Chapter 3

Just Another Day at the Office

by Joe Grand

All in all, it was a very shady operation, but I was in too far at this point to do anything about it. Besides, who was I going to complain to? The Feds? Not likely. Then I'd have the fuzz breathing down my neck *and* these guys looking to kill me. No way. I decided to go along for the ride, no matter where it took me…

Setup

I had been working at Alloy 42 (A42) since its beginning. A recruiter from around town, a guy I grew up with in Boston, gave me a call when he heard the scoop about this new research organization forming. He told me that they needed an electrical engineer on staff. The recruiter, who shall remain nameless to protect his identity, worked for a local headhunter. I had been freelancing for a few years after leaving my job at Raytheon, where I had designed the guidance-control system for the SM-3, so I was well-qualified for this position.

I didn't like working for other people, and consulting was the easiest way to earn some cash without having to kiss anyone's ass on a regular basis. Billing by the hour is sweet, especially if you can squeak out an extra hour here or there, while watching some TV or playing Super Mario Sunshine. On the other hand, having a full-time job meant I didn't need to work 16 hours a day while trying to think of the next good way to make some dough.

A42 was contracted by the U.S. Government to research new technologies for a next-generation stealth landmine. I guess that's why the U.S. didn't sign into the Mine Ban Treaty back in 2000. Now don't get me wrong, I don't necessarily enjoy strengthening The Man. I'm not a big fan of Corporate America, but the job seemed interesting, and the pay was good. Right from the beginning, A42 was run like a typical startup, swimming in government and private money, and not shy about spending it.

The first year at A42 was uneventful, and dealing with incompetent middle management became the norm. One day, out of the blue, I got a call from the recruiter. I was surprised to hear his voice. We hadn't talked since he hooked me up with A42. He told me about a few guys who wanted to meet me—they had heard good things about me and thought I might be able to help them out. Being the nice guy I am, I agreed to meet them the next night, at some alleyway joint in Roxbury.

Welcoming Committee

The scene was like something straight out of *The Godfather*. These guys sure as hell weren't politicians or executives. Everything from the Cuban cigars down to the shine on their wingtips was topnotch and of the finest quality.

The man with the commanding stare spoke first. I'll call him The Boss. I never Knew his name, which is probably for the best.

"Welcome," he said, "I'm so glad you took the advice of our mutual friend to come here." The Boss was seated at a flimsy table covered with a stained, green tablecloth, and he was flanked by some of his associates. It looked like they had been sitting there for a while. The small back room was cloudy with smoke, and the ashtrays contained the remnants of many half-smoked cigars. Poker chips were thrown all over the table, and piles of cash were stacked up in the middle. Wine in cut-crystal carafes sat beside the table, and The Boss had a half-full glass of red. He was dressed in a black, double-breasted suit, which was probably an Armani. The associates were dressed slightly more casually, in black slacks and tight, black turtlenecks, with gold chains around their thick necks. One of them shoved a chilled shotglass filled with Icelandic Brennivin towards me. I took it down in one gulp.

The Boss grumbled through a proposal. I bring them the information they want, and they bring me cash. No questions. No problems. I sat there silently for a few minutes, the schnapps warming my body and relaxing my mind. For some reason, I didn't feel guilty about taking anything from A42. It didn't even seem like stealing, actually. It's not like I'd be walking out of the office with $5,000 workstations. This guy just wanted some data—numbers on a page, bits on a disk. I had no problem keeping my questions to myself. What these people use this information for is none of my business, as long as they pay me.

I agreed to the deal. No legal documents, no signing in blood—just a handshake. And that was that. They wanted a sample of my work. I said I'd get back to them in the next few days.

Low-Hanging Fruit

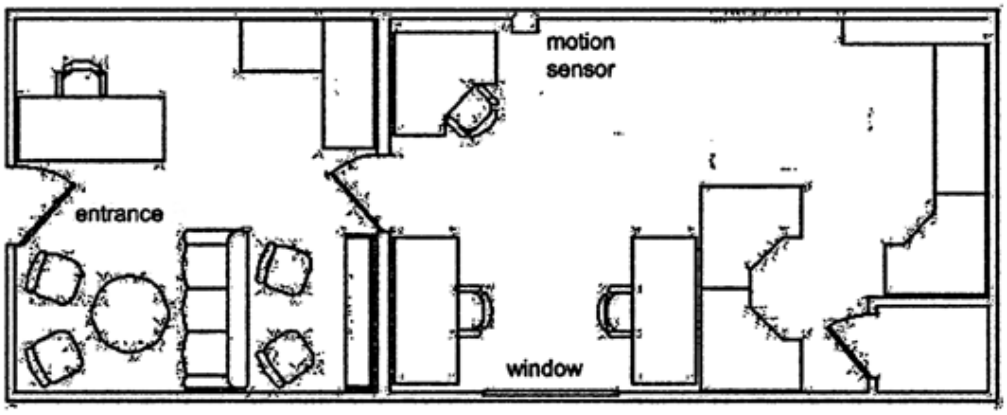
It started off easy. I decided to stay late in the office one night and go for some of the obvious pieces of information first. Flickering streetlights outside the building spilled a weak, yellowish glow over the papers strewn across the desks. Unfinished client projects lay on a small, communal meeting desk in the middle of the room. Piles of credit card receipts and invoices sat unprotected on the accounts receivable desk. "People should lock their documents up at night," I thought to myself.

I grabbed an employee directory that was tacked on a cubicle wall and ran off a quick copy. I didn't know exactly what The Boss was looking for at this point, but I stuffed the directory copy into my pocket anyway, thinking it might be good to have down the road. As harmless as it appeared, the directory contained all of the employee names, which could help me with identity theft attacks and social engineering. It also listed telephone extensions, useful if I ever wanted to target voicemail systems.

I headed down to the communal trash area, where the day's garbage is emptied and stored until the weekly pickup by the city. It's a small, unfurnished room in the basement, with cracked concrete floor and walls, reeking of stale coffee grinds and moist papers. I grabbed a few plastic bags of trash from the dumpster, laid them down on the floor, and ripped them open. I pulled out some papers that looked interesting and peeled off the candy bar wrapper that was sticking them all together.

After about 20 minutes of trash picking, or "dumpster diving" as my buddies used to call it, I had a two-inch stack of documents that would please The Boss immensely: sales account status reports, new lead lists, work agreements, lists of clients and accounts, resumes, HR offer letters with salary listings, business development plans, and personal to-do lists. A marked-up blueprint of the first-floor office showed the different entry points into the building. I set that document aside.

Floor Plan of the Office Pulled from the Dumpster



I had seen some surveillance cameras around the office, but heard rumors that they weren't monitored. I brought this up with my manager at one of my "employee reviews," and he just blew it off. In one ear and out the other.

What's the point of having a security system if you're not going to review the tapes? It's like running an IDS on your network but not monitoring the logs. Chalk one up to laziness and the typical corporate mindset.

In the Palm of My Hand

The Boss liked what I delivered and paid handsomely, as promised. I was really starting to get into this gig. I'd heard about guys getting busted for stealing trade secrets and trying to sell them to foreign governments. There were stories about government-backed foreign nationals getting jobs in legitimate U.S. organizations in order to swipe confidential project plans and genetic material from biotech firms. That all seemed like spy stuff, and they probably did something stupid to get caught. Selling a few documents to some nice gentleman for a little bit of cash wasn't going to cause me any harm.

I reserved one of the meeting rooms near the executives. I had my laptop set up on the table with schematics and documents laid out, so it looked like I was actually doing something useful. Halfway through a game of Windows Solitaire, out of the corner of my eye, I saw the CEO walk out of his office with his secretary, his door left wide open. "Probably heading off to another cushy off-site board meeting." I groaned bitterly. This was a daring mid-day raid, but it was a perfect opportunity. I stood up and casually made my way toward the office. Taking a peek around and seeing nobody, I slid craftily in and quietly closed the door.

The CEO's desk was covered with papers—business proposals, phone notes, financial reports—and a Palm m505 filling in for a paperweight on top of them. "This is a good place to start," I thought. "I can try to copy some information from his Palm, maybe getting his passwords, contact lists, or memos." I knew the IT department used PDAs, too, to keep track of passwords, hostnames, IP addresses, and dial-up information.

I hit the power button on the m505 and was prompted for a password.

Palm m505 Showing Password Lockout Screen

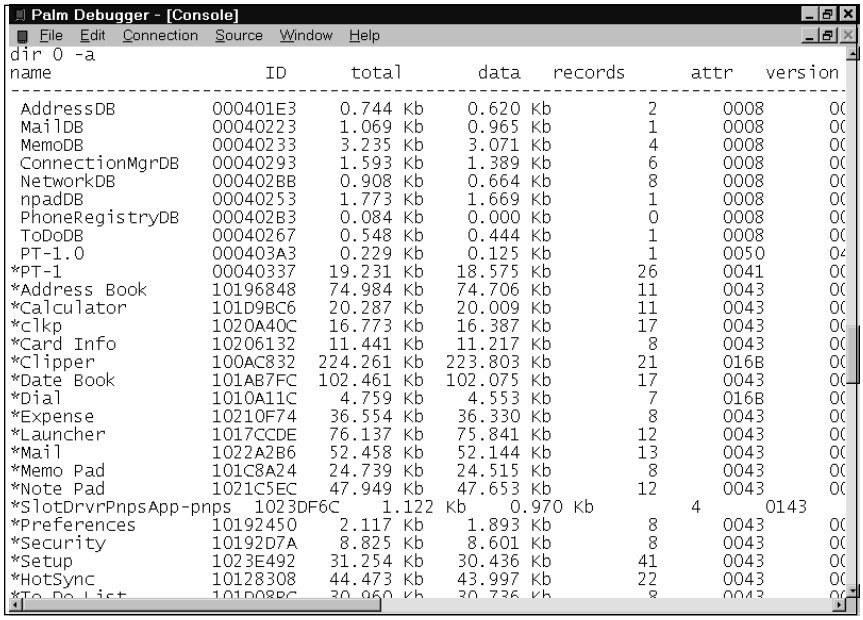
No problem. The beauty of some of these older Palm devices is that the system lockout means nothing. I had heard of the inherent weaknesses in PDAs and now I could see if it was really true. I hooked up a readily available Palm HotSync serial cable between the Palm and my laptop. Then I loaded the Palm Debugger, entered the debug mode with a few Graffiti strokes, and was in.

Graffiti Strokes Required to Enter Palm Debug Mode, Called "Shortcut Dot Dot Two"

The Palm Debugger is a software component that comes with Metrowerks CodeWarrior. The tool, designed for third-party application development and debugging, communicates with the Palm device through the serial or USB port. Through the documented debug mode, I could load and run applications, export databases, view raw memory, and erase all data from the device, among other things.

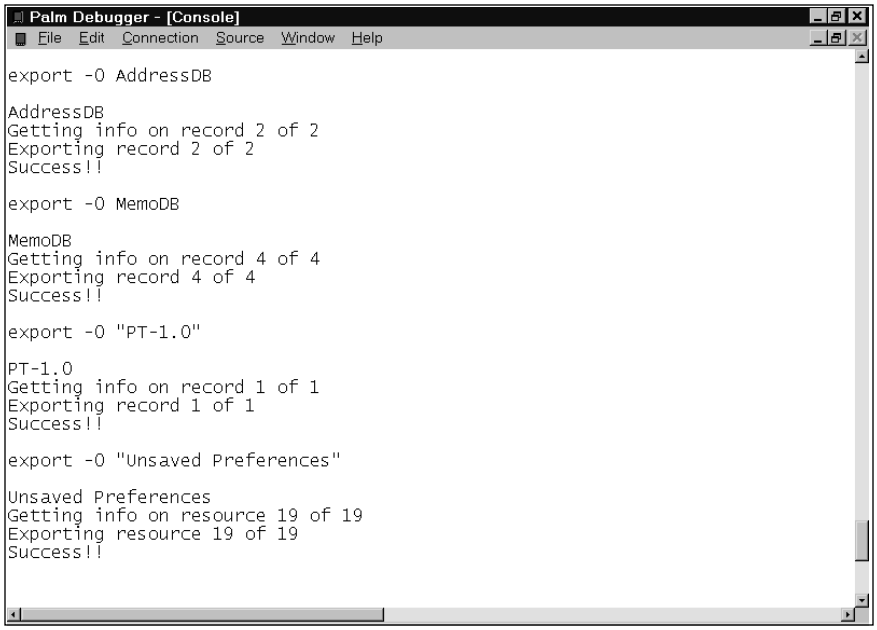
First, I listed all of the available applications and databases the CEO has stored on his Palm by using the `dir 0 -a` command. It looked like the CEO was accessing some protected system in the company using the CRYPTOCard authentication token technology. The PT-1 application is CRYPTOCard's Palm OS-based software token. I knew that it was possible to crack the private configuration information stored within the PT-1.0 database in order to clone the token and create a one-time-password to log in to the system as the CEO.

The Palm Debugger Showing a List of Databases and Applications on a Locked Palm Device



I used the simple `export` command to retrieve the Memo Pad, Address Book, CRYPTOCard database, and the Unsaved Preferences database onto my laptop. The Unsaved Preferences database can be useful, since it contains an encoded version of the Palm OS system password. The encoded hash is just an XOR against a constant block that can easily be converted back into the real ASCII password. Chances are, due to laziness and human nature, that same password is used for some of the CEO's other accounts elsewhere in the company.

Exporting Databases from a Locked Palm Device Using the Palm Debugger



I planned to analyze the exported databases later using a simple hex editor, since all the data is in plaintext and I could easily look for any useful information that way. For good measure, I removed the external SecureDigital memory card from the CEO's m505, stuck it into my SecureDigital-to-PCMCIA adapter, plugged that into my laptop, and copied the entire filesystem onto my PC. I plugged the card back into the Palm, placed the PDA back on top of the pile of papers, and stalked out of the room. Mission complete, in all of five minutes. The CEO never suspected a thing.

Feeling Good in the Network Neighborhood

Like getting addicted to a drug, I started with just one hit and kept coming back for more. The Boss was raising the ante, paying me more money for information that was more difficult to acquire. I have to admit that I liked the challenge.

The arrival of a new temp worker set the mood for the day. I heard that he was helping out the Finance department with their end-of-year paper-

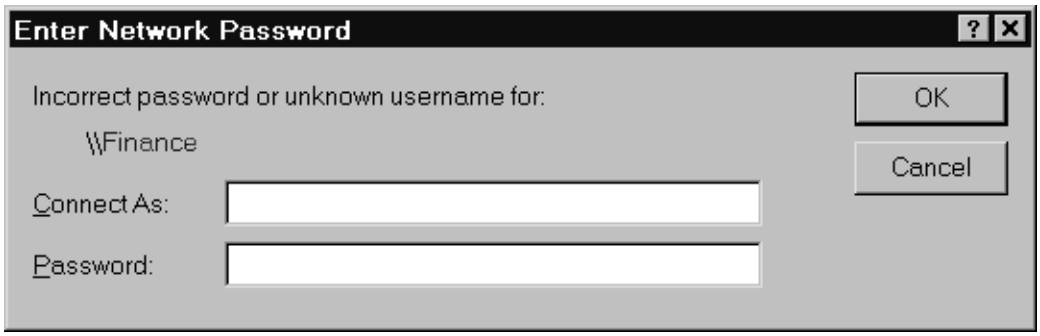
work. His eyes might have access to password-protected folders on the Windows networking share. I had heard that those folders contained the salary and employee information for everyone in the company, along with bank account information, board meeting minutes, and customer lists.

At my desk, I clicked open the Network Neighborhood folder on my Windows 2000 desktop. A list of five computers showed up under the default workgroup name, Workgroup. To my surprise, file sharing was enabled on four of them, giving me free reign to the data on each machine. I copied all of the interesting-looking programs and data from the accessible systems and burned a few CDs to pass on to The Boss.

Windows Network Neighborhood Showing Connected Computers

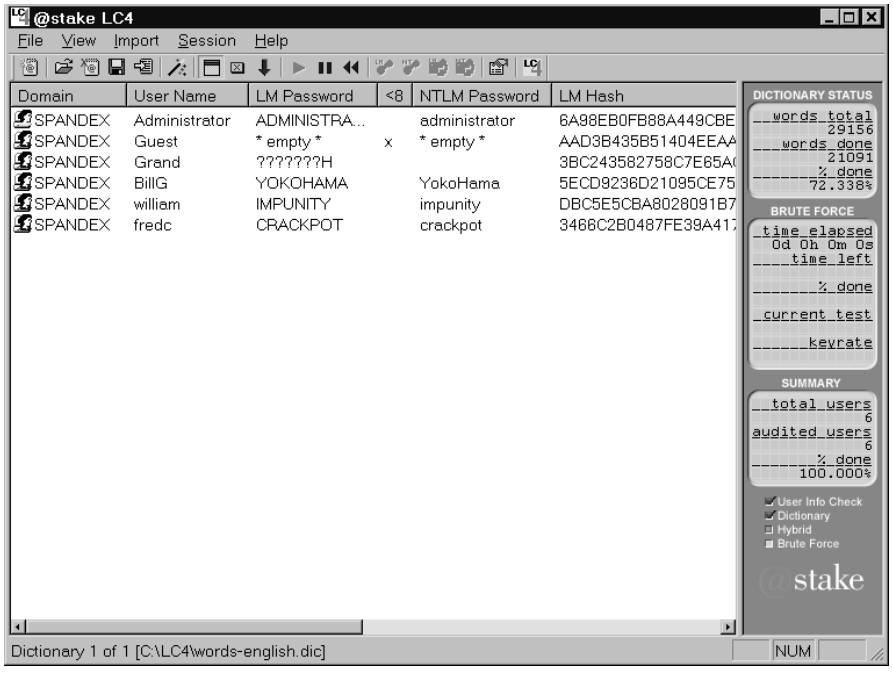
Finance was the only computer in the workgroup that was password-protected. This was where the temp worker would come in handy. Since I knew he would be accessing data in that folder during the day, I set up L0phtCrack to sniff SMB traffic and capture encrypted password hashes transmitted over the network, which was done for every login and file/print-sharing access.

Windows Networking Prompt for Username and Password



Over the next few hours, I collected a nice list of Windows usernames and encrypted password hashes, including "william," which belonged to the temp in Finance. I then had L0phtCrack attempt both a user information and a dictionary crack. It zipped through the hashes in a matter of minutes, leaving me with actual passwords. Now I knew the temp's password, "impunity," and could access the Finance system using his privileges.

L0phtCrack Showing Usernames, Hashes, and Cracked Passwords

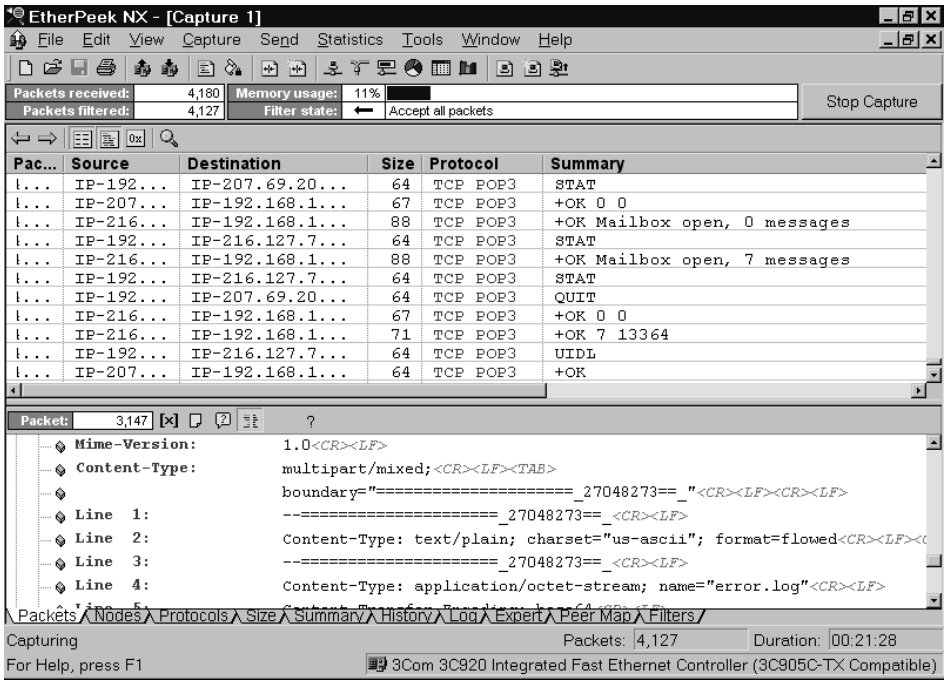


What's That Smell?

By this point, I was thoroughly enjoying myself. Seduced by the money, whatever inhibitions I once had went right out the window. For a different approach, I decided to capture the network traffic on A42's corporate LAN.

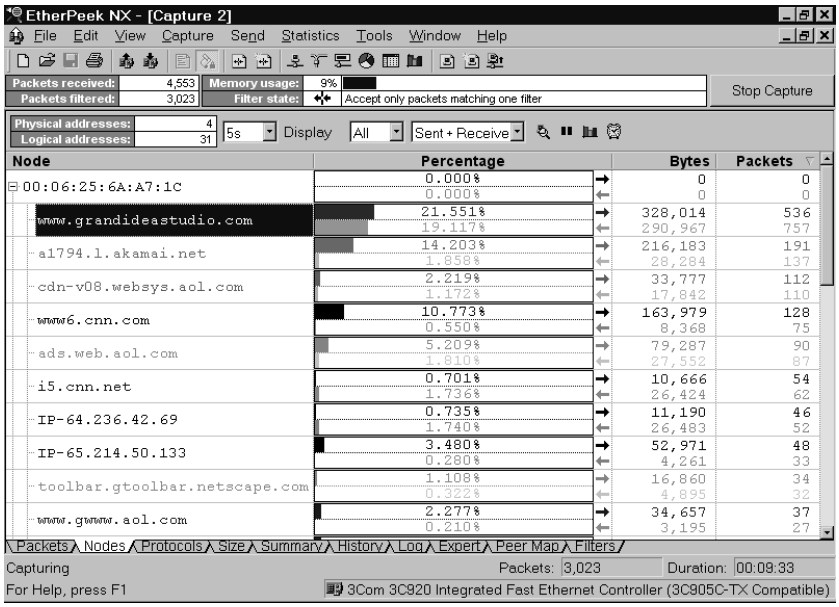
Though many other tools are available—Dsniff, Ethereal, Sniffer Pro, and so on—I used WildPacket's EtherPeek. I set it up on my laptop in the office and just let it run—no maintenance required. A single day of sniffing the network left me with tens of thousands of packets, many containing e-mail messages and attachments, passwords, and Web and instant messenger traffic.

EtherPeek NX Showing Captured Network Traffic and a Portion of an E-mail



Using EtherPeek, I performed some simple traffic analysis and generated statistics that showed me which Web pages were most frequented. I was watching only one particular network segment, because of where my machine was situated on the physical network, but my results were pleasing.

Displaying the Most Frequented Connections by Node Using EtherPeek NX

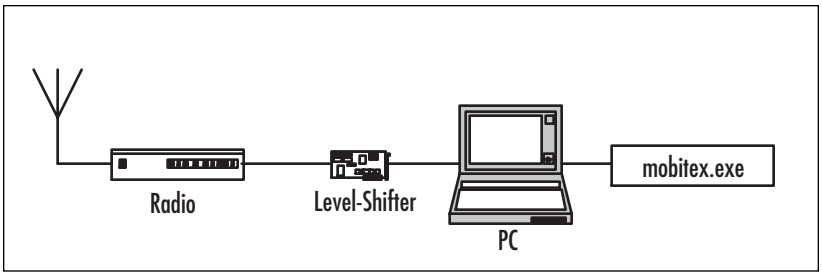


Monitoring from the wired side is great, but I knew all the A42 executives used BlackBerry wireless e-mail devices for much of their communication. I decided to try monitoring the transmissions between the devices and the wireless backbone to see if something interesting turned up.

Two BlackBerry models were distributed to the A42 executives, the RIM 950 and RIM 957, though newer models exist now. These are Internet Edition models, sold through select ISPs and bundled together with an e-mail account. All mail passes through the ISP, which is then forwarded to the correct location. (There is also an Enterprise Edition model, which integrates with Microsoft Exchange or Lotus Domino, and apparently uses triple-DES to provide end-to-end encryption of the e-mail message between the mail server and the BlackBerry.) The RIM 950 and RIM 957 models are designed to operate on the 900MHz Mobitex networks.

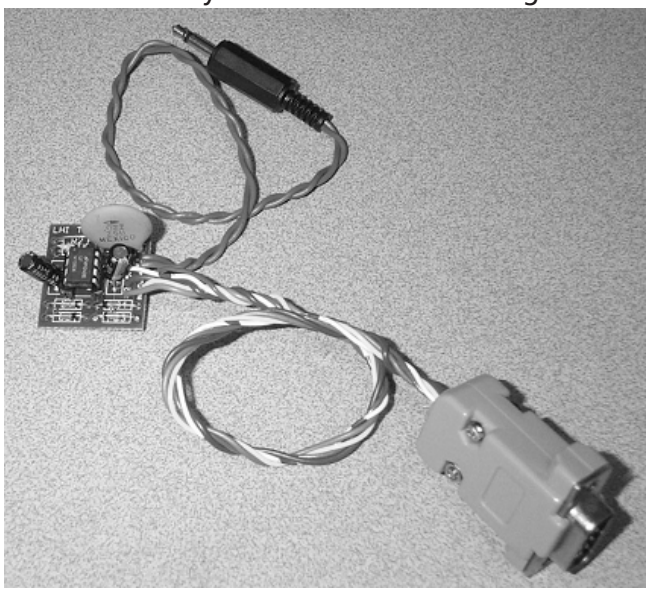
In order to monitor and decode the wireless transmissions, I needed to create a system that consisted of a scanner radio, interface circuitry, and decoding software running on my laptop.

Mobitex Wireless Monitoring and Decoding Setup



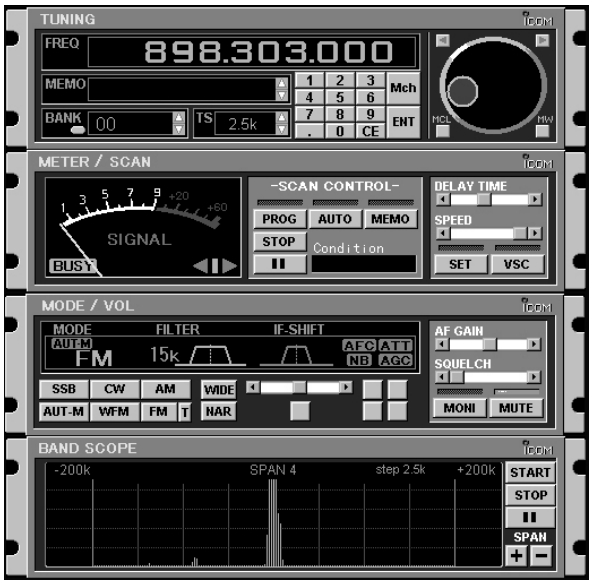
Simple circuitry is needed to convert the audio signal from the radio receiver into the proper levels for computer interfacing. I built the level-shifter hardware—some people call it a *POCSAG decoder* or *Hamcomm interface*—with a few dollars' worth of common components that we had lying around the lab. I plugged one side of it into my laptop's serial port and connected the audio output from the radio into the other side.

Level-Shifter Interface Circuitry for Mobitex Monitoring



Using my Icom PCR-1000 software-controlled, wide-band radio receiver, I started scanning the transmission frequencies of the BlackBerry devices, which range from 896MHz to 902MHz. The unfiltered audio output that the PCR-1000 provides is necessary for decoding data sent at high rates, such as the 8000 bps Mobitex protocol, although many other scanner radios will do the job.

The PC-based PCR-1000 Control Software Set to Monitor a BlackBerry Transmission



I loaded the `mobitex.exe` decoding software on my laptop and hoped for the best. The output from the software is an ASCII hex dump of the Mobitex data packet. All of the higher-level Mobitex protocol information has been stripped out, leaving just the raw data information that has been transmitted.

I let the setup run for a few days during office hours and ended up with a nice capture of messages sent between the CEO, CFO, COO, and other important-sounding titles in the company. I had to be within range of the transmitting devices in order to capture them with my gear. The packets I captured were all transmitted in the clear, which gave me access to the Mobitex header information, full e-mail message, and any attachments.

Going by the last bit of text in one of the transmissions, it looked like the A42 executives were up to some shady dealings of their own. The e-mail message consisted simply of "Bury the body." I was sure The Boss would be interested in following up on this. This heist was slightly more complicated than my previous ones, but it was well worth the time.

Captured BlackBerry Transmission Showing Raw Header Information and E-mail

```
FD236881B808FD23680186BF00020000002510DF          ?#h∞¸.?#h.†¿.....%.ß
0000000002000220200747313031313031003100A357      .......  .G101101.£W
07AFFFAB5005434D494D4503408080805400A303          .¯ÿ«P.CMIME.@   T.£.
000010C0004C021004136C756369616E6F405D94          ...À.L....luciano@]”
686F746D61696C2E636F6D01093136353839612C          hotmail.com..16589a,
3637320007043C1116E40803466F6F0B010151BA          672...<..ä..Foo...Qº
F1044B831794000102020100F4275727920A06B          ñ.Kƒ.”.......Bury  k
74686520626F64792E0A1000000000000000DE5E          the body.........Þ^
```

Working from Home

I like weekends. They remind me of when I used to work for myself, spending every day in sweatpants and slippers. I wore through three pairs of slippers and was onto my fourth before I gave up that lifestyle to work at A42.

There are many ways to steal from the inside, but I knew that I didn't always need to be at the office physically to obtain information. So, today I gave myself some time to experiment with hacking the corporate systems from the outside—from the comfort of my own home.

One of the pieces of paper I pulled out of the trash on my first day as a thief had a list of phone numbers on it. I dialed each one by hand to see what they were, remembering to disable caller ID before making the calls. Some of the numbers were disconnected, some of them were fax machines, and others were good old-fashioned modems. Yes, even with the Internet controlling our lives, modems are still used for certain applications.

Using Qmodem, my favorite DOS-based terminal program, I called back each of the modem numbers. I successfully connected to some of the modems, but banging on the keyboard didn't elicit a response. One number, halfway through the list, got my attention. The system appeared to be a standard AIX machine, and it prompted me for a login.

The only passwords I currently had access to were the ones I found while running L0phtCrack in the office. I figured it was worth a shot to try logging in with the username/password combinations I had (we all know that people use the same password on different systems, no matter how often they are told not to).

```
AIX 3.2 (portia)

login: billg
Password: <password not displayed>
Login incorrect
login: fredc
Password: <password not displayed>

Welcome to portia (AIX 3.2)
Unauthorized use prohibited
Last login: Tue Aug  6 15:17:05 2002 on pts/29 from 150.103.116.29
[YOU HAVE NEW MAIL]
$
```

Well, what do you know! Human nature prevails again, giving us shell access to the box. I knew I could do a lot of things at this point, such as using this system as a launch point to attack other machines or trying to get to root on the system to have complete control. But I wanted to keep it simple, at least this time around.

I decided to first check out the `/etc/hosts` file, which would give me a list of hard-coded IP addresses and their corresponding hostnames.

```
$ cat /etc/hosts
127.0.0.1        loopback localhost       # loopback (lo0) name/address
163.102.66.3     savmktu                   #Savannah
163.102.68.131   mntmktu                   #Montgomery
163.102.76.131   lrmktu                    #Little Rock
191.80.77.47     zeus.a42.com              zeus
191.80.77.99     theseus.a42.com           theseus
191.80.77.122    blanch.a42.com            blanch
191.80.77.123    pistol.a42.com            pistol
```

Here were seven more systems I didn't know about, and they were all part of the A42 corporate network. Since they weren't Windows boxes, they weren't broadcasting on my network segment, so I didn't pick them up with my sniffer at the office. While I was logged in, I tried to access the UNIX password file. To my joy, it was publicly readable. The `/etc/passwd` file was chock-full of unshadowed password hashes.

```
$ cat /etc/passwd
lal:UfiqkG0J228i2:2292:435:Leroy A Logan:/home/d1g/lal:/bin/csh
ajy:YoKR0sFYFLKS.:2195:446:Albert J Yarusso:/home/d2g/ajy:/bin/csh
afk:IL6Nhv3NSh7ts:7581:306:Anton F Kelso:/home/boise/afk:/bin/csh
dqc:GI9SADJDkbjBg:2317:377:Don Q Crotcho:/home/d9g/dqc:/bin/csh
val:46DaLVIZWkzYE:5296:252:Valerie A Lasgana:/home/cairo/val:/bin/csh
kms:ND21FI/uvMBb2:2908:305:Keely M Subin:/home/cairo/kms:/bin/suspend
akp:TkybEIKNN1s12:1468:306:Amet K Purhit:/home/d2g/akp:/bin/csh
rn:HkkKdzng.xcLA:4219:304:Redmond Neckus:/home/d10g/rn:/bin/suspend
ksd:5UTjjE4ndzICw:7634:435:Karen S Daminis:/home/boise/ksd:/bin/csh
dcc:EuE5oT8AX56Ts:1887:245:David C Cahill:/home/d8g/dcc:/bin/csh
adl:F8QHVzJ1QzYdY:1849:312:Amy D Lehane:/home/boise/adl:/bin/csh
kgp:wfiPGMVfuGxQE:1200:241:Kin G Pin:/home/d2g/kgp:/bin/csh
tcn:Jv5CyZuCDLb0M:1842:259:Tracy C Nuffe:/home/d2g/tcn:/bin/csh
— More —
```

I captured the password file, which ended up being around 540KB with more than 7000 users, and saved a copy to my local machine. No way did A42 have over 7000 employees. It looked like they were involved in some larger dealings.

Cracking UNIX passwords is simple, especially with the fast computers we have these days. I grabbed a copy of John the Ripper from the Web. It's my favorite UNIX password cracker because it's powerful, fast, and free. After a little less than two hours of computation, I watched as a list of 367 unencrypted passwords and their associated usernames streamed past my eyes.

```
$ john -wordfile:words a42.pwd
Loaded 7287 passwords with 3274 different salts (Standard DES [24/32
4K])
demetra          (eos)
elbereth         (slw)
forsythi         (bhb)
gandalf          (kck)
hemipter         (gjl)
kinesiol         (rvc)
lilongwe         (tdk)
monotone         (caf)
oryctola         (rv)
proteus          (jwk)
stamatis         (lp1)
tagalog          (pps)
wuzzle           (wpd)
zygomati         (tn)
— More —
```

I could have continued my attacks on the other systems in the `/etc/hosts` file (`zeus`, `theseus`, `blanch`, and `pistol`), attempting to use the username and passwords from my newly cracked password file, but I chose to move on to the next dial-up number on my list. I didn't even bother covering my tracks, since I was pretty confident about not being detected. After all, given what I've seen so far with "security" at A42, chances were no one would ever read the logs, if they were even enabled at all.

The next system I connected to was as intriguing as the previous one. I was connected to a VAX. An intimidating banner screamed across the screen at 9600 bps. "Do people ever obey those messages?" I wondered.

```
Local -010- Session 1 to VAX established


**********************************************************************
     *
*
     *                              W A R N I N G
*
     *
*
     *                            INTERNAL USE ONLY
*
     *
*
     *                    UNAUTHORIZED ACCESS IS PROHIBITED
*
     *
*

**********************************************************************

Username:
```

At the username prompt, I tried some of the accounts I had gotten from the Windows machines and the UNIX box. That led me nowhere. Not wanting to give up so soon, I began to sift through some of the sticky notes and notepad scribbles I had grabbed from the trash, hoping for a useful tidbit of information, but to no avail. Turning back around to the monitor, my jaw dropped. What the …?

```
Error reading command input
Timeout period expired
Local -011- Session 1 disconnected
>
```

"Look at that!" I squealed with excitement, "I turn my back for a second, don't even type anything, and it lets me into the system." The system I was connected to had timed out, and I was presented with a prompt. For once, I didn't complain about buggy software. I was dropped right into the previous user's session. Is this even considered hacking?

Typing HELP revealed an enormous list of commands. This system was like nothing I had ever seen before. After poking around for a while with various commands, DISP CP SUBSCR seemed most interesting. I think it stood for Display Cellular Phone Subscriber. I was prompted to enter a single mobile phone number or range of numbers. I knew the cell phones that A42 issued to us were in the 617 area code and used a 750 prefix. According to the employee directory I picked up earlier, this was true for all of us. I entered a range from 6177500000 to 6177509999, and the system responded.

```
>DISP CP SUBSCR
MOBILE ID(S) OR DEFAULT:
  Enter the single 10-digit MOBILE ID number or the range of
  10-digit MOBILE ID numbers to be accessed or DEFAULT
  [0000000000 - 9999999999, DEFAULT]
  :  6177500000-6177509999

MOBILE ID = 6177500000    COVERAGE PACKAGE = 0   SERIAL NUMBER =
                                                 C6FDA2A0
ORIGINATION CLASS = 1     TERMINATION CLASS = 0  SERVICE DENIED =  N
PRESUBSCRIBED CARRIER = Y CARRIER NUMBER = 288   OVERLOAD CLASS = 0
FEATURE PACKAGE = 2       CHARGE METER = N       LAST KNOWN EMX = 2
PAGING AREA = 1           VOICE PRIVACY = N      CALL FORWARDING = N
FORWARD # =               BUSY TRANSFER = N      NO-ANSWER TRANSFER = N
TRANSFER # =              CREDIT CARD MOBILE = N SUBSCRIBER INDEX =
                                                 98062
ROAM PACKAGE =   15       LAST KNOWN LATA = 1    CALL COMPLETION = NA
CCS RESTR SUBSCRIBER = NA CCS PAGE = NA          VMB MESSAGE PEND = NA
VMB SYSTEM NUMBER = 0     LAST REGISTR = NA      VRS FEATURE = N
VOICE MAILBOX # =         NOTIFY INDEX = 0       DYNAMIC ROAMING = Y
REMOTE SYSTEM ROAMING = N  OUT OF LATA = N       PER CALL NUMBER = N
PRESENTATION RESTRICT = NA DMS MESSAGE PENDING = NA SUBSCRIBER PIN = NA
LOCKED MOBILE = NA        LOCKED BY DEFAULT = NA
```

This was a gold mine! Listing after listing of mobile phone numbers, electronic serial numbers (known as ESNs), and other subscriber information flashed down the screen. Wow! Just the mobile number and ESN alone would be enough to clone the cell phone and get free phone calls. I knew cloning cell phones could be a huge moneymaker in certain circles, so maybe The Boss would be interested in this. Not only did I not have to provide a username or password to get access to this system, it looked like I had complete control of the system responsible for handling all of the cellular phone calls and transactions within the entire city of Boston.

I turned off my computer and decided to try my hand at some voicemail hacking. As much as voicemail systems are relied on for the flow of business these days, they are almost always left unprotected. Even if security measures are in place to force users to change their passwords every month, many users keep assigning the same password or switch between two passwords. People are usually pretty lazy when it comes to choosing voicemail passwords. It doesn't take a lot of skill to access and listen to voicemail—you can usually get in within three tries. And chances are, just as with the computer systems, the voicemail password is probably used for other systems requiring short-length passwords, like ATM PIN or phone banking numbers.

With the A42 employee directory in hand, I already had a target list of voicemail boxes. The main voicemail access number was printed right at the bottom of the paper; user convenience always outweighs security, so it seems. It would have been easy to find the voicemail access number, anyway, if I didn't already have it, by just manually dialing numbers within the company prefix until I found it. Being on the inside does have its advantages.

I called the main voicemail number. "Welcome to AUDIX," the digitized voice said to me seductively. "For help at any time, press *H. Please enter the extension and # sign." This was pretty straightforward. I picked a random extension from the employee list. "Please enter password, and # sign." Okay, I could try that. "Login incorrect. Try again." Two more tries, and I got a nasty "Contact administrator for help. Please disconnect." That didn't dissuade me.

I called the main voicemail number back and tried again. This time, I focused my sights on the "high-ranking" officers and IT staff. I spent the next part of the evening with the phone glued to my ear.

I tried various common password configurations: the voicemail box number, the box number in reverse, 0000, 1234, on and on. By the time I quit, I had access to 7 of the 50 voicemail systems I tried. If I were more dedicated, I could have gotten into more simply by trying other passwords.

The first three boxes I listened to were for regular employees, and the next was a general sales mailbox. Nothing exciting there. The fifth was intended for "confidential messages" between employees and our "Chief People Officer," a flaky, politically correct term for Human Resources. The last two were the best. One of them was the box for the COO, who unsurprisingly left his password the same as his voicemail extension. That's what the system administrator changes it to when people forget their passwords. Executives are often the worst complainers about passwords and are always sharing them with their secretaries. The other password I had was for my manager, a guy who hardly ever shows up at the office and probably doesn't even know I work for him.

Diner

The last few weeks were fruitful, to say the least. I had a bunch of successful heists with no sense of any heat coming down on me. I had picked through the trash to find all sorts of confidential documents; retrieved some data and passwords from the CEO's PDA; copied a bunch of files from the Sales, HR, Research, Legal, and Finance department's computers; captured and cracked some Windows accounts; sniffed the corporate network for e-mails and other traffic; gained control of a cellular phone system; accessed a UNIX box and cracked passwords there; and hacked some voicemail boxes. This was too easy.

I would say I'd done a damn good job, but some people are hard to please. The Boss wanted to meet right away. Two of his goons showed up at my doorstep on a Monday morning and forced me to follow them. Nice guys.

The Boss was very polite, as usual. "Don't misunderstand me. You have been a great asset to our organization, but it's time for you to get us what

we've been waiting for." The Boss stopped for a moment, as the waitress from the diner dropped two runny eggs in front of me. We were sitting four in a booth at a greasy spoon in Chinatown. It wasn't very crowded.

"We have decided to move forward with the last leg of our plan, and we have someone you will be working with." I heard the flimsy metal door slam behind me as someone entered the diner. In walked the recruiter, dressed quite a bit nicer than the last time I saw him. He was ready for business. Clean-shaven, neatly pressed black pants, loafers, and a pair of aqua socks. This guy knew style! The recruiter sat down next to me in the booth and gave me a wink.

The Boss continued, "The land mine. We want the prototype, as-is. We know it's not complete. With the rest of the data you've provided for us, we can rebuild the missing components and unload it to the Russians. Time is running out." He blew out a huge blue plume of cigar smoke, and one side of his jacket fell open to reveal a gun. "You'll be breaking in from the outside. Do not fail."

Damn. Why did he tell me all this? If I got caught, he would obviously have me killed. If I succeeded and delivered, he would probably have me killed. The Boss snuffed out his half-burned cigar right on the cheap wood table, pushed his chair back, and walked out of the diner. One of the goons, who had been sitting quietly, grabbed my arm. "Let's go!" he said, and pushed me out the door before I could leave a tip.

All in all, it was a very shady operation, but I was in too far at this point to do anything about it. Besides, who was I going to complain to? The Feds? Not likely. Then I'd have the fuzz breathing down my neck *and* these guys looking to kill me. No way. I decided to go along for the ride, no matter where it took me.

I was tired of dealing with Big Business, I was tired of layers of useless middle management. Except for the fact that this whole thing might get me killed, I just really didn't care anymore. I might as well be just like The Boss.

The Only Way Out

We had to break into the company from the outside to change my MO and misdirect some of the heat that would undoubtedly arise. With the landmine out of A42's possession, the government would instantly shut down the company.

On late Friday night, the recruiter and I walked up to the front entrance of the building. I had a duffel bag filled with everything I needed for a B&E job: lockpicks, wrench, automatic center punch, and rubber gloves.

I pulled out an Icom IC-R3, a tiny handheld radio receiver with a two-inch screen. Aside from being a scanner radio, to monitor the police frequencies, cell phones, and cordless phones, the IC-R3 can decode FM TV signals on frequencies up to 2.4GHz. It could tune in to all of the wireless surveillance cameras in the facility, as well as just about any other wireless camera system in a few blocks' radius. Flipping through the channels, I stopped on the important one—a camera right above the main entrance to the laboratory. We had to be careful to avoid being seen on the surveillance system, just in case someone was watching.

Icom IC-R3 Showing the Laboratory View from the Surveillance Camera

(Photo obtained from http://www.icomamerica.com/receivers/handheld/r3photo.html and modified)

Getting in the front door of A42 was easy. I had a key because I worked there, and it was the same front door key that everyone else in the company had. We needed to remember to break the front glass of the door on our way out, so it wouldn't be obvious that we walked in using a legitimate key. Tracing the entry back to me would be impossible. A42 didn't have an officewide alarm system. Because of the variety of hours that employees kept, there was usually somebody in the office. The executives thought that an alarm system was overkill, and besides, it would be a management nightmare to distribute alarm codes to everyone. One less thing to worry about.

We slithered upstairs through the office. There were a few desk lights on here and there, but I wasn't concerned. People leave office lights on all the time, like they expect someone else to come around and turn them off. The flashing red lights of a passing cop car reflected into the window, and we ducked down to avoid casting our shadows onto the sidewalk.

With the coast clear, we made our way over to the research laboratory. The door leading into the laboratory requires an RF proximity card and proper PIN entry in order to gain access.

You could have the best security system in the world, but if it isn't implemented properly and there is an easy way to bypass it, then you're suddenly not very secure. Think of it as "the weakest link in the chain." The laboratory door is a perfect example. Due to strict Massachusetts fire code regulations, the door also has a standard lock-and-key mechanism used to bypass the access control system. In the case of an emergency, firefighters need guaranteed physical entry into the room, even if the access control system fails.

When I was younger, I used to hang around the Student Center at MIT. There were a group of guys that would gather regularly and wander the streets at night, finding stray bristles from street cleaners and crafting them into makeshift lockpick sets. They would hone their skills on whatever doors they could find around campus, never doing harm. Tagging along on some of these journeys gave me a crystal-clear understanding of mechanical door locks. At the time, I was just having fun, but now that knowledge was turning out to be incredibly useful.

Based on some recent research I had read about, many of the conventional mechanical pin-tumbler lock systems can be bypassed given access to a single key (my office front door key, for example) and its associated master-keyed lock (the office front door). No special equipment is required. It's just

a matter of progressively cutting test keys until the correct master bitting is found, comparing a bunch of legitimate non-master keys from the installation to determine which bit depths are not used, or disassembling one lock used in the installation to determine the bitting. Then you can create a master key that will open all lock systems in a particular installation.

We knew about this ahead of time. I took the easiest way out and, a few days before, spent 10 minutes disassembling a lock on one of the doors while the rest of the company was in the weekly status meeting. I doubt I was missed. Now that I knew the actual bitting used for the master key, it was a piece of cake to fabricate a duplicate master key using a standard key-cutting machine. The recruiter pulled out our handcrafted master key and inserted it into the keyhole. Click, the lock cylinder spun around, released the latch, and the lab door squeaked open.

The laboratory was separated into two areas. The software area, to the left, had a bunch of machines with different operating systems: Windows, Linux, OpenBSD, and VMS. Down a small hallway was the hardware area, with shelves of electronic equipment, including oscilloscopes, logic analyzers, schematic capture workstations, and electronic components. Unwrapped cables and empty coffee cups littered the floor.

We knew from monitoring the wireless surveillance system that a camera watches the front door of the lab. We pulled our masks down over our faces and hugged the wall to avoid a direct shot by the camera. Once we headed left into the software area, we were out of camera range. We worked our way around to the back end of the hardware area, watching the IC-R3 to make sure the surveillance camera didn't see us.

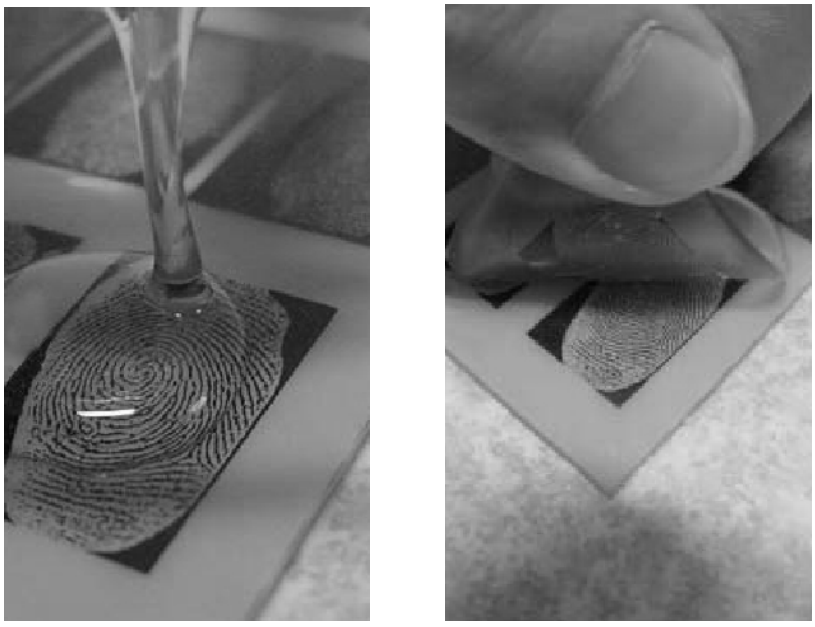
The restricted area in the laboratory, where the landmine prototype was stored, is connected to the general research laboratory with a solid-steel door. This is no door handle or mechanical lock—just a single biometric fingerprint scanner used to authenticate identity. Unlike the main door to the lab that required emergency access and egress, this door did not, based on the sensitivity of the work and a government payoff to the Massachusetts safety inspector.

Current biometric fingerprint systems are notoriously simple to bypass. Back in May 2002, Tsutomu Matsumoto presented experiments and methods to defeat a number of fingerprint scanners by using a fake finger molded out of gelatin. The gelatin finger mold even fooled newer capacitive sensors,

because a gelatin finger has moisture and resistance characteristics similar to a real human finger.

It was no problem to obtain a target fingerprint to use for our gelatin mold. There were only three people authorized for access into the restricted area, and one of them, the project lead engineer, had a desk directly across from mine. A few days earlier, in preparation for this score, I watched as he went into a meeting. I sauntered by his desk with another A42 coffee mug and swapped it with the empty one that sat on his desk. I easily lifted his residual fingerprint right off the mug. After I enhanced his fingerprint image with my laptop, I printed it onto a transparency film. Using photosensitive etching (I read about this at the local electronics store and bought all the tools I needed there), I created a printed circuit board with the image of the fingerprint. I then poured liquid gelatin onto the board and stuck it in the refrigerator to cool. Thirty minutes later, I pulled up the fake gelatin finger from the circuit board, which revealed an exact fingerprint image of my target.

Creating a Fake Gelatin Finger to Bypass a Biometric Fingerprint Sensor



(Photos obtained from http://www.itu.int/itudoc/itu-t/workshop/security/present/s5p4.pdf and modified)

The recruiter carefully removed the gelatin mold from his bag and gingerly placed it over the biometric fingerprint scanner. The red LED turned green, and the electromechanical bolt inside the door pulled back sharply. "Why is everything so easy?" I asked myself. We both walked into the tiny room and were surrounded by racks of electronics gear. We shut the door behind us. A single soldering iron lay on the small workbench, next to what looked like a giant metal egg, cracked open. "The landmine!" the recruiter exclaimed, stating the obvious. Actually being able to see the landmine gave me quite a rush, too.

The landmine was attached to a number of probes that connected to a logic analyzer. I detached the wires, as the recruiter revealed a small, padded, metal suitcase. He flipped the latches, opened it up, and placed the landmine into the case. "Thanks for the help, buddy," he said and smiled, flashing a gold tooth. Sometimes people can be so sarcastic.

As planned, we exited the building without incident, smashed the front door glass with the center punch, and walked off in opposite directions. The recruiter carried the landmine in the suitcase, and I lugged my duffle bag full of gear. I turned the corner and ran as fast as I could, never looking back.

Epilogue

I can't disclose much about my location. Let's just say it's damp and cold. But it's much better to be here than in jail, or dead. I thought I had it made—simple hacks into insecure systems for tax-free dollars. And then the ultimate heist: breaking into a sensitive lab to steal one of the most important weapons the U.S. had been developing. And now it's over. I'm in a country I know nothing about, with a new identity, doing chump work for a guy who's fresh out of school. Each day goes by having to deal with meaningless corporate policies and watching employees who can't think for themselves, just blindly following orders. And now I'm one of them. I guess it's just another day at the office.

References

In the Palm of My Hand

1. PalmSource, http://www.palmsource.com
2. Kingpin and Mudge, "Security Analysis of the Palm Operating System and its Weaknesses Against Malicious Code Threats," USENIX 10th Security Symposium, August 2001, http://www.usenix.org/publications/library/proceedings/sec01/kingpin.html
3. Kingpin, "CRYPTOCard PalmToken PIN Extraction Security Advisory," http://www.atstake.com/research/advisories/2000/cc-pinextract.txt

Feeling Good in the Network Neighborhood

4. LC4, http://www.atstake.com/research/lc

What's That Smell?

5. WildPackets EtherPeek NX, http://www.wildpackets.com/products/etherpeek_nx
6. Research In Motion, http://www.rim.net
7. Anonymous, "The Inherent Insecurity of Data Over Mobitex Wireless Packet Data Networks," http://atomicfrog.com/archives/exploits/rf/MOBITEX.TXT

Working from Home

8. John the Ripper, http://www.openwall.com/john
9. Kingpin, "Compromising Voice Messaging Systems," http://www.atstake.com/research/reports/acrobat/compromising_voice_messaging.pdf

The Only Way Out

10. Icom IC-R3,
http://www.icomamerica.com/receivers/handheld/icr3main.html
11. Matt Blaze, "Master-Keyed Lock Vulnerability,"
http://www.crypto.com/masterkey.html
12. Tsutomu Matsumoto, "Impact of Artificial 'Gummy' Fingers on Fingerprint Systems," http://cryptome.org/gummy.htm