds transfers. While it is true that there was an anomaly associated with Ms. Cryer's account, the vexing part was that the anomaly lay not with the transfers themselves, but rather with the manner in which the banks reacted to my interference with those transfers. For the most part, the banks had reacted in a predictable way. It was only the transfers on Ms. Cryer's account that were seemingly mis-handled. Even more peculiar — and sinister — was the insistence by the bank executives that the blame lay with Ms. Cryer. In phone conversations with the FBI, First Chicago Trust executives clearly pointed the finger at Cryer.

My thoughts were interrupted when I came upon a park, with a large open lawn, neatly mowed, and a narrow asphalt path winding through. Trees dotted the path, some were quite tall. I found the quiet unassuming beauty of the park quite inviting and did not hesitate to redirect my stroll off the concrete sidewalk and onto the asphalt path. I eventually sat down on one of the many benches that lined the path. It seemed to be a good place to stop and kill some time while resting my feet. As I stretched out my legs and locked my fingers behind my head, I surveyed the scene before me.

Two small boys were playing catch on the lawn across the walkway from where I sat. They were young enough that merely catching the ball was a challenge and they spent most of their time chasing after the ball and picking it up off the ground. They both wore baseball caps and dirty blue-jeans. Very dirty blue-jeans. The blonde-haired boy wore an over-sized loose-fitting shirt. The other boy, a red-head, wore a shirt that looked like it may have been over-sized at one time but was now too small; it tended to ride up his stomach as he tumbled after the ball.

The boys were under the loose supervision of a young woman who may have been a sister or perhaps was just a babysitter. She was sitting on a bench nearby. Her knees were pulled up to her chest and her bare feet were up on the bench. She had a book propped up on her knees.

I leaned my head back and half-closed my eyes to shield them from the sunlight. It was nearly 5:00 now. The sun was still high on the horizon and quite warm. I slid over on the bench a couple of feet to be under the shade of a tree branch hanging low over the left side of the bench. Immediately I noticed a difference in temperature. The tree was a Norway Maple and the leaves were quite dense and served as a cool awning, with only a twinkling of sunlight penetrating through as the leaves gently moved in the breeze. After four sleepless nights trying to analyze message protocols, I was exhausted. As I sat there in a state just this side of consciousness, I studied the shape of the tree canopy. The bark was smooth and light brown. I followed the trunk with my eyes up to the point were the lowest branch forked away and then followed that branch until I reached the part directly over my head. The leaves were only a couple of feet from my face. As I gazed upward I noticed a small inch-worm on one of the closer leaves.

A jogger ran along the path in front of me, tossing a greeting my way as he

went by. The two boys continued to throw the baseball in the vicinity of one another and chase after it. I leaned back again and rolled my head a bit to get the stiffness out of my neck.

The inch-worm was still on the same leaf, but was determined to explore other parts of the tree. It moved from one side of the leaf to the other. Upon reaching an edge, it extended itself outward into space, seeking a foothold. Curling backward upon itself, it continued to wave about in a vain attempt to find a walkway to a place more attractive than its present location. Giving up, it put its front feet firmly on the leaf and pinched its way across the surface toward the opposite edge. A passing squirrel caused the branch to shake wildly, leading me to wonder how long it would be before the inch-worm would be caught fully extended in mid-breeze and be liberated to the ground below.

Left, right, to the point furthest from the stem, and back again. Every part of the leaf was explored, sometimes more than once. Working blind as it was, and apparently unable to recognize where it had been previous, it seemed an eternity before the inch-worm was able to stumble upon the stem. Having done so, it made a bee-line down the stem and along the twig from which the stem originated. It moved from that twig to the stem of another leaf.

With a twinge of sympathy for the poor creature, I realized that, if indeed the ground were its goal then the vast complexity of the branches of the entire tree dwarfed the recently solved problem of navigating a single leaf. The difference in scale between the full tree and the recent small accomplishment was staggering. Its goal seemed insurmountable. It would take ages for the inch-worm to find the right branches using the same trial-and-error method it had used to get off the one leaf.

As I watched the progress of the inch-worm in the warm afternoon sun and listened to the chatter and laughter of young boys at play, I slowly drifted into sleep.

Chapter 4

I awoke after a time to find that the boys had left. So too had the girl with the book. They were replaced by a middle-aged man and his dog. Both the man and the dog had long shaggy hair, although the dog's hair was fuller than that of the man, for the man had a bald area on the crown of his head.

A jogger crossed in front of me on the path. The sun had moved and I was no longer shaded by the branch over my head. With the movement of the sun further down on the horizon the shadows had lengthened and the heat had subsided. A light breeze ruffled the leaves and cooled my face.

I wondered how I should explain the EFT situation to Ms. Cryer. My next chance would very likely be my last one. Did she know anything about cryptology? I doubted it; it is not a very popular field. I knew nothing at all about her personal background. If I was lucky, she would have an understanding of basic mathematics. That would make things easier. While the science of cryptology is quite complex and requires a deep grasp of number theory, complexity theory, group theory, and various other sub-disciplines of mathematics and formal reasoning, it can also be understood at a more intuitive level provided one has a head for science in general. Still not fully awake, I leaned forward and rested my elbows on my knees and reviewed in my head the content of a cryptology primer I presented to co-workers when I still worked at AT&T.

Cryptology has a long history. Early examples date back to pre-history, to a time before accurate records were kept. Early documented examples of cryptography include the private communications of Julius Caesar. Caesar wrote to Cicero and others using a cipher that is commonly referred to today as a Caesar cipher.

The Ceaser cipher is familiar to readers of Usenet, for it is essentially the same thing as ROT-13. ROT-13 encrypts a message (of alphabetic characters) by replacing each letter with the letter that occurs thirteen positions beyond it in the alphabet. For letters M-Z, the sequence wraps back around to A. So A is replaced with N, B with O, C with P, and so on. Because of the wrapping, M is replaced with A, N with B, etc. When Caesar used this technique to obscure the content of his messages, he rotated each letter by three positions instead of the thirteen used on Usenet.

How hard is it to crack a Caesar cipher? Well, while it was good enough

for Caesar to fool Brutus, ROT-13 can't stop a child from decrypting material in Usenet. ROT-13 is only used to temporarily obscure offensive news articles so that the reader has a moment to reflect on the decision to view it before it appears on the screen. It is a way to incorporate warnings into news-readers that were not designed for "rated" material. Nothing more. It is not any more "secure" than using Control-L to give the reader a chance to avoid a spoiler before inadvertently reading it on the screen.

In fact, Edgar Allan Poe's short story, *The Gold Bug*, describes all the crypt-analysis one would need to successfully crack a Caesar cipher and other similar ciphers. In addition to using exhaustive search of all possible keys (there are only 25 — hardly a big search problem!), one can use statistical methods based upon the non-uniform frequency with which various letters occur in the English language. For example, as any scrabble player knows, the letter E occurs much more frequently than any other letter, and the letter X is relatively infrequent.

The strength of a Caesar cipher breaks down quickly once the enemy knows the algorithm. With only 25 possible keys, the key-space is ridiculously small. Even without computers to search the key-space, an enemy can make short work of finding the key, given even just one encrypted message. Whether he was aware of it or not, Julius Caesar was relying upon the obscurity of his method rather than the secrecy of the key. Today we realize that a far less delicate situation is to assume that the enemy is fully aware of the algorithm used but that the same enemy remains unaware of the key. A crypto-system that remains strong even after the algorithm is known is far more flexible; it is easy to change keys but hard to invent (and evaluate) new algorithms. This principle was first put forward by A. Kerckhoffs in the 19th century. If one applies Kerckhoffs' Principle, then all of the security of a crypto-system is concentrated in the secrecy of the keys. There is no harm in divulging the algorithm. Indeed, there are advantages to making the algorithm public; if there are any flaws in the algorithm that might be exploited by your enemies, making the algorithm public gives the general population an opportunity to study your algorithm and perhaps find the flaws for you. An algorithm that has been subjected to wide-spread peer-review is much more reliable than one that has been reviewed behind closed doors by only a limited number of people.

There are three aspects to a Ceaser cipher that make it very different from modern encryption methods. The first, as already pointed out, is that it violates Kerckhoff's law. The second is that both of the communicating parties must share knowledge of the secret code. Third, it is a weak code, in that the key is easily guessed. So weak, in fact, that even in its hay-day a Ceaser cipher was vulnerable. It is not just with recent advances that we are able to look back and crack these types of codes. Even if Brutus was unable to crack Julius Caeser's code, others of that era could. Given the overall lack of respect that Julius Caeser had for mathematics, it isn't surprising that he placed his confidence in such a weak cipher. This is the same Caeser that ransacked Alexandria and burned its libraries.

Still, one cannot fault Julius Caeser entirely for using a weak crypto-system. He had little choice. At that time, all known crypto-systems were only slightly

stronger than the known attacks. The defensive side of the science, called *cryptography* was only one small step ahead of the offensive side of the science, called *cryptanalysis*. For two centuries there were no codes that where impervious to attacks based upon technology of the same era.

This all changed in the twentieth century. First, early in the twentieth century, 1926 to be exact, G. S. Vernam invented a cipher that is unbreakable. At the time Vernam published his work the cipher was only *thought* to be unbreakable; today we know that it is indeed unbreakable. It has been proved with mathematical rigor.

Vernam was an engineer working for AT&T. This was always a point of pride when I presented this material at AT&T. I used to devote considerable time to Vernam and his work, describing his career with the company as well as his technical contributions to the field. Vernam wasn't the only modern cryptographer to work for a telecommunications company; many of the recent advances in cryptology have come from the communications industry.

Vernam's innovation was to use keys only once. Not only does this mean that the key must be changed for every message sent, but it also means that each *bit* of the key can only be applied to a single bit of the message. Each bit of plain-text is treated as a separate message and is encrypted with a new (single-bit) key. Clearly this scheme has disadvantages: the key must be as long as the message and must be changed as frequently as the message. At the same time, the key must be known to both communicating parties. If one can exchange long keys securely, and do it frequently, then why bother with encryption at all? Just use whatever mechanism you are using to exchange keys to exchange the messages themselves! It is for this reason that the Vernam cipher is of limited practical use.

One example of a Vernam cipher is to rotate letters in precisely the same way as one does in a Caesar cipher, except the amount of rotation varies for each letter of the message. For example, suppose we wish to encrypt the plain-text message:

> Please meet me at the corner in one hour

First, we put the message in a canonical form by removing all the space characters and using only upper-case. Compaction of this sort is commonly used in cryptography. Without it, it would be possible to infer information from the sizes of words used in the message, unless the space character is also encrypted (i.e. rotated), which would require using a canonical character sequence other than the traditional English alphabet. This is no big deal — one could use ASCII or Unicode — but to keep things simple I stick to ordinary letters.

> PLEASEMEETMEATTHECORNERINONEHOUR

Now, for a Vernam cipher we need a key of length equal to the message, say:

> 5 8 12 2 0 8 22 5 18 25 3 0 10 3 3 15 19 12 15 3 8 5 22 20 0 1 6 2 24 16 23 4

Our cipher-text is:

UTQCSMIJWSPEKWWWXODUVJNCNPTGFERV

The important thing to remember when using a Vernam cipher is that the rotation for each letter in the message must be completely independent of the rotations for the other letters. Furthermore, the key must be selected randomly (or as close to randomly as is feasible). In the key sequence above (which I chose arbitrarily but not randomly), each member of the sequence is a number between 0 and 25, inclusive.

In practice, Vernam ciphers are applied bit-by-bit. The message is viewed as a bit-string and the key too is a bit-string. Each bit of the key specifies a rotation in the range of 0 and 1. In other words, the exclusive-or operation is used; a Vernam cipher is nothing more than an exclusive-or of the message with a one-time key of equal length. This is often referred to as "blinding" or using a one-time-pad.

Vernam ciphers have application in military settings, where a large number of one-time-pads can be distributed ahead of time via a secure means and then used to exchange encrypted messages at a later time in a hostile environment. Code-books, where soldiers in the field must decrypt messages by looking up words in a printed book and replacing each word of the code with the appropriate word from the book, are an example of a Vernam cipher (provided the keys are only used once and the set of replacement words and code words are selected from dictionaries of the same size).

In 1949 C. E. Shannon published a paper on information theory entitled, *Communication Theory of Secrecy Systems*. This marked the dawn of modern cryptology, for it was this paper that established a firm scientific basis for cryptosystems.

Shannon was an electrical engineer by training and another telecom employee, working for Bell Telephone. By 1949 he had already published a soon-to-become legendary paper on communications theory in general. Indeed, today Shannon is probably better known for his 1948 paper on communications theory than the 1949 paper on cryptology. But it is the 1949 paper that established the science of cryptology.

Prior to Shannon's work, cryptology can better be described as an art rather than a science. The best cryptographic algorithms in the pre-1949 era were developed in an ad hoc fashion, with cryptographers haphazardly permuting and convoluting the input until it seemed unfathomable that anybody could unravel the process without knowing the key. Of course, without any basis for this belief, cryptographers had no way of assessing their position. Usually it was only a matter of (sometimes brief) time before a clever cryptanalyst broke the code and the cryptographers had to start all over again.

With Shannon's work, for the first time we had a theory upon which to base the development of cryptographic algorithms. A cryptographers job is to find one-way trap-door functions. A one-way function is a computable function for which the inverse cannot be computed. The inverse of a function, f, is normally denoted by f^{-1} and it is the "undo" relation. In other words, for any value of

x, $f^{-1}(f(x)) = x$. Now f^{-1} won't always be a function; sometimes it will map more than one input to the same output. In other words, there are two distinct values, x and y, such that $f(x) = f(y)$, and therefore $f^{-1}(f(x))$ is undetermined because it may be either x or y.

A one-way trap-door function is a function that is not actually one-way at all; it has an inverse, and the inverse is itself a function, but the inverse function is difficult to compute (without the key). It is important that the inverse be a function and be computable, because the recipient of an encrypted message has to have some way to decrypt it (the "undo").

So how difficult is it to compute the inverse of a one-way trap-door function? Mathematicians are able to classify the difficulty of solving a problem by ranking the efficiency of the best (known) algorithms for solving the problem. A one-way trap-door function is a function that can be computed efficiently but for which the inverse function cannot be computed efficiently.

Cryptographic hash functions are one-way functions, with the added requirement that they be *collision-free*. Suppose h is a cryptographic hash function. Because h is one-way, it is easy to compute $y = h(x)$ for all x, but hard to compute $x = h^{-1}(y)$ for any y. The collision-free requirement means that given the value $y_0 = h(x_0)$, it is computationally infeasible to find $x_1 \neq x_0$ such that $h(x_1) = y_0$, even if such an x_1 exists.

As important as Shannon's work was, it did not have an immediate impact. It is only now, in retrospect, that we recognize and appreciate the importance of that paper. It established the necessary ground-work that we rely upon today but did not excite sufficient interest to spur further activity in the field. It wasn't until 1976 that the field really took off. In that year W. Diffie and M. E. Hellman published their revolutionary work entitled *New Directions in Cryptography*. The significance of this work is that it showed for the first time that private communication was possible even when the communicating parties shared no prior secrets. In other words, encryption did not require a "key" in the traditional sense. Up until 1976, all encryption algorithms relied upon a secret key that the two parties shared prior to exchanging encrypted messages. This "key" might be the secret algorithm, as in the case of a Ceaser cipher, or more recently SkipJack and Clipper. Or, it might be a one-time pad, as in the case of a Vernam cipher.

The traditional crypto-systems with a single key are called symmetric-key systems. In their 1976 paper, Diffie and Hellman introduced a new kind of crypto-system with two keys; one private key and one public key. The private key, which is not shared with anybody and is known only to the encrypting party, is used to encrypt messages. the public key, which is known to everybody, contains all the information needed to decrypt that message.

Suppose Alice wants to send a private message to Bob (it is customary when giving examples of cryptography to use Alice and Bob). With symmetric-key encryption, Alice and Bob would have to first agree on a key to use to encrypt and decrypt the message. But with public-key encryption Alice can use Bob's public key. There is no need to meet in person or exchange by some other means a shared secret key. There is no boot-strapping problem. Once Alice has

encrypted the message using Bob's public key, only Bob knows how to decrypt the message. Even Alice cannot decrypt the message (of course, she has no need to do so since she knows the plain-text anyway, having created it herself). Bob uses his private key, which he divulges to nobody, to decrypt the message and recover the plain-text. If Bob wants to send a reply, he uses Alice's public key to encrypt a message for her eyes only. She then uses her own private key, known only to her, to decrypt Bob's reply.

By far the most common public-key algorithm in use today is RSA, which was invented in 1978 by R. L. Rivest, A. Shamir, and L. Adleman (hence the name, derived from the last initials of the three inventors). The RSA trapdoor one-way function is the discrete exponentiation

$$f_{p,q,e}(x) = x^e \bmod n$$

where x is a nonnegative integer less than $n = pq$ and where the trapdoor is the three values p, q, and e. The secret values of p and q are carefully chosen large primes. The values of n and e are public. These two values comprise the public key. The private key is the factorization of n, namely p and q.

Anybody that has a good method for factoring large numbers can crack RSA. That person can factor the public value of n to obtain the unique prime factorization pq and thereby obtain the back-door values of p, q, and e (the last of which is public knowledge). Fortunately for those of us that rely on RSA, factoring is widely accepted as a very difficult problem, with no known efficient solutions. The best known factoring algorithms have exponential running-time and would require vast computing resources to factor large numbers. Mathematicians have been searching for better factoring algorithms for centuries. Their failure to find better algorithms is strong evidence that such algorithms don't exist, or if they do then their discovery is not imminent. (The popularity of RSA is not a significant motivator in the search for factoring algorithms, when viewed in the context of the full history of mathematics.)

I personally contributed in cracking one specific RSA key. I was working for a small telecommunications company at the time, Multi-Media Telecom, having left AT&T. The key we helped crack was 129 bits long, which would seem to be long enough to be impervious to a factoring attack. Nonetheless it was broken in April of 1994 in response to a public challenge first posed in the pages of *Scientific American* in 1977. The puzzle was cracked using a variation of the quadratic sieve factoring method. The program required about 5000 mips-years and was carried out in eight months by about 600 volunteers from more than 20 countries. The entire effort was conducted and coordinated over the Internet. I had one of my machines cranking round-the-clock on RSA-129. The challenge cipher-text was published as:

96869613754622061477140922254355882905759991124574319874695120930816298225145708356931476622883989628013391990551829945157815154

It was announced that the public exponent was 9007. The secret exponent is

easy to compute once one knows the prime factorization of the public modulus. That modulus was published as:

114381625757888867669235779976146612010218296721242362562561842935706935245733897830597123563958705058989075147599290026879543541

This modulus was factored on the net:

3490529510847650949147849619903898133417764638493387843990820577*327691329932667095499619881908344614131776429679929425397982885331

Once the prime factors are known, computing the secret exponent is easy. For RSA-129, the secret exponent is:

106698614368578024442868771328920154780709906633937862801226224496631063125911774470873340168597462306553968544513277109053606095

Using this exponent to decrypt the cipher-text yields:

200805001301070903002315180419000118050019172105011309190800151919090618010705

If one re-writes this number in base 27 using 00 = *space*, 01 = A, 02 = B, 03 = C, and so up to 26 = Z, then the result is:

THE MAGIC WORDS ARE SQUEAMISH OSSIFRAGE

The complexity of the factoring problem grows roughly exponentially with the length of the key. The above example used a key of 129 bits. Using the same methods and the same amount of computing power, a 130-bit key would take roughly twice as long to crack. Such is the nature of exponential problems. In fact, a year later a 130-bit RSA challenge was solved in the same way, over the net. Both of these public efforts made use of an awesome amount of computing power, harnessing the power of the Internet. These were world-wide cooperative efforts, the likes of which are not normally available to spies, thugs, and other evil-doers. Still, just to be on the safe side, people typically use RSA key lengths of 768 or 1024 bits, and sometimes even 2048 bits. Remember, each additional bit in key-length doubles the resources needed to crack the code. Barring a revolutionary advance in computational number theory, using key sizes of at least 1024 bits for RSA is quite safe.

The next big advance after public-key cryptology came in 1984, when Gustavus J. Simmons published his work on the theory of authenticity. This opened up a new side of the field, demonstrating that cryptology can be used to establish communication channels that are resistant to tampering. Moreover, the

property of information integrity and message authenticity, as this came to be known, can be separated from the property of message privacy. Cryptography can be used to achieve integrity without privacy or privacy without integrity (or both together of course). This opens up new areas for cryptographic applications, where secrecy is not important but integrity is. The work of Simmons, Shamir, Rivest, Adleman, Diffie, Hellman, and others has gone a long way toward moving the field of cryptology out of the back-rooms of espionage and into the fore-front of the contemporary computing and telecommunications industries. The recent blossoming and merging of those two industries has sealed the fate of modern cryptology — it is indespensible to the manner in which we exchange information today.

The significance of public-key cryptography cannot be over-estimated. When used for information integrity and authenticity, the advantages become greater still. Public-key encryption can be used "backwards" to achieve a digital signature. If Alice uses her private key to scramble a plain-text message, then while anybody can regain the original plain-text because everybody knows Alice's public key, *only Alice* can scramble a message in this way. There is no privacy when Alice uses her private key in this manner, but there is integrity and non-repudiation. If Bob has both the plain-text version of a message and the version created with Alice's private key, then Bob can be sure that Alice is the one that created the scrambled version; nobody else has the ability to scramble the bits in a way that will produce the original message when Alice's public key is applied to it. Without Alice's private key, forgeries are computationally infeasible.

Digital signatures are much more secure than hand-written signatures. There is no known way to forge a digital signature. So long as Alice keeps her private key secret, nobody can forge her signature. Therefore, if a signed message conforms to Alice's public key, then she cannot deny having signed it without also accepting that she has allowed her private key to be released to a third party.

Another advantage that digital signatures have over hand-written signatures is that the signature is applied to the *entire* message. Every bit of the digital message is perturbed by the signing key. A hand-written signature is applied to the bottom of a paper document. There is nothing that prevents alteration of the text appearing above the penned signature while leaving the signature intact. Such alterations are not possible with digital signatures. Changing even a single bit of a signed message will cause the verification procedure to fail.

It is important to recognize that while public-key cryptography eliminates the need for a private channel to exchange keys, it still requires that there be a tamper-proof channel. If one party can be tricked into accepting the wrong public key for the other party, then the system is compromised. If Alice sends a private message to Bob, but uses Joe's public key instead of Bob's key because Joe has fooled Alice, then Joe will be able to impersonate Bob. He will be able to read all of the private messages that Alice intends to send to Bob, messages that were meant to be for Bob's eyes only.

Thus, integrity and authenticity remain essential. If the two parties share

no prior information (public or otherwise) then this can pose a serious problem. One solution is to rely upon physical integrity. For example, if one party broadcasts his public key on the nightly news over network television, it is unlikely that the signal has been altered or that he has been replaced by an actor. If the viewer calls up close friends and relatives to confirm that they saw the same broadcast and the same public key was conveyed, she can be still more confident. Still, can one be completely certain? What if you have no idea what the person is supposed to look like? Is there a more practical solution?

The common solution, which is already being deployed in industry, is to use something called *certificates*. A certificate is somewhat analogous to a driver's license. I can be confident that a public-key belongs to the person claiming ownership of that key provided somebody I know and trust vouches for that person. A certificate authority provides this service. To be a certificate authority, a company must be widely known and highly trusted. That company must be trusted to behave honestly, but also must be trusted to act with competence and diligence. If I receive a certificate with your name and public key, and if that certificate is digitally signed by a certificate authority I trust, then I can be confident that the public-key does indeed belong to you.

Why? Well, first of all I am confident that the signature cannot be produced by any entity other than the certificate authority; digital signatures are unforgeable. Second, I have placed my trust in the certificate authority to take whatever steps are needed to verify your identify. For example, perhaps you are required to show up in person and produce undeniable evidence of your identity (e.g. a fingerprint, a retina scan). I can now take the contents of the certificate at face value: you claim the stated public key as your own.

Certificate authorities reduce the problem of distributing public-keys in a insecure environment to the problem of distributing *only one* public-key — that of the certificate authority. Once everybody has that key, all other public keys can be safely distributed using signed certificates. This greatly simplifies the infra-structure needed for public-key cryptography. The public key for the certificate authority is *very* public. Everybody knows it and uses it (to verify certificates). There is only one such key (or a very small number, one for each certificate authority). Because it is so widely known and widely used, it is easily verified. Because of the small number of certificate authorities, their keys can be broadcast in various news media that are hard to alter. The New York Times is one example. Or on network television much like lottery numbers are announced. Or —

I suddenly looked at my watch. I had let myself drift off in thought and lost track of the time. My watch said 5:40. I still had plenty of time to get back to Ms. Cryer's building before 6:15, but it would be silly to cut it close when I wasn't doing anything other than sitting around day-dreaming. I might as well head back and wait in the lobby.

I stood up, stretched, and began to retrace my steps toward Michigan Avenue and the walk back north. Would the black Caprice still be there? I wondered.

Chapter 5

I was sitting in the lobby of Ms. Cryer's apartment building by 6:00, enjoying the cool air-conditioned comfort. I allowed myself to doze a bit more as I waited. With my eyes only half-open I traced the pattern on the rug beneath my outstretched legs. A green line twisted and turned on a red background, forking frequently into numerous branches. Occasionally some of these branches merged back together again. While it was an abstract pattern, it gave the impression of a hopelessly tangled and twisted vine.

Ding!

An elevator door opened behind me. I shook off my drowsiness and looked up. It was Ms. Cryer. She flashed a very brief, slight smile and nodded her head as she approached. I returned her greeting and got to my feet.

I hadn't had a chance to change my clothes, of course, and upon seeing Ms. Cryer I became acutely aware of this. She had changed.

She wore a different pair of pants, although they were still stretch-pants and still black. Her grey sweatshirt was replaced by a loose-fitting white blouse that buttoned down the front. She hadn't tucked it in at the bottom, instead letting it hang loose like a jacket. The white blouse and black pants made for a sharp contrast. The blouse brought out the natural beauty of her dark face.

We turned and headed out the door without saying anything immediately. She had also put on lipstick, light-red, and earrings. The earrings were gold rings about the size of a quarter and showed with dramatic effect due to her ultra-short hair. Other than the lipstick, I couldn't tell if she was wearing make-up. Hers is the sort of beauty that either doesn't require make-up or else is the result of very expertly applied make-up. I was struck once again by the striking beauty of her eyes — large round eyes, the whites in sharp contrast to her skin. She may have had eye shadow... I wasn't sure and didn't want to peer too closely. These observations came from side-ways glances during the short walk to the restaurant. The conversation during that walk consisted of sanitized small-talk, which suited me just fine. When we reached Sid's Seafood Grill, Ms. Cryer let me hold the door for her as we went in. I also held the door for a young couple entering immediately after us. They had just stepped out of a black sport-utility vehicle parked at the curb in front of the restaurant.

I had to pause briefly inside the door to let my eyes adjust to the dim lighting.

The same blonde woman was sitting at the same spot at the bar. It looked as if she hadn't moved. She still had a cigarette in her hands and a drink sitting on the bar in front of her. The rest of the bar was empty; the two men had apparently left.

I noticed a surprised and slightly amused expression cross Ms. Cryer's face when I gave my name and mentioned our reservation, but she didn't say anything. The couple that had followed us in did not have a reservation but were shown a table in the non-smoking section along with us. Most of the tables were still empty at this point.

Ms. Cryer informed me that all of the food on the menu was good but that the swordfish, crab, and fillet of sole were especially good. I decided on swordfish.

Before making another attempt to explain the banking debacle I wanted some idea of Ms. Cryer's educational background. My guess was that she had a college degree. I hoped so. It would be even better if it were in the sciences instead of the humanities. Not wanting to seem too intrusive I gingerly broached the subject and learned to my delight that she had been a computer science major at Northwestern.

"That's great," I exclaimed, "so you can follow the details of the computer mix-up at the bank."

"Yes," she replied coldly. "I know what a hacker is and I understand the world in which they operate."

So I was a hacker in her eyes. Yuck. Time to start explaining. "It isn't like that," I said.

"Then what were you doing messing around with banking transactions?"

"All I really wanted to do was prove a point," I began. "It is my contention that nobody is making full use of the tools that are readily available for computer security. Sure, everybody worries about hackers and most people are careful to use passwords and stuff like that, but there is much more that can be done. Much more can be done by hackers than merely guessing passwords, and much more can be done by honest computer users to thwart hackers. We've come a long way since movies like *War Games*. Yet, most people don't recognize that, including people that most definitely should."

She said nothing so I continued. "The banking industry is only one example of what I'm talking about. But it also happens to be a very visible and prominent example. I figured if I could illustrate some of the weaknesses in the wholesale banking system, maybe people would wake up. And if I could do it without actually stealing any money, then I could claim the moral high road. I fancy myself as the Ralf Nadar of the information integrity business. Now you might argue with that stance, and I'll concede that what I did was highly illegal, but there you have it — you won't get any apologies from me over that. But I *will* apologize yet again for putting *you* in the hot-seat. That was entirely accidental."

Our food arrived and I paused to eat. The pause stretched for longer than I had intended, as the food was delicious and I suddenly discovered I was very hungry. Eventually I resumed where I had left off.

"All I wanted to do was double all the transfers between a pair of banks on a particular day. I chose Bendix of St. Louis and First Chicago Trust as the two banks. I could have chosen any two out of hundreds of banks. The choice of those two was entirely arbitrary."

She had stopped eating. She sat back with one arm folded across her chest while she lightly tugged at her ear with the hand of the other. I took a sip of wine to wet my throat and continued. "I took physical control of the communications line between Bendix of St. Louis and First Chicago on July 11th. By that I mean that I tapped into the phone system and rerouted all calls between the two banks so that the calls were routed through my phone number. Or, more precisely, through the computer in my apartment — this was a data line between the two banks. I won't describe how I was able to reroute the calls. Let it suffice to say that is was extremely easy and extremely illegal.

"Anyway, having done this, I could monitor all the data transmissions on my computer. Electronic Funds Transfers — EFT's for short — are sent in the clear, meaning that they are not encrypted. They are transmitted using TCP/IP and the payloads are formatted in ASCII."

"They don't use any encryption at all?" she asked. "Its all just ASCII?"

"Right. Anybody can read the messages. Well, anybody that eavesdrops on the phone line. There is no privacy beyond the privacy provided by the basic security of the phone system, which is notoriously bad. Long before there were computer hackers there were phone hackers, and very little has been done in the last three decades to change that. In fact, with the booming business of cellular phones, the situation has become worse.

"But even if the banks don't encrypt the transfers, they do at least protect them from tampering. They use something called *message authentication codes*, or MAC's for short. Each funds transfer has a MAC appended to it. The MAC is a string of bits that is derived from the content of the message in such a way that it is extremely difficult to compute a MAC without knowledge of a secret key."

"So a MAC is a form of encryption?" she asked. Wrinkles formed on her forehead. She had a very pretty face and this expression suited her features well, much like every other expression I'd seen thus far.

"Yes. It is somewhat analogous to a signature," I replied, pleased that she was warming up to the conversation. With her background I knew that she would be able to follow the details of the funds transfer protocol; I was anxious to fill her in.

"Or you can think of it as being a lot like a checksum," I said, offering an alternative intuitive explanation for a MAC. "It is like a checksum because it is a function of the entire message and is very sensitive to even small changes in the content of the message. But unlike a regular checksum, which is designed to protect against only accidental errors, a MAC is all but impossible to alter in a way that is consistent with alterations to the message itself.

"EFT MAC's are computed using a very common cryptographic algorithm. The algorithm is called DES, which stands for *Digital Encryption Standard*. DES can be used to encrypt messages or to compute message authentication

codes. The American Bankers Association has opted to use it to compute MAC's."

She nodded her head and swallowed the large mouthful of bread she had bitten off moments earlier. "OK," she said. "So you were able to pry and peek at everybody's payments, including mine. But you said something about doubling the amounts on all of those payments. Yet MAC's are supposed to make these messages tamper-proof."

Teaching had always been an ambition of mine and I was thoroughly enjoying the chance to give a lecture to such a bright and responsive pupil.

"Not quite," I replied. "I spoke of doubling the payments but not doubling the *amounts*. You're right; I can't alter the amounts because the MAC's guard against altering the content of EFT's. Or, more accurately, if I did alter the amounts, it would be detected because the MAC's wouldn't pass the verification test executed by the receiving bank. But I can send the same EFT twice. Certainly it is no trouble to record all the messages while letting them pass through, and then later send them all again. These transfers were passing over a data line routed through my computer so —"

"Is that what you did?" she interrupted. "You sent out copies of all the EFT's so that every check was cleared twice?"

"Not exactly," I answered. "There is an entire protocol for dealing with communication failures and other errors. Unfortunately the standard doesn't lay out the error handling very clearly. Consequently I have to do my research by introducing errors and observing the responses."

Between bites I gave Lisa the details of July 11th. Like many other afternoons in the last two months, on July 11th I had intercepted a phone call originating from a bank in St. Louis by the name of Bendix. The call was part of the Electronic Funds Transfer (EFT) system for the US banking infrastructure. I knew this because that is the only reason that Bendix and First Chicago use that particular line. Like many other afternoons, I then proceeded to eavesdrop on the data transmitted over the line. OK, this occasion was a bit different in that I had also inserted some messages into the traffic stream as well. But even that wasn't entirely new; I'd done it before without such strange results.

The funds transfer network is actually a collection of a several smaller networks. The largest and most important of these is the Clearing House Interbank Payments System, or CHIPS for short. As the name suggests, CHIPS is used for inter-bank transactions (otherwise known as wholesale banking). It is a closed network, where all of the member banks are pre-registered and known to each other. CHIPS handles about 182,000 messages a day. That comes out to a weekly load of about 910,000 messages. CHIPS is a world-wide banking network and is used to move an average of $1.2 trillion every business day. A single message can carry a dollar amount of as little as $50 or as much as $2 million.

Retail banking, where consumers can issue payments and check balances, uses an entirely separate network. The wholesale banking network is carefully guarded and consumers are barred from any direct interaction with the system. For wholesale banking, there is CHIPS, the Automated Clearing House (ACH),

FedWire, and several smaller networks. ACH is regulated and managed by the Federal Reserve, although it is operated privately. All of these networks operate in roughly the same way.

The use of CHIPS and it bretheren has increased dramatically in recent years. As recently as three years ago the daily load was only $400 billion. Part of the increase is due to the increased popularity of direct deposit and automatic payments. It has become quite common for employees of large companies to have their paychecks deposited into there accounts electronically. More recently, consumers have begun to make greater use of automated payment options. For example, many people have their utility bills paid automatically. Consumers give authorization to banks and utility companies to affect these payments electronically. And, of course, it has long been true that even paper checks are processed at least in part electronically.

My interest in the EFT network stems from professional curiosity. My curiosity can be labeled as "professional" because I've been trained in computer security and cryptographic protocols. My interest must be labelled as "curiosity" because no bank is paying me at the moment. This leaves me in a position of being on the outside looking in. While the design of the CHIPS network is publicly available for review, lower-level implementation details are not. Consequently I was not privy to some of the error-handling aspects of the system. My admittedly unorthodox method of determining how the banks had opted to implement error-handling is to introduce errors and observe the results.

This brought me to the important part of the story, the whole reason I'd been forced to seek out Ms. Cryer in the first place. Thus far she had listened intently with only a few interruptions for clarification.

Next I explained how, after recording the EFT messages originally bound for First Chicago from St. Louis, I sent the recorded messages on to First Chicago. This meant that First Chicago Trust recieved duplicates of all of those EFT's. I kept the connection open after sending my copies so that I would recieve the error messages from First Chicago. It was for the purpose of studying these error messages that I was sending the recorded copies in the first place. Sure enough, error messages began pouring back from First Chicago, complaining that the EFT's were replays of earlier transmissions. The security routines at the recieving bank had detected my attack and they were responding appropriately. *Except* for the transfers on Lisa Cryer's account! Those replays were not rejected; all others were. Why?

Lisa said that she had no idea. She suggested that perhaps I had corrupted the EFT on her account in some way and therefore it differed from the original and was not a replay.

"If I did corrupt it in any way, then the MAC would not have checked out," I said. "Bear in mind that the entire purpose of a MAC is to detect tampering by a third party. I would have gotten authentication errors."

At this point the waitress came to the table to refill our water classes. Neither of us said anything until after she had left again. Then Lisa asked, "what made you decide you could trust me?"

"I had to."

Puzzled, she asked why.

"It was clear that something had gone dreadfully wrong with the transfers," I explained. "As soon as I saw that a few EFT replays went through I knew something was amiss. At first I thought that maybe you were tampering with the EFT traffic too and that the your EFT was a forgery of some sort.

"I've spent a lot of time studying those EFT's over the last few days," I groaned. "Then, after I saw you in the bank I realized that you were probably an innocent victem in all of this."

"Because I don't look like a computer scientist?" she asked indignantly.

"Because you don't look like a hacker."

"Oh... I'll take that as a complement!" she smiled sweetly. "Unlike you, I don't mess around with other people's livelihood for a cheap thrill."

It seemed best to let that comment pass. Instead I elaborated on my answer to her earlier question. "Clearly something strange is going on at First Chicago Trust. I can't approach the bank. Nor can I go to the police. The first thing they would do would be to arrest me. Maybe they would ask questions later... and maybe not.

"Really, when you stop and think about it, I had no choice but to approach you," I confessed. "My only two options are to run away from the whole thing and pretend I am completely unaware of any irregularities, or to try to figure out for myself exactly what happened. I choose the latter."

"You took a chance," she said, "just by showing up in person and identifying yourself to me as the man who has made my life a living hell for the last four days. For that matter, while I'm not going to run to the police immediately, I'm not going to let this drag out forever. If you can't patch things up quickly I'll still go to the police." She looked at me pointedly as she said this. She wasn't bluffing; she was issuing a warning.

I looked around as I emptied my wine-glass and refilled both of our glasses. Odd, the place was still nearly empty and yet this should be peak hours. The two other parties that were already seated when we came in were still there. Only one additional table had been filled. The woman at the bar had either found somebody to her liking or she had been waiting for a friend who wasn't particularly punctual. Either way, a man for whom she had been waiting had finally arrived. They were sharing a light dinner now. The remainder of the roughly twenty tables were all empty.

I turned back to my dinner companion. "We really didn't need that reservation, did we?" I asked. "You probably come here often, is it always this empty?"

She let a short pretty laugh escape her lips and set down her glass. "I'm surprised they even took a reservation for you. Did they give you a funny look when you made it?" She glanced around the room. "This is a typical turn-out. And yes, I do come here often. Not a very original line; you can do better than that, can't you?" She had a glint in her eye and a slight smirk on her face as she leaned her head into her right hand with her elbow on the table and swirled her glass with her left hand.

I wasn't sure what to say next, mainly because I wasn't sure what she meant by that last comment. I hoped she was flirting. Her attitude toward me fluctuated between contempt and acceptance. We had met only hours earlier and already she had yelled at me, made snide remarks, and threatened me with the police. Yet, inbetween these hostile moments we seemed to be getting along quite well... like now for example. To cover my puzzlement I poked at the remains of my fish and tried not to look as awkward as I suddenly felt. Mistake. The moment passed.

"So what do you do now?" She straightened up as she asked this and smoothed out the napkin in her lap. Her manner became business-like. "You want my help. OK, what do you need to know? Fire away."

"Can you think of anything at all that might be unusual about the money transfers that you made this month?"

"You mean my automatic utility payments, right? No, nothing unusual."

"These utility payments are automatically deducted from you checking account every month?"

She nodded her head in the affirmative. Then she added that she had been paying her bills in that way for close to a year with no troubles up until now.

"But," she added, "when I was there yesterday the guy at the bank claimed I also recieved a payment by automatic deposit, and that it was not from my employer. While the bank won't tell me who the payment is from, I can assure I was not expecting any money transfers from anybody."

"That must be the windfall that makes the bank suspect you. Did they tell you how much it was for?"

"Nope."

Then her face suddenly lit up. "Hey!" she exclaimed, "you can probably find out can't you? Did you keep the file of EFT's that you recorded? I would also be curious to know who it is from."

Indeed I had kept the file. "Yes I have the file. I want to take a closer look at it tonight. Can you think of any clues I should look for? Say, for example, EFT's to or from a particular person? Also, what are all the payments you made on or around the 11th? That includes paper checks as well as automatic debits. I need to be able to recognize a discrepency between honest activity and illegitemate EFT's."

"All I can think of is my gas bill and electric bill. I don't know off-hand how much those two payments should be for. Also, I'm not even sure what days the automatic payments are made, so I do not even know if either one of those payments should have been made on the 11th. I can check my bills from last month and at least give you estimates."

"Do that. And please get back to me with the information," I said as I pulled a pen from my pants pocket and scribbled my phone number on a paper napkin. Pushing the napkin over to her, I continued to press gently for details. "Remember, it isn't just automatic payments that we need to think about; have you written any checks within the last two weeks that might have cleared on the 11th?"

"Well yes, I am sure I have written several checks recently, and any number of them might have gone through that day. Again, I will have to get back to you with details after I have had a chance to look at my checkbook." She took an address book out of her handbag and copied the phone number from the napkin to her book.

I wanted to make sure we did not overlook anything. "While you are thinking about those things," I said, "also try to think of any automated payments you might have recieved legitamately. I'm sure you've already given that quite a bit of thought since the bank has given you ample motivation to do so. Nonetheless..." I let the suggestion trail off.

"The bank said that they do not care about any paper checks I recieved and cashed, only automatic payments."

"Good," I exclaimed. "That helps. It means that the suspicious EFT is for an automatic deposit and not part of a check truncation whereby a paper check you deposit is converted into an electronic transfer.

"Did they tell you anything else that might be helpful?" I asked hopefully, pressing for more clues. "Anything that might help limit our scope?"

She furrowed her brow and said nothing for quite some time. Her gaze was cast downward at the table. "Not really. They were being very careful not to say anything more than they had to."

The fact that the bank was reluctant to discuss the matter only added to my suspicions about the bank's role in this entire matter. I felt that executives at First Chicago Trust were too zealous in their pursuit of Ms. Cryer. In phone conversations with the FBI these bankers claimed that internal security at the bank was iron-clad and that they only hired people of the highest moral character. They would not even listen to suggestions of a possible inside job. Instead, they pointed accusing fingers toward Lisa Cryer, a customer that I had a hard time imagining anybody viewing as a threat. I can understand being careful to view each suspect with objectivity, but how could they be so certain that she had tampered with the EFT's from the outside?

Lisa interrupted my thoughts. "Do you really think you will be able to unravel this mess? Can you solve the mystery even when the banks can't? You don't have access to the same level of information they do."

"Well, I do have a formal education in the study of cryptographic protocols. I do consulting work in the area. At the moment I don't have any contracts. The last four months have been a dry spell. Therefore, I am not privy to the details of the internal workings of wholesale banking. I have to work with whatever information is made public — which is quite a bit — and whatever other information I can collect by less honorable methods.

"In the beginning I started out by introducing errors in more mundane ways. For example I introduced bad payments into the ACH check clearing system simply by bouncing checks. I would intentionally write a bad check and then monitor the EFT activity to see how it was handled in the EFT protocols.

"I had to stop after the bank began to take exception," I added. I couldn't help but chuckle as I recalled the episode where the bank called me in to ask why I kept writing overdrafts on one of my accounts when I had more than

adequate funds in my other account to cover the checks.

Lisa slumped back in her chair and rested her chin in her hand, her elbow was perched on the edge of the table. "Uh, Carl," she said, "why don't you have a normal job like the rest of us? Bouncing checks and hacking phone lines is not computer science."

Her eyes twinkled with amusement. Such beautiful eyes they were too. She seemed to be enjoying our dinner. We had both long since finished eating but neither one seemed anxious to leave. After catching up on some much needed sleep in the park and filling up on good food and wine, I was feeling reinvigorated. It was a pleasant dinner until Lisa mentioned Psuedo-One as an example of one of the many new Internet companies that are on top of things. My disgust for Psuedo-One would not permit me to let that comment go by uncontested.

Chapter 6

There are many companies that choose to ignore the risks associated with computer crime and, even worse, ignore the wonderful defensive tools that are available. Lisa mentioned Pseudo-One, but they are only one example. I spent the remainder of our dinner conversation blasting the policies of Pseudo-One. After all, it was precisely to set such companies straight that I had chosen to take such an aggressive (and illegal) approach to EFT research.

Founded in 1994, Pseudo-One Incorporated provides a general shopping service over the Internet. The company is moving forward at full-steam with very little consideration for security. I have seen numerous posts on Usenet where the founders of the fledgling company make reckless comments about security, not to mention quotes in the print media that clearly express the company position. These comments point out that security is not equivalent to encryption, which is true enough. Security is a broader issue than encryption alone. Security includes encryption, but it also includes integrity, access control, policy, usage guidelines, and numerous other issues. This does *not* mean that security can be completely dismissed as a requirement for Electronic Commerce. Yet, strangely, this is what Pseudo-One executives seem to believe is a logical consequence of the limited scope of encryption. The non-sequiter leaves no room for rebuttal.

Many people don't understand cryptology and wrongly assume that it can only be used to exchange secret messages and therefore is limited to spying. They incorrectly believe that if secrecy is not critical to their application then they have no use for cryptography.

On the Internet, when no special precautions are taken, it is quite easy for an impersonator to go undetected. IP-spoofing is not hard and several techniques are widely known. The Internet protocol, IPv4, has no support for authentication. Every packet contains the IP address of the source, but there is absolutely nothing to prevent a hacker from changing that address.

The Internet is uncontrolled and entirely insecure. Pseudo-One spokespeople readily admit this and even distribute information to advance this claim. Pseudo-One seems to have adopted the position that because the Internet is so prone to dishonest behavior, there is little point in trying to stem the tide. But to take this attitude is to completely overlook the power of the tools readily available today. Recent advances in cryptology have put the cryptographers

at a clear advantage over the cryptanalysts. The cryptographer, acting in a defensive posture to protect information, has stronger algorithms available to him than the cryptanalyst, acting in an offensive posture attempting to crack those algorithms. There are several algorithms that are publicly known for which there are no known attacks that come close to cracking the algorithms. Moreover, these algorithms come in various forms and are extremely easy to implement, allowing one to achieve various design requirements. They can be used to protect data from eavesdropping, to protect data from tampering, to exchange keys, to produce digital signatures, to produce digital finger-prints, etc. To ignore these useful tools and instead rely upon a policy of "hang on and pray for the best" is to do a disservice to one's customers.

Part of the reason that Pseudo-One has been as successful as they have is that they guarantee financial protection to their customers. If there is any breach in security (not a very big "if" by the way), then Pseudo-One will bear the cost. To limit their own risk, Pseudo-One buys insurance. In the target-rich environment of the Internet, this is a reasonable business strategy. With so many targets for hackers to choose from, what are the odds of Pseudo-One being singled out?

Well, the odds are frightening when one considers that 20% of Internet sites had security breaches in the past year, and 30% of those were after firewalls were installed.

The fatalistic acceptance of a dangerous situation, taking comfort in the safety of numbers, is the same approach taken by the rabbit Cowslips and his followers in the story *Watership Down*. Hazel, Bigwig, Fiver, and the other rabbits of Watership Down had the sense to leave Cowslips' warren and seek a better existence. The lathargic and defeatist path taken by Cowslips was foreign to the thinking of the more enterprising and pioneering spirit of Hazel's rabbits. One hopes that Pseudo-One has as much trouble attracting new followers as Cowslips did. Why? Mainly because the "hang on and pray" approach has inherent inefficiencies. These inefficiencies lead to greater costs which ultimately must be born by both consumers and merchants. And there is no need for it. Instead of paying a middle-man to redistribute costs evenly over the entire market whenever there is an attack, why not simply prevent such attacks in the first place? Too expensive? Nope, less expensive; there is now a tight upper bound on the damages — not only a bound on the damages for any one individual, but also a limit on the damages for the entire industry.

The "hang on and pray" attitude works well for lawyers and insurance agents, but what about consumers? If one company on the Internet is hit with a major loss due to a hacker, that particular company loses and the other companies all breath a sigh of relief, but as a group, consumers lose any time any company is hit.

In press releases, Pseudo-One does a nice job of pointing out the vulnerabilities to commerce over the Internet:

- the Internet is the most open networking environment imaginable with no safeguards designed into it;

- impersonations on the Internet are easy;
- intercepting and re-routing messages is easy;
- anyone with an established brand identity on the net needs to worry about attackers tampering with the presentation of information associated with that brand;
- and any point-to-point security system based upon cryptography will require a secret key stored on a machine and therefore is vulnerable to security breaches on that machine (e.g. a virus, a password sniffer).

Curiously, these are used as reasons *not* to address security. Instead, after pointing out that the environment is very hostile, Pseudo-One relies upon an e-mail call-back feature to obtain a secure communication channel. If impersonations and re-routing of messages are easy, as Pseudo-One agrees they are, then an e-mail call-back feature is rather pointless.

Because the problem seems insurmountable, the company has thrown in the towel and opted for the inefficient solution. Better to have an inefficient solution than to completely forgo electronic commerce. Yet, anybody that has studied modern cryptology knows that privacy, integrity, authenticity, and accountability are all properties that can be achieved, provided one is careful and makes proper use of the science of cryptology.

There is no need to rely upon an e-mail call-back feature, which has very little value, and claim that this is sufficient, all the while complaining that the Internet is a hostile environment that cannot be trusted with sensitive information in any form. To state that any information that is too sensitive to appear in the clear on the Internet is also too sensitive to appear in encrypted form, is to completely ignore hundreds of years of science in cryptology, and to ignore the past couple of decades in particular. In the years following the second World War, advances in cryptology have paralleled advances in complexity theory. As mathematicians and computer scientists have learned to better qualify and measure the complexity of mathematical problems and algorithms, they have been able to apply this to cryptology so that today we can qualify, in a meaningful and precise way, the difficulty in cracking a given encryption algorithm. Thus, when we refer to "strong" cryptography, we have a formal definition behind the phrase. Therefore, given an encryption scheme, complete with key lengths and a message protocol, it is quite reasonable to make qualitative and even quantitative statements about the level of confidence in the scheme.

Certainly there are examples of data that is too sensitive to be sent in the clear over the Internet and yet can be exchanged with confidence in a well-studied and well-understood cryptographic system. The emerging credit-card payment system is an example. Nobody would place their credit-card number in the clear on the net (unless they are quite naive) yet there is reason to believe that the Secure Electronic Transactions (SET) protocol will do an adequate job of protecting such information.

Provided I have ample opportunity to study the encryption program, and know that others more knowledgeable than I have also studied it, and provided

I am confident that the system has safeguards from viruses and poor management policies, I would trust modern cryptographic methods with my (small) fortune. Because SET, IPv6, and other Internet security protocols are open to public inspection, I have good reason to trust them. This is why I become frustrated when companies like Pseudo-One turn their backs to these protocols, and furthermore, preach to the general public that the problem is unsolvable. This last stance is fraudulent. I explained to Lisa that this, more than anything else, is what drove me to take it upon myself to study electronic commerce and the protocols that support it: my goal is to demonstrate the feasibility of strong security on the Internet. If corporate America is unwilling to pay for strong security, however economical it may be, then I will work from the "outside", learning about electronic commerce through passive eavesdropping. Mostly passive anyway; I was forced to agree when Lisa reminded me that I had copied and re-inserted messages into the transaction stream between two banks.

I did my best to control my emotions as I continued to vent my feelings. It is not just Psuedo-one that spurns modern cryptographic solutions. Most corporations, large and small, while claiming to be concerned, take the same stance. The position adopted by by these companies is naive and ignorant at best; callous and disrespectful at worst.

Telephone companies are an excellant example. Every year millions of dollars are spent monitoring cell-phone usage patterns in an effort to recognize a cloned phone. When there is a sudden change in the calling pattern, the cell-phone company discontinues the service on that phone. The customer is forced to bring his or her phone into a service center to have the phone reprogrammed for a different phone number. Then the customer must notify all his or her friends and business associates that the number has changed. Then, if the phone actually was cloned, when the phone bill arrives it is usually for some astronomical amount. The customer is typically asked to pay the bill until the matter can be "sorted out", at which point a credit is issued.

Wouldn't it be better if the phone companies would simply prevent the cloning in the first place? It would cost less money to implement a strong security protocol than it costs to develop and maintain the current "solution." There are costs associated with developing and maintaining the call-monitoring software, reprogramming phones suspected of cloning, managing the reimbursements for cloned phones, and handling all the customer questions over outragious bills for cloned phones. The situation is made worse by the ease with which the phones can be cloned. The result is that a typical customer must go through this nonsense several times (before he or she gets fed up and discontinues the service).

As consumers we deserve better. There is no excuse for a company actively involved in Electronic Commerce or telecomunications not to employ affordable technology to remove barriers to efficient markets and deliver the level of security consumers expect. To misrepresent the situation and inform customers that greater security cannot be achieved is simply wrong.

There was a time when the US automobile company claimed that greater safety could not be delivered in reasonably priced automobiles. We now know

this is not true. We also see the fallacy in the argument that, because an automobile cannot be made so that a head-on collision into a brick wall at 85 mph is survivable, there is little point in building in any safety features. We recognize that while consumers must accept some risk, this is no reason to completely do away with all safety. An 85 mph collision might be fatal, but a 35 mph collision shouldn't be. Similarly, while it is true that some data may be too sensitive to be put on the Internet in any form, certainly there is some data that, while too sensitive to be put on the net in the clear, is not too sensitive to transmit in encrypted form.

Pseudo-One is right to recognize that absolute security is not possible, but as consumers we deserve those protections that can be delivered at reasonable cost. Happily, ample security is achievable at very low cost.

Chapter 7

I sat and stared at the computer monitor. My DEC Alpha workstation sits atop a card-table in the living room of my apartment. Under the card-table is a second machine, a Pentium-133 with four large SCSI disks, that serves as my file-server. Both of these machines run Linux. I have a third machine in my bedroom, also atop a card-table, that run Windows95; it is a Pentium-90. Sharing space on the card-table in the bedroom is a another Linux box — a 486-66. All four machines are networked via Ethernet. I use a dial-up PPP connection to connect to the Pentium-100 at my office. Or, I connect to my ISP and connect to the office over the Internet from there.

After changing to the directory holding all of the EFT traffic from July 11th, I located the file that contained the full set of transmissions sent out by Bendix of St. Louis and destined for First Chicago Trust on that day. I quickly did a grep for 'Cryer' and found three entries. Lisa said that there should only be one. I extracted the three EFT's into a separate file, and then printed them out on the laser printer. I carried the printout over to the kitchen table and laid out the pages side by side.

There was a transfer of $25.32 to the power company. This was the gas bill Lisa had mentioned. It seemed a bit high for an apartment gas bill in the middle of the summer... but Lisa said this payment was legitimate. The next EFT was a payment of $1021.33 to an account owned by Jonathan Rogers, whoever he was. This was one of the EFT's Lisa denied. The other, the last of the three transfers involving her account, was a deposit of $18120.11 into her account from an account at Bendix. That account was in the name of Anthony R. Lee. This is the transfer that had Lisa in hot water, for although both of these last two transfers had gone through when I replayed the file, the second one was a deposit into Lisa's account and more than cancelled out the losses of the payment to Mr. Rogers. While she claimed the EFT was bogus, the bank couldn't help but notice that Lisa gained $17098.78. Not a fortune, but more than spare change. I, of course, knew that she had benefited only because I had replayed the messages; I knew she was innocent, but the bank didn't.

I picked up the printouts and walked back to the machine. I sat down, jiggled the mouse to activate the screen which had automatically gone blank due to inactivity, and pulled the EFT log into a text editor. I scrolled through

the file absently as I tried to guess what had occured on that night.

Had somebody appended the bogus EFT's? Who? Why?

It seemed strange to illicitly deposit money into somebody else's account. Could it be that Lisa really was up to some shenaigans? I shook my head in disgust. I had already ruled out that possibility; not only did I trust her, but she couldn't possibly have known I was recording and replaying messages. Even if she had been monitoring the EFT traffic over several months and therefore would have observed my earlier experiments, she still would not have known I'd be experimenting on any given day. I don't keep a regular schedule; even I would not have known ahead of time that I'd be tinkering on that particular day.

I browsed through the other files in the same directory. My line-surveillance program was designed to log all the traffic on the leased line. The one file I had already reviewed was seperate from the main log; I had seperated the set of initial messages from Bendix to First Chicago so that I could prepare the replay. Now I turned my attention to the main log. This file would contain all the messages from the session, including my replays.

I wasn't sure what I was looking for so instead of running search utilities as I had in my earlier post-mortem analysis, I scanned through the file haphazardly with a text editor. It was a good thing too, because as I scrolled through the file I noticed something that had escaped my initial review. The log showed that following the original transmission from Bendix to First Chicago — the transmission that I recorded but let pass — a bunch of error messages were returned by First Chicago. These messages were different from the class of messages that came later in the log, after my replay. These early error messages indicated that some of the EFT's were too badly garbled for First Chicago to process.

There were a lot of these errors. Too many. I typed in search-and-count 'grep' commands to see how many. There were 893. Hmmm. Next I counted the number of EFT's in the original transmission from St. Louis. Yup; 893. Every single one of the EFT's had been rejected without any processing in Chicago.

This was strange. Had I done something to scramble the messages in transit? While an occasional bit-error over a phone connection is not unheard of, such glitches are rare with modern modems. Each EFT would have been processed seperately by the recieving bank, so an error in one EFT would normally be confined to only that EFT, leaving the others intact. Any line glitches should be isolated to a single EFT, or at worst a small number of consecutive EFT's. Yet each and every one of the EFT's in the log was rejected by First Chicago Trust on the grounds that each one was garbled beyond recognition. Strange.

I scrolled down further in the log and eventually reached the end of the error messages and the beginning of my replays. Following my 893 replayed messages were the responses from First Chicago. The bank accepted all of the replayed EFT's. And why not? Since the EFT's had not yet been recieved in uncorrupted form, this was the first time the bank was seeing them. By replaying the messages I had inadvertantly corrected the situation! The appropriate action

following a catastrophic communications failure where all of the messages are garbled is to wait a short time and then resend all of the messages. I had done that for them.

So why had the people at First Chicago been in such an uproar over extra copies of the messages? What extra copies? And what did my tinkering have to do with the illegitimate payments? How had I enabled those?

Puzzled, I leaned back in my chair, an old wooden straight-back chair in desperate need of glue. It creaked loudly and the legs wobbled with more play than they should. The bare 60-watt lightbulb in the socket over my head was burning with a dirty yellow color, reminding me that I should replace it soon. The room was gloomy, with only that one light-bulb and the computer monitor to illuminate it. I stared at the information glowing from the screen. The folding card-table upon which the computer sat was littered with old notes and printouts, most of which I had long since forgotten the purpose for making. There where two mugs, each half filled with cold coffee. One sat precariously atop a slanted stack of papers while the other occupied one of the few spots of bare table surface.

Aha! Suddenly the events that must have transpired clicked in my head. The St. Louis bank would have recieved the error messages from First Chicago. Therefore those EFT's would have been resent by the St. Louis bank. It stands to reason that the bank would have taken corrective action after getting the error messages. I couldn't confirm this with certainty because I had neglected to record any traffic subsequent to the one session, but I had no doubt now that the sending bank must have resent the messages at a later date, probably the next day. So both Bendix and I resent the EFT's. Hence the extra copies. Since my copy got there first, the Bendix replay must have been rejected by First Chicago... *except* for the two mysterious EFT's on Lisa's account.

I sighed and pushed the keyboard away. I had come full circle. What was so special about those two EFT's? Lisa said they weren't legit. Fine. I would have to assume that they were forgeries.

What reason could there be for First Chicago to reject each and every EFT? Could they all really have been garbled? How?

No, the more likely explanation was deliberate interference by some individual. Hardware glitches and electrical storms would not cause such systematic corruption. Or, another possibility was that First Chicago chose to reject the EFT's for some reason and claimed that the messages were garbled as an excuse. Why a bank would do this I could not fathom. I suspected that the answer to the strange goings-on of the week before lay with the error messages from First Chicago; if I could explain those, then perhaps I would be able to explain the special treatment of Ms. Cryer's transactions.

I yawned and rubbed my eyes. The chair creaked some more. The clock over the kitchen table read 11:55. Tired and confused, I decided to call it a night. I ran the screen-lock but left all the windows open so I could resume where I had left off. I left all of the printouts on the kitchen table as well. Perhaps after some sleep and with a fresh start in the morning I would be able to make more sense of the strange symptoms I was seeing. What happened on July 11th? After

listening to voice conversations at the bank, reviewing recorded EFT traffic, and talking to the prime suspect in the case, I was still baffled.

Chapter 8

I debated calling Lisa the next morning to tell her what I had learned about the extra error messages from First Chicago. I hesitated though, partly because I was worried that she might be under heavy surveillance, even to the point of wire-tapping her phone, and partly because I didn't want to be too pushy. She had agreed to give me a chance to sort things out but she also was understandably edgy. Better to give her time to settle down.

I didn't need to worry about the second reason, and the first was out of my control before I realized — she called me.

She told me that I wasn't the only one that had approached her about the EFT debacle. While I had been browsing through my EFT files the night before, she had another uninvited visitor at her apartment. Somebody by the name of Rudy Levinski had stopped by and introduced himself as an employee of First Chicago Trust. Like me he seemed to know her story and was anxious to solve the mystery. Like me, he needed her help but did not want to involve the police.

I didn't like the sound of this but refrained from saying so to Lisa. To condemn this man would be tantamount to condemning myself, since there was little difference in our stories. I wondered what his involvement might be. Maybe he was a whistle-blower anxious to expose illegal activity at First Chicago. But if that were the case wouldn't he go straight to the police, rather than avoid them?

"Do you know him?" Lisa asked.

"Nope. Never heard of him. Did he explain his objectives?"

"Only that he wanted to help me... the same as you."

I wondered what she must think, with good samaritans coming out of the woodwork. I also wondered what the police must think, for if they did indeed have her building under surveillance then the sight of people parading in and out must seem peculiar.

"Look," I said, "I don't know what this guy is up to. He might really be a First Chicago employee as he claims to be, but he might not be. I can't tell you what to do, but I would appreciate it if you do not take him up on his offer."

"Well I have given it some thought and I think it would be best if *you* take him up on his offer."

Huh?

She continued on without skipping a beat, "I can put you in touch with him. The two of you can sort out the mess or fend each other off, or whatever. Me, I am going to distance myself from both of you. The way I see it, both of you are petty hackers at the least and major criminals at the worst."

"Wait a minute —"

"No you wait a minute," she snapped. "I'm not done. Talk to Mr. Levinski and figure out what's going on. I won't report either one of you to the authorities right away. But if one or the other of you can't make some headway in the next couple of days then I'm going to the cops. Got it?"

Her words were crisp and she had delivered this last message seemingly without stopping for a breath. She had made up her mind; there was no room for negotiation. Plus, I had no chips with which to bargain. Reluctantly, I accepted her proposition and she gave me Mr. Levinski's phone number.

After hanging up the phone I considered what Lisa had said. I did not have much choice but to call Mr. Levinski. Ms. Cryer had deftly taken control of the entire situation. As the only person in contact with all of the players, she enjoyed a unique position and she was calling the shots.

I hesitated but called the number Lisa had given me. Mr. Levinski answered on the second ring. His European accent was noticeable immediately. He sounded as if he was probably in his 30's. I introduced myself as a friend of Ms. Cryer's. I said that she had asked me to contact him on her behalf. He sounded nervous and seemed anxious to end the conversation quickly (I had called him at work). He was, however, ready to talk to me and we arranged to meet down at the lake-front that evening at 6:00.

That afternoon I took the bus to the Aquarium and walked north along Lake Michigan to the fountain where we had agreed to meet. It was a pleasant evening. The forecast had warned of rain later in the night but there was no signs of it. The water was bright blue. Stunning. There were boats sprinkled over the surface, some small and some large. I passed by a couple of fishermen sitting at the edge of the water. As I neared the spot where Mr. Levinski and I had agreed to meet I slowed down and studied the pedestrians. Rudy Levinski had described himself over the phone as a dark-haired man in his late 30's wearing a grey suit and yellow tie. I didn't see anybody that fit that description. I looked at my watch — it was 6:15. I was fifteen minutes late. Could he have left already? I walked over closer to the street. There were many people, some appeared to be waiting for a rendez-vous, but nobody fit the description I had been given. Then, suddenly I saw him. He was walking up to me at a rapid clip, having seen me before I saw him. He was slightly plump. He was short and wore glasses. The frames of his glasses were thick black plastic and seemed too wide for his face. This, combined with the strength of the prescription, made his glasses quite prominent. His forehead glistened with sweat. He looked very uncomfortable as he extended his hand and introduced himself. He motioned toward the lake and we strolled to the water's edge as we talked.

He claimed to be working in the Electronic Commerce department of First Chicago Trust. The Electronic Commerce department is mainly EFT work, he said. His title was that of Security Technician. His job was to operate

the EFT system and take part in incident response actions, meaning that he was responsible for detecting and repairing any problems caused by hackers. Needless to say his entire group was right in the thick of things and feeling a lot of heat.

I listened carefully and tried to guess what he knew of my involvement. I could not detect any animosity or bitterness in his demeanor and concluded that Lisa had not told him about my experiments. Good. I would keep it that way, at least for the time being.

"I had hoped to speak directly to Ms. Cryer," said Levinski. "I may have some information that would be useful to her. As an employee of the bank I am aware of some aspects of this case which may still be a mystery to the authorities. However, forgive me, I must be careful who I approach on this matter. Ms. Cryer appears to me to be an innocent victim. I too am a victim of sorts. If she and I can pool our information we may be able to extricate ourselves from this matter."

His English was far better than his accent would lead one to expect. He spoke slowly and crisply, carefully enunciating every word. His hands remained clasped behind his back and he stared out across the water as he spoke. He made eye contact only occasionally. The perspiration on his brow was heavier now. He spoke so coolly and calmly yet looked so hot and uncomfortable.

"We can help each other, she and I. By trading information..." he stopped, saying nothing for a while. We stood in silence. When he did speak again, it was with the same slow and deliberate delivery.

"Working through a liaison tends to make communication less efficient. In a delicate matter such as this — and I assure you this is delicate — it is perhaps better to meet face-to-face. No?"

OK, I got the picture. He saw me as a representative for Lisa and he wanted to talk to the real thing. I was an obstruction. I didn't respond immediately. I slowly panned the surrounding area judging all the passers-by. Nobody appeared the least bit interested in us and nobody was within ear-shot.

Could I trust him? Did I have a choice? Lisa had already decided that he and I would have to work together or alone, but not with her. So far I had been unable to make much headway on my own. If he really was a bank employee and really was directly involved with EFT's and security, then he would be a valuable ally. But could I count on him as an ally? He might turn me in to the authorities the moment he learned what I had done. He had hoped to talk to a woman he viewed as an innocent victim not a person who had helped facilitate the thefts.

"I'm not merely a liaison," I began. He turned slightly in my direction but said nothing. His expression was politely inquisitive. A small smile formed on his lips and he raised one eyebrow.

"I too approached Lisa Cryer with an offer to trade information," I said. "She suggested that I meet with you because you and I both have information to trade." I was reluctant to say more. It is one thing to admit illegal activity to a private citizen such as Lisa and quite another to confess to a bank investigator.

"I see," Levinski said softly. He now turned and faced me squarely. He

appeared to study me for the first time now. He asked who I worked for. When I explained my employment situation, it seemed to please him and put him at ease. He unclasped his hands and put one in his pocket. He wiped his forehead with the other. We then danced around the matter of trading information, both of us reluctant to divulge even the nature of our secrets without first receiving at least an inkling of the other's secrets.

I wondered what he knew about the inner machinations of his bank. From the beginning the behavior of First Chicago had been suspicious to me. I recalled the strange reactions of First Chicago executives in the phone conversations I had tapped. How could they seriously have suspected Lisa Cryer of wrong-doing when it was First Chicago that rejected all of the messages in the first place?

It became clear that whatever information Rudy Levinski had — information that he was unwilling to give to the FBI — was not going to be forthcoming until I told him more about myself. But I sure as hell wasn't going to tell him that I had conducted illegal wire-taps and impersonated a US bank. I tried a different approach.

"Lisa denies two of the EFT's that were processed by your bank on July 12th," I told him. "And I believe her. The trouble is, the MAC's for the false EFT's appear to have checked out OK. Can you confirm that?"

"Yes. I know of the two EFT's to which you refer. The MAC's were proper. They were calculated using the same cryptographic key as all of the other MAC's in that batch. Either the subject knew the key or he was able to create a perfect forgery. I assure that the latter is extremely unlikely. There are no known feasible attacks on the encryption used."

This I knew, of course. DES is a strong encryption algorithm. It is somewhat dated at this point, but provided one uses long keys it remains strong to this day. It is arguably the best symmetric-key algorithm today. It has withstood three decades of intense cryptanalysis.

Rudy seemed to be opening up a bit. He still looked tense and nervous, but his last answer had been somewhat informative. He would not have known my background in cryptology and was probably making a legitemate effort to cooperate. I tried asking another question.

"Every EFT in the original transmission from Bendix was rejected by First Chicago. What was the reason for that?"

Mr. Levinski raised a hand between us and smiled gently. "I answered your question. Now it is my turn to ask you a question. How did you know that the illegal EFT's were included in the same transmission as the others?" Then, after a slight pause he added, "and how did you know that First Chicago rejected each and every EFT in the original transmission?"

"That is two questions," I pointed out, "but since the same answer covers both, I'll answer them both. I was eavesdropping on the transmission between Bendix and First Chicago on July 11th. I did not alter the transmissions at all," I added hastily. "I observed the traffic but let all messages pass back and forth unobstructed and unaltered."

He nodded his head slowly and showed no surprise. I was suddenly very anxious to absolve myself.

"I had no malicious intent. I am a security professional and was merely observing the traffic to determine the protocol used for funds transfer. The published standards are vague about error-handling. In fact, I was pleased to see the error messages from First Chicago because they were instances of error messages that I wanted to see."

I realized then that he might think that my interest in error messages drove me to take steps to cause errors (which is true) and that I intentionally garbled the messages from St. Louis to Chicago (which is untrue). I hastened to reassure him.

"I had nothing to do with the garbled messages. It was just coincidence that I was able to observe the error-handling for corrupt data transmissions. I did nothing to obstruct the communication line."

Mr. Levinski gave me an understanding smile and nodded his head slightly before turning back toward the lake and staring out over the water. It was my turn to ask him a question.

"I do not understand why each and every EFT in the transmission was scrambled. One or two might be explained by a hardware fault, but such a regular rate of errors is baffling to me. What might be the reason for that?" I asked.

He shrugged his shoulders without looking away from the water. His hands were clasped behind his back again. "A bad connection perhaps," he offered. "It happens on occasion. It could have been any number of things. Maybe there was a lightening storm somewhere between St. Louis and Chicago. Who knows."

None of these explanations sat well with me. Modern modems and modern phone lines have very low error rates. Modems have built-in error correction. On top of that, the banks were using TCP/IP as the communications protocol. TCP/IP includes error correction codes too. The TCP/IP headers apparently got through intact, so why not the payloads? Moreover, any bit-errors that did occur should be confined to a single EFT. Strange.

Thick clouds had rolled in and obscured the sun, which was lower on the horizon now. There were hints of rain. Lake Michigan had turned from blue to grey, and the water was now choppy.

When Mr. Levinski spoke again, it was with the same calculated phrasing and meticulous enunciation. "Were you targeting Bendix or First Chicago, Mr. Raymond? That is to say, were these EFT's of interest to you because they originated from the St. Louis bank, or because they were bound for my bank?"

I explained that I chose the banks I did based upon convenience, and not for any other reason. It so happens that it was First Chicago that I was watching, not Bendix. Partly to change the subject, and partly to counter the edge of accusation in his question, I decided to press the hardware failure issue.

"It seems strange to me, Mr. Levinski, that a hardware error or electrical storm would cause each and every EFT to be rejected. Bit errors should be somewhat confined, as each EFT is independent of the others — to say nothing of the error correction codes that are employed at various layers in the network protocol stack."

His response surprised me. Moments earlier he had shrugged off the errors as a minor nuisance. Now he became quite defensive.

"Have you worked in EFT operations, Mr. Raymond? No, you have not. As a member of the EFT operations staff at a large US banking institution I can assure you that errors of this sort are not unusual. We get them at First Chicago. Other banks get them too. Our error rate is not out of line with the rates at other banks."

It was at that moment that I concluded that, for whatever reason, First Chicago had chosen to reject all of those EFT's. Rudy's initial response to this matter had been to downplay the entire issue. Now, when pressed on the matter, this articulate and intelligent man was reduced to claiming superior knowledge without being able to provide a plausible explanation for the phenomenon. I found this disturbing; there was something that he was not telling me. Apparently that was not the subject that he wanted to discuss with Lisa. The mystery of the rejected EFT's would plague me still longer. What reason would a bank have to reject all EFT traffic? And why disguise the reason? This last question was easy to answer: because the real reason was less than honorable. Next question: what could that real reason be? Is there a financial advantage to be had in stalling on funds transfers?

My thoughts were interrupted by Mr. Levinski's next question. "Did you keep a record of all of the EFT's you observed that day Mr. Raymond?" he asked. "Do you still have them on tape or on disk?"

I tried my best to suppress the sudden wave of panic that swept over me. Would my disks be confiscated if I admitted having the files? Was there anything on them that could embroil me still deeper? I did not know for sure, but I certainly did not want to find out.

Or would Mr. Levinski actually want me to destroy evidence? I still knew very little about this strange man at my side asking me carefully guarded yet pointed questions.

Reacting to my tense silence, Mr. Levinski elaborated. "I wish to determine if the improper transfers were inserted upstream or downstream of your tap, Mr. Raymond. My bank has a log of all the messages received, but I am not privy to the corresponding logs at Bendix of St. Louis. Furthermore, if the improper transfers were inserted into the data stream after the messages left Bendix, it would be interesting to know if those messages appear in your logs."

OK. This was a very reasonable request, and an interesting avenue to pursue. I told him that I was unsure of the extent of the data I had, but that I would investigate this question and report back to him. After that he asked a couple more minor questions, but it became clear that he had accomplished his goal for this meeting. He wanted to establish the flow of messages into his bank; he hoped to determine the source of each message. It was becoming clear that at least some of the messages did not originate from the purported source. Little more was said and the meeting concluded shortly afterwards. We agreed to remain in touch and went our separate ways. I stood by the water and watched him as he walked away. The darkness over the water was caused by the storm clouds that were rolling in from the west and was deceptive. It was still only

about 7:00. Once the rain began to fall, the humidity would certainly drop, but for the time being it remained uncomfortably hot. I was especially aware of the muggy heat as I watched Mr. Levinski walk away — he seemed so affected by the humidity. After he was swallowed up by the darkness I turned and walked briskly to the bus-stop so as not to be caught in the rain.

Chapter 9

The one thing that troubled me most about my meeting with Rudy Levinski was that I had been unable to learn his secret. Why was he anxious to by-pass the police and approach Lisa directly? Why was he anxious to help her?

The answer seemed to lie with the garbled EFT's. His explanation of this strange event was not satisfying. I was convinced that those error messages lay at the heart of the problem. What did Mr. Levinski know and how could I draw it out of him?

I was certain that the transmissions were not corrupted by an electrical storm. Nor was the cause a faulty hardware component — after all, the error messages got through properly, as did my replays moments afterwards.

Somebody tampered with those transmissions. This tampering occurred downstream of my wire-tap. Could there have been a second tap? Maybe. Or, another possibility was that the tampering occured closer to the end point, at the First Chicago computers. Indeed, maybe there was no tampering at all. Maybe the bank only claimed that the messages were scrambled. This would be consistent with Rudy's obvious effort to downplay the importance of the entire episode. Could it be that First Chicago was behind the forgeries and the rejections were somehow related to a cover-up? This seemed unlikely; by issuing systematic rejections, First Chicago was drawing greater attention to the forgeries. Such conspicuous action with no plausible justification would be inconsistent with a cover-up effort. So why would the bank deliberately stall transfers?

Slowing the flow of money between two banks would benefit the bank with the net decrease in assets. Thus, if somebody at First Chicago had examined the EFT's and determined that First Chicago stood to pay out a large amount of money, then there would be good financial reasons for slowing those payments. Perhaps the bank was low on reserves. By stalling for twenty-four hours, the bank can build up greater reserves without turning to the lendor of last resort, the Federal Reserve. The Fed charges interest for overnight loans. Admittedly, the rates charged by the Fed are generally below market-value, but for a large loan the amount can be significant. This might be the explanation I had been looking for! I raced over to my Alpha machine and quickly typed in my password to release the screen-lock. Using perl, I quickly wrote a script to sum the

EFT's and print the net flow of dollars from Bendix to First Chicago. Sure enough, it was a negative number, meaning that more money was being paid by First Chicago to Bendix than the other way around. The net amount was $7 million. I had no idea if this was an unusually large amount, but I suspected it was. Certainly if my theory was right, then it would be. This would be the motivation I was looking for to explain why First Chicago would falsely claim that the transmissions were garbled and reject all EFT's until the next day.

Uh oh. If my theory was right then this also meant that the rejections were entirely unrelated to the forgeries. This meant my wire-tap had picked up *two* attacks on the United States banking infrastructure!

I pushed my chair away from the table. The card-table, already stressed from the weight of the Alpha, yielded to the presure of my arms and threatened to collapse. I scarcely noticed. The apartment was silent and gloomy.

Plick, plick, plick,...

The wall clock in the kitchen registered on my consciousness and took on an ominous quality with its incessant ticking. A shiver ran down my spine as I stood up and walked over to the window to draw the blind. The sky outside was overcast and the air was foggy. I kept the room light off. The paranoa that swept over me told me that it was better to let it appear that I was not home. I sat in an easy chair in the living room, across from the computer desk, and stared absently at the distant monitor screen glowing on the opposite side of the room.

The delay scam at First Chicago was clearly an inside job. The beneficiary of this crime was an institution. No longer was I chasing a two-bit crook or a prankster. If my prey was an institution, with the masterminds behind the crimes sitting on a corporate board, then there was no telling what extremes they might go to in order to escape capture. I stood up and checked the deadbolt on the door. Next I peeked through the blind and down to the street below. A week ago I had been disgusted by my fear; now I felt fully justified.

I was certain that I had surmised the meaning of the rejections correctly. I was equally certain that Rudy Levinski was fully aware of the delaying tactic taken by his bank. Perhaps he had even been the one to carry it out.

Who might have been watching or even listening to my conversation with Rudy? I racked my brain trying to remember if I had said anything that might get me in trouble. Was the FBI aware of this second crime? My meeting with Rudy took on a whole new meaning in this new context. Did the FBI have Rudy under surveillance? Had I now met with two of the prime suspects? How long could I go on associating with suspects before I (rightfully) became suspect #1?

Scared, I sat alone in the room, thinking. I was in over my head. With evidence of institutional crime by a major United States bank, clearly my next course of action should be to call on the FBI. What was the name of the agent in the phone calls I had tapped between the FBI and First Chicago? Agent Carter. I should contact him.

Instead I called Lisa. I'm not sure why. When last we has spoken, she had been distant and somewhat cold with me. She did not seem to find me

threatening... only repulsive. She viewed me as a hacker, with the full set of negative and unseemly connotations that the contemporary use of that term carries.

Still, it was Lisa that I phoned. Maybe it was because she was the only other person that knew of my involvement. There simply was nobody else to call. I needed to talk to somebody.

I used my meeting with Rudy Levinski as an excuse, telling Lisa that I needed to brief her and asking if she could come to my apartment immediately. Thankfully she did not ask any questions other than to ask for directions to my apartment. She sounded relieved that I had spoken with Rudy and that the meeting had been productive.

I did not have to wait long before Lisa arrived. In that time I turned up the lights and turned down my paranoa. Lisa walked in, cast a quick look around my living room without commenting, and asked about my meeting with Rudy. I explained the entire situation.

After I finished my story, Lisa stood up, stretched, and asked, "What do you have in the way of food Carl? I'm starving."

Oops. It was almost 7:30 and I still had not had dinner. I was too embarrassed to let her look through the barren contents of my refrigerator in search of a reasonable dinner, so I suggested pizza delivery. She opted for Chinese carry-out instead. There is a small carry-out restaurant down the street from my apartment. There isn't anyplace to sit, but the food is good and it is within walking distance. It is a long enough walk that when I leave immediately after ordering, the food is ready just when I get there.

Lisa made the call and we prepared to leave the apartment. It had started to drizzle lightly shortly after Lisa arrived so I grabbed a jacket from the hall closet. Lisa hadn't worn a jacket when she came so I searched for something she could wear. All of the coats I had were either too warm for July or too big to fit Lisa. The best I could find was an old track-team jacket from my college days at Berkeley. It was a bit too big for her, but it was lightweight and water resistant. Given the stylishly casual manner in which Lisa dressed, it actually went quite well with the rest of her outfit.

As we exited the front door of the building I noticed a light-blue sedan parked immediately across the street. The only reason I noticed it was because it was parked in a spot that is always empty, due to the fire hydrant located there. A large burly man in a trench coat was sitting at the wheel but the engine wasn't running.

I didn't bother opening the umbrella I'd brought along with us, as the rain was little more than a mist. I turned right and headed down the sidewalk with Lisa falling in step beside me. The air had the smell of burnt ozone that it takes on after a light rain in a hot city. I've always found that smell to be a pleasant one and I breathed it in as we walked. Neither of us said anything for a time. We reached the corner still in silence and turned left. After we had gone about half a block a light-blue sedan passed us. There was a man in a trench coat at the wheel. Hmmm.

"See that car?" I asked, as it reached the end of the block and turned right.

"Yeah"

"It was parked right outside my apartment. Looked as if the guy at the wheel had been sitting there for a while... maybe waiting for us to leave."

"Maybe he was waiting to pick up a friend," she suggested.

"If he was then the friend didn't show up because he is still alone in the car," I replied.

"You think he was following us?"

"I'm not sure. I will confess that I'm becoming more and more nervous about this whole affair. It is starting to grow into something larger than I'm prepared to deal with.

"Let's see if the car continues to follow us to the restaurant. If we don't see him again then I will concede that I'm being crazy. But if he is just circling the block and passes us again then I think we may have cause to be worried."

He wasn't circling the block; he was waiting for us instead. I hesitated for only an instant as we rounded the corner and saw the car parked there. Lisa didn't say anything but let out a soft whistle under her breath.

"Now what?" she asked.

"Don't stop. Keep walking."

I didn't want the driver to know that we had noticed him. Not that he seemed to be too concerned. He made no effort to feign some other purpose for being there other than to watch us. I tried my best to look him over as we went by without appearing to do just that. I had Lisa walk beside me, between the car and me, so that I could look beyond her and at the driver, all the while pretending to be involved in an animated conversation. For his part, the driver simply sat there and stared at us as we went by. Is this the way the FBI conducts surveillance? Or was it somebody other than the FBI? The CIA? NSA? I certainly didn't have any experience dealing with spooks and had no basis for even trying to determine which agency he might be from. But I had no doubt that he was a spook of some sort. The latest discovery of inside shenanigans meant I could no longer take any of this lightly. With such rampant corruption there would be plenty of blame to spread around and, innocent or not, I was bound to have some of that blame thrown my way. I was convinced that executives at First Chicago were already setting up Lisa to be a scapegoat.

As we neared the carry-out place at the end of the block the blue car passed us again. This time it slid into an empty parking spot along the curb in front of us. At the same time, a city bus pulled up to the bus-stop directly in front of the Chinese place. I turned to glance behind us. Uh oh. Two men in dark suits were following us, and walking faster than we were. I didn't like this. I grabbed Lisa's elbow and broke into a run. Lisa kept up with my pace easily, matching me stride for stride.

"Where are we going?" she asked. "Not the carry-out place."

"See that bus stopped up ahead? Do you think we can get there before it leaves?"

"No problem," she said as she sped up.

I sprinted at full speed, leaving Lisa behind. Just so long as one of us got to the bus-stop in time, that person could hold the bus for the other. I pumped my

arms and tried to control my breathing as I willed myself to move faster. I heard the doors on the bus close as I drew nearer. I was still fifty feet away. Thick black exhaust belched out of the back as the bus began to crawl away from the curb. Thirty feet away now. The bus shifted gears. Weather it was from first gear to second or second to third I don't know. Slowly, between belches and roars, it picked up speed. Very slowly; it wasn't moving fast yet. I ran up along side the filthy vehicle and beat on the glass doors with my fist. The driver turned with a startled look on her face and hit the brakes. Moments later the door opened and I stumbled up the steps.

"Thanks," I panted, "there's another person on her way."

"No problem," replied the driver. She was an overweight woman with curly blonde hair and weiging about 250 pounds. She had an amused smirk on her face; she probably doesn't get such over zealous passengers on her bus very often. Lisa trotted up the steps moments later.

Nervously I looked out the windows as the bus once again began to accelerate. We weren't out of trouble yet. Our pursuers were running toward the bus. It seemed an eternity as the bus labored to pick up speed, seemingly coming to a near stop each time the driver stepped on the clutch to shift up a gear. But we did eventually get away safely without incident.

Beside me Lisa was panting only lightly and, unlike me, was not sweating in the least. I tried to convince myself that this was only because I had been the one to run ahead, running hard.

We quickly revised our dinner plans. Lisa suggested we go to Sid's again. We changed buses three times before finally reaching what I now was convinced was Lisa's frequent watering hole. We were again shown a table by Maria. I found it hard to relax and when the waitress came to take our order a few moments later I realized that I'd been looking at the menu without actually reading it. To disguise my lack of concentration I quickly ordered the swordfish, the same dish I'd had last time. Apparently this wasn't good enough to fool Lisa.

"That car really got to you, huh?" she asked.

Should I tell her of my worst fears? I was the one that had dragged her into all of this in the first place. I hadn't given her much opportunity to distance herself from the affair from the beginning and had given her every opportunity to become enmeshed further. Didn't I have a moral obligation to inform her of the risks as best as I could evaluate them? On the other hand I really didn't have any basis for making a firm evaluation myself. She had the same information I had. Wouldn't it be disrepectful and condescending to presume that she couldn't make her own determination of the personal risk involved. Still...

"Lisa, I think you should consider the possibility that there may be some very desperate people involved in this situation," I said.

"It does sound like the scope has broadened a bit," she agreed. "Do you think the man in the car was on the side of law enforcement or on the other side?" she asked.

This is exactly what had been troubling me the most. Now that we had evidence that EFT tampering was rampant, I couldn't discount the possibility

that a large gang of thieves or even the Mafia, was in on the action. Given my choice, I would much rather be hounded by the FBI than the Mafia. The FBI operated under some legal restrictions; the Mafia had very few constraints. With bank executives involved in the delay scam, some very powerful people were operating on the wrong side of the law. Who might be working with them?

Our food arrived shortly thereafter. Once again the swordfish was excellent. Lisa had ordered the Fillet of Sole this time and reported that it too was very good. I had taken the liberty to order a bottle of wine with our meal. I felt more at ease now that I'd aired my concerns and Lisa accepted the situation. I poured the wine and was about to offer a toast to friendship and happenstance but Lisa interrupted me before I started and proposed a toast to our progress on the case and to petty thieves who interfere with the lives of innocent people. She chuckled softly as she sipped the wine. Then, as she set her glass back down, she asked me what I intended to do about the delay scam. I was still undecided. The safest and perhaps wisest approach would be to go straight to the FBI. However, I had hopes that by confronting Mr. Levinski I could learn whatever secrets he may have and enlist his help in tracking down the perpetrator. I was no longer eager to go it alone; I needed all the help I could get.

"How much money do you figure a bank could steal by delaying?" asked Lisa. "These are pretty serious charges you are making. Are you sure of yourself?"

"There is no way that those EFT's were corrupted by natural causes," I exclaimed. "The TCP/IP headers made it through, yet each and every payload failed despite error correction in the modems and in the TCP/IP protocol." I made these comments to re-establish my own convictions as much as to convince Lisa. She was right; these were serious charges. I looked around the room uneasily. I wondered if we should be talking so openly about the case in public and suggested to Lisa that we switch to a more mundane topic.

"Carl," she said with some annoyance, "look around. The closest people to us are thirty feet away and if they look like spies to you then you certainly have a great deal of respect for the creativity of the FBI in developing disguises."

She was right. The party closest to us consisted of an elderly couple seated on the other side of the room. The man was very nearly entirely bald, with only a bit of grey hair near his ears. The women had powdered white hair tied in a bun. She was quite short and stocky whereas the man was tall and stocky. Both wore glasses. They had a small boy with them. My guess is that he was between four and seven years old. They appeared to be grandparents on an outing with their grandson. This impression was reinforced by the manner in which the older two listened patiently and attentively as the boy slowly and carefully recounted a long tale of some sort. I was too far away to make out the words, but I could hear well enough to know that there were frequent pauses and what sounded like revisions to the narrative.

Not only did the elderly couple look as wholesome and innocuous as can be, but it was hard to imagine that the FBI was recruiting young children for surveillance operations. OK, I was being paranoid.

"Still, if you'd rather talk about something else, that's fine by me," Lisa offered. "I'd welcome the change. A girl can't live, eat, and breathe electronic

banking crime. Or at least I can't.

"Tell me about your job at AT&T. Why did you leave?" she asked. Then, when I didn't reply immediately she quickly apologized. "I'm sorry. I didn't mean to pry. If you don't want to talk about that we can talk about something else. I was just making conversation."

"No I don't mind," I re-assured her. "I hesitated only because it's a long story and I wasn't sure where to begin."

I told her about my move from AT&T to Multi-Media Telecommunications (MMT). That move came right after I earned my PhD in Computer Science from Princeton. As a small telecommunications company anxious to capitalize on the emerging markets in multi-media, MMT offered exciting positions in R&D. The company did quite well, with the stock surging in the first three years after I joined, but the work in cryptography within the company began to dry up. Ironically, the advances in authentication and information integrity that make cryptology applicable to business, are the same advances that caused MMT to lose interest. Unlike most computing applications in business, where information integrity is important, MMT was primarily interested in privacy. Things like digital signatures, MAC's, zero-knowledge proofs, and authentication were not on MMT's research agenda. Instead, MMT devoted the full research budget to communications hardware and multi-media technologies. I opted to go into the consulting business, and for nearly two years now I've been making a comfortable living working on protocol analysis. Admittedly, I've had to supplement that work with an occasional mundane programming assignment working on GUI's or firewalls, but for the most part the work has been interesting.

Lisa took exception to this last comment. It was then that I learned that she was a software developer working on Graphical User Interfaces (GUI's). I then had to sit through a long sermon that not all User Interface projects are mindless programming-by-example using wizards and other people's libraries. Before long I actually found myself quite interested as Lisa explained the GUI library that her company had developed in-house. She was not one of the original developers, but had joined the small company of about fifty employees threes ago. Her job was to help keep the aging GUI library current... no easy task given the rapid rate of advances in that industry.

"We produce MAC CD-ROM software for kids up to about age five — mostly educational stuff. We are able to churn out new titles today that are cutting edge, and we are still using the same basic kernal the company was founded on. Sure, we've had to make lots of changes and enhancements, but the foundation remains strong. Don't belittle the Computer Science that goes into GUI's Carl."

I was too pleased by her strong grasp of Computer Science to argue. I quickly retreated and confessed that the work she described was both interesting and challanging. We talked at length about Computer Science and about jobs. Generally, I have been pleased with the direction my career has gone... until now. Granted it is entirely my own doing, but chasing down a cunning EFT mastermind, with the FBI breathing down my neck, and with the threat of a jail sentence looming over my head, does not bode well for my career prospects.

Chapter 10

The plan was to walk in on Mr. Levinski unannounced, make it known that we were aware of the stalling tactics used by his bank to delay processing of EFT's, and use that as leverage to learn whatever it was that he knew. It took quite a bit of coaxing on my part to convince Lisa to go along with this plan. She argued that I was in no position to accuse others of tampering with bank transactions. Nonetheless, she did eventually acquiesce and agree to take the necessary time off work (I don't have that problem).

The plan worked well. Immediately upon being confronted, Mr. Levinski conceded that the bank did deliberately falsify the error messages on July 11th. He hastened to add that stunts of this sort were not as uncommon as one might think. Other banks generally turned a blind eye to this sort of thing, so long as nobody abused the unwritten privilege. In the banking world, this was the equivalent to claiming that "the check is in the mail."

Mr. Levinski went on to explain that it did not take the FBI long to uncover the scheme and to interrogate all of those involved. One of those people was Rudy Levinski himself. He was the one that actually implemented the scheme. He wrote the programs and his boss had him monitoring reserve levels and EFT amounts to determine when the bank needed to stall. It was Rudy Levinski that ran the program to generate the error messages on the 11th. My wire-tap caught the output of his program and recorded it.

Fortunately for Mr. Levinski, he was able to claim that he was little more than a pawn caught up in a corporate policy over which he had no control. To hold his job he must carry out the bank policies, irregardless of any improprieties he may find therein. Rudy explained to Lisa and me that it is his boss, Mr. Lampley, that will pay the largest price for that policy. The FBI has stated that it will prosecute Mr. Lampley and possibly some executives. This was one of the reasons that those same executives were treating Lisa as roughly as they were. I could only imagine what would happen if those men got there hands on me. Up to this point nobody at the bank was aware of my involvement. As far as they were concerned the forgeries and my replays were part of the same attack by some unknown hacker.

Lisa asked if Rudy thought that the people outside my apartment had been hired by his bosses. Rudy was adamant in insisting that the delay scam was not

a major conspiracy. It was a common ploy used by banks and did not justify a major cover-up. Yes, it was illegal, but not unusual, he said. Furthermore, he was certain that the Mafia was not involved, nor any other sinister criminal element.

Rudy said that his greatest fear was that the hacker would never be found and that the FBI would need a scapegoat and that the bank would need a fall guy. It appeared very likely that Mr. Lampley would be a fall guy, but he would probably take some of his people down with him. As the man that actually operated the EFT system at the bank, Rudy was a good candidate for both a bank fall guy and an FBI scapegoat.

"This is my motivation for approaching Ms. Cryer to assist in any way I can," Rudy explained. "That reason still stands. The fact that you two are aware of the EFT stalling operation in no way changes that. I am disappointed that you chose to visit me here at the my office, but as long as you are here anyway perhaps we can take this opportunity to review some of the forged payments together.

"Tell me Mr. Raymond, were you able to determine if the forgeries entered the EFT stream upstream or downstream of your wire-tap?"

"It was upstream — closer to St. Louis. My recordings of the traffic include the forged EFT's on Lisa's account."

This pleased him. "That will help absolve First Chicago Trust then. If it was a bank employee that created the forgeries, it appears more likely that it was an employee of Bendix of St. Louis rather than my bank." He sighed softly. "First Chicago Trust is in enough trouble as it is. It is a shame that we don't use public-key cryptography to sign messages. If Bendix had used a private signing key instead of shared secret key, then my bank could not possibly know the signing key and would be above suspicion with respect to forgeries. As it is now, since we use shared symmetric keys, it is the word of each bank against the other."

There was a brief silence and then Rudy asked gently, "what about the replays? Were those inserted into the message stream upstream or downstream of your tap?"

"Uh," I stammered, "those were actually created *at* my wire-tap; not upstream or downstream."

"I see," he said quietly, showing no surprise. "You generated those yourself... and for what purpose?"

I am not sure why I chose to come clean at that moment. Perhaps I felt sorry for him. He was clearly under a lot of stress yet was taking it well. He was the victim of circumstances; an employee working for a corrupt employer in a ruthless business. Maybe I was simply conscious of the fact that Lisa was standing beside me and, having full knowledge of my involvement, would recognize any attempt by me to mislead Rudy or misrepresent facts. For whatever reason, the moment he asked about the replays I decided to tell him the full story. This I proceeded to do.

When I was done, his attitude was one of friendship and comraderie. We were all in this together now. He suggested that we pool our efforts and study

the clues together. He pulled a small stack of papers out of the top drawer of his desk. They were computer printouts. Some of the lines on the pages were highlighted with a pink marker. He explained that these were the EFT's that his department had determined were forgeries. Recognizing a forgery was no easy task since the MAC's checked out perfectly. The highlighted lines on his printouts were found by investigating payments in a more mundane and conventional manner. Staff members had been studying payment patterns for individual account holders in an effort to weed out regular bill payments such as mortgage payments. When they came upon an unusual or large transaction, bank employees called the account holder for voice confirmation that the payment was proper. This was a pain-staking process and needed to be conducted carefully so as to avoid embarrassment to the bank.

Next Rudy laid a large sheet of paper on his desk. On this sheet was a hand-drawn diagram. The diagram consisted of points and arcs — being computer scientists, Lisa and I both recognized it immediately. It was a directed graph; an abstract data structure. The arcs represented funds transferred from one account to another. The points that were connected by arcs represented bank accounts, and where labelled with account numbers. The direction of the arcs illustrated the flow of money from one account to another. Each arc was labelled with the amount of the EFT it represented.

The first thing that would have struck anybody upon looking at the graph, was the intricacy of the structure. There were many nodes (accounts) — perhaps 50 — but there were far more arcs. There were arcs going everywhere. There were multiple arcs between the same pair of accounts even. Some accounts had as many as fifteen arcs going in and out.

Rudy explained that these represented only forged EFT's. If the diagram included arcs for legitimate EFT's it would be far more complex.

"We estimate that we have found fewer than 15% of the forgeries," Rudy announced. "As you can see, there is an excessive number of them. Most of the forgeries are on bank initiated corrections. Beyond that, there does not appear to be any pattern; they are everywhere and they go everywhere. They are in amounts ranging from ten dollars to tens of thousands of dollars."

He looked at me sideways as he said this, as if waiting for me to say something or notice something about the graph. Other than the size of the graph and the number of the arcs, I could not see anything remarkable about it. It was a cyclic directed graph with weighted arcs. Nothing more. Rudy paused to mop his forehead with a handkerchief he pulled from his pocket.

"In addition to the amounts, I've annotated each arc with a date. I've also annotated the account numbers at the nodes with a bank prefix. Very nearly all the forged EFT's we have found are error-correcting transfers, meaning that they have been assigned a code to indicate that they are funds transfers intended to correct an earlier banking error."

Some of the arcs had dates other than July 11th. There were many with dates later in that same week, as well as some with dates before the 11th.

When I mentioned this Rudy nodded but explained that far more intriguing was the amounts of the transfers.

"You will notice," he said, "that the sum of the weights of the in-arcs and out-arcs are equal at each node. For every dollar that is stolen from an account, a dollar is deposited into the same account."

Amazingly enough, this was true. Lisa and I chose a few nodes arbitrarily and added up the weights. Every time they summed to zero; no net change to the account balances. This was strange.

"In some cases the in-arcs and out-arcs are for different dates," Rudy continued. He stabbed a node near the center of the diagram. "For example, on this account here the forged withdrawals are for July 13th while the forged deposits are for July 14th. Thus, while the account balance was ultimately left unchanged, there was a twenty-four hour period when it was incorrect by..." He leaned over and studied the numbers. "By $14,213," he finished.

"Why steal money and then turn around and give it right back?," Lisa wondered out loud. "It doesn't make any sense."

"Well," offered Rudy, "the deposits come from different accounts. Perhaps the subject is some sort of Robin Hood figure and likes to redistribute wealth."

That would have made more sense if the hacker actually was redistributing wealth. In just the small number of forged EFT's that had been found, the net affect on hacked accounts was zero. In each case — except Lisa's — the balances were restored within 24 hours. No money was changing hands other than for brief transient periods. Most of the balances were restored immediately. Some were "restored" even before the money was withdrawn.

Now, for the first time, I began to understand what had happened to Lisa's account on the day I replayed the messages between Bendix of St. Louis and First Chicago Trust. It was plain now. The hacker had forged an EFT to deposit funds into her account. He also forged an EFT to withdraw part of the deposited money. Then, either he was spooked by the error messages by First Chicago or else he intended to withdraw the remaining portion the next day. The result was that Lisa Cryer's account was the only account that was used to route forged EFT's where the net change in balance was not zero. The fact that the net change was positive, and by several thousand dollars, was what had Lisa in hot water with the police.

"Do you remember who the forged payment out of your account was to?" I asked Lisa.

"Oh yeah, I remember all right," she replied with a mirthless laugh and a nod. "It was to Jonathan Rogers for about one thousand dollars." She bent over to open her handbag as she said this. Moments later she had a small piece of paper in her hand and she read from it as she continued. "The amount was $1021.33 to Jonathan Rogers. The deposit was from Anthony R. Lee for $18120.11. That makes my net profit $17098.78."

Rudy slowly thumbed through the pages before answering. "In addition to the deposit from Ms. Cryer's account there was a second illegitamate deposit into that account. Also, there was a payment out of Rogers' account. The amount of the payment equals the sum of the two forged deposits and we have confirmed that the payment was also forged.

This made Jonathan Rogers' account one of the many that the hacker was

apparantly using to launder money. The hacker was routing money through numerous accounts. Sometimes he simply deposited money from one place and then immediately paid it out to another place. Other times he split a transfer or merged two or more. In the case of Jonathan Rogers, the hacker appears to have deposited money from two seperate accounts, one of which was Lisa's, and then used a single EFT to withdrawal the money. My guess is that Lisa's account was also being used to launder money, but in that case the hacker was using a single EFT for a deposit and two EFT's for withdrawals... except the second debiting EFT was never made.

"Carl, what is the point of all of this? Why is the hacker doing this?" implored Lisa. Clearly exasperated, she was at a loss. "Except for screw-up's like the one with my account, the hacker isn't stealing any money. What's the point? Is it just a power trip?"

"Probably. Most hacks are." I myself was not fully satisfied with this explanation even as I voiced it. It is true that most intrusions into computer systems are by kids on power trips, but this attack seemed far too sophisticated to be a joy-ride. The MAC's on the bogus EFT's were perfect forgeries. Any attacker that can crack DES is no prankster. Joy-riding through the bank accounts of numerous private citizens seems too high-stakes for even the most couragous braggart. When Robert Tappem Morris unleashed his worm on the Internet in 1988, he victemized a very large number of people, but he had no malicious intent. His worm was disruptive due to a bug in the software, causing it to replicate far too rapidly. Kevin Mitnick, while a major nuisance, never directly stole money from bank accounts. He appears to have broken into computer systems as part of an obsessive hobby, collecting root passwords as trophies. All indications are that the prize that Mitnick sought was respect from his peers, be they other hackers or his adversaries fighting to keep hackers out of their systems. Indeed, the standard but dubious argument that hackers use in their own defense is that they never actually steal anything. Hackers of this type tend to exploit bugs in operating systems and server programs. The most infamous security-bug-ridden program is sendmail, but there are many others. These same hackers also rely heavily on "social engineering", which is their term for a con-job. These people are phone phreaks and OS groupies. What they lack in formal education they more than make up for in persistence. They read OS manuals and phone company service manauls. Very rarely do they have any expertise in cryptology.

Malicious cryptanalysts tend to be in a different class. They are usually highly trained mathematicians, expert in the number theory needed to fully understand today's encryption algorithms. Anyone with such a deep understanding of mathematics and computer science normally recieves plenty of respect and prestige in their regular day-job. There is no need to seek out extra-curricular activities to build up one's ego and prove one's worth. The only plausible carrot I could think of that would entice a trained cryptanalyst to forge EFT's on the scale we were seeing was the promise of tremendous personal wealth. A pat on the back and a good story to tell at the bar simply does not measure up to the risk — no matter how lonely and unhappy a person might be.

Our hacker was after money. But how? He or she doesn't steal any!

I looked at the directed graph splayed out on Rudy's desk. What can someone gain from this? I racked my brain. Rudy Levinski's bank occasionally rejects EFT's simply to avoid being caught off-guard in managing their reserves. Could this attack have a similar motivation? Perhaps. The fact that some accounts were deprived of funds for a full day might be an indicator of tinkering with reserve requirements. Or obligations for interest.

Aha! That was it! I realized then that the hacker was probably helping himself or herself to overnight loans at zero interest. Not large loans, but lots of them. The total could be quite large even if the affect on individual accounts was small. Maybe stalling on payments was not the only way First Chicago Trust met reserve requirements. Perhaps when the bank needed lots of funds fast, a few illegal and surrepticious "loans" were taken out of other banks.

"Have you told us everything about meeting reserve requirements at First Chicago, Rudy?"

"Yes. Why do you ask?"

"Take a look at the graph. Not all of the bank accounts that the hacker uses to route money are balanced immediately. Many of the accounts remain below their proper levels for a full day. It appears that somebody or some institution is using these forgeries to obtain overnight loans without interest. If my hunch is right, we will find that the net affect of all of these forgeries is a large flow of money out of Bendix and into First Chicago."

"I do not fault you for being quick to accuse my employer of wrong-doing, but I will be very surprised if you are correct, Mr. Raymond. For starters, I will point out that our delay tactics interfered with the forgeries. Even you will agree Carl that it is far-fetched to suggest that we would deliberately interfere with our own scam. Furthermore, I do not believe that my superiors would treat Ms. Cryer as roughly as they have if they knew the source of the forgeries."

Suddenly I found his exceedingly polite manner grating. "Let's take a look anyway," I snarled, unconvinced by his argument.

We had only the confirmed forgeries to work with, and the banks were convinced that these represented only a small fraction of the full set of illegitamate EFT's. Nonetheless, I was hoping that they would serve as reasonable sample from which to determine if the net affect was a large shift of money out of Bendix bank accounts and into First Chicago accounts.

Trying to track the money along a chain of bad EFT's was next to impossible. Not only was the information we had very sketchy because the banks had not yet identified all of the forgeries, but the sheer number of EFT's made the problem insurmountable. The hacker was using multiple EFT's to deposit money into an account, and then using multiple EFT's, of very different denominations, to transfer the money out again. Sometimes the in-flow was equal to the out-flow, sometimes it wasn't. When the in-flow equaled the out-flow we figured the account was being used to launder money. When the in-flow was less than the out-flow then we figured we had an example of a "loan".

After an hour and several cans of iced-tea, I was forced to concede that there was no pattern in the bad transfers. The hacker was routing money

pell-mell between the two banks and even within the two banks. There were transfers between numerous accounts at First Chicago. There were transfers into First Chicago. There were transfers out of first Chicago. There were transfers everywhere.

The data did not support my theory. The delay scam and the forged EFT's were indeed seperate attacks perpetrated by seperate entities. There would be no easy answers.

My heart sank. It was hopeless. Even writing a program to trace the money would be futile. The bogus EFT's were buried in the regular EFT traffic. EFT's number in the hundreds of thousands every day. This may not seem like a lot, after all a modern computer is capable of millions of instructions per second. Yet, with so many accounts in so many banks with so much activity, even with the use of super-computers there is no hope of being able to trace the money to determine which account is the one the attacker is using to collect his interest. It was an NP problem and for an NP problem, an input of 100,000 is hardly small.

Computer scientists have a way of classifying difficult problems. By measuring the run-time of the fastest algorithm for a problem, we can characterize the difficulty of solving the problem. We measure run-time as a function of the size of the input. For example sorting a list of words into alphabetical order is considered to be an $n \cdot log(n)$ problem. This is because the world's best sorting programs require $n \cdot log(n)$ operations, where n is the number of words in the list and log is the base-2 logarithm function.

A complexity of $n \cdot log(n)$ means that if the program takes 30 seconds to sort 100 words, it will take about 7.5 minutes to sort 1000 words. The time we must wait for an answer grows with the size of the problem. The rate of growth is $n \cdot log(n)$. This is generally considered to be an acceptable rate of growth. There are many natural problems with much higher complexity functions. Many of these problems have exponential complexity. Path enumeration in a directed graph is but one example. There are many such problems. Some of them are well-studied problems with colorful names. The cute names often bely the abstract and complex mathematical nature of the problems. These are names like the Traveling Salesman Problem, the Chinese Postman for Mixed Graphs, the Rural Postman, the Crossword Puzzle Construction Problem, the Knapsack Problem, and, my personal favorite, the Left-Right Hackenbush for Redwood Furniture Problem. These, and many more, are all programming problems for which the best known algorithms have exponential complexity. If a problem with exponential complexity takes one second to process an input of length 20, then it takes 366 centuries to process an input that is only three times that size!

	10	20	30	40	50	60
n	0.00001	0.00002	0.00003	0.00004	0.00005	0.00006
n^2	0.0001	0.0004	0.0009	0.0016	0.0025	0.0036
n^3	0.001	0.008	0.027	0.064	0.125	0.216
n^5	0.1	3.2	24.3	1.7 min	5.2 min	13.0 min
2^n	0.001	1.0	17.9 min	12.7 day	35.7 yrs	366 cent

I groaned and slumped down in the chair. It was hopeless.

Lisa was smiling broadly and shaking her head in wonderment. "This is no ordinary hacker," she laughed. "This guy knows his computer science. Embedding the attack inside an NP problem... you have to admit, he's no slouch."

She was positively beeming. I didn't share her admiration. We needed to solve this NP problem... fast. Apparently she had forgotten that the three of us were prime suspects. With every additional day Lisa spent with Rudy and I, it would be easier for the FBI to build a case against the three of us, claiming that the three of us were in cahoots. I already had a track record for tinkering with things I shouldn't; Rudy had already been implicated in the delay scam; and Lisa was several thousand dollars wealthier due to one night's work.

Even if the FBI did not believe that we were guilty of running the attack, with such a bold assault on our nation's banking system they would need a scapegoat. Any one of the three of us would serve the purpose; together we made a perfect EFT counterfeiting ring.

"It is the perfect crime!" Lisa exclaimed. "And it is all made possible by the electronic banking system. Using a computer to automate the crime, the criminal can mount an attack of staggering complexity!"

She then proceeded to tick off the steps, one by one, on her fingers:

1. find a way to forge message authentication codes for banking;
2. write a computer program to generate fake payments;
3. generate hundreds of thousands of them;
4. make it so most of them are only decoys, but also make it so a few of them result in overnight loans;
5. launder the money by routing it through thousands of accounts;
6. use a computer and do this daily so that there is a continuous flow of dollars through your account;
7. collect the interest;
8. and, to cap it off, hide the whole thing in a huge graph, making the investigation of your crimes an NP-complete problem.

"And," she continued, "the real kicker is that the entire thing would never have been discovered at all if it had not been for the coincidence of two other seperate attacks: your replay experiments Carl; and your delay scam Rudy. The interference of the three seperate attacks is the only thing that brought the counterfiet EFT's to light. Now, even when we know the forgeries exist, there is no feasible way to determine who is behind them. Whoever it is can keep right on doing it; nobody can stop it."

Rudy sat down and rested his chin in his hand. He spoke quietly, musing to himself. "Our adversary simply channels money from all over the world into his account. He returns the money as quickly as he takes it. He is careful to borrow

only small amounts from any individual. Nobody notices the absence of a few dollars for one night. Those customers that do notice the unauthorized EFT's also notice that they balance. Most of the forged EFT's are assigned the code used for error corrections, so when cautious customers do call with a complaint, the problem is quickly diagnosed as an internal matter that has been corrected by the bank, with no apparant loss to the customer – the matter never gets beyond the help-desk.

"Our adversary is clever. By forging error-correcting EFT's, very little suspicion is arroused by customers or by bank personel fielding the occasional complaint. Furthermore, our adversary does not steal money outright; instead he or she makes money off the *flow* of money. What we are witnessing is a money mill."

"Yes," I said, "and the more money flows through the graph, the more interest is paid out. It really is an electronic money mill."

And so it was. Somebody was running a large money mill right in the midst of our nation's regular banking activity. Intermixed with legitimate transactions were counterfeits. These raced through the EFT network, collecting small amounts of money from accounts all over the world. Like a millrace, these transactions poured money down the chute and over the wheel. As the wheel turns interest is paid out. Once it passes over the wheel, the money flows back to the accounts from whence it came. The total volume of money in the system is preserved. And yet, at the same time, new money, in the form of interest, is generated and paid out to the person running the mill. That person would be the millwright.

Which account did the millwright use to collect his or her interest? There must be some part of the EFT graph where all paths lead through a small number of accounts. These accounts would be the millrace — the chute down which the money flows, leading it to the wheel.

We had found the money mill; now we needed to find the millrace. If we found the millrace then we would be able to find the millwright.

The three of us were amazed at the boldness of the crime. What sort of person has the audacity to take on the world-banking infra-structure? A very powerful or very desperate person, that's who. Either way, this was becoming very dangerous for amateur investigators such as ourselves. I turned to Lisa and Rudy and voiced my fears, but they would not hear of backing down.

"Hell, Carl. Now that we know we are going up against a first-rate hacker, I'll be damned if I'm going to stop now," Lisa exclaimed. The new found admiration she had for our adversary was still evident on her face. Rudy too was eager to enter the chase.

"Not only is my own professional reputation at stake, but I feel that our world economy has been put in a precarious position," he said. "I feel it is my moral obligation to correct the current situation and remove the vulnerability that makes it possible... whatever that vulnerability might be."

A little melodramatic for my taste, but that was Rudy. OK then, we were all in agreement to press on. The three of us set to work to determine how we might be able to find the man, woman, organization, or government that

might be running the digital money mill. With the help of Rudy, we identified several EFT and account parameters relevant to financial activity. We then set to work trying to characterize suspicious activity in terms of these parameters. Rudy was especially helpful. He dug up a program the bank already had for doing essentially the same thing. This application was different only in the sort of activity that was deemed suspicious, and consequently the choice of parameters. Still, there was some overlap and we were able to borrow heavily from the designs.

We decided early on that we would evaluate and filter each account on an individual basis. We would do no traffic analysis. We wanted to avoid any complexities due to expensive searches in the EFT graph. Instead, we needed an efficient program, even if that meant that it would be only an approximate solution.

Our plan was to collect lists of suspicious EFT's and search for two types of patterns. First, we hoped to be able to identify bank accounts with a large number of illegitimate EFT's over an extended period of time. These accounts were prime candidates for accounts owned by the people running the money mill. For the mill to work, there had to be some collection accounts where large volumes of money flowed continuously. This would allow the crooks to maintain high balances using other people's money. It would take a lot of pruning before the number of such accounts would be small enough to make manual review of each one practical. All evidence indicated that there was an appallingly large number of illegitimate EFT's, to say nothing of the fact that it is next to impossible to characterize bogus EFT's accurately. Nonetheless, we set out to design and implement a Balance Inspection Filter program — BIF for short — to do just this. The design made use of a rule-based architecture whereby we could easily modify the semantics to redefine a suspicious account. Lisa took the lead, explaining that she had developed several rule-based systems for the Macintosh in the course of her work at SoftTykes.

We had a backup plan as well; a second program, which would also be written by Lisa, would tackle the problem from an entirely different angle. Given a subgraph of the EFT graph, this program simply enumerated all paths that maintain a constant balance. This was the path enumeration program — the one with exponential complexity. We hoped that we could keep the size of the input small by only processing the output of the first program. We planned to pipe the output of BIF into this program and then analyze individual paths. In we found any cyclic paths that left the balances of all the accounts in the path unchanged, then either that path would be a decoy or else it would be part of the money mill and one of the accounts in the path would be an account that the millwright was using to collect interest on the flow.

Even better, if we found an acyclic path, then it seemed likely that we would have an example of an outright theft. Our theory was the the millwright probably used collection accounts with extremely high balances; otherwise the interest payments would not be large enough to warrant the risk of executing such an elaborate and bold scheme. Rudy, who was more knowledgeable in banking matters than Lisa and I, believed that the sum of the balances in all

the collection accounts, however many there might be, was probably in the neighborhood of $1 million. Since it was unlikely that a crook would have this sort of capital available for an initial investment, the millwright probably had to steal the money used to seed these accounts. An acyclic path, if we could find one, might be an example of a theft used to seed an account. With luck (lots of luck), we might find an acyclic path and then it would be relatively easy to trace the path to its final destination, which would be an account owned by the crooks. From there the FBI could use more traditional techniques to find the account holder and apprehend him or her. Of course we would haev to be careful to avoid mistaking part of a cyclic path as an acyclic path.

We recognized that the chances of finding an acyclic path were slim indeed. Due to the to the explosive number of paths in an EFT graph, which contains a tremendous number of arcs, stumbling upon such a path within our lifetime was unlikely. Still, as long as the machines were idle anyway, we figured we might as well put them to work (we were desperate).

It was Rudy that came up with the name of deep-throat for the program that enumerates EFT paths. He pointed out that the person code-named Deep-Throat that had helped Woodward and Bernstein expose Watergate had repeatedly told them to "follow the money." And that is precisely what this program does. With luck, we would be able to follow the money down the millrace and right into the millwright's bank account. Then we would turn the matter over to the FBI and let them arrest him or her. It would not be easy though. We already had ample evidence that the millwright was a clever computer scientist and expert cryptanalyst. He or she — it was at this point that I decided to myself that I would presume the millwright was a male; it makes it much easier to think and talk. *He* might have anticipated the investigative approaches we were taking. Clearly he had anticipated a deep-throat style program and had come up with the clever trick of hiding the entire crime within an NP problem. This demonstrated strong expertise in computer science as well as a mind that is capable of devious trickery. The attack itself – counterfeiting EFT messages that rely upon DES MAC's for authentication – requires highly unusual skill in cryptanalysis. There are very few known weaknesses in the DES algorithm. The few weaknesses that have been published are directly related to key-size and not to the DES algorithm itself. Triple-DES, which makes use of two 56-bit keys and three iterations of the regular DES algorithm, is very strong indeed. The world's best cryptanalysts have not been able to come close to cracking triple-DES, and it has been in wide-spread use for three decades. If the millwright is able to forge DES MAC's — and all evidence pointed in this direction — then he was one of the worlds top cryptanalysts. Our task would not be easy. To succeed the three of would need help from deep-throat, BIF, the FBI, and fate.

Chapter 11

"Do you know where I can find the ANSI standards documents?" I asked.

"Antsy?"

"ANSI," I repeated.

I was in the Chicago Public Library, talking to the librarian at the reference desk.

"And C?"

I spelled the acronym for the librarian and explained that it stood for American National Standards Institute.

The librarian said she had no idea where to look for such things, but said that I could try "LRE." It was my turn to be confused.

"LRE?" I asked. I am familiar with LUIS and a couple of other online catalogs but not LRE. "I don't know LRE. Where is it?" I asked.

She looked at me sideways and frowned disapprovingly. She hesitated slightly and then asked, "You've seen him then? He's probably in his office."

Huh? "I'm sorry. Uh... no, I haven't seen him. Umm, what did you say his name is?"

"Ellary," she said, and then she spelled it for me. I apologized again and explained my misunderstanding. She did not appear to be entirely convinced of my sincerity but smiled anyway before showing my to Ellary's office.

After I saw Ellary I began to understand why the librarian mistook my reference to Ellary as an "it" to be an insult rather than a misunderstanding. Ellary was about 6'5" tall, and probably the skinniest man I ever met. He wore dirty blue-jeans that would have been snug on anybody else but were baggy on his pencil-like appendages. He had stains from what appeared to be motor oil on the thighs of his pants. One kneecap was badly worn and the other had a hole. He wore a plaid flannel shirt, despite the hot July temperature. By far the most striking thing about him was his face and hair. His eyes were large and bug-eyed. They had a wild look to them, as if he'd been slamming down coffee for the better part of the day. His face was extremely pale. It was hard to decide if he looked like a ghost or more like a person who had just *seen* a ghost. His hair was dark brown and tied into a long pony-tail — most of it at least; there were several loose strands of hair that had not cooperated, and these hung over his forehead and cheeks. The librarian introduced me and left

us. I explained what it was I wanted, being careful to spell out ANSI this time.

He seemed to know what I was talking about and was muttering the words 'ANSI' and 'NIST' under his breadth as he walked out of the office with me in tow. He walked across the room to a tall narrow table that stood at the end of one of the book shelves. On it was a large over-sized book that must have been about a foot and half thick. It was some sort of reference or catalog. Ellary flipped through the pages, hovering over the volume and reading the words with his eyes only a few inches away from the pages. His hands were unusually large and his fingers unusually long. He used his right index finger as a guide as he scanned the pages, all the while muttering under his breadth. Suddenly he straightened up and looked at me (or did he look *through* me?) and asked, "ANSI is different from National Bureau of Standards, right?"

"Yeah. I think National Bureau of Standards is the old name for NIST," I offered.

"Hmmm, yes." He went back to thumbing through the book. I heard him muttering. "NIST... National Institute of Standards."

He paused and turned to me again. This time he didn't bother straightening up, but instead turned his head and looked up from his bent position over the book. "Some ANSI standards also have ISO numbers. I've got the ISO index here. Is that good enough?"

"I don't think so," I replied. I wasn't sure if X9.17 had an ISO equivalent or not.

"Got all of ISO," he muttered petulantly as he went back to work. "Got ISO on micro-fiche... Got ISO on CD-ROM... You want X9 you say?"

I nodded.

"Says here that X9 is also published by ABA, does that sound like what you want?"

"Yes, that's the one." ABA stood for the American Bankers Association.

Ellary announced that they had X9.3, X9.9, X9.17, X9.24, and X9.26, but that they were missing X9.2 and X9.32. He added that X3.92 was listed along with the X9 documents and asked if I wanted that one too. I answered that I would look at all the ones they had. He turned and headed back across the room, beckoning me to follow him. We went back into a private room with row upon row of shelves filled with brown cardboard magazine boxes. They appeared to contain unusual conference proceedings and standards documents. Ellary walked right into the middle of the shelves and had no trouble locating the box containing the X9 documents. He pulled the box off the shelf and put it in my arms. He hesitated before letting go of the box and explained that I couldn't take them out of the library. Again, he seemed to stare right through me as he spoke. He had an almost haunted look in his eyes. I had no intention of taking the documents with me (I'd brought more than one roll of quarters for the copy machine) but if I did have any inclination to take the documents, Ellary's haunted stare would have chased away any such thoughts. I thanked Ellary and carried the box to a reading table in the main room of the library.

I approached the nearest table, where a young Asian woman was already sitting on the far end of the table. It was a large enough table that I did not feel

I was imposing by using the other end, and set the box down with a thud. I felt as if I was unwrapping a Christmas present as I took out the documents one by one and set them on the table in front of me. The woman at the other end of the table did not look up from her work. She was taking notes on a yellow pad of paper as she slowly flipped the pages of a thick, brown, somewhat tattered, book.

I started with X3.92. It is the DES standard, entitled, *American National Standard for Information Systems – Data Encryption Algorithm.* I had come to the library in search of clues to the money mill forgeries. While it is true that the millwright may have discovered a flaw in DES, the far more likely explanation was a flaw in one of the EFT protocols. Cracking DES would be a serious breakthrough in cryptanaysis. DES has enjoyed great popularity over the last twenty years. It has been incorporated into numerous products and has been applied to a large number of wide-spread applications. Every cryptanalyst in the world has studied DES. It is hard to imagine a flaw that could have escaped all of this scrutiny. Protocols, on the other hand, are far less general. They are closely tied to the application and the trust model. For this reason, the set of cryptanalysts interested in any particular protocol is a much smaller group of people than those interested in DES. Protocols have a much narrower audiance than do cryptographic functions and algorithms.

I decided not to bother copying X3.92 and instead turned to the X9 documents. The X9 family of standards is used for all American banking applications. Because all banks in the country follow these standards for all inter-bank financial services, interoperability is ensured between cryptographic equipment and facilities.

X9.9 is entitled *Financial Institution Message Authentication (Wholesale).* It describes the algorithm used to compute the MAC's. It confirmed what I already knew: the MAC's are based on DES. I copied that one, using four of my quarters.

In among the X9 documents was a NIST document. Numbered FIPS-171, it was entitled *Key Management Using ANSI X9.17.* It was dated 1992. Apparently NIST recommended that ANSI X9.17 be used for all government applications. FIPS-171 listed various guidelines for how X9.17 should be used for government applications. I put this one aside to be photocopied later and looked through the other documents for X9.17.

Financial Institution Key Management (Wholesale) (aka X9.17), covers the distribution of cryptographic keys used to calculate EFT MAC's. It covers both the manual and automated management of keying material. It is designed to prevent unauthorized disclosure, modification, or substitution of keys. For those situations where loss of integrity is suspected, the standard includes provisions to regain security.

In the forward to the document it states that while the protocol specified in X9.17 is designed to protect the security and integrity of keys, it in no way guarantees that a particular implementation of the standard is secure.

I glanced up and met the eyes of the woman down the table. She smiled briefly before quickly tilting her head down and flipping a page of the book

before her. She had not been watching me; only staring pensively in my general direction. She reached down at her side and lifted a briefcase up onto the table. She wore a yellow pant-suit with a white blouse underneath. Her hair was shoulder length and permed.

I wondered when Lisa would be getting off work. She had hinted that her newest enhancements to the filtering program might put us over the threshold and begin to uncover some promising leads.

Many quarters later and after several trips to the copy machine, I was interrupted by a rumbling of my stomach reminding me that I had not eaten since breakfast. It was now 2:00. I began to collect my things and prepare to leave. The woman at the end of the table was packing her belongings as well. I followed her toward the check-out desk.

The librarian smiled as she took back the documents and said, "Thank you Sir. Will that be all?"

"Yes, thank you."

"Have a nice day."

I smiled and turned for the door. I briefly held the door for the lady with the briefcase. She nodded her head sweetly as she stepped through ahead of me into the glare of the early afternoon sun.

"Nice day," she said.

"Very," I replied.

And it was too. The late afternoon sun was bright and warm without being uncomfortably so. There was a strong breeze. As I headed down the street in the opposite direction as the woman from the library, a small piece of paper rode on the breeze before me. It hopped and skipped down the sidewalk. I watched the small impromptu kite flitter and flutter as I followed it. We were both headed toward the bus-stop, the kite and I. The wind was sufficient to carry the paper at the same pace as my own gait, although my rate of progress was much more steady than that of the paper, which danced in fits and spurts, until it eventually became entangled in a wrought-iron fence. Here it stayed, a loose corner continuing to flap the breeze.

I reached the bus-stop and did not have to wait long before catching the bus back to my apartment. Once there I saw the sorry contents of my refrigerator and decided to go out for food. I left the X9 documents on the table next to the Pentiums in the bedroom, lending even more height to a dangerously tall stack of papers there, and walked back out the door. I was on my way to the fast-food restaurant around the corner. I had not gone far when a dark green car sped past me and then suddenly swerved into a parking spot along the curb about four car-lengths in front of me. No sooner did the car come to a full stop than did all four doors open and four men in dark suits step out. They immediately turned back and walked in my direction, fanning out as they did so.

Uh oh.

I stopped walking. I looked behind me. There were four more men in suits and dark glasses approaching from that direction. There was no doubt in my mind what was happening, especially when I saw another two men crossing the

street in my direction. With the four from the car and the four behind me, that made ten all together. And nowhere to run.

The first set of four were upon me. The one closest to the curb grabbed my left arm just above the elbow. Another circled around behind me and put both of his hands on my shoulders. Still another was now saying, "Carl Raymond?" It was a statement not a question.

"We are with the FBI," he said, stating the obvious. One of the men that had approached from behind patted me from head to foot, searching for weapons. The other one was still speaking as he held a piece of paper up between us. "We have a warrant for your arrest. Please come with us."

Hands on my arms, shoulders, and now on my shirt front, assisted me as I was whisked into the green car. The engine was still running and one of the agents wasted no time in putting the car in gear and pulling away from the curb. There were four of us in the car; one of the four agents that had stepped out of the car must have found a different ride. As we pulled away from the curb and merged with traffic, the agent sitting in the back with me quickly recited my Miranda rights. After that nobody said anything; we rode in silence. The silence dragged on long enough that it became quite noticeable and awkward. I didn't know what to say so I stayed quiet. In fact, I hadn't spoken a single word yet. I decided this was prudent; let them explain the charges and their intentions first.

We pulled up in front of a glass office building, the kind with color-tinted mirrored glass. The glass on this building was tinted rust-brown. The driver turned onto a garage ramp leading under the building. He brought the car to a halt before we had gone very far into the garage, stopping directly in front of a large steel door. There were two other agents standing there waiting for us. One of the two reached out and opened my car-door. He grabbed my wrist and pulled me out of the car without saying anything. The other three occupants immediately got out of the car as well. Together, the six of us went through the steel door and down a long brightly lit corridor. There were very few door-ways along the hallway and it seemed longer than I would have expected from the exterior view of the building. Eventually we reached an elevator, which opened instantly upon being summoned. Only five of us entered the elevator, one of the agents remained behind in the hallway (whether he was one of the ones from the car-ride or one of the new ones, I do not know).

After exiting the elevator I was lead to a small room with only a small table and five straight-back wooden chairs for furniture. Perhaps the room was ten feet square; perhaps smaller. A single panel of fluorescent lights illuminated the room in stark, white light. I was told to sit in one of the chairs. As I did so, the tallest of the four agents dragged one of the chairs over to the wall, near the door. He turned the chair around so that it faced the wall and sat down facing me, leaning against the back of the chair with his arms folded across the top, his legs spread wide. He leaned forward slightly so the front legs of the chair lifted off the floor behind him. He still had not taken off his sunglasses. His short blonde hair and fair complexion stood out in sharp contrast to the dark glasses.

The other three agents pulled the remaining three chairs over to the the opposite side of the table from where I sat. For the next four hours the three agents at the table fired questions at me. I answered as best I could, not holding anything back. I had already decided during the car ride that I would cooperate fully and tell them everything I knew. I was in big trouble and now was not the time to play games. I kept reminding myself that I had not actually stolen any money, nor had I ever planned to do so. Meanwhile, there seemed to be no shortage of other people who had indeed stolen money. *Somebody* altered the amounts of Lisa's EFT's. *Somebody* was accountable for the delay scams practiced by banks world-wide. *Somebody* would have to take the fall for these crimes. In a situation such as this, my best bet seemed to be to help the FBI find some of the real criminals and thereby ingratiate myself to them and clear my own name. Otherwise, I feared, I might end up the scape-goat.

Most of the questions came from the biggest of the three agents. A burly black man with a shaved head, he wore a black suit and a white shirt, like the other three. Unlike the other three, his suit looked as if it would split at the seems, especially at his biceps. The bulging muscles in his upper arms ballooned against the fabric of his coat.

The questioning was somewhat hostile, but nobody threatened physical violence. They remained on their side of the table throughout. The blonde-haired agent with the sunglasses never did get out of his chair. Nor did he ask any questions. He simply sat, chewing gum with his chin resting on his arms, which were in turn resting on the chair-back, and he listened.

Did I have an account with First Chicago, they asked. No. Did I have an account with Bendix? No. What was my association with Jeff Newstrom? Never heard of him. Had I traveled outside the country in the last two years? Nope. Had I traveled outside Chicago in the last three months? Yes. Where?

The questions were delivered in rapid succession, one atop another. My answers were terse, but this did not bother them. Perhaps they preferred it that way. There were no breaks; whenever the large overpowering agent in the center seemed to run out of questions, one or the other of the two agents flanking him chimed in with questions of their own. They never skipped a beat; never gave me time to reflect. After a couple of questions from one of the flanking agents, the leader in the middle would resume the questioning, having recharged his batteries and replenished his arsenal. The questions were not all entirely new; they were occasionally repeated, worded slightly differently with each asking.

The agent sitting to the right, when he spoke at all, tended to ask the easy questions, sticking to simple facts about my background. He was a tall black man with short hair and a handsome face. He was not intimidating like the other agents. When was I born, he asked. Where? Where had I gone to school? When did I graduate?

When the questions eventually turned to the funds transfers between First Chicago and Bendix, my answers were no longer brief. I was careful to explain my involvement fully, making sure that there was no confusion over the limited nature of my role. I explained that I hadn't actually altered any messages. I

had not forged any message authentication codes.

Unfortunately, they did not draw the same distinction I did between replaying messages and inserting false messages. Both were interfering with electronic banking transmissions, a federal offense. Furthermore, they reminded me that I had a history of tinkering with banking protocols, including the early check bouncing incidents, and suggested that forged messages fit my pattern perfectly. I remained steadfast in my position: I did not deny that I had engaged in some illegal activity, but I had not stolen, nor did I ever intend to steal, any money from any individual or institution.

Thwapp!

I stiffened in my chair, startled. It was the agent sitting on the left that had slammed his palm onto the table and leaped from his chair. He was a young man with very short blonde hair, a square jaw, and a lightweight but athletic build. He walked across the room and stood facing the bare white wall with his back to me. Then, abruptly, he spun around and strode over to where I sat.

"Listen," he hissed, "all of you hackers are the same. You think that every computer is your playground, every phone message your toy. You think that every bank and company is your opponent in some high-tech game of wits. You all claim that you aren't criminals because there are no victims to your crimes.

"What about the hard-working employees at those companies? The ones who have to clean up after the mess you leave in your wake? Huh? They have to work overtime to reproduce the data you destroy.

"What about the talented programmers that can't produce challenging and innovative programs because no company will pay a salary for software that will be pirated, driving the market value down to zero."

"I'm not a hacker," I said sullenly.

"No?" he cried, his voice rising an octave. "What do you call yourself then? A security analyst?" he sneered. "Let me guess, you probably think you are doing the banks a big favor by pointing out weaknesses in the system. Well I got news for you buddy, if the banks wanted that service they would hire you. But you can't get a job can you? Huh?"

He turned away in disgust. "Geek," he muttered. Then, suddenly he was back upon me. "Who are you working for right now?"

This was getting personal and insulting. I remained silent. He was leaning over me now, his face only a few feet from mine. The veins at his temples bulging visibly, as were those running down the sides of his neck. His chin jutted outward. Every muscle in his svelte frame was taunt. He reached out and grabbed my wrist, pulling my arm so that I faced him squarely.

"The bureau has years of experience prosecuting organized crime for protection rackets. I can recognize a protection racket when I see one," he hissed.

"I'm not running a protection racket," I said quietly.

The agent stood up straight. He cracked the knuckles in his hands but said nothing immediately. Nobody moved; the room was silent. Then, quietly and levelly, he asked, "do you deny that you illegally falsified EFT messages on July 11th?"

"Yes."

"Yes?!" he shot back shrilly, having lost all of the self-control he had regained just moments before. "Earlier you confessed to recording and replaying EFT's. You labeled it as illegal activity yourself!"

"Right," I replied quietly, "I replayed EFT's; I didn't falsify them."

He looked at me. He looked at the other three agents. He threw up his hands in exasperation. He walked across the room and back. Then...

"On July 11th," he began calmly, "shortly after receiving a bunch of garbled messages, First Chicago received several clean EFT messages. Those messages were purported to be directly from Bendix. Instead you were the one that sent them to First Chicago. Correct?"

"Yes, thereby correcting the communication errors from the garbled transmission."

He ignored the last part of my response, cutting me off.

"What is your profession? You are a computer security expert. Correct?"

"Yes."

"You design systems to guard against hacking, correct? Things like false messages."

I could see where this was going. I didn't answer. He continued anyway.

"So, you falsify EFT messages and you also offer your services as an expert at protecting banks from false EFT messages. Here at the bureau we call that a protection racket. Other people call it blackmail. Call it what you will, it is illegal."

He turned on his heel, walked back to the table and collapsed into the chair he had vacated earlier.

"The pathetic part of all of this," he muttered, "is that, like every other hacker, you probably honestly believe that what you do is morally justified. It's not. It is against the law, and there are good reasons for having those laws. You, sir, are morally bankrupt."

The agent sitting to the right resumed the questioning at that point. This agent had done very little talking. This is not to say that he sat still like the blonde haired agent with the sunglasses sitting by the wall. No, the quiet agent sitting at the table spent most of the interrogation tapping his pencil on the table. His hands appeared soft but strong. Indeed, his entire physique was soft but strong. He was not burly like the agent in the center, nor did he have the wirey but hard and tough appearance of the other agents. He held his hyperactive pencil between long fingers. His nervous fidgeting was infectious, putting me on edge. Perhaps that was his intention. He was not intimidating like the other agents. He continued to stay with straight-forward questions about facts. What type of computer did I own, he wanted to know. What long-distance telephone carrier do I use, he asked, What Internet service provider do I use? What is my mother's maiden name?

It was impossible to tell where he was heading with his questions; I simply answered directly and honestly. As I answered these questions I thought about the charges made by the excitable agent on the left.

Was I committing a form of extortion? Even if that was not my intent, I would benefit by a heightened awareness of security concerns, would I not? And

by tinkering with EFT traffic I was bound to interfere in ways that would not go entirely unnoticed. So, indirectly I was drumming up business. And, there was no denying that my tinkering was illegal, even if it wasn't outright theft. Wire-tapping is against the law. My mind was too groggy to allow myself to start questioning my own motives. I did not trust myself to be able to parry the self-doubt that began to well up inside of me.

After four hours of answering questions with no breaks, not for water and not to visit the restroom, I was exhausted. It is good that I had decided early to tell the truth and hold nothing back; toward the end of the interrogation I had little memory of the questions that came earlier. It would have been easy to catch me in an inconsistency now.

Then, quite abruptly, the four men trooped out of the room, telling me to wait there. A moment later the silent agent with the blonde hair and sunglasses returned with a glass of water. He escorted me to the restroom. We then returned to the interrogation room and he left me there alone.

I was deflated. The experiments that I claimed where part of innocent research activity were undeniably illegal. Now I had to face the possibility that my experiments were morally wrong too because they artificially inflated the symptoms of computer crime. Maybe the FBI agent was right. Maybe I was a hacker. Had I slipped over the line between a security analyst working on behalf of security and a hacker contributing to the hostile environment of electronic data interchange?

Or do intentions count for something? Certainly it had never been my intention to create a security incident and then use that as a selling point to the banks. I continued to contemplate my role in the EFT incident as I sat there alone in that small bare room.

After a time the door opened. I was too exhausted and dejected to look up. I heard them walk in. I saw the multiple pairs of feet as they crossed the room in front of me. There were three pairs of black wing-tip shoes and one pair of white sandals and stockings. I looked up.

Lisa!

What was *she* doing here? I looked into her eyes, but she only met my gaze with a cold stare. I felt a chill. Did she turn me in?

"This is the man you know as Carl Raymond, correct Ms. Cryer?" the big man asked.

"Yes," she answered. Her voice was strong and assertive, her manner calm and confident.

"Carl has confessed to you that he tampered with EFT transmissions between First Chicago Trust and Bendix of St. Louis on July 11th, correct?"

"Yes," she answered once more.

Why was she doing this? Why turn me in? I hadn't done anything to lose her trust. She had been willing to give me a chance to repair the damage. What caused her to change her mind?

"You are certain this is the man?"

"Yes, I am certain," she replied levelly. Her manner reinforced her words.

"Thank you Ms. Cryer," said the big man. She turned on her heel abruptly and left without even a glance in my direction. I'm not sure what the remaining two agents said next. They were talking but I wasn't listening. Why did she do it? Why? She had been so cold. Was she an undercover agent? No, they had treated her as an outsider. An informant then? Damn her whatever she was!

Had she told them of her own involvement, I wondered bitterly. She had written most of the code for BIF and deep-throat. These were part of an unauthorized investigation. Both BIF and deep-throat processed data that neither Lisa nor I were authorized to see. First Chicago Trust did not know that Rudy Levinski had taken it upon himself to mount his own investigation. Lisa had shown no hesitation in helping Rudy in his effort. She had been so friendly the other day in Rudy's office. The three of us had worked well as a team. Why turn on me now? We were making progress!

I closed my eyes tight and leaned my head back in my arms. In the space of a few hours everything had come unraveled. Now, in all likelihood, I would be imprisoned and Rudy would fare no better. BIF and deep-throat would be confiscated. The FBI, with no understanding of sophisticated computer crimes and cryptology, would bumble the case. The millwright would succeed in pulling off the perfect crime. I would be made the scape-goat for the FBI while Rudy would be forced to take the fall for First Chicago Trust. It would have been better for both Rudy and me if Lisa Cryer had not become involved at all. Had she refused to speak to me on that first day when I buzzed her apartment, I would be no worse off — and most likely better off — than I was now. To turn me in at this point was a remarkable display of bad timing.

Chapter 12

As it turns out I wasn't thrown in prison. The FBI certainly had enough evidence against me to convict me of telephone fraud and tampering with money transfers, but they were more interesting in finding the man behind the money mill attack. Of the three crimes that were committed on July 11th, the money mill was by far the most serious.

The FBI released me late that same night. Instead of arresting me they struck a deal with me; I would be working with them now, however reluctantly. As the person closest to events on the 11th, I was in the best position to assist them. I would remain the prime suspect, but I was free to move about. I could not leave the country and I had to inform them of any travel outside of Chicago.

As I plodded through the door I could not help but think that it seemed an eternity since I had last walked out that same door on my way to dinner, having obtained what I hoped would be the key to unlocking the mystery of the money mill. I had been optimistic that the X9 documents would hold the information I needed to block the flow of money going through the mill.

Exhausted, I slumped in the chair by the TV; not the broken chair but the other one. As I sat there listening to the incessant sound of the leaky faucet in the kitchen, I recalled the conversation I had with Rudy the night before. I had stopped at his apartment on the way home. There was no need to be concerned about being followed now; I had already been arrested. I had nothing more to hide.

After I had told Rudy what happened, he explained that he too had been arrested. They held him overnight but eventually released him for lack of evidence. Apparently the FBI wasn't ready to start going after the "check is in the mail" variety of crimes.

Rudy explained that his interrogation had not been pleasant. "They did not break any laws," he said, "but they were still rather menacing: bright lights in my eyes; six hours of questioning with no interruption; verbal abuse..." He sighed deeply. "One of the agents — a large gentleman, must have weighed 250 pounds, all muscle — was quite overbearing and for a full hour shouted continuously. I think they were disappointed I do not have family here in the States; they insinuated that they would not hesitate to inconvenience my family. I honestly believe they were disappointed to learn that I have no strong

attachments."

I looked down at my sneakers and said nothing. I began to feel guilty for complaining about my own less extreme treatment.

Rudy continued. "My father grew up under the Nicolae Ceausescu regime in Romania. He used to tell me frightening stories. My brother was in Timisoara during the demonstrations. During the FBI questioning I actually experienced flashbacks to their accounts of Romania." He shuddered visibly as he said this. We did not talk long after that. Rudy let me sleep at his apartment that night. By the time I awoke the next morning, sore from sleeping on the floor, Rudy had already left for work. I scribbled a short note thanking him and left for my apartment.

Now, back in my apartment, I pulled myself out the chair and walked over to the Alpha to check my mail. I had two e-mail messages from Lisa. They said she wanted to get together and talk. This angered me. I didn't send a reply. I didn't have anything to say to her. I deleted the messages, took a quick shower, and left the apartment to go for a walk and blow off steam.

I couldn't decide if I was angrier with her or myself. I had misjudged her. I had been under the impression that there was a bond between us and that we understood each other.

Why would she turn me in? Yes, I was engaged in illegal activity, and yes, I had tampered with her financial transactions. But she was not adversely affected by this — other than the rough treatment by the bank executives, and she had forgiven me for that (supposedly). Suddenly I wondered what had transpired behind the closed doors of the meeting she had at First Chicago on the day I had my first glimpse of her. Or what about the interval between our meeting in her apartment lobby and our dinner conversation later that day? Had she called the police then? Had she been in contact with the FBI all this time? Had she been a spy? Working directly with Rudy and I as she had, she was in the perfect position to spy.

Surely Lisa realized that I was not an evil person out to do real harm. Surely. Surely? Was it possible that she actually suspected me of the other EFT crimes?

Again I found myself wondering if I had crossed the line and fallen into the sleazy side of computer security. I recalled the accusations of the wiry fair-haired FBI agent from the day before. Suddenly I felt more like a modern-day Al Cappone than a modern-day Ralph Nadar. Once I fancied myself as a consumer advocate, but perhaps I was only a menace to people that would use computers benevolently and courteously.

As if to dampen my mood still further, rain-drops began pelting down on me as I walked. They were fat heavy drops, the sort of rain-drops that are never followed by anything less than a torential downpour. I needed to find cover quickly if I was going to avoid getting drenched. I turned into the nearest store, which happened to be a liquor store. I hesitated. As depressed as I was feeling, a liquor store probably wasn't the best place to end up. I wondered if I could make a dash for the pool-hall down the street without getting too wet. I do not go to the hall often, but I have found that on occasion it can be a great place to forget about mundane troubles. For one thing, many of

the other people at Jake's Pool Hall have larger problems than I do. Also, it is precisely because I don't go there often that I have such a good time when I do go. The atmosphere is a nice change of pace from my usual academic, high-tech, puzzle palace, techno-geek environment. On more than one occasion that pool-hall has revived and refreshed my spirits. A long night of drinking cheap beer and breathing stale smoke-laden air, squinting down the length of a pool cue in dim light through tired and stinging eyes, as loud rock music blares out of over-strained speakers in the corner of the room, is a great way to lose oneself. The conversations I've had with the regulars — I'm convinced I've seen the same faces each time I've gone, despite the long intervals between visits — are refreshing too. When I'm feeling burned-out, challenging and thought-provoking debate is not what I'm after. And of course the fact that I shoot a mean game of pool also plays a part in my reasons for liking the place. I had met my first steady girlfriend in a pool-hall. It was freshman year of college at Berkeley in a pool-hall close to campus. She was a physics major. Gloria was her name. She frequented pool-halls mainly because she was an extremely good pool shooter. Her political views were further to the left than mine, which is unusual. Gloria and I had dated for a little over a year, and it was politics that eventually came between us. Too bad too, because I really liked her. I recalled her long wavy black hair. Her bangs used to hang down over her left eye. I wondered what Gloria would think of me now. Here I was, steeped in economic intrigue and high-stakes bank robberies. At least she could no longer complain that I lead a complacent and boring life. On the the other hand, she would be disgusted that I was now working for the FBI.

I sighed. The rain was already coming down harder and the thought of standing in the dank smokey pool-hall with wet clothes did not appeal to me. That diversion would have to wait. I entered the liquor store and wandered up and down the aisles staring absently at the rows of bottles. Should I get beer or wine? Whiskey?

Annoyed, I looked out the window. The rain was letting up. Apparently this was going to be a hard but short rain. Disgusted with myself for thinking about buying booze just to have something to do, and then even more disgusted with myself for not being able to decide what to buy, I turned for the exit and headed back home.

When and how had I let myself fall into the underside of computer security? My tampering on the 11th had been innocent enough, but it was also illegal. My intentions were harmless, but the result was not. Ultimately, my actions had lead to my arrest. I was now finding it difficult to justify those actions. Yet just a few weeks ago I had been comfortable with my own ethics... where had I gone astray? Had I lost perspective? What made me believe that the banking infrastructure was a game, with the innocent participants my pawns? The EFT protocols are not a puzzle to be solved. They are a critical component to a vital part of our economy. This is why tampering with EFT's is illegal. I recalled again the accusations made by the FBI. I had become a nuisance and a criminal. When had I crossed that line? How far had I slipped? I fretted over these questions as I trudged down the wet streets and skirted the water along

the curb.

I stared at the sidewalk beneath my feet. The rain had stopped entirely now. It had been a heavy rain and the gutters beside the sidewalk were still streaming. There were puddles littering the path and I was wearing only sneakers. My socks were soaked through despite my efforts to avoid the deeper puddles. I turned onto the front walk leading up to my apartment building. I dug into my pocket for the key to the door to the building, and as I looked up I nearly bumped into Lisa.

Startled, I nearly dropped my keys before regaining my composure and looking into her eyes with what I hoped was a cold glare. Her eyes met mine and she was not happy. For one thing she was completely drenched. Her face and hair didn't look any different from usual — her hair is too short to be affected by rain — but her clothes looked as if she had just stepped out of a swimming pool. She had the wrong clothes for it too. She was wearing long royal-blue pants that should have been loose but due to the rain were clamped to her thighs and shins, with thick wrinkles around her knees. The bottom of the left pant-leg was clinging to her calf about mid-way between her ankle and knee, leaving the bottom half of her leg exposed. She wasn't wearing stockings. On her feet she wore white sandals that were spattered with mud.

"I'm sorry," she said simply and softly.

Not good enough.

Dammit, I had trusted her. I had not needed to help her; I could have left her to fend for herself. Instead I had chosen to help. In return all I had asked is that she provide me with a little information and that she give me some time to sort things out before she went to the police. She re-neged and went to the police anyway.

"Yeah, well I'm sorry too," I said as I side-stepped around her and unlocked the door. I opened the door and closed it behind me in one motion, leaving her outside. As I walked down the hallway toward the stairs I felt a rage surging. Her betrayal was nearly tangible. The wave of anger traveled swiftly upward through my frame, beginning in the pit of my stomach and ending in my head, right behind the eyes. My vision was blurred and my forehead was burning. I could taste bile in my mouth. Not only had she betrayed our trust, but worse, she had caused me to question my own morals. That I found my morals lacking made me all the angrier. Perhaps it was unfair to blame her for the last part... but I did. I clenched both my fists and jammed them into my pockets. I hadn't stomped very far down the hallway before the air was filled with the din of the doorbell ringing continuously and furiously.

Ling-pong! Ling-pong! Ling-pong! ...

I whirled around and stamped back toward the front door, letting my temper fly. If she wanted to talk that badly, then I was going to give her an ear-full. Suddenly I had lots to say to her, and it would not be pretty. I threw the door open, nearly tearing it off the hinges. But I said nothing; Lisa was in tears. My anger ebbed as abruptly as it had risen. I stood there in silence for a time. She said nothing, but her shoulders fluttered gently as she stood shaking her head back and forth. She choked back more tears.

"C'mon in," I offered softly.

She said nothing as she crossed over the threshold and followed me down the hallway and up the staircase. The hallway echoed with our footsteps. I opened the door to my apartment, gestured toward the sofa, and went in search of a tissue. When I returned to the living room moments later with a box of kleenex, Lisa had already composed herself and had already gotten a tissue from her purse and was wiping her eyes. She accepted my kleenex anyway, thanking me.

"What was I supposed to do?" she asked beseechingly. "I don't want to go to jail. I explained to them that you were not the hacker they are after, that your hacking is harmless. But they would have none of it, Carl."

"When did this happen?" I asked.

"The day before yesterday. They know about BIF and deep-throat. They knew all about everything that had transpired in Rudy's office. They threatened to throw me in jail and basically gave me no choice but to cooperate.

"Carl, I was scared. You have to understand that."

I did. I had to concede that she had not done anything unreasonable or unfair. Nor particularly harmful. It sounded like the FBI already knew all about me and what I had done (I wondered if they had bugs in Rudy's office). Lisa only confirmed what they already knew. What she did not do, indeed could not do, was implicate me for anything more than harmless tinkering. Despite the fact that my tinkering was highly illegal, it would not be of great concern to the FBI. They had their hands full trying to find the real EFT criminals, the ones making money. By substantiating my story, and by doing it before I was arrested, Lisa had probably helped my cause considerably.

It was at this point that my manners finally caught up with events. Lisa's clothes were still soaking wet, even to the point of forming a large wet area on the carpet beneath her feet.

"I'm sorry, I should have offered sooner: is there anything I can do to help you dry off? Let me get you a towel."

I left her there as I went down the hallway to the linen closet. I dug down to the bottom of the stack of towels to get one of my rarely-used guest towels. Poor Lisa; she was soaked. I returned with the towel and she stood up to take it.

"Lisa, I was quick to jump to conclusions when I saw you in the FBI offices. I'm sorry. How long were you waiting outside the apartment before I got back."

"I don't know... a while I suppose. It didn't rain long, but it sure did come down hard. I had no umbrella and there was no place to take cover." She was patting herself with the towel as she spoke.

"I'm sorry," I said again.

Having rubbed her clothes with the towel, she now stood with her arms spread wide to show me the results. "Ta da," she said, "dry as can be."

We both burst out laughing as she slowly turned, with her arms still extended. Her clothes looked no dryer than when I had first walked up the path to the front door. True, they no longer dripped, but they still clung to her body and were badly wrinkled.

"I think I'll be needing about ten more towels, Carl."

"Maybe I can find some clothes you can borrow," I suggested. "We can put your clothes in the dryer."

"Thanks."

Not really sure what to offer her, I set out for the bedroom to look through my closet. As I rummaged through my clothes in search of something appropriate, I mused over Lisa's story. I had to admit to myself that I would have behaved the same way if the FBI had gotten to me first. It wasn't as if she and I had a long history. I had been very quick to suspect the worst when she walked into the interrogation room. We did not really know each other. Sometimes it was easy to forget that.

Hmmm. The pair of pants most likely to fit were a pair of old blue corduroy pants. They were badly worn; I had held on to them this long only because they were useful for painting and other messy work. I wasn't sure if they would fit Lisa — she has wide hips — but they were the best I could find. For a top I chose my biggest dress shirt. I was confident it would be long enough, and the tapered cut wouldn't be a problem for Lisa's narrow waist. The only question-mark was the chest. Would she be able to button the front around her breasts?

When I brought my choices back, Lisa looked them over with a critical eye. I pointed her toward the bathroom and she went to try them on. I went to the refrigerator and got two cans of iced-tea. I set the iced-tea down on the coffee table and sat down on the sofa. Oops... sat down where Lisa had been sitting. I got up and moved to the other end of the sofa where it was dry.

Shortly afterwards Lisa opened the bathroom door and stepped out. She was wearing only the white dress shirt and carrying my pants in one hand and her wet clothes in the other.

"The pants didn't fit," she informed me. "Where's the dryer?"

I tried to hide my surprise. Then I tried to hide my interest. I'm not sure I succeeded at either effort. The shirt came down low enough to cover her about as well as a short dress might. A very short dress. It covered her front and rear well. On the sides, where the bottom of the shirt arches upward, the upper part of her legs were exposed up to above her hip bones, like a French cut bathing suit. Her skin, smooth and dark, was beautiful. Her legs, sleek and firm, were more shapely than I had realized; the stretch pants she is fond of wearing do not do them justice. As I'd guessed, the shirt was straining to cover her chest, with the button directly between her breasts threatening to burst at any moment.

I collected myself and nonchalantly (I hoped) accepted my corduroy pants and showed her where to find the dryer. She tossed her wet clothes in the dryer and started it up. We both went back into the living room. I sat on the dry end of the sofa and, warning her that the sofa was damp, suggested she sit in the easy-chair on the other side of the coffee table. She did so, sitting down very gingerly and being careful not to show any more than necessary.

"So what did they do to you?" she asked.

I described the events at the FBI building. Lisa listened with few interruptions... until I described the mild-mannered agent that kept fidgeting with his

pencil.

"Oh, that would be Jonny Carter!" she announced excitedly. "He is their computer crime expert. Did he tell you that he solved the MetroSavings case? That was a $4 million case. Jonny is a nice guy; went to college at Georgia Tech. He majored in Political Science, but has slowly moved progressively deeper into computer crimes."

She acted as if the FBI guys were old friends, or co-workers. I had not found them to be so chummy.

"Jonny is taking the lead on this investigation," Lisa continued.

"Well, I guess that means I'll have a chance to get to know him better tomorrow then," I said. "I have to go back to get my assignment. The conclusion of yesterday's 'meeting' was that I would assist the FBI in their investigation. I am now a technical consultant to the FBI. They are going to pay me, but at the same time I remain a suspect. If we don't find the real bad guys then I will take the fall. They actually told me that... said that might give me the 'incentive' I needed to solve this case."

"When do you go?"

"Tomorrow."

"I'm going with you," she announced.

"Why?"

"Because you are their prime suspect and need help clearing yourself. You offered your help to me when I was in a similar situation."

"Yeah, and I was also the one responsible for your situation."

"As I am for yours now. I implicated you," she said. "Now when do they expect us?"

"They don't. They expect *me* tomorrow at 9:00."

"OK, I'll be ready."

She made it clear that there would be no further negotiation; she was going. I changed the subject.

"So you like Agent Carter?" I asked.

"Yeah," she said. Then she paused and then added, "He's married; has two kids.

"You will like him too, Carl," she informed me, "after you get a chance to know him better. He seems to know his stuff. Agent Brown, Jonny's boss, is nice too. A no-nonsense person. She also seems to know her stuff."

Lisa's clothes had long since finished drying by the time we finished our conversation, and she got dressed to go home. She did not apologize again before leaving. There was no need to. My anger had long since subsided and there was a new level of understanding between us. She had done what she had to do. We were still very much in this together. Lisa had implicated me under duress and with great reluctance. The end result had been harmless. I not only forgave her; I understood and sympathized with her.

Chapter 13

As it turned out, Lisa was right; I did like Agent Carter. The moment Lisa and I walked into his office I recognized him as the fidgety man who asked the easy questions at the table during my interrogation. He introduced himself to me with a broad smile and a firm handshake. He clapped his hand on my shoulder as he pumped my hand. Lisa was greeted in a similar manner. The unpleasantness of two days previous was furthest from his mind. He was determined to do all he could to drive those thoughts from my mind as well.

After pulling out two chairs in front of his desk and waiting for Lisa and I to be seated, Agent Carter circled around behind his desk. Without sitting down himself, he explained that he was taking the lead on this investigation and that I would be working with him. He went on to describe his background in detail.

Agent Jonny Carter joined the FBI straight out of college. He obtained his BS degree in Political Science from Georgetown University in Washington D.C. He grew up in Maryland, not far from Baltimore. He married young and he and his wife now have two children, both girls. He is now working in the division that handles computer crime, with an emphasis on banking. Agent Carter was quick to point out that there are other groups in the FBI that handle other aspects of computer crime such as mail fraud. His group concentrates on ATM crime, EFT crime, and other aspects of automated banking. This was already too wide a focus as far as he was concerned. Too many incidents and not enough investigators. Allowing some frustration to show, Jonny said that sometimes he feels that he alone is concerned with computer crime in the banking industry.

The number of actual computer crimes is far greater than police and FBI records show, explained Jonny, still standing behind his desk. He paced back and forth and fidgeted as he spoke. He explained that the number of reported cases is low partly because victems fear embarrassment in the press. For example, banks and other financial institutions are a favorite target for hackers. However, banks base their entire business on trust. Once customers begin to doubt the ability of a bank to protect their assets, the bank is in serious trouble. Every bank must factor the reduced customer base that results from embarrassing press coverage into any decisions concerning computer crimes. For example, suppose bank X fully expects to lose about \$1 million per year in computer theft. How much should that bank spend to correct the problem? There are

options available to the bank, such as installing firewalls and making wiser use of cryptography, but these cost money. On the face of it, it would seem that $5 million is quite reasonable; the bank can expect the solution to "pay for itself" within a few years. However, this fails to take into account the very real losses that result from admitting that there is a problem in the first place.

Fixing a problem requires first acknowledging that the problem exists. Acknowledging that a hacker problem exists results in a severe drop in public confidence. Once lost, public confidence is very hard to regain. It may take several years, even after the new remedies are in place. The loss is made all the worse if all other banks continue to deny the problem exists, thereby making the one honest bank appear to be sloppy and vulnerable when in fact exactly the opposite is true!

Lisa pointed out that the area that is most vulnereable is the Internet. Everybody is racing to move serious applications and businesses to the Internet and nobody is willing to wait for strong security to be incorporated into the Internet Protocol (IP). Instead, most proponents of Electronic Commerce prefer to downplay the risks and fool even themselves into complacency.

Agent Carter agreed. The Internet will never be free of hackers, he said. Even if stringent laws are passed protecting privacy and integrity on the net, without a technical solution that *prevents* such activity, we are reduced to relying upon deterants. And deterants alone are unlikely to solve the problem, no matter how harsh they may be. Students, being the free-spirits they are, young and anxious to learn through experimentation, will continue to tinker with the net in every manner they can.

I pointed out that it is hard to distinguish "innocent" probing from malicious hacks. For example, the traceroute command looks like a suspicious attempt to use source-routing for a man-in-the-middle attack. Often an apparent attack — one that sets off alarms in a firewall — is nothing more than an innocent mistake by a naive user who isn't familiar with the application he or she is trying to run (e.g. a first-time user of telnet). This is one of the greatest challenges in firewall design.

"That's right," Jonny agreed. "I don't know the technical details, but I can appreciate what you are saying Carl. This is what makes my job so tough."

Jonny explained that it is not at all unusual today for a systems administrator to correct a problem when an attack occurs but not bother investigating the actual crime. Very few people make even a feable effort to find the culprits. It is simply too costly. It took Clifford Stoll the better part of a year to track down the hacker he first detected on the machines at Lawrence Berkeley labs in 1988. Tsutomu Shimomura succeeded in tracking down Kevin Mitnick in only a couple of months, but he had the help of numerous people and he himself worked on the case full-time (and even over-time) during those months. Shimomura was relentless. A corporation, faced with the option of spending many person-months pursuing an intruder, with a very real possibility that the culprit will turn out to be a prankster trying to impress his cronies or girlfriend, is more than likely going to choose to repair the damage and get back to the business of making money. Even a very diligent company, one that opts to pursue an

intruder, is going to have difficulty enlisting the help of other companies and organizations. For example, if the intruder is traced back to a university, the systems administrators at that university are more than likely to be somewhat jaded; no doubt they recieve complaints about hacking on a regular basis.

Jonny tapped his pencil on his knee as he said this. He had a good point. I was in complete agreement. The benifits to tenaciously pursuing an intruder are even more questionable when one considers the possibility that the intruder may not be an American. Dealing with the miriad of foriegn laws, and lack of laws, can be more trouble than it is worth. When researchers at AT&T traced a hacker on their system back to a Dutch computer, they discovered that hacking was not a crime in the Netherlands. There was little AT&T and numerous other victems in the USA could do. It was not until after Dutch companies began to fall prey to hacking that the Netherlands officially recognized computer crimes. Buferd, as the AT&T hacker had been dubbed, was eventually arrested by police in the Netherlands.

Given this environment, it is far more prudent to concentrate on *prevention* rather than *detection*. Detection does little good if nobody is motivated to investigate. And, because nobody is motivated to investigate, it is foolish for a cautious company to rely upon the security practices of other organizations. Instead, a cautious company should take measures that can be taken unilaterally. Fortunately, there are substantial measures a single site can take on its own. A good firewall is a start... but only a start. For any sensitive data that leaves the site, cryptography can be used to protect the data from prying eyes and also to protect the data from tampering or mis-use. In this way, the cautious company can prevent trouble before it ever occurs. Both the high cost of investigations and the small reward for successful investigations become a moot point.

Jonny straightened abruptly as a heavy-set woman with wavy dark hair walked into the room. She had olive skin and a wide mouth. Her lipstick was dark red, her eyes brown and penetrating. She appeared to be in her forties.

"Is this him?" she asked Jonny curtly. He nodded.

"Hello Mr. Raymond," said the woman as she turned to face me. "My name is Agnes Brown. I am Agent Carter's immediate superior. In a few moments we will be joined by the chair of the American Bankers Association. We have a few questions to ask you. Our conversation will be recorded. I expect your full cooperation." She turned and walked behind Jonny's desk. She sat down in the seat that Jonny vacated when she entered the room.

I nodded my head once in reply and remained silent. This woman was all business. Had I not spoken to Jonny first, Agnes Brown would have reinforced my image of the FBI: cold, inpersonal, aloof, arrogant, and still enthralled with 1960's technology. My conversation with Jonny had gone a long way in dispelling that image. He was not at all what I would have expected from an FBI agent. Far from being a technically inept policeman with pretensions of being an expert on computer crime, he was both knowledgable and well aware of the limits of his knowledge. For the first time I appreciated the difficulty that he and his bretheren have when trying to enforce conventional laws in a new and rapidly changing environment. I understood and sympathized with

his frustration over the task of investigating crimes that nobody, not even the victems, are motivated to solve. Very few people fully grasp the seriousness of these crimes and fewer still have the energy to investigate them.

I had already decided that I would do all I could to help Jonny at the point when Agnes Brown strode into the room. After talking to Jonny, my motivation grew beyond self-preservation. No longer was I only concerned with staying out of jail and staying close to Lisa's pretty face. Now, for the first time I had more honorable motives. Somebody was stealing large amounts of money from a US bank and there was a good chance he would get away with it. The FBI was ill-equipped to handle the case, not because of any short-comings on their part, but because of a general lack of concern in society and because of a lack of earnest effort by the banks. I was now determined to do all I could to help Jonny solve this case.

A young blonde receptionist tapped gently on the open door. She had a pencil tucked in her hair behind her ear. Her winged bangs hung down to almost cover the glasses she was wearing. She looked at Agnes and said, "Mr. Templemeyer with the ABA is here."

"Fine Ms. Reynolds. Show him in," came the curt reply. Then, when a tall slender man with grey temples and short blond hair on his crown stepped in the room, Mrs. Brown stood up and walked around to the front of Jonny's desk.

"Hello Mr. Templemeyer. Nice to see you again," she said while extending her hand and shaking his. He wore a light grey suit. His tie was navy blue but appeared almost black in contrast to his white shirt. He appeared to be in his early sixties. There were crows-feet on the outsides of his eyes, which lent an amused twinkle to his features. He manner was amiable and unassuming.

After the introductions and brief pleasantries were over, Agnes explained that Mr. Templemeyer had requested the meeting so that he might learn first-hand all that I had uncovered. He wanted a full explanation of the money mill. I told him the story from the top, beginning with my initial observations on the 11th. I explained how, because First Chicago Trust sent error messages for all of the EFT's from Bendix of St. Louis on that day, that Bendix resent the EFT's the next day, on the 12th. This meant that First Chicago Trust got three copies of all of the EFT's: the legitimate copies which First Chicago rejected as part of their delaying tactics; my copies which followed close on the heels of the rejected copies; and the copies sent by Bendix the next day in response to the error messages from First Chicago.

"What did First Chicago do with all of these copies?" asked Mr Templemeyer.

"Because the versions I sent were the first ones to arrive after the supposed transmission error, they were the ones that were accepted by First Chicago Trust. My versions were the ones that actually caused money to change hands.

"The copies sent by Bendix the next day were replays of EFT's that had already been processed and, save for the two EFT's on Ms. Cryer's account, they were rejected."

Templemeyer furrowed his brow and looked at the ceiling for a moment. He lowered his head and nodded toward Lisa. "And we still don't know why those

two transfers on this young lady's account made it through twice?" he asked.

Lisa answered. "We know that somebody forged those EFT's; they did not originate from Bendix of St. Louis. And they certainly do not represent legitimate payments I made or recieved."

"Right," I added, "somebody has found a way to forge the message authentication codes used in funds transfers. We don't know how they are doing it. As unlikely as it seems, he or she may have found a way to crack DES. DES – the Digital Encryption Standard – is a widely used encryption algorithm. So long as adequate key sizes are used, it is believed to be very strong, with no known weaknesses to speak of."

"How vulnerable is the banking industry if DES has been cracked," asked Templemeyer.

"Very. It forms the basis of EFT security."

He took this news well. He nodded his head slowly and turned to Agnes. "Do you have any leads?"

"We have some. Our team has made progress since the last update I gave you, but it is not something I'm prepared to discuss at this time," she said as she glanced in the direction of Lisa and me.

There was an awkward silence that followed. Templemeyer eased the tension by asking for clarification on some points. "Why did the forgeries go through when the legitimate EFT's didn't?" he wanted to know.

"Well," Lisa began, "since those EFT's were forged and inserted into the message stream by the hacker, when Bendix got the error messages from First Chicago, those forged EFT's were not included in the batch of repeated transmissions. From the vantage point of workers at First Chicago, it appeared as if somebody had tried to duplicate all the EFT's except two. There was Carl's set of messages, which included all the EFT's including the forgeries, and there was Bendix re-transmission, which included only the legitimate EFT's that Bendix actually created. The duplicates were easily spotted and rejected, but the non-duplicated EFT's — the forgeries — were accepted. The fact that these two EFT's were the only ones that weren't duplicated focused attention on them. These are the two transfers that netted about $17,000 into my account. That focused attention on me."

Templemeyer nodded slowly. "OK, so the point here is that the forged EFT's were not treated in the same way as the legitimate ones when Bendix tried to correct for the errors reported by First Chicago. I can understand that."

"And," Lisa continued, "since the hacker thought that his EFT's had been been rejected by First Chicago, he did not bother following up with a second batch of EFT's to withdraw his money out of my account and move it on to another account. Normally he leaves the account balances unchanged and only passes money through accounts."

Now Templemeyer was confused again. "How does the hacker profit from this?"

"The hacker profits on the float," Lisa explained.

"What does that mean?" This time it was Agent Carter that was puzzled.

Lisa smiled. This is the question she was waiting for. "It means that the hacker is profiting from the *flow* of money. We are certain that somewhere in the tangle of bogus EFT's, there is a bank account owned by the hacker and that he is earning interest on continuous 24-hour loans. By routing large amounts money through his bank account, the hacker collects interest. By making sure that he returns the money quickly, and by borrowing only a small amount of money from any individual account, the hacker ensures that nobody misses their money. By using error-correcting EFT's, the hacker avoids leaving any evidence on customers' monthly statements."

Lisa looked around the room to make sure that her point had sunk in. It had. Jonny whistled softly. Templemeyer nodded slowly to himself. Agnes was not as impressed.

"Surely it is an easy matter to determine which bank account is the focal point for all of the bogus EFT's," she snappped. "We can put a stop to this soon enough."

"It isn't that easy," said Lisa. "The hacker is quite clever and has obscured his activities by generating thousands of decoys. It is hard enough to recognize a bogus EFT — because they are perfect forgeries — without the added complication of chasing down false leads caused by decoys. It simply takes too long to track down every bogus EFT and trace the flow of counterfeit money."

"That problem is easily solved," Agnes interrupted. "I can assign more people to the case."

Lisa shook her head. "There are too many. Tens of thousands of bogus EFT's daily, only a small fraction of which will lead to the hacker. Some of the EFT's are for only a few pennies. In many cases a single deposit is seperated into several withdrawals. For example a deposit of $500 might be balanced by five withdrawals of $100. Now tracing one route through the banking network becomes a matter of tracing five routes. A few more splits like that and very soon we find ourselves tracing hundreds of routes just to see what happens to the original $500. And it isn't like there is an obvious place to start looking. In that last example, the original $500 EFT is part of a larger loop. Keep in mind that very rarely is money stolen... only borrowed."

Jonny leaned back in his chair and twirled his pencil in his hand. He fumbled it. As he leaned forward to pick it up he cleared his throat to speak. He directed his comments toward me.

"Can't you write a program to track the money throught the system?"

"We have," Lisa said before I could respond. "But the shear number of paths the money takes is too much even for a computer to track. Path enumeration in a graph is an NP-complete problem."

She was met with blank stares. Struggling to find the right words, she pressed on. "We have written a program to trace the flow of illicit money through the system, just as you suggest, but it is unlikely that we will ever uncover anything. The millwright is smart enough to use lots of decoys. He must be using a computer himself to generate the decoys and to route them through the system so that they move money in long convoluted circles. The money is divided and re-combined in complex patterns. Our program might

never find the millrace no matter how long we let it run."

The amused twinkle returned to Templemeyer's eyes despite the gravity of the situation described by Lisa. "The millwright?" he asked. "Did you say millwright Ms. Cryer?"

Lisa smiled sheepishly and shrugged her shoulders. She glanced at me, embarrased. I straightened up and came to her support.

"It is the name we have given the hacker," I explained. "The flow of small amounts of counterfeit money throughout a complex network, with profits derived from the carefully engineered redirection of the flow, conjures up the image of a water mill. The bank accounts where interest payments are collected by the hacker would be analogous to the water wheel. A millwright is a person that runs a mill. A millrace is the chute that directs water over the wheel.

"We need to find the millrace. Find that, and we can find the water wheel — the bank account owned by the millwright."

"I see," Templemeyer said with with some amusement. "You people have been investigating this matter for some time I suppose. You seem to have a good understanding of the nature of the crimes. How do you propose we go about solving this case?" Then, with a light chuckle, he rephrased his question. "How do we find the millrace and thereby expose the millwright?"

"The program Lisa mentioned is a start," I said. "However, as Lisa said, it is a long-shot. An NP-complete problem is a computer problem for which there are no known efficient solutions. Tracing money throughout the EFT network happens to be an example of such a problem. If the money we are tracing is divided into several seperate transactions before it is moved to the next account, and then if each of those transactions is divided still further before being routed to the accounts after that, then the number of paths that we must trace increases dramatically in very short order. If the millwright divides transactions into ten parts each step of the way, then after tracking the money through four such divisions, we are up to ten thousand paths. It is even worse than that because the forgeries are indistinguishable from the real EFT traffic. It is like following a gallon of water as it flows down a river, where the river splits, joins other rivers, reunites, splits again, and so on. Like the gallon of water, bogus EFT's are indistinguishable from real EFT's. Like the gallon of water, the money of the original EFT is seperated, with a few pennies going here and few pennies going there."

"But then how can the hacker keep it all straight?" asked Agnes, letting her exasperation show as she threw her hands in the air.

"I don't know," I replied. "He must be using a computer to orchestrate the whole thing. The decoy paths are generated by a program. I am certain of it. It is easy to write a program to generate an NP problem — solving one is the tricky part."

Templemeyer's face turned pale. "Are you telling me that this is unstoppable? Is that what you two Computer Scientists are saying? Is there no way to track down the counterfiet money?"

"Not that I can see."

"I... I don't think anybody at the ABA anticipated an attack which uses

computers to such a degree. Hundreds, no thousands of forged transfers ocurring daily! Most of them mere decoys to obscure a small number of profitable counterfeits... and even those are laundered through many different accounts...

"How long has this been going on?" he asked imploringly.

"I don't know," I replied curtly. I feared that it had been going on for a long time. Why not? It was the perfect crime. We would still be ignorant of the entire matter if not for the triple coincidence of my replays, the delay scam, and the mill. It was the interference pattern of these three seperate attacks that lead to the detection of all three. Without the other two, any one of these attacks would have gone undetected. This is especially true for the money mill, for it was disguised in a truelly ingenious manner.

"For all we know the mill has been running for years," I said. This news brought out muttered curses from everybody in the room. Templemeyer was near panic. He turned to Agnes.

"What do we do?"

Agnes refused to be rattled. Her reply was calm and her thinking clear. "If Carl is right and this criminal activity has been taking place of a long time – maybe even years – then there is no immediate threat. We have survived thus far while the mill is in full swing; we can survive a while longer. If computer-aided investigation won't work then we must try more conventional forensics. This we are already doing. I will have Mr. Levinski brought in for questioning. Clearly he has a great deal of information to share with us. Carl, I want you and Lisa to sit down with Agent Carter and give him a full briefing. I was told that you have a second computer program that is also supposed to help with the investigation; be sure to give Agent Carter a full explanation of both programs. He is an expert in computers."

She leaned over her desk and looked around the room at her make-shift team. One FBI agent, one scared banker, and two computer geeks. If she was dissappointed with what she saw she did not let it show. Her clenched fists pressed against her desk-top as she used her straightened arms to support herself.

"I want to get to the bottom of this... now! Let's move quickly on this. Templemeyer, I'm going to take this matter up with Samuelson and I want you in attendance."

Templemeyer nodded and wet his lips. He still had not recovered from his shock over the gravity of the situation. Agnes slammed a fist on her desk. She turned to me as she continued to issue instructions.

"Carl, I want you and Lisa to get those programs running as soon as possible. Carter, make sure they have all the hardware they need. Also, talk to Agent Peterson and arrange for a trip to St. Louis."

The lathargic bohemith had been prodded out of apathy. The government had been awakened. The FBI was in full gear now. This would be one electronic banking crime that would not go unreported. The FBI would have their chance. This crime was too large for banks to ignore, too great for banks to bear the cost without working to prevent repeat episodes.

I was filled with renewed hope. No longer would I have to illegally eavesdrop

on conversations to collect information. No longer did I have to fear every pedestrian on the sidewalk and every slow moving car. Everything was in the open now. With our new alliance, the FBI, Lisa, and I would undoubtedly make substantial progress.

Chapter 14

"Ladies and gentleman, we will be delayed a bit longer. We expect to have clearance for take-off in about fifteen minutes. We apologize for the delay."

Agent Carter groaned and slouched deeper into the seat beside me. We were sitting on a 727 bound for St. Louis. The plane was still resting on the runway at O'Hare, in the same spot as it had been for the last twenty minutes. And now it sounded like it would be at least another fifteen minutes more.

Agent Carter loosened his tie and sighed loudly. He was wearing a black suit, white shirt, and a navy tie. He had not taken off his suit-coat when he sat down and he now looked quite uncomfortable.

I was wearing casual pants and a T-shirt. I had been tempted to put on my "munitions" T-shirt that morning, but had decided against it. No point in destroying my good relations with the FBI only days after it began.

My munitions T-shirt is a shirt that I own that has the full implementation of the RSA encryption algorithm printed on it. RSA is not a complex algorithm, and it can be implemented in only a four lines of (highly optimized and very unreadable) Perl. Since the US State Department has declared that any RSA program is to be classified as a munition and therefore can't be exported, my shirt is a munition. I bought the shirt from a fellow that printed a large number of them and sold them over the Web. The shirt was intended to be a barb directed more toward the State Department and NSA, rather than the FBI. Still, I don't think that Agent Carter would have found it as amusing as I did.

The plane did eventually take off, about a half hour after the captain had promised us that it would be only fifteen more minutes. The flight was extremely short. It was one of those flights where the plane never really has a chance to level off. No sooner did it fully ascend before it started descending. Agent Carter and I filled that short time with talk of the latest developments in the case. Apparently the FBI had confiscated several of the computers at First Chicago, particularly the desktop machines used in the security department. The hard-drives on those machines contained ample evidence of the delay scam. There were numerous memo's and e-mail messages that not only detailed specific instances of the scam, but also described the unofficial bank policies outlining circumstances under which the scam should be used and how it should be covered up if questioned.

He said that Lampley had made an effort to delete most of these files, but it is difficult to erase data from a hard-drive such that it can't be recovered by forensics experts. Jonny spent a good part of the trip bragging about how the FBI was able to recover the data despite Lampley's efforts to conceal the evidence. I had already heard stories (mainly from the net and other questionable sources) of forensics experts recovering data from disks even after the entire disk had been overwritten with random data. Supposedly, by physically examining the magnetic patterns *between* tracks on the disk, one can infer what has recently been stored *on* the tracks. I have also read the FIPS document, where it requires that RAM be zeroized by first powering down the machine, and then powering it back up and overwriting the RAM 1000 times with successive 1's and 0's. If proper clearing of RAM requires such elaborate precautions, it comes as no surprise to me that removing all physical evidence of information stored on hard-drives, without actually destroying the drive, is difficult.

When we landed in St. Louis, Jonny took care of the car rental. He got us a grey Taurus, with air-conditioning, thankfully. St. Louis is hot and extremely humid in July.

As it turns out, Bendix of St. Louis is not located in St. Louis. The Bendix headquarters is in Clayton, which is a suburb west of the city. The airport, which is northwest of the city, is directly north of Clayton, and I-170 runs between the two. It was a short drive down I-170 and we reached the bank by 10:30. The building itself was a typical bank headquarters, a glass tower of about thirty floors with a square footprint. Clayton contained many other buildings of a similar nature, at least a couple of which were undoubtedly competing banks. There was parking both under the building and another around in the back. Jonny chose to park in the lot in the back.

Inside, we were met with a strange scene. The bank was a bustle of activity, very little of which appeared to be related to finance. This would not have been a good time to go to Bendix of St. Louis for a loan.

The hallways were filled with people trotting in and out of offices. We passed one room where a women in a beige dress was standing in front of shredder feeding documents in at a steady pace. It looked as if she had been at it for quite some time, judging from the bored expression on her face.

Managers called out from behind their desks at passers-by in the hallway. I overheard shouted requests for "security audits" and "activity reports."

There were security guards posted at regular intervals down the hallway. I wondered how an uninformed guard could possibly recognize inappropriate behavior in the midst of such unusual activity as people bustled back and forth with stacks of papers in their arms.

We passed a short middle-aged man in a black suit crawling along the floor with a tape measure in his hand. He appeared to be measuring the length of the hallway, although I could not fathom his purpose. I glanced at Jonny, but he wasn't looking in my direction so I couldn't see his reaction. Instead he was looking further down the hallway, where a workman was standing atop a step-ladder and mounting a surveillance camera high on the wall.

Still more workmen had been putting in lights in the parking lot when we

parked the Taurus. They appeared to be new additions rather than replacements for old lights. Despite the mid-morning sun, the lights shone bright when they tested them as we stepped out of the Taurus. These were bright halogen lights, seemingly capable of lighting a small baseball stadium.

Before we reached the workman on the step-ladder, a voice called out to us through one of the open office doorways. A very young man hurried out into the hallway to greet us. He could not have been older than twenty-eight. His hair was black and longish for someone dressed as conservatively as he was. He wore a grey pinstripe three-piece suit with a white dress shirt underneath. The shirt had French cuffs and he wore silver cufflinks. His tie was red and conservative. On his feet he wore neatly polished black wing-tips. He introduced himself as Tony Miccuzzi, the man we had come to see. He was an information security officer at Bendix of St. Louis.

"Have you got the tape we requested?" Jonny asked after the introductions were over.

"Yup, it contains all of our interaction with First C over the last twenty business days," Tony said as he extended an 8mm tape cartridge out to Jonny.

Jonny immediately opened his briefcase, resting it on a lifted knee while balancing himself on the other foot. He took a manilla folder out of the briefcase at the same time that hie put the tape in. He opened the folder and laid a single piece of paper on the desk. On the page were neatly typed notes.

"We'll look over the contents of the tape back in Chicago; I dragged Carl down to St. Louis because I want him to see your EFT operations in action. He was the one that picked up on the delay scam at First Chicago and he may be able to assist us with the investigation. We are already familiar with the protocols; we want to review the policies and practices that are specific to Bendix. For starters, who knows the master key?"

"You really should talk to management about stuff like that," Tony said hesitantly. "I am too far down the ladder to know all of our policies."

"We will be talking to management too," Jonny assured him, "but my experience as an investigator has been that it is the people in the trenches that know how things really get done."

This appeared to please Tony who now said, "I can tell you right off that I don't know the master key. Nor do I have access to it."

For the remainder of the morning the young information security officer reviewed the Bendix security policy with us. He also gave us a tour of the EFT operations room and let us look in on some transfers. Jonny asked lots of questions and took lots of notes. I only watched and listened, choosing to interpret my role as an observer very literally. Jonny did not limit his questions to Tony, but also directed many questions to members of the EFT Operations group. On three seperate occasions Jonny spoke to employees individually, out of ear-shot of Tony and other Bendix employees. For the most part, Jonny's questions related to procedural aspects of EFT operations. All of the questions were posed in a non-threatening and friendly manner. Jonny played the part of an outsider interested in the logistics of wholesale banking.

After lunch Jonny and I met with several managers, each on an individual basis. To each manager Jonny posed the same two questions:

- How closely does Bendix adhere to the bank's security policy?
- What do you estimate the probability of failure to be?

These questions were familiar to me, as he had asked the same questions in one form or another of each of the employees we had interviewed in the morning.

All of the managers were in agreement in their responses. Every one stated that he was sure that policy was followed to the letter. Two of the managers gave long and condescending answers, explaining to us the importance of security to Bendix and the need to follow the official corporate security policy.

The estimates by the managers for the probability of failure ranged from 10^{-6} to 10^{-15}. The manager that claimed 10^{-15} explained his estimate by claiming that the only point of vulnerability in the entire system was DES and that the best cryptanalytic attacks he knew of for DES required on the order of 10^{15} operations. I bit my tongue and did not comment on his oversight of numerous other points of vulnerability, nor on his flawed reasoning.

On one occasion when a middle manager was especially vocal in asserting that he saw to it that procedures were followed rigidly, Jonny informed him of our morning interviews and, without naming names or giving too many details, explained that we had learned of four different security procedures that were ignored in his branch office alone.

"And this isn't an isolated example," Jonny added. He then explained how the probability of failure estimates provided by the operations personnel, the people in the trenches, was many orders of magnitude more pessimistic. I myself was shocked not only at the disparity between the views of management and the views of the lower-level employees, but also at the consistency with which the two groups adhered to their differences. I was reminded of the situation at NASA following the space shuttle explosion. Another example I had heard involved a government minister in Britain. This man was responsible for all of Britain's banking industry a short time ago. He was claiming an error rate of 1 in 1.5 million when most others quoted something closer to 1 in 20,000.

I did not say much in the interviews, not even when the one manager gave his estimates for vulnerability based entirely on the number of operations in a brute-force attack on DES. Instead I let Jonny do his job without interference. I was impressed with the efficiency with which he was able to pull information out of people. He had certain questions which he asked every person we interviewed. He did not follow a script and the prepared questions came out at different points in the different interviews, seemingly fresh and spontaneous each time. He never let the conversation wander, remaining in control at all times. It was a long process — we spoke to fourteen people that day — but Jonny knew how to obtain the maximum (useful) information in the minimum time.

Despite the fact that both Jonny and I were exhausted after a full day of interviews, we went back to Tony's office to do more investigative work. We found Tony hunched over his keyboard. Jonny explained that he and I were

booked on a flight for the following morning. Since this meant that we had the rest of the day and the evening free, he suggested that he, Tony, and I pool our wits and see if we could figure out how the money mill forgeries were being made. Tony enthusiastically agreed and we set to work.

Using the whiteboard on the wall of his office, Tony walked us through a full EFT session between Bendix and First Chicago. Each step of the way, both Jonny and I interrupted with many questions as we tried to find weak points in the protocol and in the business policies of both banks. Things got a little complicated when we reached the point where the Chicago bank executed the delay scam, as this muddied the picture. I suggested that we leave out that aspect of the scenario, since it was unrelated to the money mill attack, but Jonny was reluctant to change any aspect of the timeline of July 11th.

Several hours later we reached the end of the timeline with no new insights into the forgeries. The end of the work-day had long since passed and everybody else had left. The halls outside Tony's office were now quiet. The silence was eery, especially in comparison to the earlier chaos.

"Yeah," Tony replied when I commented on the sudden solitude. "This place has been like a zoo the last couple of days. Did you notice the new lights and cameras in the parking lot?"

Tony loosened his tie, a red one with a brown paisley print. He left it around his neck but loose enough that he was able to unbutton his collar button as well. He then excused himself to go to the restroom.

Now that we were alone I asked Jonny why he kept asking the managers about policy and the probability of failure. It was a question that I'd been waiting to ask for some time. After all, we were not business consultants; what did the FBI care if Bendix managers were out of touch with the reality of the technical situation? Why harp on it?

"Because," Jonny explained, "any time upper management denies there is lax security, and refuses to look into breaches when they occur, the door is left wide open for an inside attack. Do not think for a moment that the employees are unaware of management's attitude."

I whistled softly between my teeth. It made sense. If employees know that managers turn a blind eye to security incidents, then there is no deterant. By covering up problems, the banks make themselves all the more vulnerable.

Banking relies upon trust; it is the very essence of the business. A bank fails when consumers lose faith in the bank's ability to safeguard money. When there is a security breach at a bank, it would seem quite rational for the bank to gloss over the problem. Even if a bank must sustain the financial losses associated with a successful hack, that may well be preferable to letting the inability of the bank to protect itself and its customers become public knowledge. This is the point that Jonny had made upon our first meeting, in Agnes' office.

"I was trying to establish that the Bendix employees had the opportunity to commit inside attacks on the EFT system," Jonny finished.

I would say he succeeded! The environment at Bendix was ripe for fraud.

"We see this all the time with ATM fraud," Jonny said conversationally. "It isn't at all uncommon for security personnel at banks to be quietly fired

for disciplinary reasons. On the other hand, it *is* uncommon to hear a public admission by a bank that recent ATM fraud was traced back to the bank's own security department. The numbers don't add up; people are being fired for theft but nobody is reporting the thefts.

"Not only do the security personnel know better than anybody where the flaws are, but they know better than anybody just how strong the impulse is to deny that a problem exists. I learned during my case-work on ATM fraud that bank managers like to fool themselves into thinking that each and every case of ATM fraud is an isolated incident, a fluke, that can't possibly be repeated and therefore requires no corrective action. You saw that for yourself this morning."

Tony still had not returned. I took advantage of Jonny's talkative mood and asked why the current case was different. Why was this case getting so much attention, both from the FBI and from the banks? Neither Bendix nor First Chicago appeared to be sweeping it under the rug. At Bendix the signs of upheaval were obvious.

He reminded me that the Bendix reaction was very ambiguous. On the one hand the offices were a site of mass hysteria and over-reaction. On the other hand, the bank managers attributed the problem to a fluke occurence that was unlikely to be repeated. They claimed that Bendix security was exemplary.

Jonny answered my question by noting that there were several reasons why this case was different. He tapped his pencil on his fingers as he ticked them off.

- The bogus EFT's were perfect forgeries, meaning that whoever was responsible was capable of doing substantial damage. The gravity of the situation had the banks in a panic.

- The FBI was making a concerted effort of late to turn up pressure on the banks.

He started to give another reason but then stopped abruptly. Whatever that last reason was, he thought better of telling me. Instead he changed the subject slightly and said, "if you want an example of the sort of tolerance I'm talking about, just consider the delay scam you discovered. Do you think for a moment that anybody would have paid much attention to that if it weren't for the high level of overall panic right now?

"Hell," he said as tossed his pencil on the desk and leaned back in the chair. "Even I would have shrugged it off as another example of tricks of the trade and let the banks deal with it themselves.

"Or take the Argenina heist as another example — twelve million dollars stolen by a couple of hackers, and scarcely a murmer in the press. If it had been an armed robbery it would have been all over the news."

Tony returned and we changed the subject back to the EFT forgeries. We all agreed that the money mill was probably being run by an individual or a small group of people. Unlike the delay scam, the money mill did not appear to be a case of institutional fraud. MAC's are not like digital signatures; they do not provide strong non-repudiation with a third-party. Both the sender

and the recipient of an authenticated message know the authentication key. The recipient cannot prove to a third party (e.g. a judge or arbitrator) that the message originated from the sender because the recipient can attach valid MAC's to messages just as easily as the sender can (since both know the key). Therefore, an insider at First Chicago, the recieving bank, would understand that creating messages that purportedly came from Bendix would not absolve First Chicago from suspicion. And certainly an insider with access to the key at Bendix would not be so foolish as to think that he or she would be overlooked in an investigation. The FBI was targeting each and every employee that might conceivably know EFT keys at either bank.

During the course of this conversation I learned that the FBI was using a very broad definition for "employee that might conceivably know". Apparently the FBI was investigating each and every employee at both banks, although the focus of the investigation was in the information security and EFT departments. Shortly after saying this Jonny excused himself to call his wife and say goodnight to his children. Tony took his tie all the way off and tossed it on the desk. He was wearing only a black pair of socks on his feet, having taken off his shoes at some point. His shoes were sitting under the desk, beside the waste basket.

"It's been rough," he groaned. He slumped down in his chair and let his arms drop straight down to either side of his slight frame. Tony wasn't bulky enough to fill out his suit even under the best of circumstances. Now, having missed dinner and working late into the night, his suit was wrinkled and disheveled. He stretched his legs out and rested one foot on the waste basket. Leaning back in his chair he stared at the ceiling.

"They gave me a hard time too," I said. "Of course in my case they had good reason to, seeing as how I was a prime suspect at the time. I don't feel justified in getting indignant about it."

"Well, the same goes for me too," he conceded. "I was warned when I was hired that if anything went wrong the entire security department would be put under the microscope. Its crazy. Nobody in the security department would be foolish enough to run the mill. I never thought there would be an incident on the scale of this one." He grimaced, seemingly in pain. All of us were exhausted.

"I'll admit we have occasional minor incidents," Tony said with a shrug. "Happens all the time actually. But do you realize how big this one could be?" he asked. He shuddered visibly as he said this. He slumped down further in the chair (I would not have thought it possible) and put his hands over his face for a moment. His long wavy black hair was unkempt. Fatigue had set in for both of us. I massaged my eyes; I would have preferred to splash some cold water over my face. What I needed was a sink. Or a bed.

"I'm scared Carl. Really scared. The forgeries we are seeing are perfect forgeries. Somebody has cracked DES or has broken into a key center — take your pick. Either way we got trouble.

"The worst part about it is that it does not look like this case is going to be solved. The FBI is in over their heads. Jonny doesn't know what to try next and he is the best they've got. Even worse, why is it that —"

Tony stopped abruptly and a moment later I saw why. Jonny stepped up

behind me. "Max gave me one of his 7-Up's," he said. "Either of you want some? He didn't have anything with caffeine," he sighed. Then, seeing the uncomprehending look on our faces, he added, "Max is the guard down the hall. Nice guy."

"Thanks," I said as I held out a hand for the low-octane soda. I took a swig and passed the can to Tony. "I don't think we're going to get any further tonight. We'd better call it a night and head home," I suggested.

"You mean call it another day," Tony said. "It's 4:30 already. In fact we'd better get out of here before people show up for work. We don't meet the dress code anymore. Wrinkles aren't considered a valid substitute for pin-stripes," he smirked. Not the best of jokes, but it was 4:30 and we were all way behind on sleep so I let it go and returned the smirk with one of my own.

The three of us made a feeble attempt to neaten up the papers strewn about the room, and tossed out the styrofoam cups. It took Tony a bit longer, mainly because it was his office and most of the papers were his, but also because he seemed to have "made himself at home" more than Jonny and me. Jonny and I were waiting in the hallway when Tony finally left the room and shut off the light behind him. He had his neck-tie in one hand and his suit-coat in the other.

The emergency lighting illuminated the hallway with an eery glow as the three of us walked down the hall. Twenty hours and little progress to show for it, I thought. We were all feeling dejected. Tomorrow – no, today – Jonny and I would be heading back to Chicago. Lisa wouldn't be pleased; she had pinned high hopes on this trip. She wasn't the only one.

I glanced to my left at the two men walking beside me down the hall. I didn't envy Jonny. I only had to deal with Lisa; he had to answer to Agnes. And Tony was still in hot water and now seemed likely to remain so for quite a long time. There were no leads left to explore at this point; we had run out of ideas.

We reached the end of the hall and turned left and then left again. We came up to the locked door with the guard station immediately inside.

"Hey Max," Jonny greeted the guard. "Thanks again for the pop, man. We're headin' out."

"Nice meetin' ya Jonny," replied the guard as he slid the log book across the desk in our direction. Jonny wrote in the time (4:51 now), our names, and our purpose. The three of us then signed it and, with a final nod to Max, walked out the door and into the elevators. Nothing was said as we waited for the elevator and descended to the lobby. The three of us walked out to the cars together.

"Sure is nice that they puts these lights up," Tony remarked with a smirk. "Now I can find my car more easily. I can even find the keyhole for the door-lock. My car doesn't have a remote-control door-lock." We were all tired, but Tony most of all. He laughed a little too hysterically at his own (poor) joke as he said goodbye and collapsed into his dirty rusty clunker.

Too exhausted to bother with elaborate goodbye's Jonny and I waved our hands, said we would see Tony the next time we were in town, and climbed into the Taurus. I immediately reclined the seat-back as far as it would go. I stretched and let out a long sigh. It is amazing how comfortable a car-seat can

be when compared to cheap office furniture and when the evaluation is made after considerable sleep deprivation. I didn't even mind the clammy feeling from my clothes as the sweat that had soaked into them over the hours cooled down from the air-conditioning in the car. Jonny didn't look or smell like he was any fresher. I wondered if somebody would have to sit next to me on the airplane. I hoped not. I wondered if I would have to sit next to Jonny on the airplane. I hoped not. I slipped into sleep.

Chapter 15

There were the usual and customary delays at the airport and it was not until early afternoon that I arrived back in Chicago. It was a dreary day, with a light drizzle falling during the entire cab-ride back from the airport. The humidity was oppressive. I flicked on the light switch as I stepped through the door and into my apartment. No sooner did the light come on than a sharp pain sliced through the back of my neck. The last thought that went through my head as the floor tiles rushed up to greet me was that they were very much in need of mopping.

I was unconcious before I hit the floor.

I don't know how long it was before I awoke. At first I was not sure if I was really awake or not. I willed my eye-lids open, but everything remained black. Slowly I became aware that I was indeed conscious but that the room was dark. Very dark. It is late at night, I realized. I must have been out for a long time.

A small orange bead danced in the dark before me. It had an eery glow that brightened and faded, and then brightened again as I watched. Even at its brightest it was too dim to illuminate anything. With my eyes straining to penetrate the blackness and my brain struggling to sweep away the fog in my mind, I watched the dancing orange bead. I became aware of the smell of tobacco smoke.

Of course. The orange glow was that of a burning cigarette. It was too dark to see who held it. I squinted my eyes. That made my head hurt so I stopped. The smoker must have realized that I had awakened, for he now spoke.

"I am sorry I had to hit you Mr. Raymond," came the easily recognized European accent and exceedingly polite manner.

"Why did you have to knock me out, Rudy?" I asked beseechingly. What reason could there possibly be for attacking me in my own apartment?

"I was not certain it was you," he explained. "I was afraid you might have been the FBI and I do not wish to speak to the FBI at this time. Indeed, I do not want the FBI to know where I am."

Suddenly I realized that even *I* did not know where we were. Even in the dark I could tell we were not in my apartment. For one thing, the easy-chair in which I sat was far too firm and new.

"Where are we?" I asked with sudden alarm.

"Someplace where the FBI cannot listen to our conversations," he replied. The glowing embers of the cigarette continued to bob up and down. "This is another reason why I knocked you unconcious; I did not want you blurting out my name in your apartment. I suspect that the FBI has your apartment bugged."

Now I was annoyed. What was he talking about? Why all the silly theatrics. Why knock me out? Rudy Levinski had become even more paranoid and cynical than me. Did he really think that my apartment was bugged? Did he really have reason to fear the FBI to such an extent? The First Chicago delaying scam was minor compared to the mill; surely he did not think that the FBI would move aggressively against Lampley. Even if the FBI did so, perhaps out of frustration over their failure to make headway on the larger case, it would be Lampley, and not Rudy, who would pay the price.

When I voiced these thoughts to Rudy his reply was quiet and level. "They already have a warrant for my arrest Carl. They came to my apartment two days ago. I was not home at the time, but when I returned some time later I found my front door off the hinges and my personal belongings ransacked. A neighbor informed me that there were six men that entered my apartment and that they were there for about two hours."

"Are you sure they were FBI?"

"One can never by sure, I suppose. Regardless, I do not wish to be found right now."

The orange glow of the cigarette darted downward and then disappeared. He had rubbed it out in an ashtray by his side. With a sigh he rose from the chair in which he had been sitting. His large black shadow moved across the room. He opened the blinds on the window, allowing the moonlight to stream in. He stood and stared out of the window in silence for a moment. There was no moon, but even so I was almost sure I could see a faint reflection from his glistening forehead. He turned and leaned against the window-sill so he could face me.

"I have learned from other sources that Lampley is in custody," came the quiet and calm voice. "This same source tells me that you seem to be in good standing with the FBI Carl."

Rudy made it sound as if he was accusing me of unethical behavior. "It was either that or face arrest myself," I offered. "You know the story, I stopped at your apartment the same day I was released by the FBI," I reminded him.

"You did not tell me you cut a deal with them," came the petulent reply.

"So what if I did? I didn't implicate you in any way. We all want to see this entire matter cleared up. Helping the FBI find the real millwright will clear us all: you, me, Lisa, Lampley, everybody."

"Why has the FBI arrested Lampley? Why do they have a warrant out for my arrest?"

I didn't know. This was news to me. Nothing that had been said in the FBI meetings I had attended indicated that Rudy or Lampley were targets of the investigation. I had spent the last 24 hours with the agent spear-heading the

investigation and, while the topic of Rudy Levinski had never come up, I could not think of anything he had said or done that would indicate that he was aware that Rudy's apartment was being raided while I helped the FBI interview bank employees at Bendix. Then I remembered the manner in which the FBI had played Lisa against me. They were nice enough once one got to know them, but they could be ruthless. I would have to keep that in mind. Rudy was right; I had become quite chummy with FBI. Now I resolved not to allow myself to be lulled into complacency.

"What do you want me to do Rudy? I can put in a good word for you if you like, but I hardly think it will help. The FBI isn't *that* friendly with me. They are not going to call off an arrest order just because I ask them to."

Rudy lit another cigarette before answering. He turned and sat down hard in his chair. He sucked in a breath and blew the smoke out slowly and pensively.

"I have some source code," he said. "I want you to incorporate it into BIF. As you yourself said moments ago Carl, all of us will benefit from a successful outcome to the FBI's investigation. Like you, I want to help the FBI solve this case. Unlike you, I have not been invited to do so. Therefore, I will help from a distance, operating through you."

It was not a suggestion; it was an anouncement of a decision that had already been made. I was not at all sure I liked the idea. My newfound friendship with the FBI would not last long if I began harboring suspects and allowing those same suspects to make anonymous changes to source-code under the FBI's control. What would happen to me if I inadvertantly introduced a virus into FBI computers? OK, so Rudy was not the type of person to unleash a virus... or was he? The day before I would have thought it preposterous that this bulky wimpy European that sat across from me would hide in the shadows of my apartment and strike me from behind. Did I know him as well as I thought? He had been the point-man on the First Chicago EFT-delaying scam. In our first meeting, on the lake-front, he had conceled the truth... as had I of course.

He interrupted my thoughts. "You are wondering if you can trust me." His tone was not hostile. There was no hint of accusation or indignation. "You have no choice Carl," he continued softly. "We need to help each other, remember? The situation has not changed as much as you may think. Both you and I have contributed to this problem. You can claim that your intentions were honorable — and I will agree — but the fact remains that you are guilty of tampering with financial banking transactions. Perhaps the FBI has chosen not to press charges at this time... but that is a decision that can be reversed very quickly should you fall out of favor."

He sighed softly. "As for me, I seem to have fallen out of favor already, but you are in a position to further our cause. I have written several new routines for BIF. I believe they will allow us to specify profiling rules that take into account international transfers. I think we should broaden our investigation.

His paused to take a hankerchief out of his pocket and wipe his forehead. He removed his glasses and sighed gently. Speaking softly while wiping the lenses of his glasses, he said, "you can check the source-code before you install it, Carl. Don't install the changes if you feel they will cause trouble. Or take credit for

them yourself if you wish. Just install them."

With some effort Rudy pulled himself out the chair and walked across the room. He gently tossed a floppy disk into my lap. I stared at it. Could I trust him? What harm could it do to accept his changes. It seemed too far-fetched even to me to think that he might try to introduce a virus. No, he probably was being honest; he needs to clear his name and the best way to do that is to help further the investigation. I picked the disk up and absently fanned my face with it. The air was muggy. It was obvious that the air-conditioner was not on. I realized that the electricity might not be connected in the apartment. Who's apartment was this anyway? It was furnished yet vacant... odd.

Rudy interrupted my thoughts. "You will find that my changes allow for conditions on the country attribute. In particular, with these changes we can easily distinguish between domestic traffic and traffic that crosses national borders.

Rudy's mouth twitched with a slight smirk as he headed for the door.

"Goodnight Mr. Raymond. You will find that you are in the apartment across the hall from your own. Again, Goodnight."

And then he was gone.

I sat in the dark and reflected on the strange meeting that had just transpired. Rudy Levinski was trapped on the outside. He had not been able to earn the trust and cooperation of the FBI as I had. Like me, he was a prime suspect, but for some reason the FBI seemed unwilling to open a dialogue with him and make a deal. Or, perhaps Rudy had not been careless enough to give them a chance. I recalled my own arrest. I would not describe the initial behavior of the FBI agents as cooperative. Still, that was behind me now, yet for some reason the FBI was not as quick to cooperate with Rudy. Did they know something about Rudy Levinski that I did not know? Something that I should know?

Chapter 16

It was 9:20 Tuesday morning and I was sitting in the office of Agnes Brown. Hers is a corner office. The windows look out over South Dearborn Street in Chicago. The curtains on the windows are drab and worn. All of the decor is in sharp contrast to the plum location of the office. The office is spacious but very nearly barren of furniture. The most prominent piece of furniture, indeed the only piece of any note, is her desk. Rather than facing toward the door, in the natural position, the desk faces away from the door and toward the window opposite the door. I can understand why. The office is on the seventh floor and the view out the window, while not spectacular, is nicer than that of the hallway. The window faces west where the view is dominated by the Sears Tower.

Agnes was perched on the edge of the desk, with one foot on the floor. It would have been awkward for her to sit at her desk at that moment, as she would have to turn her back to all of the people in the room. Those people were Jonny, Lisa, and me. In another forty-five minutes people from the NSA would be coming to discuss the money mill.

I leaned on the window sill. Lisa and Jonny sat in straight-back chairs. Jonny had turned his around and was leaning forward with his arms crossed over the back of the chair.

I was nervous as I waited. The NSA is the country's foremost authority on cryptology. The acronym stands for National Security Agency, although some joke that it actually stands for Never Say Anything or No Such Agency. Created by Harry Truman following World War II, the mandate of the NSA is to listen to (and decode) all foreign communications of interest to the United States. The NSA is known to be the world's largest employer of mathematicians and the largest buyer of computer hardware. No other organization in the world has more expertise in cryptology. No other organization in the world has better code breakers.

Adding to my unease was the fact that Jonny and Agnes weren't any less nervous than I was. Throughout our conversation Jonny was tapping on his shoe with his pen as usual, but the tempo was faster and he skipped a beat occasionally as he shot a nervous glance in Agnes' direction.

For her part, Agnes Brown seemed to be more irritable than nervous. She

met each of Jonny's glances with a level stare, followed by a quick glance at his tapping pen. For the past several minutes Jonny had been ranting about the controversies that always seem to go hand-in-hand with cryptology.

He paused now as he walked over to a small coffee machine which sat on a small table near the window. There was no sink in the room and the machine did not have a water feed of its own. Instead, there were several plastic milk jugs of water. Jonny filled the machine using the remaining water in one of these jugs and placed the empty jug under the table, along with two other jugs. Next he disposed of the old filter and coffee grounds in a waste basket under the table. They were using a plastic grocery bag as a liner for the waste basket. Beside the machine was an assortment of coffee blends: mountain, regular, de-caff, French roast, and almond vanilla. Jonny chose the regular.

Jonny didn't say anything while making the coffee, but having finished, he now resumed his story where he had left off.

"Everybody always blames new technology for life's problems," he said. "Yeah, it's true that the booming progress of computers — the Internet and telecommunications — has opened up a whole new area of crime, and I'll be the first to admit that the Bureau has been slow to keep up. We are only beginning to come to grips with computer crime. You're seeing the leading edge of our hacker-cracker methods in this investigation... I shouldn't be telling you that, seeing as how you're still a suspect, at least officially."

I wasn't surprised that the FBI was lagging in this area. "I suppose there is always a transient period when new technology is first introduced where the crooks have the upper-hand until the law enforcement people come up to speed with the new environment," I offered.

"Hey, you make it sound like the Bureau is a bunch of bumbling bozos man," Jonny objected. "I didn't mean to make it sound that bad. And we haven't fumbled computer crime yet — at least not big-time. Of course if we blow this case, and it is leaked to the public, it would be a major embarrassment."

Agnes turned to me and added quickly and pointedly, "You'd be the first person we'd investigate for any leaks, Carl."

Jonny apparently hadn't finished making his point about blaming technology for he then went on to say, "When cars were invented they were a big improvement over horses and walking, but they also made it easier to make a clean get-away from the scene of a crime. Does this mean that cars should be banned? Or that they should be blamed for all of society's problems?" (I resisted the temptation to reply in the affirmative just to goad him into a big debate over pollution, safety, and the like.) "No," Jonny answered in reply to his own rhetorical question. "Really, the situation was unchanged because the cops also had new cars. Technology gives better tools to the crooks but also to the cops.

"Man, think of all the other examples," Jonny continued. "Paper money is easier to carry than heavy coins, but it is also easier to counterfeit. Airplanes are better than cars for long distances but airplanes put a large concentration of people into a confined space making them vulnerable to hijacking and terrorism.

"Part of the price we pay for progress is that crooks can make use of the

new technology as easily as the rest of us can. Technology doesn't discriminate.

"That goes both ways. Any technology that crooks use, can also be used against them. The way I see it, the playing field is level and always will be. Technology doesn't change that."

The coffee was done by now and Jonny served everybody, starting with Agnes and ending with me. The small coffee-maker brewed just enough coffee to fill our four cups with a small amount left over. I don't particularly like coffee, but when I do have it I like it black without sugar. Adding cream and sugar only makes a distasteful drink worse in my opinion.

"This millwright dude might be able to exploit weaknesses in the bank network to steal money, and he might be a hot-shot crypto guy, but we can match him with the same technology. Hell, we can call in the NSA."

"That shouldn't be necessary Jonny," Agnes interjected firmly. "The NSA is coming only to comment on the strength of DES."

I'd heard about the rivalry between government agencies and I suspect this was an example of where the rivalry was blocking the most efficient path to a solution. It was clear to me that the FBI didn't really have the resources to deal with hackers as skilled in cryptology as the millrace team appeared to be.

Lisa chimed in with an anecdote about the invention of cars helping crooks. According to Lisa, Clyde — of Bonnie and Clyde fame — wrote a letter to Henry Ford congratulating him on the speed of his new cars. Clyde stated that Ford automobiles made excellent get-away vehicles and thanked Henry. Lisa insisted that this was a true story.

I took a sip of my coffee. Jonny had already finished his. He walked over to the table and poured himself another cup. Then he carried the pot over and topped off Lisa's cup.

Showing a weakness in character, I opened up a can of worms. "Hey Jonny, if a level playing field is all the FBI asks, then why impose restrictions on key sizes? Why ask for legislation?"

Agnes cut in. "We didn't invite you here to discuss politics Mr. Raymond," she snapped.

"I'll give them until 10:30," Agnes continued as she pushed her chair back from the desk and stood up. She walked across the room to the coffee pot, found it empty, glanced at Jonny, and began to prepare a fresh pot of coffee.

"They called this meeting, the least they can do is be on time," she muttered. From what I had heard it had been Agnes' superior, not the NSA, that had called the meeting. I said nothing.

Agnes filled the machine with water from one of the gallon jugs under the table. She continued to mutter under her breath as she tried to peel a filter away from the others, but instead peeled off two or three. It took a while for her to separate a single filter, and she muttered under her breath all the while. Picking up a pair of scissors from the counter beside the machine, she cut open an envelope of coffee grinds, dumped them in the machine, and jabbed the 'brew' button with her finger. I noticed she made de-caff this time. She stood and glared at the machine while the coffee brewed, as if she expected the machine to quit the moment she turned her back. Finally, apparently satisfied

that she had intimidated the machine into loyal service, she whirled around and headed back to her desk.

"What time do you have, Jonny," she snapped.

"10:11," came the reply.

"When these people do finally show up, let me do the talking, understand?" Agnes said to me.

"Fine. These people are from your corner, not mine."

The room fell silent. Jonny said nothing more about the fluctuations between strong cryptography and strong cryptanalysis. Agnes had made it clear that she didn't want to hear it. I found it interesting that those comments came from an FBI agent. It is the very agency for which Jonny works that seems to be unaware of these fluctuations. The FBI argument for key escrow hinges upon the belief that the latest swing in these fluctuations is an unprecedented event; past fluctuations are ignored.

As I sat there in the awkward silence, I mused over the key escrow debate. Key escrow is a procedure whereby part or all of a key is made available to a third party so that it can be recovered without the direct consent of the owner. The FBI would like to be able to use search warrants to access cryptographic keys used by private citizens. The FBI would like all domestic users of cryptography to place their keys in escrow. With the US government acting as the escrow agent, the FBI can gain access to these keys when the courts deem it appropriate.

Not long ago, the director of the FBI, Frank S. Samuelson, had gone before Congress to argue in favor of key escrow. A colleague had sent me a transcript of the opening remarks prepared by Samuelson. Among other things, he had said:

> In a very fundamental way, conventional encryption has the effect of upsetting the delicate legal balance of the Fourth Amendment, since when a judge issues a search warrant it will be of no practical value when this type of encryption is encountered. Constitutionally-effective search and seizure law assumes, and the American public fully expects, that with warrant in hand law enforcement officers will be able to quickly act upon seized materials to solve and prevent crimes, and that prosecutors will be able to put understandable evidence before a jury. Conventional encryption virtually destroys this centuries old legal principle.

The references to a centuries old legal principle and to the upsetting of a delicate legal balance irked me most when I read this. What Samuelson fails to note anywhere in his speech is that the delicate balance to which he refers is so very delicate that it has swayed back and forth numerous times throughout the history of civilization. The latest swing is but the most recent fluctuation of many. There is no more reason to be alarmed with the current change than with any other shift.

Yes, as Samuelson says, the law and the public expect law enforcement to present any evidence that is obtainable (after getting a search warrant). I agree. Unfortunately for the Jonny, Agnes, and their associates, the content of recorded

communications may no longer be obtained as easily as it once was. So be it; if the information is not obtainable, then neither the law nor the public expects law enforcement to be able to present it as evidence.

Surely nobody, including Samuelson, thinks that law enforcement should present as evidence the private musings of a suspected criminal. Such information is unobtainable, as everybody is well aware. Nobody expects the FBI to be mind readers. The FBI is expected only to present obtainable information.

If the FBI seizes my sneakers, they would be expected to attempt to learn as much as possible about them — e.g. the manufacturer — but if they are unable to determine where I was walking a year ago, even after careful examination of my sneakers by forensics experts, then does this mean that we must feel obligated to impose social constraints that make such information apparent from my sneakers? The suggestion seems ludicrous. Yet the only difference between the sneaker example and key escrow is that sneakers are common-place and well-understood. Cryptography is still new and unfamiliar to most people.

Nobody at the FBI complained when advances in technology opened up entirely new sources of evidence. Wire-tapping and electronic listening devices (bugs) are but two modern examples of technology that lend more power, not less, to a search warrant. It is now commonplace for whispered conversations, well out of ear-shot of the closest human being, to be obtainable by law enforcement. If Samuelson is going to appeal to the "centuries old legal principle" of search and seizure, then he must concede that the "delicate balance" has long since been destroyed. Encryption does not "virtually destroy" a centuries old legal principle, it merely sets it back closer to where it was a scant forty years ago, to a time when electronic surveillance was not practical.

I say let the FBI use wire-taps to collect any information they can (when they have a search warrant). There is no need to be alarmist about this. Should we ban water sprinklers and stereos? After all, people often use both of these devices to drown out personal conversations when they suspect they are being bugged. Do stereos represent a threat to American public safety? Of course not. To put the whole key escrow debate in context, one should keep two thoughts in mind:

1. modern encryption takes away two search and surveillance tools — wire-tapping and access to computer files;

2. both of these tools are themselves only recent developments.

It is hard to believe that a temporary setback, one that cancels some of the advantages brought about by other recent developments, will wreck havoc on our way of life. Has wire-tapping become such an integral part of American public safety in the few decades it has been feasible that any reduction in its effectiveness represents a potential collapse of society? To answer in the affirmative seems far-fetched, especially in light of other recent advances in forensics (e.g. DNA evidence, high-resolution satellite images).

Methinks Samuelson exaggerates the threat to national security and public safety. More likely he is fiercely guarding an advantage attained about forty

years ago by law enforcement — an advantage he should have realized was undoubtedly only a temporary fluctuation in the periodic ebbing and flooding of the tide that is the game of cops and robbers.

Granted, when the beneficial uses of a new technology have been limited, and the detrimental uses apparent, our society has a history of restricting use. Guns must be registered, for example. Some narcotics are banned. But cryptography is different in that the primary use is beneficial — protecting the privacy and integrity of remote communications. Banning or otherwise restricting cryptography is closer to banning automobiles than it is to banning firearms. Jonny's analogy was a good one, but I would take it a step further and draw a parallel between key escrow and a requirement that all cars have built-in rev-limiters to slow them down to less than 50 mph... except for police cars which would be capable of 80 mph so that law enforcement officers can chase and catch suspected criminals. This speed advantage would enable police to "quickly act upon obtained information to solve a case," as Samuelson claims the American public demands.

Or, to stretch the analogy nearly to the breaking point, because key escrow lets the public use long keys but gives part of the keys to the FBI, it is analogous to cars that are manufactured with remote-control rev-limiters such that the police can push a button while sitting in a patrol car and slow down a getaway car. This would have foiled Bonnie and Clyde in their speedy Ford.

Proponents of key escrow argue that honest citizens should not mind such things. If the police are the only ones with the remote control units for rev-limiters, then it is still possible for one citizen to speed away from another. And, if police must have a search warrant before pushing the button, and if we trust the US government, then what is there to worry about?

Hmmm... Watergate... Federal taps on Martin Luther King... Hoover... Tokyo Rose... Iran-Contra... Do I trust the United States government? Only to a degree. I prefer to think of search warrants as a necessary protection against government intrusion, a protection that is necessary only because the ability of government to intrude is too great, not too weak.

Consider this: a natural progression from key escrow is full information escrow. Why not archive all human interaction (neverminding the impracticalities for the time being)? I could wear a microphone around my neck; all of my conversations could be encrypted with an escrowed key and recorded for later access with a search warrant. Now, when the FBI gets a warrant they can obtain not only any information they can gather from my house, but all of the escrowed voice recordings. Even whispered face-to-face conversations in a secluded outdoor setting would not be beyond the reach of a search warrant. Ludicrous? Orwellian? I agree. I will not voluntarily escrow private one-on-one face-to-face conversations. Nor will I voluntarily escrow private one-on-one remote message exchanges. I fail to see any great distinction between the two situations other than the small difference that the FBI has become accustomed to eavesdropping on electronic communications without any cooperation, whereas eavesdropping on a face-to-face rendez-vous is harder in today's world. I take the same stand on both: no microphone around my neck; no key escrow. No Big Brother.

Such a stand is not so terrible for society. Civilization existed prior to electronic surveillance. It is not as if the world suddenly became a safer and more comfortable place to live once wire-tapping became technically feasible. Furthermore, even when strong encryption is permitted, the FBI can still tap unencrypted communications. Not everybody will use strong encryption for everything — its too expensive, too slow, and too awkward. Even when people do use cryptography, the same information is often available in other (unencrypted) forms (e.g. papers, books, disk files, and other forms of physical evidence). There is no shortage of forensics methods. The FBI has cited cases where "unbreakable" cryptography was used in crimes. Yet the crimes cited were solved. How? By more traditional forensic techniques.

Cryptography can even help, by making it harder for users of the Internet to hide. The next version of the Internet Protocol, IPv6, will include provisions for strong authentication. Technologies such as public-key cryptography give us the equivalent to unforgeable digital signatures and digital fingerprints. For that matter —

The buzzer sounded on Agnes' desk, rudely interrupting my silent rebuttal to Samuelson's stance on cryptography. We all were startled by the buzzer. For a moment all four of us just stared at it. Nobody moved. The buzzer sounded a second time and now Agnes reached out and acknowledged it.

"Mr. Templemeyer is here Mrs. Brown," said the voice on the other end of the line. "He has two gentlemen with him: Walt Little and Lorenzo Thomas."

"Show them in."

Then, to the three of us she said, "It's showtime."

As it turns out, 'Little' was not only Walt's last name but also an apt description of his stature. As he and his associate walked into the room one could not help but note the contrast. Walt Little was probably about five feet tall and thin. He couldn't have weighed more than 120 pounds. I'd place him at about fifty-five years old, but his hair was still dark brown (and didn't appear to be dyed). A neatly trimmed beard and mustache adorned his face. Despite this, or perhaps because of it, his face had a sharply chiseled look.

Lorenzo Thomas, on the other hand, was much bigger, weighing about 175 pounds, none of which was flab. He had an imposing physique for somebody of his years. Mr. Thomas had short white hair which was beginning to thin a bit at the top. He too appeared to be in his late-fifties.

Templemeyer I already knew from our earlier meeting. Once again he was wearing a light grey suit with a white shirt. His tie was Burgundy with brown paisley.

Little and Agnes exchanged handshakes and pleasantries. Agnes showed none of the irritation over their punctuality that she had voiced earlier.

Jonny, Lisa, and I stood by waiting for our turn to be introduced. Mr. Thomas did the same.

"I'm pleased to have the assistance of the NSA on this matter," Agnes was saying. "The FBI has been able to unravel much of the case and to uncover some of the lower-level culprits, but we have run into a bit of an impasse recently. I'm hoping that the NSA can help us move forward."

"We received your memo earlier in the week," said Mr. Little. "And of course Mr. Templemeyer has discussed the matter with us as well. The work of the FBI up to this stage has been quite impressive. No doubt you have pursued all available leads; I'm not sure if there is much we have to offer, but if we can be of any assistance at all..."

Nobody was willing to take the lead. Before Little and his companions had arrived Agnes had claimed that the NSA called the meeting. Now Little was implying that somebody at the FBI called the meeting, as I had suspected.

"Please have a seat," Agnes said as she gestured to the row of chairs lined up in front of her desk.

Little remained standing. "This is Lorenzo Thomas," he said. "He is our leading expert on DES. Based upon the content of your memo, I thought we might want his consultation in this meeting." Little had to look up to the man beside him as he said this. "Lorenzo is a leader in the field. He has a PhD from MIT, was instrumental in the original work on DES, and more recently has contributed to Clipper and Skipjack. Don't hold that last part against him!" Little looked in Lisa's direction as he said this, apparently having already guessed that she was not FBI. Lisa responded with a polite smile but said nothing. Agnes was not as amused. She motioned in Jonny's direction.

"This is James Carter. He is a case officer with the FBI. He specializes in cases of electronic crime. And, of course, the FBI in general is quite experienced in cases of banking crimes," she reminded Little.

Jonny nodded to both Little and Dr. Thomas and said, "Please call me Jonny."

Next was my turn. Agnes gestured toward me and said, "Carl Raymond has been kind enough to join us today. He is in part responsible for this mess. You see Carl took it upon himself to explore the EFT network. In so doing he facilitated the crimes we are investigating. His methods are illegal, but he has been cooperating with us recently."

OK, this wasn't the kindest of introductions, but I have to concede that it is accurate. I wasn't quite sure what to say. Should I apologize after an introduction like that? Before I could say anything Agnes continued with her introductions.

"This is Lisa Cryer. She is an ordinary bank customer that was victimized by Mr. Raymond's actions."

Lisa was not as taken aback as I was by Agnes' cool remarks.

"Hello Mr. Little, Dr. Thomas," she said sweetly, extending her hand toward Mr. Little. As she shook hands with the two of them she said, "I think you will find that Carl has been quite instrumental in the investigation."

"Tell me about it," Little asked her pleasantly. He settled down into the seat Agnes had indicated earlier. Dr. Thomas and Mr. Templemeyer did the same. I stepped back a couple of steps and leaned against the window sill. As I sat listening to Lisa's explanation I tried to read Agnes' expression. She had introduced Lisa as an innocent bystander and yet it was Lisa that Little had turned to for a briefing. Agnes is a woman that is not accustomed to anything less than full control. Outwardly she remained neutral. She sat with her elbows

on the arms of her chair and her hands pressed together in a steeple point under her nose as she listened to Lisa's explanation.

"What can we do to help?" Little asked after Lisa had finished her lengthy narrative. "All of you have done impressive work. All that seems to remain to be done is identify the culprit — the 'millwright' as you folks refer to him.

"I brought Lorenzo with me because of his knowledge of DES and MAC's, but now I am wondering if the NSA can help in a different capacity.

"My initial guess is that we are dealing with a protocol attack here and not a cryptanalytic attack on the MAC's themselves. It certainly would not surprise me. Cryptographic failures are usually at the protocol level and not in the underlying algorithms. In fact, we at the NSA joke that all the fuss over export restrictions is a moot point because it does not matter how strong the encryption algorithms are that people are exporting if they are using those algorithms in weak protocols. Of course, the NSA is the main proponent of export restrictions so we are laughing at ourselves when we say this.

"I will have our top protocol analysts take another look at the cryptographic protocols used for funds transfer." Little let out a short sigh and admitted that the NSA was part of the development process for all of the cryptographic standards for banking. If there were any flaws in those standards then they would be flaws that the NSA overlooked the first time around. He was hopeful, however, that with actual data and attack symptoms to study, the NSA analysts might find something they had overlooked the first time.

"Is there anything else we can do to help?" Little asked Agnes. At this point I stood up from the window sill. I had been hoping to be able to bring the computing power of the NSA to bear on the problem. The NSA is rumored to have an awesome amount of computer power. Supposedly the NSA has more MIPS at their disposal than IBM, DEC, HP, and Hitachi combined. Nobody knows for sure. Everything about the NSA is classified; even the budget is classified because knowledge of the NSA budget would allow people to estimate the computer resources the NSA can bring to bear on code-cracking problems.

Even if the rumors are exaggerated, even a small fraction of the NSA resources would speed up our automated search. I was sure that this was what Little was offering. Unfortunately, before I could make the request, Agnes responded. She apparently had interpreted Little's comments differently.

"Thank you, Walt. You are correct in describing our situation as one of knowing how the crime was committed but not yet knowing the identity of the perpetrator. Nor do we know his motive, although financial gain seems the obvious reason.

"As I'm sure you will agree, the Bureau has considerable experience with criminal profiles. We are confident that we can build an accurate profile for this case. In fact, Jonny can report on some of our progress. Jonny?"

Jonny stood up and walked over to an easel that had been set up near the window. I would have to wait for a better chance to ask Little for CPU help. I stepped away to give Jonny more room and walked over toward Lisa. When our eyes met Lisa rolled her eyes slightly and twitched her lips in a subtle smile. I briefly acknowledged her reaction with a similar one of my own, hoping that

Agnes didn't notice. I did not need to worry; Agnes was attentively watching Jonny's presentation. He was flipping through the pages on the easel, having already finished with the first page. The second page listed several traits the FBI believed described the millwright:

- Loner
- Computer geek
- College graduate, probably PhD
- Male
- US Citizen, born in USA
- Living in USA
- Age: 28-65

I wasn't sure how they had arrived at some of these characteristics. The list had grown since the last time I'd seen it. I noticed that they still hadn't narrowed the age range much. At least they were ruling out the stereo-typical 16-year-old hackers that seem to be blamed for everything ever since the movie *War Games* came out.

Lisa had chuckled softly when Jonny mentioned that the suspect was known to be a "computer geek." And she showed her skepticism (or was it irritation over perceived sexism?) when he said the suspect was "known to be male."

After completing the millwright profile, Jonny went on to explain that the FBI was reluctant to alert all banks of the trouble. The FBI feared that doing so would have the affect of also alerting the millwright. If the millwright were to shut down the mill and go into hiding, then he might never be caught. Given the scope of the crime, the FBI desperately wanted to catch the man behind the mill. Agnes hastened to explain that she had gotten clearance from the highest levels of the Justice Department to allow the mill to continue to operate in the hopes that the continued operation would expose new clues. As a result, First Chicago Trust and Bendix of St. Louis were the only two banks in the world that were aware of any peculiar activity in the EFT networks.

Of course the issue of allowing the mill to continue was a moot point since nobody had the foggiest idea how to shut it down. How do you stop someone from cracking DES? DES is supposed to be uncrackable. It is an integral part of the EFT system.

The two NSA men and Templemeyer listened to Jonny's carefully scripted presentation without interruption. When he was finished Little said, "yes, well it looks like you have the criminal investigation under control. As you said Agnes, the FBI is in their element there and while the NSA would be happy to help, I doubt that there is much we can do for you there.

"On the other hand, perhaps more can be done on the technical side..."

I wasn't going to let this opportunity slip by a second time. I said, "One area where we can use some immediate help is CPU cycles."

Little turned in my direction. "We can certainly let you have some cycles. Just give us your source code," Little replied. He seemed relieved to be discussing the technical issues again.

"What does your program do?" Dr. Thomas asked.

"We have two programs," Lisa answered. "The first is a more-or-less futile attempt to trace the bogus EFT's through the full graph. The program simply tests paths haphazardly. We recognize, of course, that there is an exponential number of paths, but we're desperate enough to try anything. Who knows, maybe we can stumble upon one of the millwright's bank accounts." She paused briefly and smiled sheepishly toward Dr. Thomas. I doubt that his response helped ease her embarrassment.

"Yeah, I'd say that's a long shot. What's the other program?"

Anxious to re-establish her credibility, Lisa told him about BIF. "The other program uses a statistical approach to try to identify suspect bank accounts. We analyze each bank account in isolation. We are hoping to be able to sift through all of the accounts in the system for suspicious accounts and then analyze those by hand. We are looking for any accounts with unusual activity. Of course writing programs to automate the search requires that we define what we mean by 'unusual'.

"We've designed and implemented a small rule-based language that allows us to write simple rules to characterize unusual account activity. This makes it possible to change the rules easily and thereby redefine the profiles for suspicious accounts."

I picked up the explanation at this point. "We have several rule sets that we have developed already," I explained, "and we have been experimenting with them. The trouble is that the program is extremely slow. Testing a single bank account is order n^2 where n is the number of rules. On top of that, some of the individual rules take a long time to run against a single account. When you consider that there are millions of bank accounts in the EFT network you can appreciate just how big the problem is. Even for our current rule sets, which are still much smaller than the profiles we anticipate we'll want to use soon, it takes us about a week to run through all the data we have."

"What are you running it on now?"

Lisa answered. "We are using a couple of Pentiums running Linux. I think they are 150 MHz and 90 MHz," she said, as she glanced toward me for confirmation. I nodded and added that the code was written in C. Dr. Thomas nodded his head, apparently satisfied with this answer.

"That should be easy to port," he said. "Would you be upset if we tinkered with the source a bit? We have some people that are quite skilled at optimizing programs for performance. In fact, it sounds like this problem may lend itself quite nicely to a parallel algorithm."

"Absolutely!" exclaimed Lisa. "This is an excellent opportunity for parallelism. Not only do we test each bank account independently, but even within the tests for a single account there are opportunities for parallel testing of rules."

"How soon can you get the source to us?" asked Little.

"We can give you a tape before you leave here today," Lisa replied.

Both Mr. Little and Dr. Thomas seemed pleased with this and Mr. Little stood up as if to go. Agnes still had some matters she apparently wanted to discuss, but seemed reluctant to do so with the rest of us in the room. Sensing this, I suggested that Lisa and I go prepare the tape. Jonny said he'd join us, and the three of us left. As we closed the door behind us I heard Agnes saying once again that the Bureau was pleased to have the assistance of the NSA but that the criminal investigation was well under control and that they really didn't need help.

"Turf wars," muttered Jonny. I wasn't sure whether I should feel sorry for Agnes or disgusted. I decided to feel sorry; I liked Agnes.

Chapter 17

The next morning I slept late. After fixing myself a breakfast around noon, I settled in for a long bout with the X9.17 protocol. This is the ANSI standard I had gotten at the Chicago Public Library on the day of my arrest. I was hoping that I might be able to find a weakness in the protocol that would explain the money mill. Little had suggested that the mill was probably an attack on the protocol used to exchange encrypted messages rather than an attack on DES directly. This was a plausible explanation.

This left me with the question of how the millwright was getting the MAC keys. Was he a trusted insider? Or was he an outsider that had discovered a way to circumvent the security measures designed in the key-exchange protocol used by all banks worldwide? I was determined to find out.

I fixed myself a peanut butter and jelly sandwich, grabbed a can of iced-tea, and sat down at the kitchen table. I opened my copy of the X9.17 standard. On the blue and white cover, in the upper right corner, it was dated 1985 but it also indicated that the standard was reaffirmed without any modifications in 1991. The title of the standard is *Financial Institution Key Management (Wholesale)*. I cracked the cover, sat back with my can of iced-tea (I've always found it more convenient to buy it by the can than to make my own) and, with great determination, set out to learn the protocol. As it turns out, determination was an important requirement; without it I would have tired quickly from all of the acronyms. As it was, they slowed me down but did not deter me.

X9.17 is intended for the exchange of cryptographic keys used in applications for wholesale financial institutions. In other words, for electronic funds transfer. This is the standard used for automatic deposits, automatic payments, wire transfers, and even the automated clearing of paper checks. To maintain the secrecy of keys, all exchanged keys are encrypted using key-encrypting keys. This encryption is done using DES. To provide integrity for exchanged keys, the protocol again uses DES, this time to compute message authentication codes (MAC's).

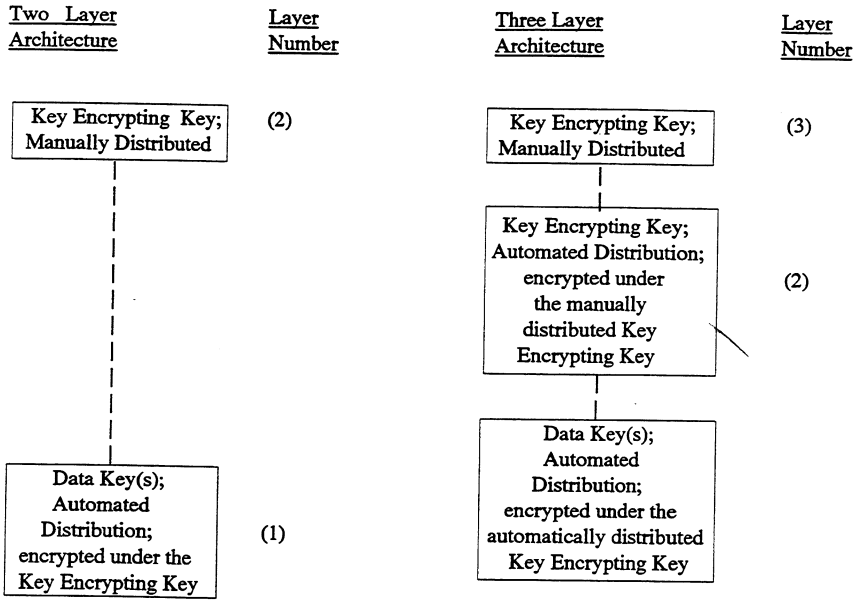
X9.17 supports the exchange of two types of session keys: keys used to encrypt data for privacy; and keys used to compute MAC's for integrity. The standard refers to both types as data-encrypting keys. The cryptographic keys used to encrypt data-encrypting keys during a key exchange are referred to

as key-encrypting keys. So key-encrypting keys are only used to encrypt and authenticate other keys, which in turn are used for EFT's and other inter-bank traffic. X9.17 only specifies key exchange, not key use (i.e. not EFT), but since all evidence indicated that the millwright had knowledge of keys, I wanted to study the X9.17 document to determine if there might be some way for an outsider to eavesdrop on MAC keys.

The standard includes two different architectures. The simpler architecture, called the two-layer version, uses manually distributed key-encrypting keys to exchange data-encrypting keys. The second architecture is a three-layer architecture that supports an additional layer of key-encrypting keys. The manually distributed key-encrypting keys are used to encrypt a layer of automatically distributed key-encrypting keys which are used in turn to encrypt data-encrypting keys. I noted that both architectures require that there be a secure mechanism external to the protocol for exchanging top-level key-encrypting keys.

FIGURE I

Key Distribution Architecture



The standard allows for three different "environments" (not to be confused with architectures). Because X9.17 has these three environments, it is really three separate protocols in one standard. The first, the point-to-point environment, is a protocol whereby two parties can agree upon a session key that is generated by one of the parties and is encrypted by that same party. The second environment, the key distribution center environment, is meant to be used

when neither of the parties wishing to establish a session key is able to generate a good key or encrypt a key for use by the other party (i.e. the two parties share no prior secrets). In this environment, one of the two parties requests a key from a trusted distribution center and receives two ciphertexts, one of which can be decrypted by that party and the other of which is relayed on to the other party for decryption. The third environment, the key translation environment, makes it possible for one of the two communicating parties to generate the key. The trusted translation center is used to encrypt the key for transmission to the other party. This environment is appropriate when one of the pair is able to generate good keys but the pair does not share a prior secret.

OK, so far so good. I stood up and walked over to the refrigerator. Rummaging through the contents turned up very little in the way of snack foods and I didn't want to prepare anything elaborate, so I settled for a second can of iced-tea.

I found the various message formats for each of the three environments on pages 47 through 50 of the document. Many of the fields are optional. Indeed, many of the messages are optional. I decided that the best way to tackle this was to filter out all of the optional features and concentrate first on the core of the standard. I got up from the table and went over to the telephone stand for a couple of clean pieces of paper. Sitting back down, I opened the iced-tea and took a long sip. Doing so, I noticed that the clock on the wall above the dishwasher read 3:05. Hmmmm, this might be a long afternoon. I used the first sheet of paper to jot down all the acronyms so that I would be able to refer to them easily. The standard already had a table of all the acronyms, listed on pages 4 through 7, but I wanted a list that only included those acronyms I expected to use. I left out all the acronyms for optional features, for example. The first part of my list consisted of the acronyms for the five message types that comprised the core of the protocol. The remainder of the list consisted of acronyms for required field types.

The standard actually contains many more acronyms than my small list. Being a computer scientist I am used to dealing with acronyms, even like it. But enough is a enough! Being inundated with dozens of new three-letter acronyms all at once, while trying to come to grips with the protocol in sufficient detail that I might be able to unravel the mysterious traffic patterns we'd been seeing lately, was a bit much.

Acronyms	
RSI	Request Service Initiation (optional)
RFS	Request For Service
RTR	Response to Request message
RSM	Response Service Message
KSM	Key Service Message (contains encrypted key)
MCL	Message Class (type code)
RCV	Intended Recipient (identifier)
ORG	Originator (identifier)
IDC	Server used (identifier)
SVR	Service Class (type code)
NOS	Notarization indicator (flag)
IDU	Ultimate Recipient of encrypted key (identifier)
KD	Encrypted key (ciphertext)
KDU	Encrypted and notarized key (ciphertext)
CTA	Request counter for A
CTB	Request counter for B
MAC	Message Authentication Code for all preceding fields

I needed some notation for my notes. I chose A and B to represent arbitrary banks. S_d denoted a trusted key distribution server and S_t denoted a trusted key translation server.

What is the difference between the KD field and the KDU field, I wondered. Both hold a session key, encrypted with a key-encrypting key. Flipping back to the definitions section I learned that the computation for the KDU field includes a notarization step. OK, so how do they stipulate that notarization of keys be done? After another iced-tea, two trips to the restroom, and two or three separate moments staring out the window, I had successfully waded through the explanation of notarization contained on pages 28 through 30. It isn't a lengthy explanation, but I had to be careful to understand it fully and not read anything more into it than was there.

I concluded that notarization is a method for sealing a key with the identities of the intended users of that key. A key is notarized by first blinding the key-encrypting key with a notary seal before using it to encrypt (notarize) the data-encrypting key. The notary seal is a function of the key-encrypting key and the two identities, and is designed such that it is difficult to compute a notary seal without prior knowledge of the key-encrypting key (i.e. it is a one-way function).

As I was writing down the basic protocol for the Key Translation Center environment, I was struck by how useful a key translation service might be to an outside attacker. The "translation" process involves accepting a key that has been encrypted by one key-encrypting key and returning the same key encrypted with the key-encrypting key of the requestor's choice. How convenient! This is exactly the sort of thing that encrypting the key is supposed to protect against! If anybody can ask to have a key encrypted using any other key, then what

protection does it afford? In affect, any member of the network can ask the key translation center to encrypt any key-sized collection of bits using the secret key known only to the translation center and some other member. The Key Translation Center is an encrypting service, using other people's keys!

Well, no. The X9.17 designers apparently anticipated attacks on the Key Translation Center because the standard requires that the requester send a MAC with the Request For Service (RFS). An outsider cannot forge a legitimate RFS. And an eavesdropper of a legitimate RFS and Response To Request (RTR) pair learns nothing because the keys in the KD and KDU fields are encrypted.

This was getting way too confusing. I walked across the room and got a ruler and took out a fresh piece of paper. A glance at the clock told me it was well past time for dinner. My stomach confirmed this. Reluctant to stop now that I was fully focused, I pushed on. I then wrote down the minimal protocol, leaving out all the optional parts.

Key Translation Center Environment			
$A \rightarrow S_t$: RFS	$S_t \rightarrow A$: RTR	$A \rightarrow B$: KSM	$B \rightarrow A$: RSM
MCL	MCL	MCL	MCL
RCV	RCV	RCV	RCV
ORG	ORG	ORG	ORG
IDU	IDU	IDC	IDC
KD	KDU	KDU	MAC
CTA	CTB	CTB	
MAC	MAC	MAC	

I used an arrow from X to Y to indicate that X sends a message to Y in that step of the protocol. In the Key Translation Center Environment, the protocol consists of four core messages. The first, the Request for Service (RFS) is from A to the center. This was the first column of my table. Then the center sends a reply (RTR) back to A. Then there is a message from A to B, and finally a message from B back to A.

Laid out in this way, the protocol began to make more sense. The first thing I noticed is that all of the messages contain the identifiers for the intended sender and recipient, as well as a MAC. In each message the MAC was written as the last field. The first three fields were always the same: the MCL holds the message class; the RCV holds the identifier of the intended recipient; and the ORG holds the identifier of the purported sender.

The fact that each message contained an explicit identifier for the recipient, as well as a MAC, would make it hard, if not impossible, to re-route messages. Because the messages contain MAC's, they cannot be altered (unless the attacker knows the MAC key).

I wondered what would happen if an attacker tried to fool B into using the wrong data-encrypting key in the Key Translation Center Environment. The attacker might try intercepting the KSM message sent by A and intended for B.

However, there is little that the attacker can do with the intercepted message. The key contained in the KDU field is encrypted and therefore inaccessible. The attacker might try to substitute a different key by replacing KDU with bits of his own choosing, but he will be foiled by the MAC that must be appended to the KSM message. Without knowing the key-encrypting key, there is no way for the attacker to recalculate the MAC for the new KDU field such that it will pass the verification check performed by B. This is the essential function of MAC's — to make it infeasible to alter intercepted messages or to produce fake messages.

Next I turned to the Key Distribution Center Environment. According to the standard, at a minimum the protocol for a key distribution center environment consists of three basic messages. the first important message is the RTR message. Flipping back to page 7, I discovered that RTR stands for Response to Request, and the actual request (called and RSI or Request Service Initiation) is one of the optional messages I was ignoring for the time being. The table on page 47 indicates that RTR messages in this environment have nine fields. The first of these nine fields is the Message Class (MCL), which indicates the type of message. In this case the MCL field indicates that the message is a Response to Request (RTR). The next field, RCV, specifies the intended recipient. It is an identifier. This is followed by the identifier for the sender, or originator, of the message. The IDU field holds the identifier for the ultimate recipient of the (second) encrypted key. The entity that receives the RTR message is expected to relay a copy of the encrypted key on to the entity named in the IDU field. The next two fields hold encrypted copies of a key to be used in an EFT session. The KD field holds a encrypted copy for the recipient of the RTR message (i.e. entity A), while the KDU field holds an encrypted copy for the other entity (i.e. B). Thus, KD and KDU will be encrypted using different keys since they are intended for decryption by separate entities. The ciphertext fields are followed by two counters in plaintext. These counters are used to recognize replays of old messages. The first counter is a tally of the number of keys sent to entity B while the second counter is a tally of the number of keys sent to A. Finally, appended to the RTR message is a MAC. The MAC is computed over the entire message (i.e. eight fields, beginning with MCL and ending with CTA).

The content of the fields in the remaining message types is similar to that of the RTR. The next message, the Response to Service Message (RSM) is an acknowledgment sent by A back to the key distribution center. At this point A has a copy of the key (after decrypting the contents of the KD field in the RTR). Next A sends a Key Service Message (KSM) to B. The KSM message contains the KDU field, which A cannot decrypt but B can. The KSM is the heart of the protocol in each of the three environments; it is the message that sends the encrypted key to the ultimate recipient. Each of the protocols ends with a Response to Service Message (RSM) which is an acknowledgment of the KSM.

Key Distribution Center Environment				
$A \rightarrow S_d$: RSI	$S_d \rightarrow A$: RTR	$A \rightarrow S_d$: RSM	$A \rightarrow B$: KSM	$B \rightarrow A$: RSM
MCL	MCL	MCL	MCL	MCL
RCV	RCV	RCV	RCV	RCV
ORG	ORG	ORG	ORG	ORG
IDU	IDU	IDU	IDC	IDC
SVR	KD	MAC	KDU	MAC
	KDU		CTB	
	CTB		MAC	
	CTA			
	MAC			

Ahh, but wait a minute! The key translation center environment allows a participant to generate a session key and submit it to the trusted third party for packaging. In other words, the party that generates the session key and sends it to the ultimate recipient does not need to share any prior secrets with the ultimate recipient. Might there be some way for one party to impersonate another party and request a key translation? Some sort of inside attack?

The party sending the RFS to the Key Translation Center still needs a legitimate key because, as I had noticed earlier, the RFS includes a MAC, which cannot be computed without the key. OK fine. Some other bank, separate from A and B partaking in the key exchange, would have a legitimate key. So that requirement can be met.

I hurriedly took notes on this train of thought, afraid that I might forget it. Damn — broke the pencil lead again. I renewed the pencil point and pressed on. So as not to add a new level of confusion and make it difficult to relate my notes to the X9.17 standard, I continued to use the notation of the standard, although I did yield to the temptation to deviate slightly.

OK, let's see... The ciphertexts for encrypted session keys are not always notarized. Due to this lack of explicit type information in the ciphertext portion of some messages, it is possible for an attacker to use the ciphertext in a manner different from the intended use. Namely, the attacker can use un-notarized ciphertext to impersonate a party making a seemingly legitimate request for key translation. There is no MAC in the RSI message format used to request service from a key distribution center. Presumably the ciphertext in the response from the server is meant to guard against misuse.

Hmmm. I wonder if the lack of explicit information in keys might make them susceptible to replay attacks. The attacker would need to be able to predict the values of counters expected by recipients of forged messages (e.g. CTA and CTB), but this is easily handled by eavesdropping on a short history of messages. The counters are sequential and are sent in the clear.

I jumped out of my chair and ran over to the telephone stand, grabbed the entire stack of scrap paper, and hurried back to the table. I needed to get this down on paper before I forgot it. I hurriedly took notes, not bothering to write

things down neatly; there would be plenty of time later to polish it up and fill in details.

I used Y_Z to denote entity Y attempting to impersonate entity Z in the protocol. The attacker, a legitimate member of the network, will be denoted by X. KD_Z shall denote a key encrypted using a key-encrypting key known to Z. KDU_{YZ} shall denote a key encrypted using a key-encrypting key known to Z and notarized with the identities of both Y and Z.

To start things off, the attacker, X, impersonates A requesting a key from the key distribution center. In the request, X claims that A wishes to communicate with the attacker (X). Request messages of this type (RSI) do not contain any authentication codes and are easily forged.

$$\boldsymbol{X_A \rightarrow S_d:} \qquad RSI \parallel S_d \parallel A \parallel X \parallel SVR$$

The key distribution center responds by generating a data-encrypting key. That key is encrypted using the key-encrypting key associated with A and included in the KD field. Also, the same key is encrypted and notarized using the key associated with X. Because KDU_{AX} is encrypted using X's secret key, X can obtain the plaintext for KDU_{AX}.

$$\boldsymbol{S_d \rightarrow X_A:} \qquad RTR \parallel A \parallel S_d \parallel X \parallel KD_A \parallel KDU_{AX} \parallel CTX \parallel CTA \parallel MAC$$

X now sends an RFS message to the Key Translation Center, asking for a key translation. It is easy for X to forge this message, despite the MAC, because X knows the value of the key used to compute the MAC — it is the same key as is encrypted in KD_A and KDU_{AX}, the latter of which X can decrypt.

$$\boldsymbol{X_A \rightarrow S_t:} \qquad RFS \parallel S_t \parallel A \parallel B \parallel KD_A \parallel CTA \parallel MAC$$

In response to this last message the key translation center notarizes and encrypts the session key using B's key-encrypting key and returns that ciphertext to X (thinking that X is A).

$$\boldsymbol{S_t \rightarrow X_A:} \qquad RTR \parallel A \parallel S_t \parallel B \parallel KDU_{AB} \parallel CTB \parallel MAC$$

The attacker now has a notarized and encrypted version of the session key he originally obtained from S_d. Impersonating A, the attacker can pass this notarized key on to B.

$$\boldsymbol{X_A \rightarrow B:} \qquad KSM \parallel B \parallel A \parallel S_t \parallel KDU_{AB} \parallel CTB \parallel MAC$$

At this point, X can fool B into executing a session with X where B believes that B is communicating with A. Or, X can go on to inform A of the new key

and allow both A and B to believe they share a secret key when in fact X knows the key. If X chooses the latter version of the attack then X impersonates the key distribution center and sends the following message to A.

$$\boldsymbol{X_{S_d} \rightarrow A:} \qquad RTR \parallel A \parallel S_d \parallel B \parallel KD_A \parallel KDU_{AB} \parallel CTB \parallel CTA \parallel MAC$$

I twirled my pencil between my fingers and leaned back in the chair. I pursed my lips and whistled silently to myself. Let's see now... X can either send this message to A as an unsolicited RTR message or X can wait until A requests a key for use with B. After sending this message, X then intercepts the response from A to B and discards it.

At this point A and B believe that they share a secret key known only to them (and the trusted key server). However, the key is also known to X.

Hot damn! This was it! This attack works! I leaned forward and let the front legs of the chair hit the floor with a loud thud. I took a deep breath. I reminded myself that this attack requires some preliminary setup by the attacker. It cannot be used to learn keys already in use. Nonetheless, with minimal effort, an attacker can obtain the session keys used by any communicating pair in the network. Thus, the use of separate keys for each communicating pair is overkill — the protocol might just as well use a single key shared by the entire network. There is no additional security obtained by the use of separate keys.

I walked over to the window. What are my assumptions? First of all, the attacker needs to have access to somebody's key-encrypting key...

Whoa! My blood ran cold. In a sudden fit of paranoia I glanced at the door, confirming that it was closed and the chain drawn. I slowly laid my pencil on the desk and walked over to the window. A shiver ran down my spine. Staring at the street below, I allowed myself to come to grips with the realization that the millwright definitely was an insider, but not necessarily at Bendix. The easiest way to meet my assumption is to assume that the attacker was part of the EFT network — i.e. a member bank, *any* member bank. We had always assumed that if the money mill was an inside job at all, then the insider was probably at either First Chicago or Bendix. Strangely, I found it far more disturbing that the mill was being run by an insider with access to all X9.17 keys than if the millwright were a lone hacker that had figured a way to crack DES. A banker with the cleverness and Computer Science know-how to devise the mill was a very dangerous adversary. Quite probably with powerful allies.

I shuddered and ran a hand through my already disheveled hair as I continued to stare at the dark street below (sometimes it seemed I spent more time staring at that same empty street than I spent at my desk). All manner of questions raced through my mind. Which bank? Was it an institutional effort being run from the top or was it a single rogue employee? Even if it were the latter, the employee would have to be one of a small number of highly trusted employees if he or she had access to a triple-DES key-encrypting key.

Finally, I turned back to the desk. I was forced to conclude that the X9.17 standard, approved by the American Bankers Association in 1985, re-affirmed

by the same group in 1991, and recommended by NIST in 1992 for all government key exchange, was completely vulnerable to impersonations of one member institution by another member institution. There is little point in the banks using separate key-encrypting keys because any bank can impersonate any other bank; *they might as well all be sharing a single key.*

The protocol completely fails to satisfy requirements 4-6 and 9, as laid out on page 12 of the standard. Those requirements state:

(4) A data key or key-encrypting key shared between a communicating pair shall not be disclosed to a third party (except for a Key Translation Center (CKT) or a Key Distribution Center (CKD)).

(5) A data key shared between a communicating pair shall be secured from third party usage (except for a CKD or CKT).

(6) The compromise of any key shared between any communicating pair shall not compromise any third party.

(9) Key security and integrity shall be ensured.

None of these hold! Not a single one. The standard fails to meet four of the sixteen objectives clearly laid out on page 12. How could such a grievous oversight occur in such an important standard? Trillions of dollars were distributed every day by EFT. CHIPS alone handles well over 150,000 messages every day. The CHIPS network spans the globe and includes all of the major banks.

Nevermind all that, who was the millwright? If I was right in assuming that the millwright was able to obtain a primary key-encrypting key because he was a privileged employee of one of the banks, that limited the number of people somewhat. But only somewhat. He might be working for any one of the several thousand banks in the network. If he was a privileged employee of a bank, regardless of whether he was acting alone or on behalf of a corrupt bank, he was likely very knowledgeable in the mechanics of funds transfers. Far more so than I was, for example. Could it be that the millwright already knew we were tracking him? Might he be watching my every move from afar? I shook off a feeling of being watched. It was an absurd thought. Somewhat annoyed with myself, I crossed the room and lifted the phone and began punching in Lisa's number — a number I'd long since memorized but never bothered to store in the phone's memory. But after only one ring I abruptly hung up, having suddenly decided that it might be better to tell her in person than over the phone. I knew all too well that phones were not secure from nosy people, especially nosy people with an interest in noting any progress in my detective work. In other words, I hadn't succeeded in ridding the feeling of paranoia.

Grabbing my wallet off the kitchen table, I glanced at the clock above the dishwasher and headed for the door. Hmmm, 11:45. It would be 12:30 by the time I got all the way over to Lisa's place. I wondered if our friendship was close enough to allow for an unannounced visit at that hour. Then I wondered if *any* friendship is close enough to allow for such an intrusion (excluding friendships that are no longer referred to as merely friendships). I decided I'd better take

the opportunity to catch up on eating and sleeping and visit Lisa in the morning. No good. She would be at work (*she* had a real job). Reluctantly I realized I would have to take this discovery straight to the FBI. Still, it would have to wait until morning.

Chapter 18

"What?!"

Agnes Brown was agahst. She threw up her hands and leaned back in her chair. It was a high-backed leather chair that creaked loudly when she stood moments later. Jonny stepped out of her way. He glanced in my direction but said nothing.

Jonny had reacted to my news with great excitement and had rushed to Agnes' office to give her an update. He had expected Agnes to be pleased with the breakthrough in the case. Instead she was distraught over the flaw.

"How," she asked, "can a security system that has been in use for over a decade be so badly flawed? The NSA helped develop that standard! It has been reviewed by security experts at DEC, IBM, Burroughs, Citibank, Mellon Bank, NCR, AmEx, Honeywell, and countless other high-tech companies." She flung an arm in my direction. "And *he* finds a flaw after just a couple of days of study."

I do not think that the derision in her voice was intentional, nor do I think she meant to insult me personally. Probably what she meant to say was that a single individual managed to find a flaw that a panal of expects had either overlooked or else deemed unimportant.

"When was the last time it was reviewed?" she asked.

"It was reviewed and re-affirmed in 1991," Jonny answered. "In 1995 there was a revision. The 1995 version is quite different from the 1985 and 1991 versions."

I was surprised by the swiftness and accuracy of his reply. Apparently Jonny too had been studying the EFT protocols. "Right," I said, "but the flaw remains in the revised standard as well. I already checked. The 1995 changes do not correct this flaw. Indeed, the protocol itself remains unchanged. The changes made to X9.17 in 1995 are primarily involved with the notation and the drafting of the document... cosmetic stuff."

Agnes strode from the room, beckoning to Jonny and me to follow. Not sure where we were going, or why, I fell in behind Jonny. Down the hall and to our left. Past the elevators. Through a door at the end of the hall and up a narrow staircase. We went up three flights. That put us on the tenth floor. We entered a wide outer office with a young male receptionist sitting at a long low desk. He

looked up critically and raised an eyebrow.

"Do you have an appointment Mrs. Brown?" he asked.

"Is he in?" came the curt reply.

"He's busy," the receptionist shot back.

Without another word Agnes headed straight for the inner office door. Whoever "he" was, the fact that he was busy did not slow Agnes in the least. Jonny followed, but two or three paces behind now. The receptionist sighed and punched the key on the intercom with an air of resignation.

The intercom was buzzing on the desk as we walked in. The man sitting behind the desk looked away from the intercom and up at us. Agnes sat down into the chair immediately in front of the desk.

"What is it now Agnes?" the man asked with a deep sigh and a forlorn glance at the papers lying in front of him. He took off his glasses and massaged his temple.

"The First Chicago case has heated up," said Agnes.

The man behind the desk sat up and let out a mirthless laugh and said, "heated up? That case was red-hot already. What happened now?"

He listened without comment as Agnes told him that our banking system has a security hole large enough to funnel out billions of dollars. He was a portly man, in his early 50's. His hair was beginning to thin at the top. He had a strong air of authority about him. I later learned that his name is Charles Fisk and that he is head of the Chicago office of the FBI. His responsibilities include general oversight of all Midwest operations. He had been appointed to the post only six months prior to that meeting and was still getting used to Agnes' no-nonsense style. He tended to keep the reigns loose on people under him, Agnes especially. Now, though, he wanted a full status report and wanted the details on all leads. No sooner did Agnes finish explaining the flaw (as best she could (I did not dare correct her)) than Fisk wanted a run-down on all of the suspects.

"What have you got so far?" he asked.

Agnes took a deep breath and glanced toward Jonny. "Our best leads at this point are going to be whatever we get from a computer program that was written by a young woman that was an early victem."

"Yeah, you told me about that. You mean Cryer. What was her first name?"

"Lisa."

Agnes was referring of course to the program that Lisa, Rudy, and I had written. Actually we had written a pair of programs, but I was sure Mrs. Brown was talking about BIF and not Deep Throat. Of course Agnes would have been unaware of Rudy's recent contributions to BIF.

Jonny took a step forward and began to explain to Fisk the findings of BIF. I was surprised at the amount of success the FBI had already had with the program. With the help of BIF, the FBI had found a bank account at Chase Manhatten that was being used to funnel a large number of EFT's that they believed to be counterfiet. Like many other accounts, this account had a large volume of money passing through with the account balance remaining roughly level. On any given day, the deposits into the account were nearly equal to the

withdrawals. This despite the fact that tens of thousands of dollars were passing through the account daily.

What made this account especially interesting was that many of the payments were directed to a bank account in France. Could this account be one of the main arteries out of the country? It was the first solid evidence we had of laundering. Money was apparently being laundered through this account and then shipped overseas. Although they had not yet confirmed it, the FBI was convinced that they would find that the next destination for the money, after the French bank, would be a bank in Switzerland. Fisk immediately urged Agnes to have her agents confirm this as soon a possible.

"We are working on it," she replied. She swept her hair off her forehead and out of her eyes. With a nod to Jonny, she said to Fisk, "the most interesting thing about these forgeries that Agent Carter has described is not so much where the money is headed, but rather where it came from."

Fisk raised an eyebrow and turned to Jonny. In response to this cue, Jonny continued.

"We traced the money backward through the EFT network. When we did this we discovered that much of the money that was being routed to the French account was stolen from the accounts for a Major League baseball team — not borrowed but stolen. All of the other forgeries we have seen have been loans. As you know, the way the mill works is that the hacker borrows money from lots of accounts and promptly returns it. Usually within 24 hours. Sometimes, just to throw us off the trail, the money is returned even sooner, in which case there is no loan — just laundering. We have even seen cases where the money is deposited a day or two before it is withdrawn. This is why it so hard to trace the counterfeit money. There is no pattern to it and most of it is only borrowed.

"The baseball team's bank account is the first example we have found of an outright theft. We figured all along that such accounts must exist. After all, the millwright has to seed his operations somehow. Now we have an example. We think that the choice of accounts is not random."

I was baffled. Why would a computer hacker single out a baseball team as a target?

Agnes answered my unvoiced question. Speaking to Fisk, she said, "We are developing a profile. We believe the subject is a young male computer professional, a loner. He probably does not have an active social life. He appears to have a great deal of time to devote to devising clever ways to undermine our banking infrastructure... not to mention the time to operate the mill on a daily basis. It is likely that he is lacking athletic prowess. Perhaps he harbors some resentment toward professional athletes."

Fisk wasn't buying it. Neither was I. They were attaching too much importance to the baseball connection. Sure it was unusual that the first example of a theft in the mill that the FBI stumbles upon happens to be on an account of a high-visibility organization, but was it really as unusual as they seemed to believe? It reminded me of the common situation where a person flips the top card on a deck of cards and then claims that a very low probability event has occurred when the card is, say, the Ace of Diamonds. Would the result have

been any more atsonishing had it been the Ace of Spades? Or the any other Ace? What about the Joker, the Jack of Diamonds, or the Queen of Spades? Without first declaring which cards we consider "unusual", it is not meaningful to discuss the liklihood of flipping over an unusual card.

Was it really that surprising that one of the victems of the mill was a sports club? Would we be any less surprised if it were a movie star, a politician, or a religious organization? Or if it had been IBM, Microsoft, or GM?

I don't normally follow baseball. In fact, the only reason I had even heard about the team Jonny mentioned, was because the shortstop was rather infamous for his off-field exploits. Although an apparent leader on the field, he had been involved in a very public legal battle involving domestic violence and alcaholism. His legal troubles had come to a head when he had been involved in a drunk driving accident. All of this had occurred after I had left MMT and started consulting. Now that I work in a private office I do not have the opportunity to gather around the water cooler and catch up on gossip and current events. Without that casual source of news, I have a tendancy to fall behind. I do not know if the player was suspended from the team or not — at the time there was considerable public debate over that decision. The team itself was going nowhere fast.

Fisk sat staring sternly at this desk. Noboby spoke. Seemingly aware that all eyes were on him, Fisk grunted crossly and continued to stare downward in deep thought. "What about the international connection?" he asked. "Why France?"

Jonny shrugged his shoulders. "Dunno. Probably as good a country as any."

Fisk wasn't about to give up that easily. "Maybe the subject is a French citizen. Is this the first international transfer we have uncovered?"

"No," said Jonny, "but it is the first international *theft* we have found." After only a brief pause he added, "It is the first theft of this magnitude too. We have seen other international loans. Not all to France. Some have been to England and Japan. Several were to Germany... A few to Brazil and Argentina... One to Canada..."

"Argentina was the country with the bank that lost $12 million a couple of years ago, right?" Fisk asked. Then, realizing he was getting side-tracked he waved off any reply and instead asked, "France has unusual laws governing privacy and electronic surveillance doesn't it?"

It was Agnes who provided Fisk with a confirmation. She said that France has no laws against electronic surveillance. In that country, it is perfectly legal to tape a phone conversation without informing the other party that he or she is being taped. Every utterance that is recorded on tape is admissable in court. She turned to me with one corner of her mouth pulled up in the slightest of smirks saying wryly, "If Carl is unhappy with the FBI's invasions into civil liberties and privacy, he should try living in France."

It was the first time I had seen Agnes show a sense of humor. Was she softening?

Fisk grunted. "Tell me more about this computer program. Could it be be used to test specific profiles?" he wanted to know.

"What do you mean?" I asked.

"Well, suppose we want to test a hypothesis that the millwright is motivated by politics rather than financial gain. Could we look for accounts with high volumes of activity yet no net change in balance, where a number of payments are made to political campaign contributions? Or perhaps to a specific charity?"

"I don't see why not," I replied, thinking to myself that it would take Rudy no time at all to fulfill such a request.

Fisk was clearly excited now. He reached over his desk and jabbed at the intercom. As soon as his secretary responded Fisk demanded that he get Ms. Lisa Cryer on the speaker-phone immediately. Fisk suggested that the secretary try her work number first. With a wide grin on his face, Fisk turned back to Agnes. "This could turn the case around. Bust it wide open, really. We should use the millwright's own tools against him.

"As I understand it, the reason the money mill was so hard to detect, and the reason it is so hard to trace the illegal transactions even now when we are fully aware of their existance, is that the scoundrel behind this has used computers to automate his attack. It seems that nobody anticipated a carefully choreagraphed and yet still massive attack on our banking system. After all, the larger the attack, the harder it is too coordinate and manage... *unless* you use computers to process hundreds of thousands of forged checks faster than you can blink."

Fisk hopped out of his chair and walked to the front of his desk. He clasped his hands behind his back and paced briskly in front of his desk. Agnes was still seated in the chair. She uncrossed her legs to make more room for Fisk to walk between her and the desk. Jonny stood over by the window. I still had not stepped more than a couple of paces into the room and stood behind Agnes with one hand resting on the back of the chair.

"It is ingenious really," continued Fisk. "The same computers that allow us to process millions of bank transactions in a day, also allow the hacker to create millions of forgeries in a day. By making most of them decoys, he makes our task of tracing the money he borrows next to impossible. On top of that, we can't even distinguish a bogus EFT from a legitimate one!"

He threw his hands up in despair. Then, without missing a beat he spun on his heels and walked back across the room with his hands once again clasped behind his back.

"What we must do is beat him at his own game. Let's turn the tables. We will use computers as a tool against *him.* He uses computers to automate a highly coordinated and massive attack on our banking system; we use computers to track the money through the system."

"Uh... Sir?" Jonny gently interrupted. "We can try, but that probably won't work."

Fisk stopped walking. He said nothing but Jonny had his full attention. Jonny gave a quick sideways glance in my direction, took a deep breath, and explained. "We have another program that does as you suggest, but it is a long shot. It works with recorded EFT data and follows the money through the system. By starting from a payment that we know is counterfeit, and then

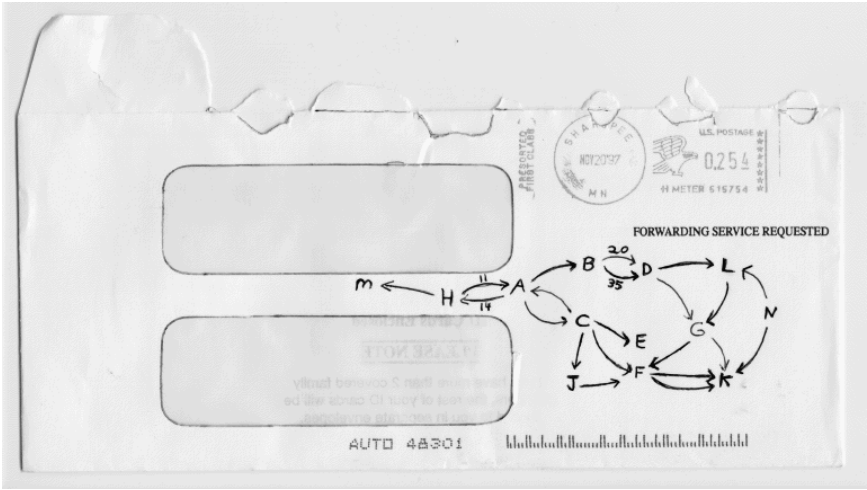
tracking money into and out of that account, we hope to find other counterfeits. If we can string together enough counterfeit payments, we should be be able to trace the money into a bank account that the hacker is using to collect interest.

"This is not an easy thing to do. The counterfeits are perfect forgeries and are mixed in with legitamate traffic. The amount of EFT traffic along any given path, even through fairly inactive accounts, is very large. It is a pain-staking and labor-intensive task to investigate the validity of each EFT as we trace through the graph."

"Graph? What graph?" asked Fisk.

"Sorry, Sir. That is a computer science term that Carl has taught us. It is an abstract data structure — a way of organizing data in computer memory. A graph is a set of nodes and arcs. Arcs connect one node to another node. The nodes represent bank accounts. The arcs represent funds transfers. The direction of the arc represents the direction of the transfer. When there are several payments between two accounts, there are several arcs, one for each payment."

Fisk nodded his head slowly. It was apparant that he was only half-following Jonny's explanation. Jonny glanced at me, then Agnes. He strode over to the desk and took a pencil out of Fisk's pencil-holder. Next he pulled a crumpled envelope out of the waste-basket. He quickly sketched a graph for Fisk.



"See. Now suppose I trace a path in the graph starting here at point A. I have two choices: I can go to node B or C. Suppose I choose C. Now I have four choices, one of which is to go back to A. Just to keep things interesting, I'll go back to A, and then from there I'll take the arc to B. At node B there are two out-going arcs, both going to D. I'll take the arc labelled as twenty dollars. From D, I can go to G, then K, and so on."

Jonny paused while he counted up the arcs in his example. "Even in this small graph, with only about twenty arcs, there are dozens of possible paths. Now imagine we have the full EFT graph, which has hundreds of thousands of new arcs every day. Then possible paths number in the trillions. Or more. To

make things even more complicated, when the paths get very long it is difficult to recognize when you re-visit the same node; you can go around in circles without even realizing it! This is because the EFT graph has cycles. This is the whole point behind the money mill — the millwright is using cycles in the graph to skim off interest payments from banks. Even if we had a way to quickly identify the forgeries, we still would not have a good way to track the money. There are so many forgeries in the network today that even after we single out only the forged arcs in the graph and trace those, the graph is *still* too complex. There are too many bogus paths. This is what it means to mount a *massive* attack against the system."

"Dammit, we have to do something." This was Agnes.

Fisk's reaction was more calm. H3 was undeterred. "Fine. I can understand that. What about the other program?"

I stepped forward. "The other program takes a very different approach. Rather than try to trace the stolen money through the network, we look at each bank account in isolation. In this way we circumvent the inherant inefficiencies in the problem. BIF ignores the flow of money and instead focuses on the activity in individual bank accounts. Bank accounts are analized in isolation, without worrying about the inter-action between multiple accounts. We try to identify suspicious activity in individual accounts."

Fisk drummed his fingers on his desk and, with his chin resting in the palm of his other hand, stared sternly at the Mahogany surface. "OK, what about our newest discovery? We now know how the attack is being carried out. How does that help us? Surely that makes is easier."

Nobody answered.

"Mr. Fisk?" It was the squawk of the intercom on his desk. Everybody except Fisk startled at the high volume and annoyingly nasal sound. "Lisa Cryer of SoftTykes is on the phone."

"Put her on the speaker-phone," came the excited reply. Fisk rubbed his hands together as a he leaned forward on this desk.

"Hello?" It was Lisa. She sounded hesitent. No doubt she had not been supplied with much of an explanation from the secretary, given that the secretary himself had been given no explanation for the requested phone call.

"Hello Ms. Cryer. Sorry to interrupt you at the office. Hopefully you can spare a few moments to discuss an important matter with us. My name is Charles Fisk. I work for the FBI. I have a few questions for you concerning a computer program you have written for us. With me in the room are Agnes Brown, James Carter, and a gentleman named Carl Raymond."

Lisa said nothing immediately so Fisk continued, getting straight to the point. He sat back in his chair and swiveled side-ways so that he could direct his comments towards the rest of us in the room while still turning his head toward the microphone on the speaker-phone.

"How hard would it be," he asked, "to modify your program so that it could discover bank accounts like the ones it already finds, but where there is an unusually large number of payments to a political campaign fund?"

Lisa's anwer was more conservative than mine. She was hesitent with her reply. "The limits to the sorts of profiles we can test are imposed by the expressive power of the rule language," she explained. "No doubt some profiles will require extensions to the language, which could take considerable time."

"What about the example I just gave you," pressed Fisk. "Could you do that one without any major extensions to your language, or whatever."

"Yes, that one we can do. We would need a list of political groups and funds."

"Then let's do it immediately." Fisk turned to Agnes. "We should pursue this case along conventional lines as well as the high-tech approach you are already using. Talk to Burns and have him assign one of his top profilers to this case full-time. I want an accurate profile. Have Burns' man make full use of this program of Lisa's to test various hypotheses. Let's get moving on this. I'm assigning this top priority. Tomorrow I will meet with Samuelson to discuss this case and I want something positive to report. At the very least, I want to be able to tell him we have some promising leads."

Fisk hunched over the speaker-phone. Enunciating carefully for Lisa's benefit, he asked, "What about net-zero accounts where the bulk of the payments are directed to a specific country?"

"That one won't be so easy," came the reply over the phone. "You see we have certain parameters that we already have set up to measure... things like the payee and payer for an EFT, the paying and recieving bank, the amount, the date, and so on. The country of origin or the destination country happens to be a parameter that we do not already have defined. It will require writing a small amount of code to pull that information out of the EFT message format and store it in a way that it can be accessed by BIF. That requires changes to the parser that processes the EFT's. Then we have to extend the rule language of BIF to include predicates on the country parameter."

Lisa could not see the blank stare that began to settle in on Fisk's face, but perhaps she could sense it; she paused momentarily and then summed up quickly. "It shouldn't be hard, but it won't be as easy as your first example," she said abruptly.

Fisk crossed his arms over his chest and sighed deeply. His heavy eyebrows furrowed, he pressed his lips together tightly and stared intently at the carpeting beneath his feet. Nobody said anything. In the silence Fisk began slowly pacing the width of the office. The idea of profiling hacked bank accounts clearly appealed to him and he was not going to dismiss the topic until he had come up with an interesting hypothesis to test.

"Hmmm. Without going into details, would it be hard to test for an international connection?" he asked.

Without mentioning Rudy, I told Fisk that recent changes to the program made it easy to flag EFT's that cross national borders.

"Good," he said. "Let's pursue that Mr. Carter." Turning back toward me he asked, "what about analysis of the times of day that the millwright is most active? Perhaps we can determine what time-zone he is in by noting the time of day when there is highest mill churning."

"We can do that," I acknowledged.

"Let's not forget to take into account that the millwright might be a computer geek that keeps strange hours," Jonny warned.

I was intrigued now. Fisk was right. By analizing the forged EFT traffic in terms of international routes and time of day, we had a reasonable chance of determining where the millwright lived. We might be able to narrow it down to a particular country and a particular time zone. If we were persistent and whittled away at the problem, eventually BIF might reduce the problem enough that deep-throat would have a chance. It just might work.

Chapter 19

The following Monday at 8:15 in the morning Lisa and I were in the J. Edgar Hoover Building on Pennsylvania Avenue in Washington D.C. The meeting wasn't supposed to begin until 9:00 but neither one of us are the type that likes to cut these things close and if the people at this meeting were even half as important as Agnes said then it did not seem like it would be wise to keep them waiting. Not that I was at all sure that they would even bother waiting for us if we were late. That was another reason for being on time — I didn't want to miss anything.

Lisa and I had flown in together that morning. Our flight landed at National Airport at about 7:30. It was the earliest flight we could get out of Chicago.

Lisa used to have a friend that worked in D.C. and she had visited the city several times in the past so I left all the travel arrangements to her (I had never been there before). Lisa had no trouble finding the "Metro", Washington's name for the subway. Lisa informed me that my startled reaction to the cleanliness of the subway cars and the stations was typical of American tourists in D.C. I was used to the Chicago subway, which like any other American subway except the Metro, featured cars with the full spectrum of modern American graffitee, everything from hastily scrawled profanities to elobarate still-life painted with painstaking attention to detail.

Not only was the cleanliness of the subway system impressive, but it was nice to see that our nation's capital uses a token system based upon magnetic-strip cards. The cards can be purchased in nearly any denomination from vending machines. The rates vary depending upon how far one is traveling. Magnetic-strip readers at the turn-styles automatically debit the cards appropriately based upon the station of origin and the destination. I have no idea if they use any sort of cryptographic algorithms to thwart forgeries and tampering. Probably not. Even so, the system is fast and convenient; nice.

We took the "yellow" line to L'Enfant Plaza, a station where nearly all of the lines meet. There we switched to the blue line, which we took to Federal Triangle. Lisa explained that we could have picked up the blue line at the airport and avoided the need to switch trains, but it is faster to do it as we had because the blue line takes a very circumspect route from National Airport to Federal Triangle.

The Federal Triangle Metro station is underground, beneath 12th Street and Pennsylvania Avenue. I inserted my token card into the turn-style and it promptly popped out of the return slot with a soft *phlifft*. I followed Lisa up the escalators to street level.

We had no trouble finding the FBI building; it was clearly labeled as such with a large sign on the lawn. The building itself was on Pennsylvania Avenue between 9th and 10th streets, placing it near the mid-point between the White House on one end of Pennsylvania Avenue and the Capital Building on the other. As it turns out, the walk from the L'Enfant Plaza metro station would not have been any longer than the walk from Federal Triangle; we had been fooled by the name of the latter into believing it would be the closer of the two.

We had more trouble finding the conference room than we did the building. After receiving our visitor clearances Lisa and I spent several minutes wandering the halls looking for the room where the conference was supposed to be. We hadn't been given a room number and nobody had come out to escort us. I was a little surprised at the lack of escort, not because I expected better hospitality, but rather because I expected tighter security. We knew only that the meeting was to take place at 9:00 and was supposed to be somewhere on the third floor. We eventually met up with Jonny and he showed us to the conference room.

It was a mid-sized room with seating for about forty. The room was longer from front-to-back than it was wide, with a doorway near the front and a second door near the rear. We entered from the rear entrance. There were long tables that were fixed to the ground and ran nearly the full width of the room. The chairs were also fixed to the ground, but were free to swivel. There were about seven chairs per row and about ten rows. The front of the room had a wide empty space between the front wall and the first row of seats. Part of this space was filled by a lecturn positioned slightly off-center, closer to the left side of the room, where windows lined the wall. The room reminded me of the classroom where I had taken Complexity Theory at Princeton.

Most of the second and third row were already filled. Nobody had chosen to sit in the first row yet, and not enough people had arrived to fill more than two rows.

Lisa and I chose seats at the far end of the fourth row, near the windows. Jonny sat down with us for a moment but almost immediately popped out of his chair, excused himself, and hurried off to talk to a group of three men that had just entered the room through the door at the front. I recognized one of these men from television news reports; he was Louis Weld, the director of the CIA.

Louis Weld had been appointed CIA director less than a year previous, and already he was making quite an impression. All of the weekly news magazines featured quotes by Weld on a regular basis. Unlike past CIA directors, Weld maintained a very high profile and was quite outspoken about seemingly everything. I liked what I read about him. He was investing a lot of time and effort into re-tooling the CIA to accommodate the changing geopolitical scene following the collapse of the Soviet Union.

The room slowly filled, and as it did so, the buzz of the semi-hushed conversa-

tions increased. Jonny reappeared with a young man at his side. He introduced him to Lisa and I as Danial Smith, a computer operator at an X9.17 Key Translation Center managed by Chase-Manhattan. Jonny explained that a few of the Key Center operators had been invited to the meeting to provide any insights they might have from their perspective in the trenches of electronic banking. They, better than anybody else, understood the practicalities governing any effort to mount a counter-offensive against the millwright.

Danial Smith was young. He could not have been older than twenty-five. He was red-haired and had extremely fair skin. His face was lightly freckled. He appeared to be out of his element in his brown tweed suit and red tie. I was sure he did not normally wear a suit to work.

"Danial generally agrees with the technicians at Bendix," Jonny said pointedly.

"Something like this was bound to happen sooner or later," Danial said. When he spoke, he sounded even younger than he appeared. He had a high-pitched voice and a slight lisp in his speech.

"Maybe it has already happened a few times in the past..." said Jonny. He let the comment trail off and nobody replied immediately. He had a point; would any of us have heard about it if something like the money mill had happened before? Perhaps Jonny actually did have knowledge of a similar incident, but was barred from mentioning it.

"What do you do exactly?" Lisa asked Danial.

"I run the key translation service. Mostly that means that I make sure the machines stay running... lots of systems administration work."

"What Operating System?" she asked.

"Mostly Unix. We still do a little bit of work on mainframes. What Operating Systems do you use Ms. Cryer? Agent Carter tells me you are a programmer."

"Yes, that's right. I've worked some with Unix but most of my work is on Mac's. I prefer developing for the Mac, but that might be because the applications tend to be more fun. I try to stay objective about such things."

"In our business? Good luck. I haven't met anybody that has a balanced and objective position when it comes to Operating Systems or programming languages," laughed Danial. He dug his hands into his pockets. His hands were balled into fists. He appeared nervous for some reason. "Most of my programming is in Perl and other scripting languages," Danial offered, "what about you?".

"Mostly Smalltalk, but it looks like we will be switching over to Java soon," she replied. "The company that I work for makes educational applications for toddlers and preschoolers. Our original system, which is starting to show its age at this point, was implemented entirely in Smalltalk. Our next product is going to be web-based... hence the switch to Java."

As he and Lisa continued to exchange computer science banter, I looked around the room again. This was America's banking and cryptographic brain-trust that was being assembled. Would they be able to devise a solution to our predicament? News of my X9.17 discovery had spread quickly. The rapid

distribution of the news was the result of Agnes' hard work. I recalled her initial reaction when Jonny and I told her the news. Jonny had forced her to cancel a meeting already in progress so that she could hear my story. The cold glare of disapproval that Agnes had directed toward Jonny had slowly given way to a look of bafflement at first and then, as comprehension began to settle in, her attitude changed to one of excitement and enthusiasm.

"You've done it!" she exclaimed. "If we know how the millwright is getting his keys, then we are well on the way to cracking this case!

This praise and her glee over the discovery would have made me a lot more comfortable if she had not mentioned later in the conversation that it was peculiar that I was making all of these discoveries single-handed, despite the large number of cryptanalysts and computer scientists on the case. She credited me with discovering the mill in the first place, ignoring the contributions of Rudy Levinski and Lisa. She reminded me that I was the first one to realize that First Chicago was running a delay scam. And now it was I who discovered a flaw in X9.17. This, despite the wide-spread review that the protocol had received since its inception in 1985. A review process that included analysis by the world's best cryptanalysts. Agnes clearly did not include me in that group. The nature of my early involvement in this case would forever taint my image in Agnes' eyes. I will always remain a petty hacker, an upstart, and a nuisance by her assessment.

Actually, what troubled me most about Agnes' comments was that the same observations and accusations could be directed at Rudy Levinski. Hadn't he made several important discoveries? Many of the most significant contributions had been his. The additions he made to BIF were proving to be a major advance. Rudy was the first one to explore an international connection. I felt uneasy. I never should have accepted that disk from him. Where was he now?

Lisa poured a glass of water from the pitcher on the table and extended the pitcher toward me. I filled my glass and looked around the room. It was filling rapidly now. As I surveyed the room I decided that the chances of the entire case being cracked were good. The speed at which this meeting had been called and the feed-back I had already received regarding the key-exchange protocol, suggested that those in positions of authority were taking swift and expert action. I watched as a short heavy-set man wearing a dark suit approached the lecturn. Danial quickly left to join his own kind and everybody settled down into their seats. The room quieted quickly. The man at the lecturn was overweight enough that he looked uncomfortably warm despite the air-conditioning. His hair was thinning despite his relatively young age. He began by introducing himself and I learned that he was Frank S. Samuelson, head of the FBI. He pulled a handkerchief out of his pocket and patted his forehead as he spoke.

Mr. Samuelson explained that the purpose of the meeting was two-fold. First, we were to determine the extent to which the now apparent weaknesses in the EFT system posed a threat to United States national security. Second, we were to pool resources and develop a plan for immediate implementation that would identify and locate the culprits and apprehend them. He informed us that the people in attendance today represented the FBI, the CIA, the NSA,

DISA, the ABA, and "other knowledgeable people." I suppose Lisa and I fell into the last category. As I looked around the room I concluded that we were the *only* ones in the last category. It wasn't hard to guess who was from which agency.

The bankers were all in the fifth row, to my right (the seats immediately behind me were still empty). Templemeyer was among them. Apparently Rudy had not been invited, for I did not see him. The group was easily identifiable as ABA people from their dress — they looked like bankers. All of them wore light grey suits, and several of the suits were three-piece. Their ties were mostly yellow; those that were not were generally light colors. All of them had chosen to leave their suit-coats on, despite the fact that most of the other people in the room were in shirt-sleeves. If they were not bankers then my next guess would have been accountants.

Other than myself and Lisa, the NSA people were the only ones wearing casual clothes. I knew they were NSA because, like everybody else, they chose to sit with their own kind and I spotted Lorenzo and Mr. Little among them. Little and company had been the last to arrive and were seated near the back of the room.

The DISA group was easy to spot since they were all dressed in military uniforms. DISA is the Defense Intelligence Security Agency. They are a joint forces group that spans all of the defense units (army, navy, air-force, etc.). DISA is responsible for overall information security — both strategic planning and implementation. Curiously, the NSA falls under the authority of DISA, although I have no doubt that DISA takes orders from the NSA in all matters related to cryptography; DISA is left to address security matters that lie closer to physical security, I suspect.

Even the FBI and CIA were easily distinguishable, although I would have known which group was which anyway simply because I knew the FBI people and I recognized the face of one of the CIA (Weld). The FBI agents seemed to adhere to the stereotype of a spook more than the CIA did. The CIA agents had a bit more variety in their dress code, whereas the FBI might as well sell clothes in the basement of their headquarters; it looked as if they all shopped at the same store anyway.

My survey of the room eventually brought my attention back to Lisa and myself. It was at this point that I noticed that Lisa and Agnes were the only women in the room. Agnes must be a bit of an anomaly, being a female in a position of authority in a business still very much dominated by men. She handles it well. I was never consciously aware of her gender; never really stopped to think about it, until now. Suddenly I wondered if she had children. I realized then that I knew very little about her personal life. I suppose that is part of the reason she has risen to the level she has — she is capable enough that her gender never has a chance to become an issue.

My chair was jostled slightly from behind and I turned to see what the disruption was. It was Jonny, trying to slip into the room as quietly as possible. He mouthed an apology when our eyes met and took the seat directly behind. I was pleased he was back. With all of these spooks in the room I might need

an interpreter... or a diplomat.

Eventually Mr. Samuelson finished speaking. Much of what he had to say had been wasted on me for I could not keep up with the acronyms. Apparently the FBI has some sort of "initiative" called C3E that they are implementing in four stages. The first stage consists of training and re-educating the FBI work-force and is only now just nearing completion. The next three stages, to be implemented over five years, are the actual program. Apparently most of the other attendees in the room already knew about the program because Samuelson did not tell us what the acronym actually stood for until much later in the talk. It is 'Combating Computer Crime and Espionage'. Much of his talk detailed the FBI's (lack of?) progress in re-tooling to adapt to the rapid proliferation of computers and their use as telecommunications devices.

Samuelson asked for, and received, questions from the audience. There were one or two questions about the C3E program, all of them from the DISA contingent. The DISA people seemed to be at the meeting due to some bureaucratic necessity and not particularly interested in the issue at hand. Then, somebody in the CIA, a man in a beige sports-jacket and blue-jeans, with a yellow pencil in one hand and small spiral-bound notebook in the other (making him look a little like a journalist and very much out of place), asked if the FBI profile for the "hacker" included any international connections. Mr. Samuelson replied that technical details on the current status of "Case #228-CC/FFU-296" would be forthcoming in the presentations to follow. He actually rattled off the entire case number, as if we wouldn't know which case he meant, this despite the fact that he had no doubts about which case the questioner meant without that person citing the case number. This last question provided Samuelson with a nice seguey into the next presentation and he took advantage of it. He introduced the next speaker — another FBI agent — and stepped down from the lecturn, while patting his forehead with his handkerchief.

The next speaker was a young man with an athletic build, although he walked with a slight limp as he slowly made his way to the front of the room. I missed his name when Samuelson introduced him and he did not repeat it. He began with the profile. The FBI was still convinced that our adversary was a loner male computer geek with a PhD. They still believed that he was living in the United States. Two interesting changes in the profile were that they no longer listed him as a US citizen and that he was likely an employee of a bank. The speaker suggested that the subject might be an international graduate student at an American university or a permanent resident working for a US bank. The reasoning behind these changes was that the attacks were too sophisticated for an outsider, and they were no longer limited to domestic banks; counterfeit EFT's had been found that were directed to foreign banks. The FBI was concentrating on France, Germany, and Russia.

The speaker said that, despite the international scope, the FBI still believed that the subject was living in the States. Indeed, the FBI now suspected that the attacker was living on the west coast, probably California. Furthermore, there was some evidence that the subject was targeting American cultural icons. This suggested that the subject was either a foriegn national living in the United

States, or else an American citizen with strong political feelings against the United States.

This completed the latest update on the millwright profile. The speaker then went on to discuss other issues. He related the NASA syndrome that Jonny had discovered at the Bendix offices in St. Louis. This helped support the theory that the subject was an employee of a bank. If the millwright was working in the security department of a bank, then this might provide him with access to the X9.17 key-encrypting keys for that bank. Even if he did not work in the EFT or security departments, given the sloppy practices at some banks, an employee in good standing with the company would have ample opportunity to steal the master keys.

I only half-listened to this part of the talk. Jonny had leaned forward and was loudly whispering in Lisa's ear. He was recounting anecdotes from that St. Louis trip. This was not distracting so much as it was interesting. I found myself listening to their conversation instead of the speaker's far dryer coverage of the same facts. I did, however, catch a comment by the speaker saying that the President had been briefed on the entire money mill investigation and that he had requested that he be kept up to date with all new developments. This pleased me; nobody was taking this matter lightly now. There had already been enough down-playing of the incident early on: First Chicago executives had hoped to pin the blame on Lisa and sweep the entire affair under the rug; later it had appeared that Lampley and Levinski would take the fall; there were indications that I might be a scapegoat; Bendix had been working feverishly to shred documents and weather what they hoped was a brief squall; and Agnes had been reluctant to concede that the FBI needed assistance from the NSA. Now though, the matter had escalated up to the highest levels of government. Everybody recognized that we were no longer dealing with a high school phone phreak bent on impressing his friends with childish exploits of computer crime.

Next it was Weld's turn to speak. I was anxious to hear what he had to say. Everybody in the room seemed to lean a bit further forward in their seats and set down their pencils.

"Gentlemen, Ladies... let's step back for a moment and take a look at the big picture. What do we have here? What is the *potential* threat?

"I'm not asking how much money was stolen. Nor am I asking how much money we think might be stolen before this is over.

"I'm asking about the potential for harm to an international banking system we now know has security flaws at several levels. I'm sure our friends from the ABA will excuse me if I stipulate that the operations personnel at some banks have been somewhat blazé about certain aspects of security. I very much doubt that Bendix is unique. But putting that aside, far more importantly, we now know that the key management protocol has design flaws. We have seen the impact of these flaws. Have we seen the *full* impact?"

At this point Weld placed a viewgraph on the projector. The title of the slide read simply, "Scope." The slide itself had only one sentence on it. Actually, it was only a sentence fragment, and it read, "flaws evaluated in the context of geopolitical threat models."

Upon placing this slide on the screen Weld said, "my question is this: is anybody considering the possibility of a terrorist attack on the US banking infra-structure? I know that the FBI profile for the millwright and the recent money mill operations indicate a single person working for personal gain, but forget that for a moment. Concentrate instead on the larger problem. We have weaknesses in technical design, in bureaucratic procedures, in inter-department communications, and in banking procedures. So I ask again: what is the *potential* cost?"

Weld paused and slowly gazed around the room. He stood with both arms outstretched before him, hands resting on either side of the lecturn, leaning slightly forward. His eyes went from one person to the next, making eye contact with anybody that returned his gaze. Weld had not changed the viewgraph slide since putting up that initial slide asking about the threat potential. He had no need for slides; everybody had their eyes fixed on him. After surveying his entire audience Weld took a sip of water from the glass in front of him.

"Here's a hypothetical situation," he said. He had everybody riveted to their chairs and he knew it. I had been hoping for a chance to see why Weld was becoming somewhat of a celebrity and I was not disappointed.

"Suppose the actual attack hasn't even started yet. Suppose all we have seen so far are a few practice runs. Furthermore, suppose our 'attacker' is merely the computer programmer that engineered the attack on behalf of a larger group. What group? Oh let's say... the Iraqi government. Or even an extremist group within the United States such as the Patriots. The FBI has already told us that the group behind the attacks is probably opposed to our government.

"'But wait,' you say. 'All evidence we have indicates that the millwright is operating for personal gain.' True. But perhaps that personal gain is payment for a job well done in cracking the American banking network. Maybe all we've seen so far is the initial payment for a different attack. An initial payment and a test-run rolled into one. The real attack doesn't have to be a whole lot different from what we've already seen. It might be the same thing, only on a larger scale. Say... ten thousand times the scale. And why not? Surely it is a small matter of programming to step up the frequency of the bogus EFT's. The attackers wouldn't even have to increase the dollar amounts on individual EFT's. After all, using unusually high amounts might draw attention to the illegitimate EFT's. Remember, they probably don't know we are on to them."

I looked around the room to see how the others were reacting. Normally in a gathering like this there are two or three quiet conversations being carried out, either in whispered exchanges or on notes scribbled on a neighbor's papers. Not so here. Weld had everybody hooked.

"Or maybe drawing attention to themselves is not a concern. Does the Iraqi government care if we know they are the culprits after they have succeeded in bringing the American banking system to its knees? Do they care if we trace the origin of the attack back to a computer in Baghdad after they have declared war on a nation where every bank account has been altered and the economy is in collapse?

"Repairing the damage won't be easy. There will be secondary and tertiary

affects. I would expect a public reaction that puts the 1929 crash and all previous bank runs to shame. It took American investors forty years to recover from the 1929 crash. Maybe some of the bankers in the room can estimate the overall economic impact of a temporary but *massive* loss of integrity in the entire international banking infra-structure. I can't. But I have my suspicions. Thank you gentlemen."

Weld strode off the podium, sat in his seat, crossed one leg over the other, and sat facing the front of the room with his hands resting in his lap. I think everybody was caught be surprise by his abrupt finish. But then, there really was no need to say anything more. And, by way of a summary, his sole view-graph remained on the screen, asking that same question about seemingly small flaws becoming large when viewed in a different context. Weld's scenario, while perhaps unlikely, was certainly plausible.

Nobody took the podium right away. Nobody did anything right away. You could almost hear the collective breathing in the room quicken as the ramifications of Weld's argument hit home. Weld had delivered his message with very few pauses, speaking quickly and succinctly. Much of what he said was only now sinking in. Many in the room had come out of bureaucratic necessity and had not been terribly interested initially. Now these same people were itching to pursue the case with new fervor. Suddenly the FBI profile seemed short-sighted, and Weld's scenario did not seem far-fetched at all.

I glanced at Lisa, who had turned to speak to Jonny. Jonny was dumb-struck. After working on this case for weeks, it was not until this moment that he realized the nearly boundless importance of the case. I too had been sobered by Weld's comments. The fate of the entire world economy hung in the balance! I felt a dizziness wash over me. Moments earlier I had been pleased that people were no longer under-estimating the gravity of the situation; now I realized that I myself had under-estimated!

Ours is a society that takes for granted the comfort of a strong and reliable banking infra-structure. Runs on banks are a thing of the past, to be studied by children in history class. Individual investors are protected by the FDIC and scarcely pause to think about such matters. When we put our money in a bank, the only risk we even consider is the financial risk associated with the opportunity cost for that fixed-income investment *vs.* other investments. Yet the FDIC cannot save all of us if the banking infra-structure collapses. Who will save the FDIC?

Every day trillions of dollars pulse through wires and over air-waves. Hundreds of thousands of transactions are carried out electronically each day. The routing of pennies through the network is no less intricate than drops of water in a river system. The ACH, CHIPS, Fedwire, and other clearing houses form the main arteries in a world-wide network of rivers, dikes, reservoirs, brooks, and streams.

For some length of time — nobody is sure how long — money has been leaking out of the waterways. New feeder streams have opened. These streams form the millrace. Every day the millrace directs vast quantities of water over the wheels. More money pours into these accounts. The wheels turn faster.

Interest payments are made. Money is lost. Stolen. Nobody notices. The mill runs unabated. Continuously. Money is siphoned off, yet the overall volume of water in the system remains unchanged. The siphoned money is paid in the form of increased interest payments ground out by the rapidly spinning water wheel. Account balances are preserved. One successful mill builds confidence. Two mills build wealth. Three builds an empire. More mills destroy the world economy.

Without any way to detect the money mills, nevermind prevent them, we cannot even be sure how many are already running. If one millwright discovered the flaw and learned how to exploit it, why not two? Or two hundred? How close are we to a catastrophe? Is our wholesale banking system already a sieve? How can we know?

Chapter 20

Following the meeting in Washington D.C. it was decided that the money mill could not be permitted to continue. The risks were simply too great. The FBI and ABA had to stop the mill, at any cost. This meant that first and foremost the key translation server had to be shut down. This would stop the current string of thefts immediately. Of course a longer term solution was needed to prevent future attacks of a similar nature. The X9.17 protocol would need to be amended, but that could wait until after a careful review process.

I had briefed Rudy Levinski on the meeting early the next morning. He had left a handwritten note on my pillow while I was out of town. It made me somewhat uneasy to know that he had been in my apartment in my absence. Could I really trust him? What did I really know about him? Didn't he fit the FBI profile rather well? He is a loner. he is a bank employee working in the EFT department. He lives in the United States but is a foreign national, European even. This certainly fit the FBI profile.

Rudy was an enigma. Weather willingly or not, he had helped Lampley tamper with EFT payments on behalf of First chicago. Later he had helped analize the forgeries and had been the first to realize the workings of the mill. Yet he had done this only after Lisa and I had forced his hand. Now, he was helping with the case by providing us with valuable characterizations of illicit EFT traffic. His rules for the BIF program were proving quite valuable. There was reason to believe that his rules might finally break the case. Pretty soon we would be able to pipe the output from BIF into deep-throat and let it crunch on the graph. Lisa was about to install a new patch for BIF that might push us over the hump. This patch had potential. Also, the NSA had very nearly completed their parallel implementation of deep-throat. We just needed a little more time... more time to finish implementing the changes to the programs, and more time to let the computers crunch.

I still had not made up my mind how to deal with Rudy when Lisa and I arrived at Jonny's office the next day. It was early in the afternoon on a dreary day. We had trotted through a drizzle to cover the short distance from her car to the front entrance of the E. M. Dirksen Federal Office Building in Chicago.

Now, as we stood in Jonny's office, I was on the phone with Leon Anderson. Leon is a Federal Reserve Board staffer. He had called Jonny but was now

talking to me while Jonny and Lisa held a quiet conversation at Jonny's desk. Leon was explaining to me the bulliten that the Fed had sent to all banks that morning. Ironically the bulliten was distributed over the same data network that is used for EFT's. I had already read a printed copy of the bulliten; Jonny had shown it to Lisa and me the moment we entered his office. It now lay on his desk.

"Everybody," came Leon's gravelly voice over the phone. It was in response to my query about which banks had recieved notification of the shutdown. "The bulliten should have cascaded down through the entire EFT network by now."

"This is really going to grind the economy to a halt," I muttered. I masaged my face with the hand not holding the phone and absently watched Lisa giving Jonny a tutorial on C programming. The two of them sat on the other side of the room hunched over the latest listings for deep-throat. "The banks must be raising hell," I said into the phone. "Are any of them demanding explanations?"

"The banks are fine until the end of business today," he explained. "In fact some banks should be able to make minor adjustments before then."

"What do you mean?"

"They have a few hours. The EFT system will remain in operation for the remainder of the day. The service will be stopped first thing tomorrow morning..."

He went on talking but I was no longer listening. I felt a chill start at my head and work its way down my back all the way to me feet. I actually shivered. I felt dizzy. I turned to Lisa. My throat was dry and I had a hard time speaking the words that followed.

"It's not down," I choked out. "The announcement has gone out but it's not down. Everybody knows but *it's not down.*"

Lisa stared back, not saying anything. She backed up slowly to the desk behind her. She gently bumped into the desk and reached down with one hand to support herself as she sat on the corner of the desk. She understood my fear. Jonny didn't. He looked at me, then at her, and then back to me again.

"It's goin' down tomorrow, ain't it?" he asked.

"Not good enough!" Lisa snapped. "Not if everybody knows about it today." She slammed the desk with both hands and was on her feet. She turned to me. "Now what?"

I didn't know. Was it already too late? How could this have happened? What was Leon thinking? I felt my forehead become moist with cold sweat. What to do? I needed to talk to somebody, but who? Leon? I turned to Jonny.

"That server has to go down *now*! Who do we call?"

"Leon, I guess." He was still unconcerned.

No, I needed to call Daniel. Only he was in a position to take immediate unilateral action. Damn! I didn't know his number.

"Lisa, how do we get Danial Smith's number?"

"I have it," she responded. "You mean the red-headed sys-admin at the Key Center, right?"

She practically flew across the room as she hurried over to her bag. Tearing it open she began emptying the contents in a frenzy, creating a pile of her

belongings on the floor in front of her. She finally found what she was looking for and straightened with a red address book in her hands. She set it on the desk and began rapidly flipping through the pages. Meanwhile I still held the phone in my hand with the open connection to Leon. I hurriedly told him I had to hang up, without bothering to explain why. When Lisa found the number, she called it out and I dialed.

One ring. Two rings. Three. Four. It was the middle of the business day; *somebody* had to answer. Doesn't Daniel have voice mail?

"Chase-Manhattan EFT operations, this is Daniel," came the familiar high-pitched voice with the slight lisp.

"Daniel! Carl Raymond here. We met at the Money Mill meeting in Washington. Is the Key Translation Center still up?"

"Oh hi Carl. Yeah it's still up. Word is that it'll be up until the end of today and then that's it."

"But word has already gone out! Everybody knows we plan to shut it down. Including the millwright! Doesn't anybody realize that once we've tipped off the millwright he might react with an all-out blitz? And we are leaving him with about four hours in which to do it."

Daniel said nothing immediately, but Jonny was listening to my side of the conversation and he asked, "How much time would he need?"

Lisa answered before I could. "If he uses a script or a program he could completely hose the entire banking network in about ten minutes." Jonny blanched visibly.

"She's right," I agreed.

"Oh no!" It was Daniel's high-pitched voice on the phone. He couldn't be responding to Lisa because he could not possibly have heard her.

"Carl, you there?" Daniel asked.

"Yeah."

"We've got dozens of hits here. All in the last few minutes."

"What's a 'hit'? What are you talking about?"

Danial's voice was strained. "I... I... I'm looking at a dump of recent activity here for the Key Translation Center. Carl, the number of requests is way up. Way more activity than normal," he stammered. "Way more," he repeated. "It should be less than normal. Most legit banks have stopped using the center already."

I began shouting questions into the phone. "Who? Where are the requests coming from? How many? What banks?" Lisa jumped up and came over to stand next to me and put her ear near the phone. "It's happening," I said for her benefit, although she probably had guessed as much already.

I could feel a wave of panic threatening to sweep over me. I suppressed the feeling and tried to think. How far would the millwright go? What was his motive and how desperate was he? Were we witnessing the first tremors of the utter collapse of the world banking system?

Meanwhile the voice on the other end of the phone was silent. I stood waiting. I could hear the faint clicking of keystrokes on the other end.

"Everywhere, Carl," groaned Daniel. "The requests are coming from everywhere. And the number is up to about 150 now."

"Are all of the requests for the same ultimate recipient?" I asked.

It didn't take Daniel long to answer this time. "Doesn't look like it," he responded. "The requests are still coming in as we speak. It's up to 161 now! We gotta shut this sucker down! I gotta go. D'ya have anything else, Carl?"

"No. Go. Shut it down. Bye."

"Yeah. Later."

Maybe Jonny recalled Weld's words. Maybe panic is infectious. Whatever the reason, Jonny was waking up to the seriousness of the situation. He stood up and strode over to the desk. Leaning over he examined the bulletin again.

"We can't wait for Daniel to shut it down," I said. "By the time he gets approval it'll be tomorrow morning anyway. Either he is going to have to pull the plug literally or we are going to have to go straight to the top."

"Can he do that?" Lisa asked. "Is Daniel in a position where he can kill the power to the server? That might be our best bet."

We didn't have any time to follow bureaucratic procedures. Even a few more seconds might be too late. The millwright already had over 150 keys. I had been hoping that the millwright was only planning to dump massive amounts of money into his account and then withdraw the money and run, but Danial had said that the key requests were for many different banks. If he was collecting keys for every bank in the network, which is what I now suspected, then he still had a long way to go. Still, if I were in his shoes I would mount the attack before I was finished collecting the keys. He could run a cancer program at the same time he collected keys. Even 150 keys, while only a small fraction of the number of banks in the network, was enough to completely scramble account balances world-wide. Each of those keys gave him the power to fabricate and alter all EFT's between a different pair of banks. He could forge payments between hundreds of thousands of accounts. He wouldn't be maintaining constant balances now. The coming attack would not be a money mill — it would be an all-out cancer. This time he would be moving money all over the place at random and in random denominations. Money would be scattered pell-mell throughout bank accounts nation-wide, perhaps even world-wide.

At last Jonny swung into action. He was trained for crisis management and it now showed. He was calm and efficient as he picked up the phone and began placing calls. First he called Agnes and informed her of the situation — in about four sentences. That call was over before it even started and he was calling Fisk next. A moment later and he had clearance to contact both Samuelson and Weld. He placed both calls and in very short order had both of them convinced that the system had to come down immediately, even if it meant all banks had to close for the day, and Wall Street too.

Weld told Jonny that he would contact the President and Samuelson would contact the Chairman of the Federal Reserve as well as the Secretary of Treasury. Yet questions of timing still plagued me. Would we get authorization to shut it down fast enough? How long would the bureaucratic procedures take? Admittedly, Jonny had succeeded in five minutes to convince the top authorities

in the country of the gravity of the situation. But how long would it take for them to get word down to the operators in the field? I posed these questions to Jonny.

"It'll be a while," he admitted. "No doubt the President will want to discuss it before taking any decisive action. The same goes for the Fed Chairman. Both will be worried about the negative press that will follow from a drastic step like an emergency shutdown of the US banking industry. It is too late to merely shut down the server; the keys are already out. At this point we need to put a stop to all EFT traffic."

Right. That had not occurred to me. I was so pre-occupied with shutting down the server that I had not realized that the horses were already out of the barn. Shutting down the server now would accomplish very little.

"Do they know that?" Lisa asked.

"Mr. Weld was the one who pointed it out to me," replied Jonny.

I hesitated before asking my next question. I wasn't sure how to approach Jonny on this matter. Still, if the powers that be were really going to take as long as Jonny suggested then we had to do something. A program could forge and transmit hundreds of EFT's per minute. If the millwright was sending EFT's in parallel to collecting keys, then he may very well have sent out several thousand already. By the time that number got up into the millions it would be too late to unravel the mess. The only correction that would be possible at that point would be to turn back the clock and revert all balances to the levels from the day before. Any business carried out after this morning and before the correction, which would be tomorrow or even the day after, would have to be erased. Several days of economic activity would be wiped out.

"Jonny..."

I didn't know how to continue so I stopped. Jonny turned to look at me but said nothing, waiting for me to continue. After a long pause in which I remained silent, his expression softened a bit and he said, "it ain't going to be fast enough is it? We're in big trouble, huh?"

"Let me put it this way, I'm afraid that there is a chance that if you walked into your bank right now and checked your balance you'd be surprised. Perhaps pleasantly surprised. Perhaps unpleasantly surprised. But surprised nonetheless.

"It's only a slim chance right now — my guess is that only a very small fraction of the banking system has been infected — but wait another hour and it might be a very good chance indeed. There is a cancer in our banking infrastructure, and it is growing unchecked."

"The way I see it we have two choices," said Jonny. "We can let the President and his men deal with this in their way, knowing full well that they don't have a clue how fast this can blow up. Or, we can pull the plug now and deal with the consequences.

"I don't know about you, but I ain't gonna sit by and watch the entire US economy go down the tubes just because some loser with a computer saw us coming. Maybe we are chasing a ghost. Maybe not. I got only one question: what is he collecting those keys *for* if not to screw up the entire EFT network?"

There was no need to reply.

In the short silence that followed, Jonny once again turned to the phone. He reached Fisk and the two of them began to discuss contingency plans. Meanwhile Lisa turned to me. She reminded me of our optimism over the newest improvements to the filtering rules for BIF. At her urging I interrupted Jonny to say that there was at least a slim chance that BIF could find the millwright before he could do significant damage... *if* we did not have any bugs and *if* we could begin executing it on NSA hardware immediately.

Jonny handed the phone to me and told me to talk to Fisk. Before I could say anything, Fisk began speaking.

"Carl? You're a phone phreak; how hard would it be to sabatoge the communications at the world's biggest banks?"

"I really don't know. I only have tangential knowledge of phone hacking."

"Well, in a few minutes we are going to have to bring the EFT system to a grinding halt, by whatever means. If the President and the Fed don't clear the shutdown fast, then we will have to sabatoge the system. I will take responsibility."

Had the situation become that desperate? Suddenly I was not so sure. It is one thing to ask the president to temporarily shut down a key service, it is another thing altogether to deliberately sabatage the US banking system.

Exactly what the millwright intended to do with the stolen keys was still unclear. As of yet we still had not seen a single bogus EFT, nevermind millions.

Fisk said that he would take responsibility even if we were over-reacting, but would he? I had been set up to be the scapegoat once; I did not want it to happen again. What would happen if I sabotaged the phone system and then it was determined that the banks were never in real jeopardy? Bringing down the phones will stop the EFT's but it does nothing to help identify and apprehend the millwright.

On the other hand, did I really have a choice? If I waited until the millwrights intentions are clear, it would probably be too late. Once we see one bogus EFT, we will probably see billions.

Fisk was still talking. "We have no choice Carl. If we wait for each individual bank to respond then it will be a case of too little too late. You, of all people, must realize that we have to make absolutely certain that no banks can exchange EFT's.

"You and Lisa go and do whatever you need to do to run the new program. Fast. If that doesn't work, then I want you to stand by for instructions from me. I'll get our top specialists on wire-tapping and electronic surveillance; together you guys will have to figure out a way to crash the nation's phone system."

I gulped, deferred, and gave the phone back to Jonny. Without bothering to tell Lisa about Fisk's still half-baked and wreckless "plan B" I turned for the door and motioned for Lisa to follow.

Deeming the elevators too slow, I took the stairs, three at a time, down to the ground floor with Lisa clamoring down behind me. I explained to Lisa where we were going between gasps for air as I ran. We needed to get back to my apartment. That was where I had left the data tape with the latest patch for

BIF. We ran across the wet pavement to her car. Lisa had automatic door locks and the doors were already unlocked by the time we reached the car. We tore the doors open and threw ourselves into the seats. She had the engine running before I had my door closed. The park brake was situated between the two front seats and she told me to release it as she threw the gearshift into reverse. No sooner had I released the park brake than the car rocketed backward and swung around in a tight arc until it was facing the exit of the parking lot. Lisa didn't stop to look for other cars; into first gear went the gearshift and out of the parking lot went the car, with the wheels squeeling in protest. We sped down the street, heading toward Jackson Blvd. There Lisa careened around the corner, swinging dangerously wide and over the curb as she turned left. After correcting her steering she slammed her foot down on the gas and sped east on Jackson.

Other cars on the street seemed to be stationary relative to the speed of our own vehicle. Lisa bobbed and weaved between cars, never using the brake. She pushed down hard on the accelerator, urging the car to go still faster.

I was glad Lisa was driving. Had I been driving, and driving the way I normally do, we would not have made nearly as much progress. And had I been driving, and driving as she was, then we certainly would have ended up in a ditch or through a store window.

The rain had stopped, and for this I was grateful. It had been a heavy rain, and the streets were still very wet, with standing water in places. Visibility was perfect, however, for the rain had washed away the haze that had been in the air earlier in the day. The sun was even breaking through the clouds in places. Or were the flashes of light blinding my eyes not sunlight but rather visions of the after-life dancing before me as Lisa continued to push the car beyond engineering tolerences? She careened around the corners and flew down the straights. The wheels squealed and the engine whined. I was buffeted in my seat, first against the doors and then against the straining seatbelt across my torso.

When we joined the traffic on Michigan, Lisa was forced to slow down, but only slightly. Traffic became heavier and Lisa was having some difficulty weaving. We should have taken Columbus instead. I looked at my watch. Already ten minutes since we left Jonny's office. The car in front of us was moving slowly and we were penned in by another car on our left. A motorcycle on our right kept pace with our car, leaving no means of escape. The feeling of helplessness was unbearable. Lisa honked, but there was no noticeable affect. Something needed to be done. I swallowed hard, dreading what I was about to suggest.

"Lisa, we've got to pick up the pace," I said. "If there was ever an emergency, this is it. The world economy is in jeopardy. What difference does it make if we commit a few minor traffic infractions?

"Don't stop for any more red lights. Go through the intersections as soon as you can without colliding with anybody. Drive on the sidewalk if you have to."

She didn't respond immediately, concentrating instead on avoiding the yellow cab on the left and the motorcycle on our right. She veered away from the

motorcycle, sent the cab-driver in a panic to his left, and managed to miss both by inches as we screamed into a small gap that had opened between the cab and the car immediately in front of us.

"Right," she said. "Hang on."

I had never let go. It was then that I noticed that I still held the park brake handle in my left hand. My right hand was clenched to the door handle. My feet were firmly planted on the floor. I was bracing myself in the same position I'd been in since we left the parking lot.

"I'm ready," I lied.

She took my suggestion to heart and swerved sharply to the right, cutting across two lanes and darting between two cars parked along the curb. Lisa slowed only slightly as we bounced over the curb and up onto the sidewalk. Pedestrians scrambled to give us a wide margin as Lisa maneuvered to avoid sign-posts on our left and pedestrians on our right. I could see a blur of astonished faces flash by my window as we hurled down the walkway. Everywhere I looked people were pressed up against the fronts of buildings in an effort to give us every inch of sidewalk possible.

In the seat beside me Lisa was pressed up against the steering wheel. Perspiration formed on her furrowed forehead as she concentrated on maneuvering the vehicle down the tight corridor with parked cars on our left and buildings, stoops, and people on our right. She squinted through her eyes with her neck craning forward, as if straining to catch a glimpse of each oncoming obstacle moments sooner than she would have otherwise.

I pressed my eyes tightly shut, not wanting to see any more. I would have covered my ears if only I had been willing to release the strangle-hold both of my hands had on the door handle. I tried to project my thoughts to someplace else... someplace serene. It didn't work. As the car veered to the side, spurted forward, slowed abruptly, and then veered again, I was forced to acknowledge that I was in a car vaulting down a sidewalk with pedestrians scrambling for safety while the world economy was dissolving into nothingness. Fiat money cannot exist without tokens and without accurate records. Electronic transfers reduce the reliance upon tokens and the millwright was in the midst of destroying all accuracy in records. I pressed my eyelids together tighter.

Then, suddenly, the car came to a full stop. I heard the driver's side door open and then shut. Slowly, carefully, I opened my eyes and looked around. Lisa was trotting back toward the car.

"What's the matter?" she called through the window. Her forehead was furrowed in puzzlement. "Aren't you coming? Let's go! C'mon!"

"I'm right behind you," I muttered in a silly effort to hide my confusion and bewilderment. Together we ran to the building and down the hallway to my apartment. I hurriedly unlocked my door and pushed it open. Lisa went in ahead of me and immediately turned toward my primary machine. I went straight to the phone. I called Lorenzo Thomas at the NSA. We needed to get the latest source code for BIF to Lorenzo so that he could execute it on the NSA computers. Does the NSA really have enough computing power to solve daunting computer problems in minutes? Can they really crack 56-bit DES is

real-time? Can they actually solve NP problems? I sincerely hoped all of the rumors were true.

Lorenzo had already been briefed and was waiting for my call. I told him that we would send the files via the Internet as soon as Lisa had them loaded.

"You'll never get it through our firewall," said Lorenzo. "Our packet filter blocks any incoming traffic, including e-mail, except stuff that has been cleared ahead of time. Hmmm... Maybe we can set it up on this end so we can use ftp. Do you have an anonymous ftp server on your machine?"

I groaned. I didn't. My machine was not set up to provide any network services to outsiders. I use it mainly as a client to other Internet servers. There was silence; nobody had any ideas. Now what? Then Lorenzo asked, "Where are the files? Are they still on the tape?"

"Yeah."

"OK, gimme your IP address. I'll go in and pull them off myself. Is the tape in the drive?"

Huh?

"You there?" Lorenzo asked impatiently. "Just tell me your IP address. Come on, hurry."

"172.16.104.23"

"OK, leave the tape in the drive," he said. "I should be able to get in and pull the files out directly."

"Uh... Lorenzo? I have a firewall here too," I said.

He chuckled. "Well, we'll just have to see how good it is won't we?"

He hung up the phone before I had a chance to say anything more. I turned to Lisa. "He's going to try to break in. I don't know how long that is going to take, or if he can even do it."

"We don't have much time," she said. "We should start taking down the firewall."

We immediately went to work. Lisa had already walked into the bedroom to the bastion host and was sitting at the keyboard. I leaned over her shoulder and typed in the root password at the login prompt and we went to work. There was no time for careful flushing of logs and a proper shutdown. The important thing to do was disable all the packet filtering rules. My router is set up so that in the absence of any filters it denies all packets; it would not be easy to configure it to accept everything. Editing filter rules is always a time-consuming and aggravating task, not quite as bad as working with sendmail config files, but almost. Lisa dumped the rules to the screen and the two of us leaned forward, craning our necks, to study the screen. How could we open up the flood-gates with minimal changes? The easiest thing to do was drop all the rules and then add a single rule that explicitly permits all incoming and outgoing packets on all ports. We had to be careful though because presumably Lorenzo would be trying to get in soon; if we deleted all of the rules first and then worked on adding the new rule, the router would not permit *any* packets during the interem.

I glanced at the clock icon in the upper right corner of the screen; it was 3:12. I grabbed a pen and began to compose the rule we would need. It would

have to permit connections on any port and from any Internet host.

Just then the tape drive pulled itself out of power-saver mode. No sooner had the fan reached full power than the tape itself began to rewind.

Whhirrr... klunk, whheee... klunk, whhirrr...

The tape was advancing a short distance, then rewinding, and then repeating.

"Is that you?" I asked Lisa.

She just stared at it, her mouth drooped open, her hands no longer moving across the keyboard. Neither of us said anything for a moment as we both looked at the small cream-colored box of the tape drive, with the green status light blinking.

"Lorenzo..." whispered Lisa, in a hushed tone.

Of course! He must have gotten in. So fast? We hadn't even dismantled any of our firewall defenses yet. We both ran back over to my primary machine.

"Do a 'ps'," I said. "Find out which TTY he's using."

Lisa had already typed in the 'what' command before I had said this, and the output was now on the screen. The only user runnning 'tar' was 'root'. Lisa and I both laughed.

"It's him all right!" exclaimed Lisa. "Where is he putting the files? Do you think he has he gotten any of them off the tape yet?"

As she asked this she ran the 'ps' command with various command line switches so as to get a full read-out of the 'tar' command that Lorenzo was running. The files were being dumped into '/tmp/mmp'. We also saw that Lorenzo was using ftp to move them back to the NSA.

My head began to swim. I didn't have ftp on my machine! Yet there it was, already running. Lorenzo must have down-loaded a version from the NSA and compiled it on my machine. Lisa was checking some of the Internet packets going through the router. She announced that the new BIF files were already being ferried off our machine and were bound for the Internet.

I was flabbergasted. In the space of less than five minutes Lorenzo had managed to break through my firewall, compile and install his own version of an ftp server, pull the files off the tape, and begin sending them to the NSA. It was at that moment that I learned to never underestimate the capabilities of the NSA. These guys operate in a whole different league.

Lisa turned, saw the expression on my face, and burst out laughing. Her laughter became almost hysterical as she put her hands on her stomach and leaned back in her chair. "That's some firewall you have there Carl," she said after she had caught her breath.

Already the tape drive had stopped. Another 'ps' revealed that the ftp transfer had stopped as well. Moments later we saw that root had logged out; Lorenzo had what he wanted.

The phone rang. It was Lorenzo.

"I've got somebody installing the patches now," he said. "There has been a change of plans. Fisk wants you back at the FBI offices. He said something about a contingency plan. You two should head back immediately. I'll get in touch with you there."

We wasted no time in following this suggestion. This time Lisa kept the car on the street, but that seemed to be the only constraint she was operating under in her effort to minimize travel time.

When we reached Jonny's office he was still on the phone. He cupped his hand over the mouthpiece and quickly brought us up to date. The translation service was still running. The President, the Chairman of the Fed, and the Secretary of Treasury, had all been briefed. Danial had prepared the machines for rapid shutdown; all he needed was voice confirmation from the Fed Chairman. FBI agents were on alert in every major city in the US. Friendly foreign intelligence agencies had also been informed to stand by. Meanwhile, the Key Distribution service (as opposed to the Key Translation service) had already been disabled. All banks had been notified not to even attempt to use the distribution center. This meant that the millwright could still collect keys from the translation center but couldn't distribute his keys by impersonating the distribution center. Of course this also meant we had tipped our hand to an even greater extent.

A second phone rang on the other end of Jonny's desk. It was Lorenzo, asking for Lisa. She took the phone as both Tony and I looked on. Other than noticing that her jaw was tightly clenched and that her eyes burned with fierce intensity, I could not read her expression. Was it good news or bad? Had they succeeded in installing the patches? Did the new program run without dumping core?

"You should run it with the -v2 option," Lisa said. Good, it sounds like they have it properly installed and are ready to start running it. With the computing power of the NSA it shouldn't take long to execute. I was a little puzzled that Lisa recommended the v2 option though. Wouldn't it be better to run it without the slower rules first? Better to get a rough result quickly than to take the extra cpu-time to try to pinpoint the culprit.

"I wouldn't," Lisa replied to some question from the other end of the line. "Really? Ha!"

This was getting frustrating. I was just about to ask Jonny if there was another extension we could listen in on when Lisa hung up. She turned to us and announced that they had found the millwright! "And," she continued with delight, "the millwright is a 'she' not a 'he'."

"They've already arrested her?" Jonny asked, taking no time to adjust to the new pronoun.

"Not yet, but the FBI has been instructed to make the arrest. Her name is Susan Ignassi. She works for an Oakland branch of Fourth Nationwide Bank of California. The FBI already has a signed warrant; her arrest is immenent."

Chapter 21

I would have liked to have slept in the following morning but that was not an option. I was awakened at 6:30 by the telephone beside my bed. It was Fisk's secretary, informing me that I was to report to his office at 8:30. That left me just enough time to pull myself out of bed and prepare a quick breakfast before walking down the street to catch the bus to downtown Chicago.

As it was, I was late, arriving at the FBI building at close to 9:00. Still bleary eyed, I mumbled my name to the receptionist and was escorted without comment to a large conference room at the end of the hall. I still had not fully recovered from the previous day's mad dash across town with Lisa at the wheel of her off-road Mustang convertable.

Nobody seemed to notice my tardiness, as a large number of people had been requested to attend the debriefing and many of the others were late too. Lisa was already there by the time I had arrived however. The attendees included all of the people that had been at the meeting in D.C. Rudy Levinski was there, sitting near the back. I later learned that each and every person that was aware of the money mill was in attendance, with the exception of the President and his cabinet. The main message that was conveyed at the meeting was that no part of the entire incident would be released to the public. Anybody who leaked word of the the EFT crimes to the press would be treated in a manner in accordance with the importance of the secrecy of the entire affair. Nobody dared to ask what this meant, especially me. I feared that I would be the prime suspect if there were a leak. Everybody knew that my involvement was not due to a professional obligation nor my political stance. Or, to be more accurate, my involvement *was* due to my political stance on computer security, but that initial involvement was more closely related to the crimes rather than the shutting down of the mill. I said very little during the entire debriefing, speaking up only when Samuelson stated that we had entered a new era; law enforcement can no longer preserve public safety. This sounded too much like a lead-in to the argument for key escrow. It was at this point that I interjected into the proceedings. Far from being cause for trepidation and consternation, the shift to electronic banking should be reason to be optimistic. If deployed carefully and responsibly, digital messaging systems and Electronic Commerce can be far more reliable than more conventional means of conducting banking

and business. With digital commerce, we have a theoretical basis upon which to pin our confidence.

Digital signatures are unforgeable without access to the private key. The private key can be stored on tamper-resistant smart-cards such that nobody — not even the cardbearer — can read the key off the card. The signing functions are implemented in hardware on the card. Modern public-key cryptography can be used for key-exchange in a way that avoids the sort of attack used to run the money mill. Indeed, in the modern era of cryptology, there is little justification for continued use of shared-key key-exchange protocols such as X9.17. It would behoove the ABA to give serious consideration to a public-key-based protocol for key exchange.

To further avoid future trouble in the EFT network, the member banks should employ secret-sharing procedures. Secret sharing is similar in concept to the procedures for launching nuclear weapons where two officers must simultaneously insert physical keys into keyholes on opposite sides of the room. The idea is that neither officer can unilaterally make the decision to launch; it requires the full cooperation of both officers. Cryptographic key-sharing divides a key into several parts and entrusts different people with each part. Knowing only one part of the key is of no practical value toward the reconstruction of the key. Secret sharing is based upon strong cryptographic theory, enabling cryptologists to prove with mathematical rigor that knowledge of only a limited number of key-shares is useless. Not only would this have prevented Susan Ignassi from causing all the trouble she did, but even a renegade bank president would be unable to obtain his own bank's master key without the cooperation of other officers of the bank. Susan Ignassi was able to learn the key-encrypting key used by Fourth Nationwide Bank of California because of her position as a manager of the security department. Agent Jonny Carter had diagnosed part of the problem correctly; Ignassi provided compelling evidence of the danger of the NASA syndrome in international banking. Without secret-sharing procedures to eliminate the possibility of any one individual learning the entire master key, the banking industry is vulnerable to dishonest security officers. Combined with the sloppy procedures and lax attitudes in these same banks, it appears that Susan Ignassi is not an anomaly.

Digital signatures and secret-sharing are not the only recent advances in cryptology. Zero-knowledge proofs make it possible to establish that a remote party knows a secret without either party ever divulging to eavesdroppers what that key is, all without the use of encryption! These only touch upon the surface of the tremendous volumes of powerful new information-sharing and information-protection features that are now achievable using modern cryptography. We live in an era with great reason for confidence. Ours is a time of exciting potential. Information is something to be held sacred. There is no pursuit more noble than the pursuit of knowledge and information. Key-escrow and export limitations on cryptographic tools only hinder the free exchange of information over public networks.

All of this assumes that strong cryptographic tools are used. Fortunately, such technology is available today. Very strong encryption algorithms are widely

known and easy to implement. Admittedly, perfect security is not obtainable, but very good security is. We live in a time where the cost of security grows at a rate similar to a logarithm function. At relatively little expense it is possible to deploy very tight information protection. Additional dollars beyond that initial cost have a low marginal return. The result is that even small enterprises can implement strong encryption and only extremely powerful entities, such as the NSA, can develop encryption algorithms that are significantly stronger than the status quo.

Development of good cryptographic protocols is a different matter. Unfortunately good protocols are closely tied to the applications they serve. This makes it harder to deploy them widely and defray costs. For this reason the weakest component of most cryptographic systems is the protocol. It is not surprising that the money mill exploited a weakness in X9.17 and not a weakness in DES. DES has been submitted to more extensive analysis and has been field tested in far more systems than has X9.17.

The solution is two-fold. First, a basic level of protection should be built into infra-structure. There is no reason why we, as consumers, should accept insecure digital communications. Every cordless phone and cell phone should support encryption. The Internet should have strong authentication and privacy. Phone cloning and eavesdropping are preventable. IP spoofing is preventable.

It is absurd for phone companies to spend millions to monitor cell-phone traffic and discontinue accounts with sharp changes in calling patterns. It would be far better to spend *less* and actually *solve* the problem.

Second, we must recognize that the supply of cryptographic products is market driven. Until consumers recognize the need for better protection, and until consumers learn to distinguish true protection from the silly platitudes of companies like Pseudo-One, we will continue to get the same slip-shod systems. It is time to start paying the developers and stop paying the insurance companies and those in the legal or law enforcement professions. The tools and technology are available to *prevent* hacking; let's start using them. No longer must be live with the threat of another money mill or a disaster of the magnitude of Weld's hypothetical scenario. Internet E-mail can be elevated to a status better than that of a simple postcard. We should not have to change cell-phone numbers every few months.

To use strong encryption we have to be willing to pay for it. The principal cost is protocol development and protocol analysis. Excellent encryption programs are cheap (even free) and readily available, but current market research leads all but a few companies to opt for off-the-shelf solutions that either use a protocol originally intended for some other purpose, or else use a half-baked protocol developed by novices. Due to the extreme sensitivity of security properties in cryptographic protocols, a solid off-the-shelf cryptographic protocol is very nearly a contradiction in terms. The money spent on development of a security protocol should be proportional to the size of the threat. Lisa, Rudy, and I were able to detect the mill in a week. With the help of the NSA, the FBI, and the Information Security departments of two banks, we were able to crack the case and arrest Ignassi in less than a month. This is good evidence

that the X9.17 flaw that made the mill possible was avoidable. In one night of analysis I discovered the flaw. Had the ABA recognized that protocols are the single most likely point of failure in a cryptographic system, and had they put an appropriate emphasis (e.g. time and money) into design and analysis of X9.17, then the flaw would have been discovered early on and it would have been repaired before any thefts were carried out. Our banking infra-structure was on the brink of collapse not because the flaw was too subtle to be found ahead of time, but because those in a position to do so did not appreciate the likelihood that such a flaw might be there to be found. I have no doubt that next time they will be more careful.

Even after it is repaired, it is important to recognize that X9.17, like any cryptographic protocol, is very sensitive to the trust model and the operating environment. X9.17 was designed for wholesale banking. Using it for any other purpose requires careful analysis to validate it for the new purpose. If X9.17 is used in an environment where there is open hostility between some members of the network, the flaw that made the money mill possible becomes even more ominous. The design specifications for X9.17 state that key exchanges between parties A and B should be protected from tampering and eavesdropping by C, even if C is a legitimate member of the network. Because of the flaw, this property does not hold. Luckily, the protocol appears to protect key exchanges from entities outside the network (i.e. you and me). Susan Ignassi was an insider and already had legitimate access to the master key for one bank in the network.

I am troubled when I see a protocol that was designed for one purpose being deployed for an entirely different application. The 1992 NIST recommendation that X9.17 be used for *all* government applications is unwise. Such recommendations should be made only after a very careful study of the protocol... the sort of study that surely would have uncovered the money mill flaw. The use of X9.17 in DES modems is questionable for the same reasons. The argument that "it is good enough for banking applications so it must be good enough for your applications" does not hold water. With such careless attitudes we were lucky the mill had not been even more damaging. We are lucky that Weld's scenario remains hypothetical.

My attention returned to the meeting when somebody asked Samuelson what would become of Susan Ignassi. Samuelson explained to the audience that she would be fired for misconduct and accused of international banking crimes. The FBI was seeking, and expected to get, a plea-bargaining arrangement so that the case would not go to trial. Allowing the case to go to trial would make it difficult to suppress the extent of the EFT counterfeiting and the possibility of economic catastrophe that was very nearly realized by Ignassi's crimes. The US government was unwilling to allow this to happen, and had the support of numerous other governments.

As it turns out, the FBI profile was not far off the mark. They had erred only in failing to consider that the millwright might be the mother of the man for whom they had developed their profile. George Ignassi was the son of Susan Ignassi. George, who was 29 years old, had a PhD in Number Theory and

studied cryptology at Rice University. His undergraduate degree in Computer Science was also from Rice University. Single and living in San Jose, George's social life fit the FBI profile of a computer geek. He had few friends and tended to spend most of his free time alone in his apartment playing with his computers. He worked for a small computer security company that sells DES modems.

It was George that discovered the X9.17 flaw and told his mother. At first Susan tried to alert her superiors of the flaw, but she was met with warnings that if she wished to continue to work in banking security it would be in her best interests not to stir up trouble. The banking industry was far too heavily reliant upon X9.17, she was told. Revisions to the protocol are a slow and tedious process. Susan's superiors explained that by informing them of flaws, she was doing the bank a disservice, for now Fourth Nationwide Bank of California could not claim ignorance of the flaw in the event of a lawsuit.

For several years Susan did nothing more about the flaw. Apparently, George too, did nothing. But when George lost his life a year ago in car accident, Susan's attitude about many things changed. It had been raining heavily when George's Geo Metro was struck head-on by a Dodge Ram, but rain was not the cause of the accident. The driver of the Ram was charged with Driving Under the Influence. He was not charged with involuntary manslaughter. Evidence that George may have been speeding, as well as the high standing in the community of the defendant, quickly quieted state prosecutors who might have otherwise pressed more zealously for manslaughter charges. The driver of the Dodge Ram was a popular sports figure and had already expressed remorse. Susan had been in attendance the day the hockey hero limped into the courtroom for his DUI hearing. His left leg was still sore from the accident. There was some concern that he might not be ready in time for opening day later that month. Team officials said that he would be 100% for the playoffs.

When the team made the playoffs eight months later, Susan did not watch. She never watched another hockey game after the accident. Alone for the first time in her life, Susan had no parents, no husband, and no son. The digital money mill was devised during the hockey playoffs that year. The mill was in operation just five weeks later. It was motivated partly as a tribute to the discovery of her late son, partly out of bitterness toward her superiors, and partly out of selfishness.

She seeded the mill with money stolen from the accounts of several hockey teams. Later she went after other sports teams. She was able to run the mill for a full year before anybody was even aware of its existence. Then, after twelve months of gradual escalation, her downfall was brought about by the serendipitous concurrency of three seperate attacks on the EFT network. By that time the millrace had spread to include numerous individual accounts in nearly every bank in the network. And yet no alarms were triggered. Nobody noticed the thefts, for no individual person or institution was disproportionately harmed; money was created in the form of interest payments on a massive number of negligible loans... surrepticious loans.

The FBI estimates that Ignassi was accumulating about $300 a day in interest payments. Nobody is sure, but the FBI believes that over the lifetime of

the mill, the cumulative thefts amounted to nearly $250,000, with most of the money aquired in the last three months.

Samuelson informed us that Susan Ignassi would not be going to jail for her crimes (a trial would make it impossible to bury the incident). This did not give me satisfaction. Her sex was not the only attribute of Susan Ignassi that did not fit my mental image of the millwright. I had envisioned our adversary as the very embodiment of evil. Now, far from being a devious and sinister member of the under-world, Susan Ignassi was an unhappy widow with no surviving children. Pilfering pennies out of the bank accounts of countless innocent people had been her way of lending credence to the unheeded warnings of the son she lost.

I could not help but feel empathy for this woman I had never met... and never will meet. Samuelson had pulled me aside before the meeting and told me that the government would appreciate it if I refrained from any communications with Susan Ignassi. He said that while the FBI now realized that I had not played a part in the money mill, they would not be disposing of my file. He said that my "liberal political stance and tendancy to play computer hacking games" were sufficient cause for the FBI to continue to keep tabs on me. He did soften this message with a faint smile and a congratulatory handshake for the uncovering of the money mill.

The FBI was not the only agency in my own government to treat me with with a dichotomous mix of distrust and friendship. My friends at the NSA thanked me for my services by confiscating my machine. They had already removed it from my apartment by the time I got back from Jonny's office the day before. This seems to be the reason Lorenzo directed Lisa and me back to the FBI building after we gave him the updates for BIF. Apparently the FBI got court approval to enter my apartment at the same time they got approval to arrest Ignassi. They weren't taking any chances that Lorenzo had left some inadvertent tell-tale evidence of the manner in which he broke through my firewall. Lorenzo must have used some top-secret methods that the NSA does not want leaking out to the public. There isn't much point in protesting; I don't have any room to negotiate. The NSA reminded me that everything that had occurred in the last month goes in the "never happened" category. The strange interruption to international banking that occurred on July 31st was blamed on a computer error at a key exchange center. There was no mention of any wrong-doing. In fact, when one TV station inquired if there had been any thefts that may have been caused by the computer error, the ABA released a strongly worded statement claiming that no money was stolen from any accounts and that no funds were in jeopardy at any time.

The backlog of funds transfers that would normally have been sent on July 31st were sent the next day instead. All banking activity returned to normal. The only difference is that the Key Translation service for X9.17 is no longer offered. All banks must use the Point-to-Point Environment or the Key Distribution Environment. Those banks that had been using the Key Translation Environment were forced to switch over to the Key Distribution Environment. Since the key distribution service places no additional operational requirements on the participating banks, this is an easy switch to make and even these banks

were able to resume normal EFT operations the next day. The public would remain forever oblivious of the peril that the banking infrastructure had suffered just days before. The United States had been brought to the brink of economic collapse. People that just days before had stood at the precipice and witnessed the near-plunge, filed slowly out of the room. The debriefing was over. There were only fifty of us, not counting the President and his cabinet. And it would remain fifty forever more. This was the theme that was emphasized most heavily in the debriefing: tell no one. Not ever.

As I walked out of the debriefing room with Lisa, neither one of us spoke. The meeting had ended on a somber note. We had been the first to leave, exiting quietly and promptly after the meeting concluded. While I considered several of the people in that room my friends, I was not sure I wanted to play in their world. Too dark, sinister, and secretive. Lisa and I walked down the empty hallway side by side. Lisa pushed the button to summon the elevator. The elevator doors opened and we stepped in. Lisa pressed the button for the lobby. The doors shut. She heaved a great sigh. "I want to forget everything and everybody from the last month," she said. "If I never see another FBI agent in my life I'll be happy... although Jonny was kinda cute," she added with a smirk. Then her face contorted back into one of of complete exhaustion. "It has been exciting, I must admit. Nonetheless I'm glad it is over."

As we stepped out of the elevator I suddenly realized that it was indeed over. Lisa and I would be going our separate ways. Apparently she was in a hurry to resume the life she was living a few weeks prior, before I interfered with her financial transactions. We had come together due to a coincidence: hers was one of the accounts that the millwright had selected on July 11th; and it was on that same day that I decided to study EFT error-handling procedures at First Chicago. Now, that which had brought us together was resolved.

"I guess this is it," I offered.

"Yup. Finally! Now everything can return to normal," she replied.

Yes, normal. The last few weeks had been wild; it would take me a while to settle back into my old routine... I was going to miss her.

"It was nice meeting you..." I let the words trail off.

She cocked her head to one side and adjusted the flap on her collar with her left hand. I tried to read her expression but couldn't. Was she sorry to be saying goodbye? Her comments and attitude in the elevator would lead one to believe that she was all too happy to part ways.

"Well..." I didn't know what to say next. I took a few steps toward the door.

"Uh... Carl," she said. "Where do you think you're going?"

"Umm... I dunno."

The corners of her mouth twitched upward in a hint of a smile while her eyes sparkled with obvious amusement. She stepped closer. Her hand slipped behind my head and her fingers slid up my neck and into my hair. She gently brought my head down to hers. Her lips gently brushed against mine. They were warm, her breath warmer still. I reached out and wrapped my arms around her midriff.

She pressed her abdomen against mine; I hugged her tighter. Her flesh was firm and yet it welcomed the pressure from mine. Her breathing came faster.

Ding!

The elevator doors parted wide. I felt Lisa's frame stiffen as she straightened up. I ungrasped my hands and let my arms fall away from her waist. She busied herself straightening the front of her blouse. A man I did not recognize stepped out of the elevator, glanced in our direction, nodded his head slightly, and walked on by and out the revolving door. Lisa looked up at me and smiled sheepishly.

"Well, where are you headed Mr. Hacker-Cracker?"

I didn't know. I had no plans; I had not looked ahead beyond the resolution of the money mill.

"Uh. I'm following you... umm... wherever you go."

"In that case, you're heading to Carl Raymond's apartment," she said. "He is a good friend of mine... one that I would like to get to know better."

We walked through the revolving door together and out into the sunlight. It was early August in Chicago. The sky was cloudy but bright; it looked as if it might rain but it was more likely to remain clear. A gentle breeze kept the temperature in check.

Months later, far away, an electronic signal was racing through a phone wire, up a satellite link, back down, and through a T1 line into an X9.17 Key Translation Center in Atlanta. The signal was interpreted as a bit-stream and was separated into a series of fixed-length fields. It was an RFS (Request for Service) message. The ORG field indicated that the sender was a bank in Germany. Curiously, the KD field was not notarized as the newly revised protocol required. The message was rejected.

Moments later another RFS message was received by the same center in Atlanta. This one also appeared to originate from Germany. This time the KD field was notarized, but curiously the MAC had not been computed properly. The authentication procedure failed and the message was rejected.

Shortly thereafter a third message was received by the Atlanta key center. By this time German authorities had been notified of an attempted attack on the EFT infra-structure. There were no more peculiar messages.