Chapter 8

No-Tech Hacking

by Johnny Long

Johnny Long is the author of the bestselling *Google Hacking for Penetration Testers*, as well as a contributing author to *Stealing the Network: How to Own a Shadow* in the popular "Stealing" series. He is a professional hacker by trade and a security researcher and author. His home on the Web is http://johnny.ihackstuff.com. His popular "Death by a Thousand Cuts" presentation was one of the most-talked-about sessions at conferences this past year.

Introduction: What Is "No-Tech Hacking?"

When I got into this field, I knew I would have to stay ahead of the tech curve. I spent many sleepless nights worming through my home network trying to learn the ropes. My practice paid off. After years of hard work and dedicated study, I founded a small but elite pen testing team. I was good, my *foo* strong. Networks fell prostrate before me. My co-workers looked up to me, and I thought I was The Man. Then I met Vince.

In his mid-40s, hawk-eyed, and vaguely European looking, Vince blended in with the corporate crowd. His usual attire consisted of a pair of black wing tips, a nice dress shirt, a black leather trench coat, and every now and then, he topped it all off with a black fedora. He had a definite aura. Tales of his exploits were legendary. Some said he had been a fed, working deep-black projects for the government. Other insisted he was some kind of mercenary genius, selling his dark secrets to the highest bidder.

Vince was brilliant. In fact, brilliant was an understatement. He held several college degrees—or so I heard—but it wasn't his academic knowledge that people talked about. He could do interesting and seemingly impossible things. He could pick locks, short-circuit electronic systems, and pluck information out of the air with fancy electronic gear. He once showed me a system he built called a "van Eck" something-or-other.[1] It could sniff the electromagnetic radiation coming from a CRT and reassemble it, allowing him to eavesdrop on someone's computer monitor from a quarter mile away. He taught me that a black-and-white TV could be used to monitor 900MHz cellular phone conversations. I still remember hunching over a table in my basement going at the UHF tuner post of an old black-and-white TV with a pair of needle-nosed pliers. When I heard a cellular phone conversation coming through that old TV's speaker, I decided then and there I would learn everything I could from Vince.

I was incredibly intimidated before our first gig. Fortunately, we had different roles. I was to perform an internal assessment, which emulated an insider threat. If an employee went rogue, he could do unspeakable damage to a network. In order to properly emulate this, our clients provided us a workspace, a network jack, and the username and password of a legitimate, non-administrative user. I was tasked with leveraging those credentials to gain administrative control of critical network systems. If I gained access to confidential records stored within a corporate database, for example, my efforts were considered successful. I had a near-perfect record with internal assessments and was confident in my abilities.

Vince was to perform a physical assessment that emulated an external physical threat. The facility had top-notch physical security. They had poured a ton of money into expensive locks, sensors, and surveillance gear. I knew Vince would obliterate them all with his high-tech superpowers. The gig looked to be a real slam-dunk with him working the physical and me working the internal. We were the "dream team" of security geeks.

When Vince insisted I help him with the physical part of the assessment, I just about fell over. I imagined a James Bond movie, with Vince as "Q" and myself (of course) as James Bond in ninja assault gear. Vince would supply the gadgets, like the van Eck thingamabob and I would infiltrate the perimeter and spy on their surveillance monitors or something. I giggled to myself about the unnatural things we would do to the electronic keypad systems or the proximity locks. I imagined the looks on the guard's faces when we duct-taped them to their chairs after silently rappelling down from the ceiling of the surveillance room.

I couldn't wait to get started. I told Vince to hand over the alien gadgets we would use to pop the security. When he told me he hadn't brought any gadgets, I laughed and poked him. I never knew Vince was a kidder. When he told me he really didn't bring any gear, I briefly considered pushing him over, but I had heard he was a black belt in like six different martial arts, so I just politely asked him what the heck he was thinking. He said we were going to be creative. The mercenary genius, the storm center of all the swirling rumors, hadn't brought any gear. I asked him how creative a person could be when attacking a highly secured building without any gear. He just looked at me and gave me this goofy grin. I'll never forget that grin.

We spent the morning checking out the site. It consisted of several multistory buildings and a few employee parking lots, all enclosed by protective fencing. Everyone came and went through a front gate. Fortunately, the gate was open and unguarded. With Vince driving, we rounded one building and parked behind it, in view of the loading docks.

"There," he said.

"Where?" I asked.

"There," he repeated.

Vince's sense of humor sucked sometimes. I could never quite tell when he was giving me crap. I followed the finger and saw a loading dock. Just past the bay doors, several workers carried packages around. "The loading dock?" I asked.

"That's your way in."

I made a "Pffft" sound.

"Exactly. Easy." he said.

"I didn't mean 'Pffft' as in *easy*. I meant 'Pffft' as in *there's people there* and you said *I* was going in."

"There are, and you are," he said. Vince was helpful that way. "Just look like you belong. Say hello to the employees. Be friendly. Comment on the weather."

I did, and I did. Then I did, and I did and I found myself inside. I walked around, picked up some blueprints of tanks and military-looking stuff, photocopied them and left. Just like that. I'm skipping the description of my heart pounding at 400 beats per minute and the thoughts of what military prison would be like and whether or not the rumors about Bubba were true, but I did it. And it was an incredible rush. It was social engineering at its simplest, and it worked wonders. No one questioned me. I suppose it was just too awkward for them. I couldn't hide my grin as I walked to the car. Vince was nowhere to be found. He emerged from the building a few minutes later, carrying a small stack of letter-sized paper.

"How did you get in?" I asked.

"Same way you did."

"So why didn't you just do it yourself?" I asked.

"I had to make sure it would work first."

I was Vince's guinea pig but it didn't really matter. I was thrilled and ready for more. The next building we targeted looked like an absolute fortress. There were no loading docks and the only visible entrance was the front door. It was wood and steel—too much like a castle door for my taste—and approximately six inches thick, sporting a proximity card-reader device. We watched as employees swiped a badge, pulled open the doors and walked in. I suggested we tailgate. I was on a roll. Vince shook his head. He obviously had other plans. He walked towards the building and slowed as we approached the front door. Six feet from the door, he stopped. I walked a step past him and turned around, my back to the door.

"Nice weather," he said, looking past me at the door.

"Ehrmm, yeah," I managed.

"Good day for rock climbing."

I began to turn around to look at the building. I hadn't considered climbing it.

"No," he said. "Don't turn around. Let's chat."

"Chat?" I asked. "About what?"

"You see that Bears game last night?" he asked. I had no clue what he was talking about or even who the Bears were but he continued. "Man, that was something else. The way that team works together, it's almost as if..." Vince stopped in mid-sentence as the front door opened. An employee pushed the door open, and headed towards the parking lot. "They move as a single unit," he continued. I couldn't help myself. I turned around. The door had already closed.

"Crap," I said. "We could have made it inside."

"Yes, a coat hanger."

Vince said strange stuff sometimes. That was just part of the package. It wasn't crazy-person stuff, it was just stuff that most people were too dense to understand. I had a pretty good idea I had just witnessed his first crazy-person moment. "Let's go," he said. "I need a washcloth. I need to go back to the hotel." I had no idea why he needed a washcloth, but I was relieved to hear he was still a safe crazy person. I had heard of axe murderers, but never washcloth murderers.

We passed the ride back to the hotel in silence; Vince seemed lost in his thoughts. He pulled up in front of the hotel, parked, and told me to wait for him. He emerged a few minutes later with a wire coat hanger and a damp washcloth. He tossed them into the back seat. "This should work," he said, sliding into his seat and closing the doors. I was afraid to ask. Pulling away from the hotel, he continued. "I should be able to get in with these."

I gave him a look. I can't exactly say what the look was, but I imagine it was somewhere between "I've had an unpleasant olfactory encounter" and "There's a tarantula on your head." Either way, I was pretty convinced he'd lost his mind or had it stolen by aliens. I pretended not to hear him. He continued anyhow.

"Every building has to have exits," he said. "Federal law dictates that in the case of an emergency, exit doors must operate from the inside out without the user having any prior knowledge of its operation." I blinked and looked up at the sky through the windshield. I wondered if the aliens were coming for me next. "Furthermore, the exit must not require the use of any key or special token. Exit doors are therefore very easy to get out of."

"This has something to do with that door we were looking at, doesn't it?" I asked. The words surprised me. Vince and I were close to the same operating frequency.

He looked at me, and then I knew what *my look* looked like. I instinctively swatted at the tarantula that I could practically feel on my head. "This has *everything* to do with that door," he said, looking out the front window and hanging a left. We were headed back to the site. "The front door of that facility," he continued, "is formidable. It uses a very heavy-duty magnetic bolting system. My guess is that it would resist the impact of a 40-mile-an-hour vehicle. The doors are very thick, probably shielded, and the prox system is expensive."

"But you have a washcloth," I said. I couldn't resist.

"Exactly. Did you notice the exit mechanism on the door?"

I hadn't, and bluffing was out of the question. "No," I admitted.

"You need to notice *everything*," he said, pausing to glare at me. I nodded and he continued. "The exit mechanism is a silver-colored metal bar about waist-high."

I took my shot. "Oh, right. A push bar." The term sounded technical enough.

"No, not a push bar." Access denied. "The bar on that door is touch-sensitive. It doesn't operate by pressure; it operates when it senses it has been touched. Very handy in a fire." We pulled through the site's gate and parked. Vince unbuckled and grabbed the hanger and the washcloth from the back seat. He had untwisted the hanger, creating one long straight piece of strong, thin wire. He folded it in half, laid the washcloth on one end and folded the end of the hanger around it, then bent the whole thing to form a funny 90-degree-angled white washcloth flag. I smartly avoided any comment about using it to surrender to the guards. "Let's go," he said.

We walked to the front door. It was nearly 6:00 P.M. and very few employees were around. He walked up to the door, jammed the washcloth end of the hangar between the doors at waist height and started twisting the hanger around. I could hear the washcloth flopping around on the other side of the door. Within seconds, I heard a muffled *cla-chunk* and Vince pulled the door open and walked inside. I stood there gawking at the door as it closed behind him. The door reopened, and Vince stuck his head out. "You coming?"

The customer brief was a thing to behold. After the millions of dollars they had spent to secure that building, they learned that the entire system had been defeated with a washcloth and a wire coat hanger, all for want of a $50 gap plate for the door. The executives were incredulous and demanded proof, which Vince provided in the form of a field trip. I never learned what happened as a result of that demonstration, but I will never forget the lesson I learned: the simplest solutions are often the most practical.

Sure we could have messed with the prox system, figured out the magnetic tolerances on the lock or scaled the walls and used our welding torches—just like in the movies—to cut a hole in the ceiling, but we didn't have to. This is the essence of no-tech hacking. It requires technical knowledge to reap the full benefit of a no-tech attack, but technical knowledge is not required to repeat it. Worst of all, despite the simplicity, a no-tech attack is perhaps the most deadly and misunderstood.

Through the years, I've learned to follow Vince's advice. I now notice *everything,* and I try to keep complicated thinking reined in. Now, I'm hardly ever off duty. I constantly see new attack vectors, the most dangerous of which can be executed by anyone possessing the will to do so.

TIP

The Key to No-Tech Hacking The key to no-tech hacking is to think simply, be aware, and to travel eyes open, head up. For example, when I go to a mall or some other socially dense atmosphere, I watch people. To me, strangers are an interesting puzzle and I reflexively try to figure out as much about them as I can. When I pass a businessman in an airport, my mind goes into overdrive as I try to sense his seat number and social status; make out his medical problems; fathom his family situation (or sense his sexual orientation); figure out his financial standing; infer his income level; deduce his dietary habits; and have a guess at his home address. When I go to a restaurant, I drift in and out of conversations around me, siphoning interesting tidbits of information. My attention wanders as I analyze my surroundings, taking it all in. When I walk through the parking lot of a building, I check out the vehicles along the way to determine what goes on inside and who the building's residents might be. I do all this stuff not because of my undiagnosed attention deficit disorder but because it's become a habit as a result of my job. I have personally witnessed the power of perception. When faced with tough security challenges, I don't charge. I hang back and I watch. A good dose of heightened perception levels the playing field every time.

A Word about Social Engineering Jack Wiles talks quite a bit about social engineering in his chapter, so I won't belabor it here. Suffice it to say that a good no-tech hacker is also a good social engineer. As we discuss these techniques, bear in mind that an attacker employing good social engineering skills alongside these attacks makes for a very worthy adversary.

Physical Security

I remember my first physical assessment. I imagined myself picking locks and disabling electronic surveillance systems. I imagined myself as that marine in the movie *Aliens*, frantically noodling with wires in an electronic lock, desperately trying to get my team inside to safety. Although I ended up breaking into all sorts of amazing places in real life—and eventually did bypass a number of electronic surveillance systems—I never had to resort to picking a single lock. Simpler techniques always prevailed. In this section, I'll share some of what worked best for me.

Tailgating

Tailgating describes the act of gaining unauthorized access to a restricted area by following closely behind an authorized individual. When I suggested tailgating into the fortress, Vince opted for the washcloth trick. His idea was better given the situation, but tailgating is still one of the best no-tech methods for gaining access to a facility.

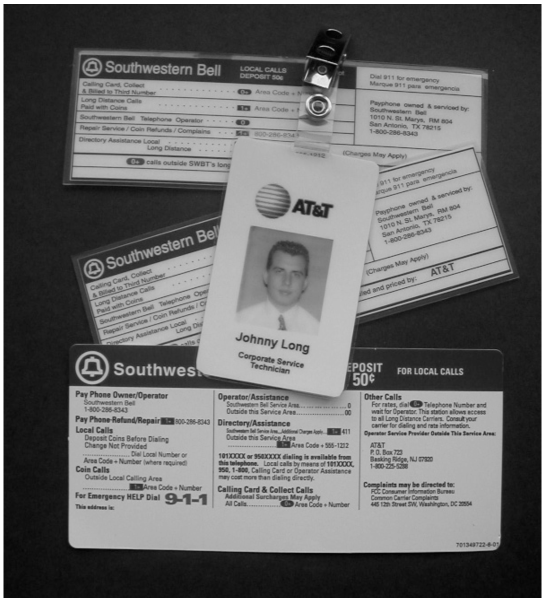
Through the years, I've noticed signs and placards reminding employees to be on the lookout for tailgaters. The fact that "tailgater" has become a common term in the business environment testifies that this is a common problem. Still, it works.

Years ago, I was tasked with a physical assessment against a state government facility. The facility was broken into two distinct areas: an open area to accommodate the general public and a restricted area for state employees. We were tasked with entering the restricted area and gaining access to the closed computer network inside. Our initial reconnaissance revealed that the open and restricted buildings were interconnected, but an armed guard stood watch over the connecting hallway. The restricted building's front door was similarly protected. Swipe card readers—none of which appeared vulnerable to the washcloth trick—protected the side doors. Armed guards in marked vehicles patrolled the parking lots. Somewhat discouraged, we continued monitoring the buildings. Eventually we came upon a cluster of smokers huddled outside near a door. I knew immediately we had found our way in. We headed to the nearest gas station and I bought a pack of cigarettes and a lighter.

I had come prepared to social engineer my way into the building as a phone technician.[2.] I was wearing cruddy jeans, work boots, and a white T-shirt with a phone company logo. I had a phone company employee badge clipped to my collar. My bright-yellow toolbox sported phone company logos and the clear top revealed a small stack of branded payphone info-strips. The toolbox was filled with phone test equipment. A battered hardhat completed the look.

The official-looking getup was, of course, a complete fabrication. I downloaded the phone company logo from the Internet. I printed the T-shirt myself using iron-on transfer paper. I printed the badge on my home printer and laminated it with a $2 kit. The payphone strips were liberated from some local payphones. The phone test gear was legitimate; I had collected it for just such an occasion. I found the hardhat abandoned on the side of the road—its battered condition made it more convincing. (See Figure 8.1.)

Figure 8.1 Paraphernalia of a Phony Phone Technician



Approaching the group of smokers would have been a bad idea, regardless of how good an actor I turned out to be. If they watched me wander towards them from the parking lot, they would certainly consider me an outsider. If instead they came out of the building and found me already there, halfway through a smoke, they might assume I had come *out* of the building for a break.

I waited for the smokers to disburse and made my way to the side door. A pair of employees eventually came out for a smoke and talked amongst themselves. I greeted them casually and joined in their small talk. They chattered about company politics and I nodded appropriately, making sure to blow smoke up into the air every now and then to convince them of my familiarity with cigarettes. I grunted about how the phone system was a pain in the rear-end. They laughed and I tried not to gag on the cigarette, wondering the whole time if I was turning as green as I felt. As they put out their smokes, they swiped their badges. I flicked my cigarette into the road and held the door open for them. They thanked me for the kind gesture and I filed in behind them. Once inside I wished them a good day and had my way with the facility.

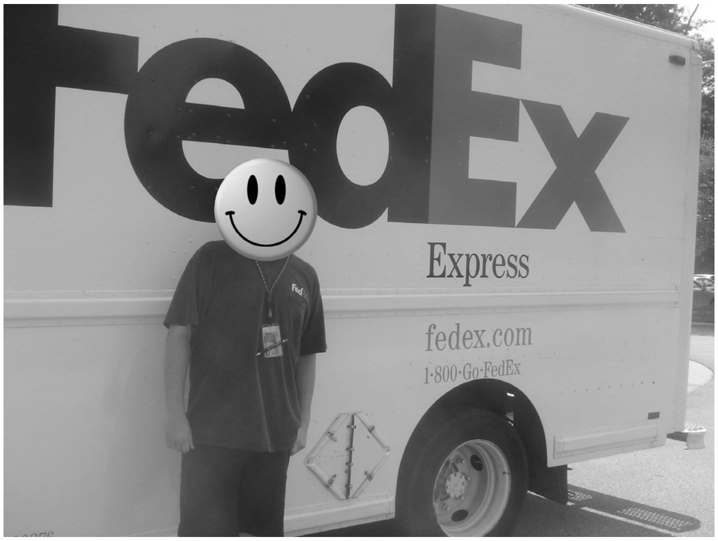
I made my way through the building and was never challenged. At one point, I even walked through the security office. The receptionist looked surprised to see me until I pointed to an empty desk and told her the phone was broken. She wasn't sure whether the phone was broken or not but she let me in—I was the phone guy after all. I plopped my toolbox on the desk, picked up the phone and heard a dial tone. I shook my head, put the phone back on the cradle and lifted my toolbox off the desk, taking with it a stack of important looking documents. I left the office grumbling about stupid work orders and how they always give me the wrong jack number and how it always made me look like an idiot. The receptionist giggled and told me to come back any time. I think she liked me.

All in all, it was a good day. The facility was simple to gain access to despite the expensive safeguards. I left with hardcopy proof of my presence and I had softcopy proof of my intrusion into their network thanks to the data on my paperback-sized computer. The employees never challenged me because they recognized the logo and knew that it belonged to a phone company. If the logo looked legit, the credentials looked legit. If the credentials looked legit, I looked legit. But I had purposely played the role of a technician from the *wrong* phone company. The company I selected was a recognized data and voice service provider. They did not provide local hardware support. In layman's terms, even if I was an employee of that phone company, I had no business being in the facility, and even if I did, I wouldn't have been testing phone handsets.

It all boiled down to playing a convincing role. I used the age-old technique of tailgating to gain initial access to the building and then threw in a healthy dose of social engineering to schmooze those I met inside. Every step of the way an employee took me at face value, even though any one of them could have put an immediate end to the break-in.

Bear in mind that the phone technician gag isn't the only one at my disposal. Depending on the situation, I could have played the role of a delivery person, an electrician, a plumber, an elevator repairman or any other kind of service personnel. The choices are endless. All I need to do is be in the right place at the right time, present a convincing demeanor, and dress the part. Finding the right place and time takes patience. Schmoozing takes practice. Dressing the part simply requires that I get a decent photo of the person I'm interested in imitating. At first, I found this difficult. I would sneak around trying to get a crisp candid photo to work from, but failed miserably. The pictures would end up blurred or off-centered, and in most cases I couldn't make out the small details that render the outfit convincing. Eventually I learned to follow my own advice and take the simplest approach. Now, I just *ask* for permission to photograph service personnel. I ask in a polite, non-threatening way and most workers are more than happy to oblige me. The guy shown in Figure 8.2 was extremely accommodating, allowing me to photograph his outfit, his truck and even his employee badge.

Figure 8.2



NOTE

You'll certainly tire of hearing this, but it bears repeating. The delivery company is not at fault for allowing their employees to be photographed. The security weakness lies in allowing your employees to remain non-confrontational when something seems off. Employees need to understand that tailgating should never be permitted, and service personnel should not be taken at face value. Challenge their presence, especially if they are unfamiliar or something seems out of place.

Where Are Your Badges?

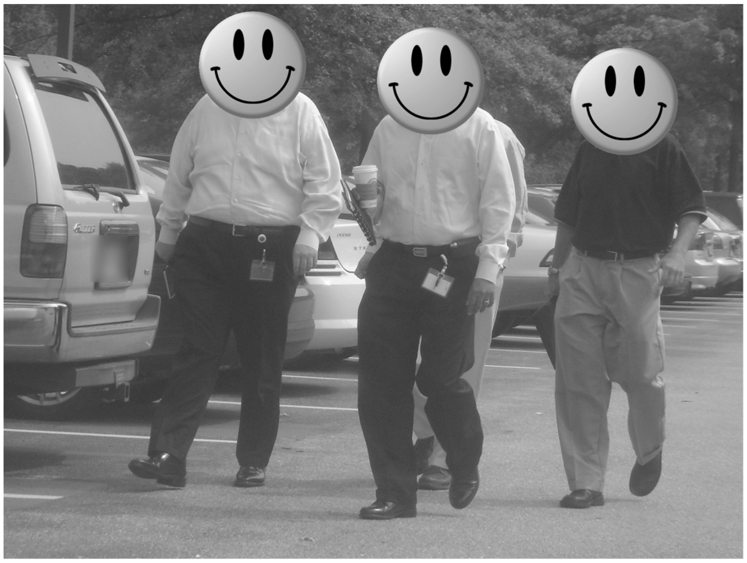
My phone company getup was convincing, but without the badge I doubt I would have made it inside. The badge identified me as a phone guy. However, the badge was nothing more than a laminated bit of printer paper. To use security jargon, that laminated paper was my *authentication token*. By letting someone visually inspect it, they could draw a conclusion about whether or not I was legitimate. This type of visual identification is a weak authentication mechanism because it is so easily duplicated. Unfortunately, many facilities rely on exactly this type of security, yet it amazes me how many badges I see worn out in public.

I spot at least ten different types of badges a day. If I had a nickel for every time I saw a new badge, I'd have a *whole* lot of nickels. Even though I've seen hundreds or thousands of badges in my lifetime, I still get giddy when I see a new one because I know beyond a shadow of a doubt that I could somehow use it to gain access to that company. Even if they employ some sort of electronic system to validate the card—we'll talk more about those systems later in this section—I could probably use the badge to tailgate or social engineer my way inside. Getting giddy about site badges is admittedly strange, but I've long since given up on the doldrums of normality. These days I go all the way; I carry a camera wherever I go to capture badges I spot in the wild. I spotted the badge shown in Figure 8.3 in a local mall.

Figure 8.3

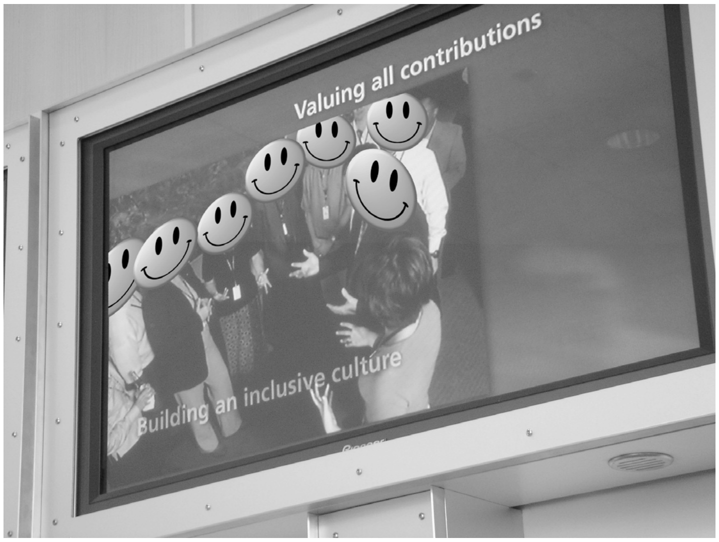
Badges sometimes appear in packs, as the photo in Figure 8.4 reveals.

Figure 8.4



I captured this next photo (see Figure 8.5) as I sat in a corporate lobby. The walls were lined with all sorts of plaques and awards that the company had earned through the years. Several flat-screen monitors droned through PowerPoint presentations extolling their corporate virtues. I amused myself with a game of "count the buzzwords" until I saw this particular slide and nearly flipped backwards out of the overstuffed leather armchair.

Figure 8.5

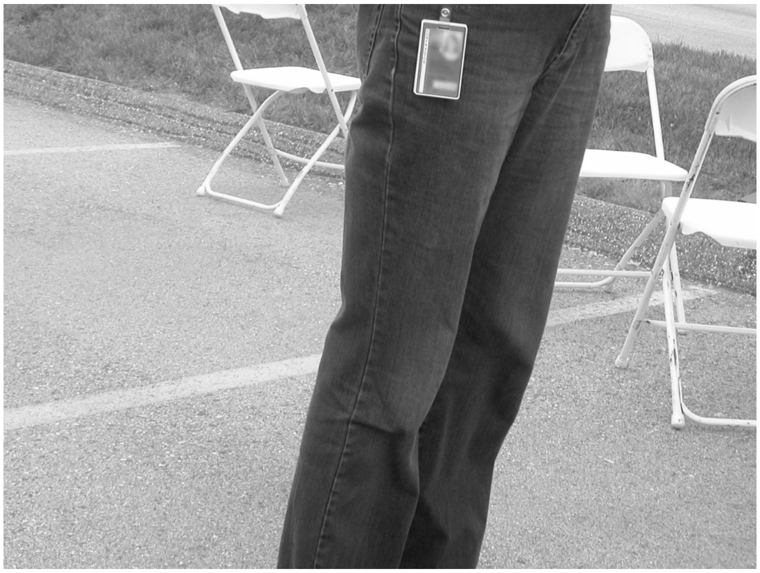


This slide was one of several that showed groups of employees—in various stages of corporate bonding—all wearing their badges. After spending a total of two minutes in the building's open lobby, I had no less than ten badge photos. Fortunately for this company, I was "off duty" and never discovered if a laminated bit of printer paper would be enough to work my way inside.

Government agencies have known for years that employee badges should be removed when leaving the workplace. The more secretive agencies are very proactive when it comes to enforcing this policy. I was not surprised to discover so few open-air badges around more secretive government buildings. The keyword here is *few*. While spending some time in the D.C. corridor, I came upon an outdoor barbeque catered by an office leasing company. The event was designed to show appreciation for the various corporate tenants, some of which were government related. As I wandered around the large catering tent, I was amazed at the number of badges I spotted. I was so busy snapping pictures of people that I nearly forgot to take advantage of the free grub.

Although I saw badges belonging to several different companies, some were more surprising than others, like the airfield badge shown in Figure 8.6.

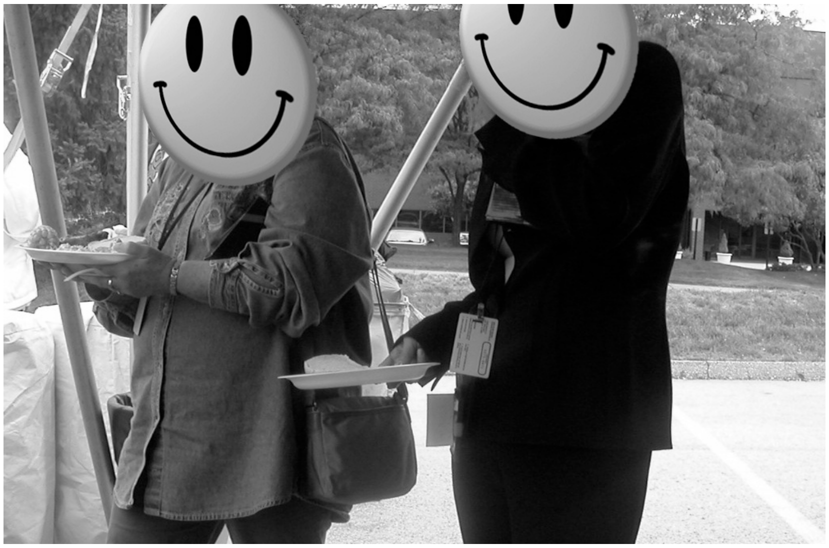
Figure 8.6



I am relatively certain that airport security personnel do not rely solely on visual badge identification as an authentication mechanism, but the photo is interesting nonetheless considering it was taken well away from airport property.

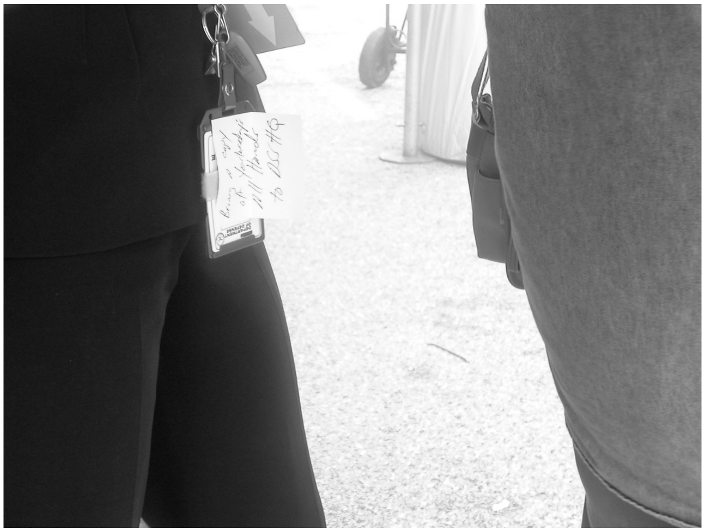
Two women waiting in line caught my eye (not in that way). The taller of the two was very important-looking. She was dressed in a smart black suit and was having an important-sounding conversation on her Blackberry cell phone. It wasn't the geek-chic cell phone that caught my eye, but rather the plethora of badges and paraphernalia dangling from her lanyard. Traveling in tech circles, I've seen my share of lanyard clutter, but this nice lady took the prize for most neck-flair toted by a female. (See Figure 8.7.)

Figure 8.7



As I drew closer, I realized that her badge was decidedly governmental in appearance. I took a few photos—which neither of them seemed to notice—and after reviewing them, I realized I had a horrible angle on the more interesting badges. As she continued chatting into the phone, I swung around to the other side of her and stepped in as close as I could without triggering her (admittedly impaired) stalker detection system. Less than a foot away from her, I snapped the photo shown in Figure 8.8.

Figure 8.8



This particular badge is issued to government employees stationed at the Pentagon. The Post-It note reminds her to "bring a copy of yesterday's all hands to DSS H.Q." Granted, security at the Pentagon is second to none. I know from personal experience that the guards stationed at the Pentagon mean business. They are not to be trifled with. I also know that visual identification of a badge at the Pentagon means absolutely nothing. All badges are electronically verified, and the security of that electronic process is world-class. Still, I had no doubt that Pentagon security personnel would not take kindly to employees exhibiting this kind of careless behavior. I'm not pointing the finger at the Pentagon, but I need to illustrate an important point: even the most die-hard government agencies hire sometimes-careless human beings. The *policies* in place at the Pentagon ensure that careless behavior does not negatively impact the security posture of the facility. Corporate security officers should take this lesson to heart. Visual identification of an employee badge is not a secure authentication mechanism. Do not allow any avenue for social engineers. Establish a secure access mechanism and back it up with sound, enforceable policy that employees understand and are bound to. Employees should understand that security is not someone else's problem.

Electronic Badge Authentication

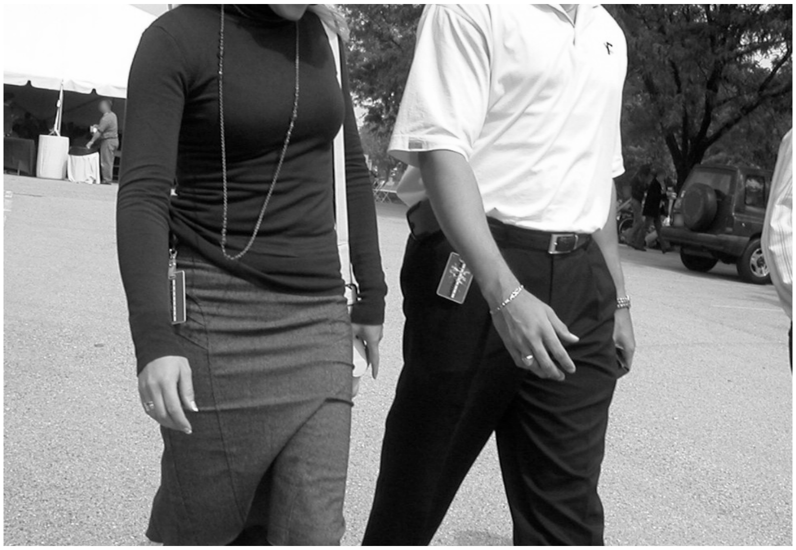
I think I have successfully established that visual badge identification is inherently insecure. Electronic verification is a much more secure method of authentication. Although electronic systems have security issues as well (see the sidebar) there are some no-tech attacks that are interesting as well. It is not uncommon to see proximity-type cards in plain view, as shown in the photo in Figure 8.9.

Security Alert…

High-Tech Badge Attacks

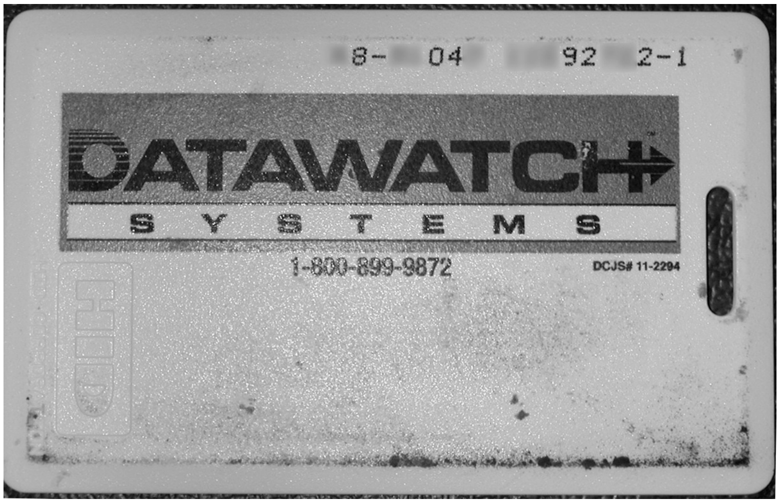
Many technological differences exist between *swipe* cards and *proximity* or *contactless* cards, but they can be attacked in similar ways. Both can be copied, but thanks to the device developed by Jonathan Westhues (detailed at http://cq.cx/prox.pl) contactless cards can be copied from a distance even when they are carried in a pocket or purse. To prevent this type of attack, consider combining access cards with PIN identification schemes, or deploy a system that relies on encryption, challenge-response systems, or reader access lists, like HiD's *iClass* line.

Figure 8.9



This pair had executed good common sense and removed their site badges. However, their access cards were still in plain view. Although the possibility existed for cloning the cards, in the spirit of no-tech I suggest that an adversary can use visual inspection to learn quite a bit about the card's owner. Consider the typical *Datawatch* card shown in Figure 8.10.

Figure 8.10



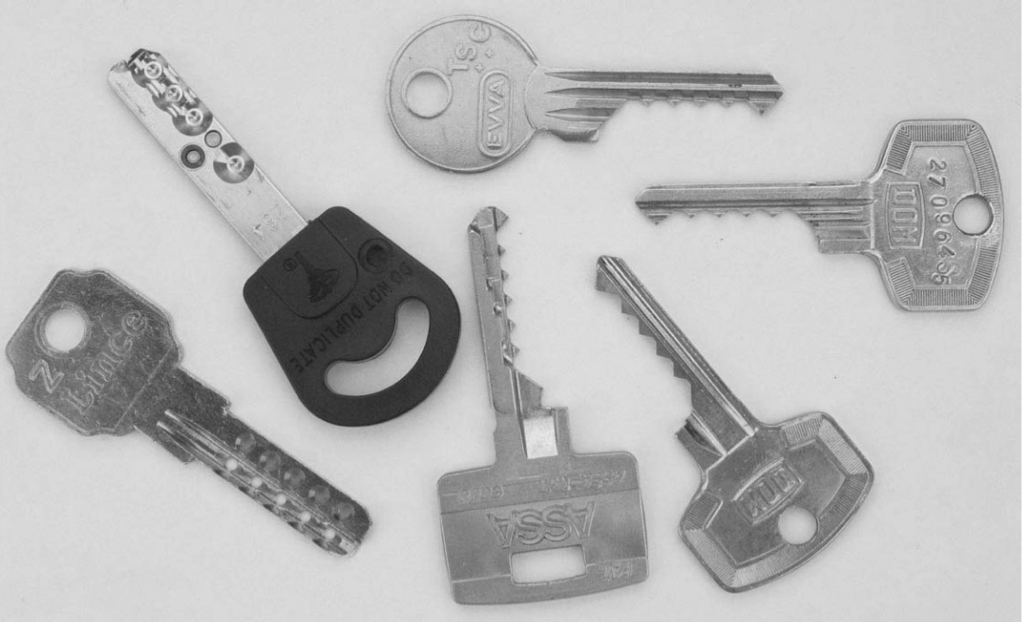
The logo on the left-hand side of the photo reveals it was manufactured by HiD Corporation (http://www.hidcorp.com). The physical characteristics and lack of additional logos on the card suggest it is *proximity*-based and is not an *iClass* card. This means the card may be prone to duplication. The toll-free number on the card belongs to Datawatch Systems. An adversary can call this number, speak to a representative, read off the top row of numbers, and learn not only the address and building number the card will work on, but in some cases the suite or room number as well.

Most people would never consider wearing a Post-It note on their forehead revealing their work address, but it's surprising how many people wear these electronic cards in plain sight which reveal essentially the same information. Access cards like these should be removed when leaving a work area.

Lock Bumping

Lock picking is a fairly technical exercise. It requires knowledge of lock mechanics and internals, and perfecting the technique takes quite a bit of practice. *Lock bumping*, on the other hand, falls firmly into the no-tech hacking category. The technique involves the use of *bump keys*, or *999 keys*, which are keys that have been made by cutting a key blank so each cut is made to a maximum depth and the tip and shoulder have been filed down by approximately half a millimeter. To a trained eye, bump keys have a very distinct look—the cuts are too uniform—as shown in Figure 8.11.

Figure 8.11



Permission Granted by Toool—The Open Organization Of Lockpickers

The technique works by inserting a bump key into a lock and tapping the key while turning the key slightly in the lock. The bottom internal pins in the lock are nudged, transferring momentum to the pins sitting above them. As the top pins fly upwards, the bottom pins remain down. When the pins separate, the cylinder can be turned, and if done correctly, the lock will open. Bypassing a lock with a bump key takes much less skill than picking the lock with a traditional lock pick set or electronic pick device. This means that just about anyone can compromise a vulnerable lock. For more information on prevention and identification of vulnerable locks, see the references mentioned in the sidebar, or personally contact a professional locksmith or security provider.

Security Alert…

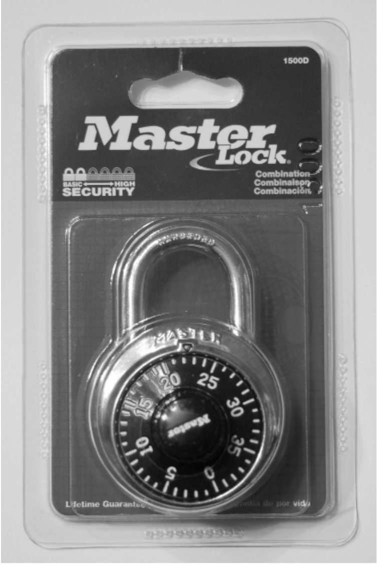
Treasure Trove of Bumping Info

Lock Bumping has been around for many years, but has gained popularity because of several recent works. Marc Tobias's book *Locks, Safes, and Security* is an excellent reference book for professionals, and includes a great piece on bumping or "rapping" as it is sometimes called. His Web site (http://security.org) and alerts page (http://security.org/dial-90/alerts.htm) is also an excellent resource. If you're looking for more accessible material, I highly recommend the awesome whitepaper *Bumping Locks* (http://www.toool.nl/bumping.pdf) by Barry Wels and Rop Gonggrijp of Toool, The Open Organization of Lockpickers, and their awesome video workshop *What the Bump?* at http://connectmedia.waag.org/toool/whatthebump.wmv. The Toool Web site (http://connect.waag.org/toool) has a ton of resources and videos I highly recommend.

Master Lock Brute Forcing

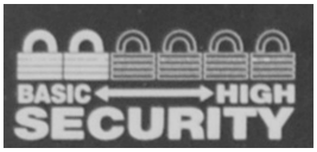
As a kid, I remember seeing the cool Master Lock commercial with the lock that was secure even after being drilled clean through by a rifle round. For me, and for many others, Master Lock became synonymous with security. To this day, I purchase Master Locks based on the brand name alone. However, do not buy just based on the brand name. Always investigate all the product offerings to make sure you're getting a product that suits your needs. For example, the Master Lock model 1500D combination lock is ubiquitous (see Figure 8.12).

Figure 8.12



However, as Figure 8.13 shows, the packaging clearly reveals that the lock is meant for only basic security tasks.

Figure 8.13



Still, I see this exact lock used in high-security applications almost daily, despite the fact that a dangerous brute-force attack against it has come to light.

Brute forcing describes a technique in which every possible solution for a problem is checked to see if it is the solution. For example, a hacker could brute force a password by trying every combination of possible passwords until one works. This technique is relatively slow, even when automated, but if every possible combination is tested, it works reliably. Most mechanical combination locks can be brute-forced if an adversary has enough time and patience to complete the attack—and therein lies the rub. Most adversaries have neither the time nor the patience to brute force a combination lock. In the case of the Master Lock, if we assume each of the numbers on the dial is active—which is not the case—we are left with 40^3 or 64,000 possible combinations. If an attacker tries one combination every five seconds—a reasonable speed considering the clearing process and the left-right turns—it could take as long as 88 hours, or nearly four days, to work through every combination. At this rate, the attacker would fall before the combination did.

A shortcut was discovered that reduces the number of combinations to 100. At five seconds per attempt, it would take an attacker a mere eight minutes to brute force one hundred combinations. Since this book is about protecting your own assets, I won't go into all the details required to open a lock using this technique, but rather I will describe how to arrive at the last number in the combination. If you use this technique against your own locks and are able to determine the last number of the combination, you may want to have a professional locksmith evaluate your situation, or choose a higher-security Master Lock.

To begin, you will need to apply tension to the shackle of the lock. A simple way to do this is to hold the lock in one hand and use a finger to apply upward pressure as shown in Figure 8.14. The stylish thumb ring is optional for this exercise.

Next, begin turning the dial. If enough tension is applied, the dial should stick between two numbers. This is called a *sticking point*; 12 sticking points exist on each affected lock. The first goal is to keep a record of the location of each sticking point. For example, the lower boundary of this lock's first sticking point is one. (See Figure 8.15.)

Figure 8.14

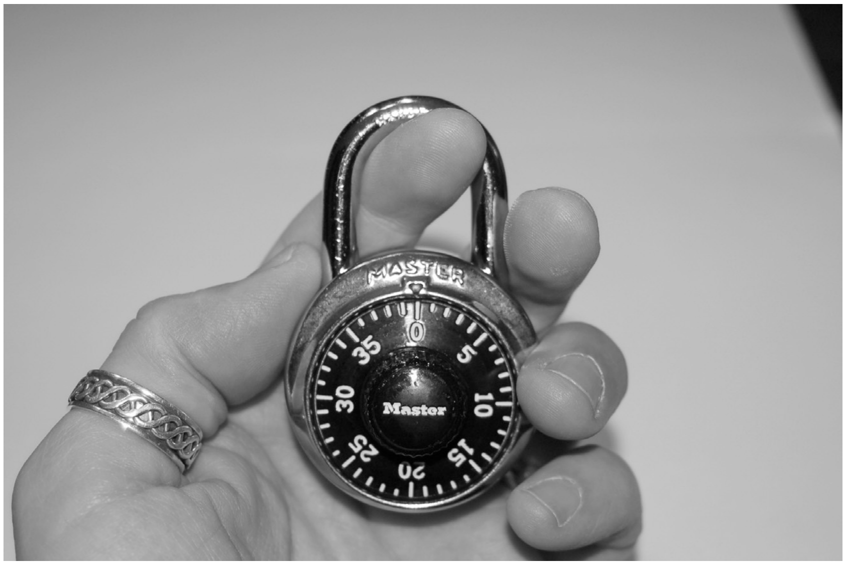
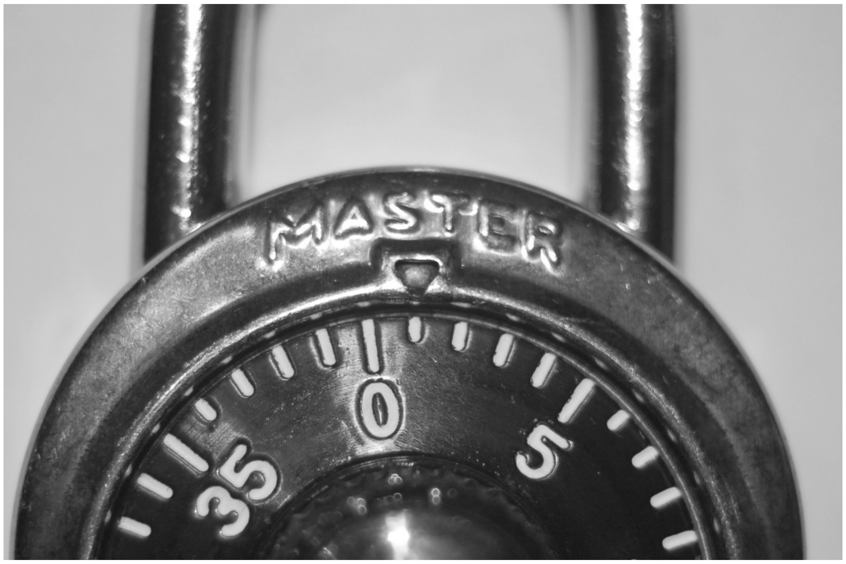
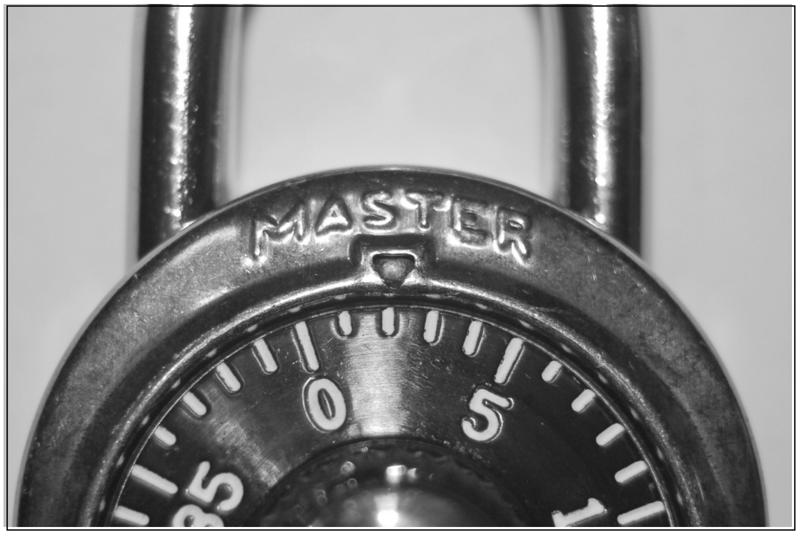


Figure 8.15



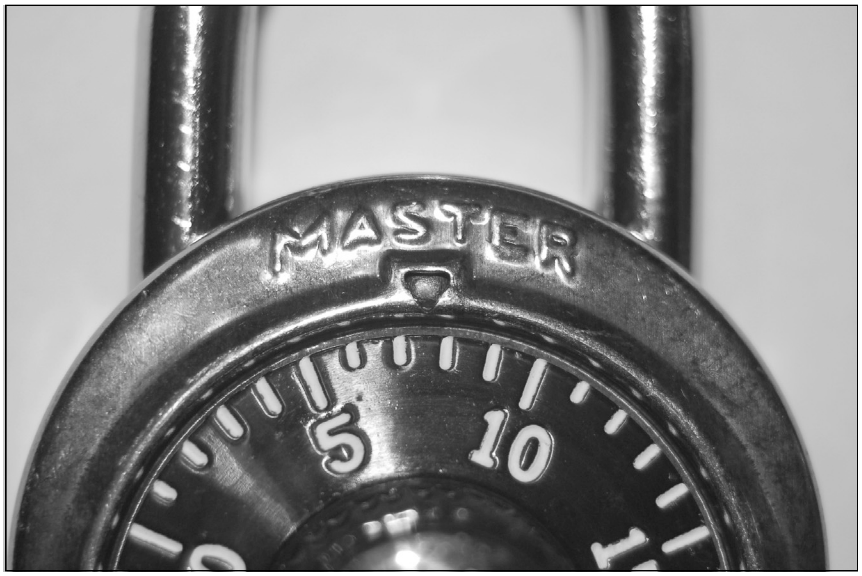
The high boundary of this same sticking point is the number two as shown in Figure 8.16.

Figure 8.16



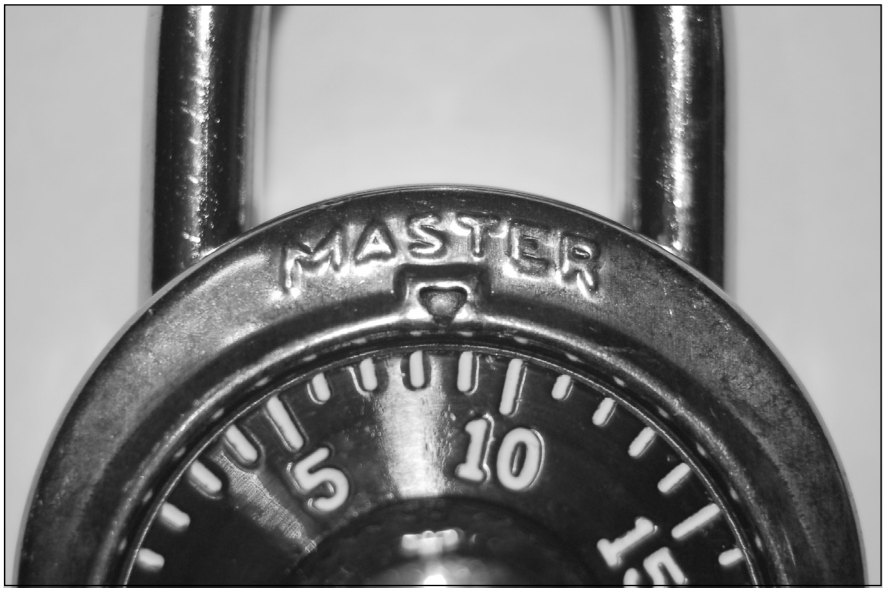
The location of the first sticking point rests between these numbers at 1.5, which is obviously not a whole number. To find the next sticking point, release the tension on the shackle, turn the dial past the current sticking point's high boundary and reapply tension. The dial should stick again, revealing the location of the next sticking point. Some sticking points will rest on whole numbers. For example, the low boundary of this sticking point is 7.5. (See Figure 8.17.)

Figure 8.17



The high boundary of this same sticking point is 8.5 as shown in Figure 8.18.

Figure 8.18



This means that the sticking point rests on eight. Keep a record of each sticking point. Table 8.1 shows the sticking points of my test lock.

Table 8.1 The Sticking Points on My Lock

Low Boundary	High Boundary	Sticking Point
1	2	1.5
4	5	4.5
7.5	8.5	8
11	12	11.5
14.5	15.5	15
17.5	18.5	18
21	22	21.5
24	25	24.5
27.5	28.5	28
31	32	31.5
34	35	34.5
37.5	38.5	38

Notice that more than half of the sticking points do not land on whole numbers. These are decoys and should be removed from the list of potential combination digits. In our example, we are left with five numbers: 8, 15, 18, 28, and 38. Notice that each of these numbers end in the same digit—the number eight. These matching numbers should be removed from the list as well, leaving only one number, 15, which is the last digit of my lock's combination.

If this technique works on your lock, there's a good chance the lock is vulnerable to a brute-force attack. If the technique does not work, you may have a newer 1500D Master Lock. It is speculated (on www.wikihow.com/Crack-a-Master-Combination-Lock) that 1500D Master Locks with serial numbers beginning with the number 800 are not vulnerable to this attack, although unverified sources have reported success against these newer locks as well. Either way, don't be quick to throw stones at Master Lock. Do your research, and don't purchase basic security products for high-security tasks. Consider purchasing a higher security Master Lock for your application, or get the advice of a professional locksmith or security professional.

NOTE

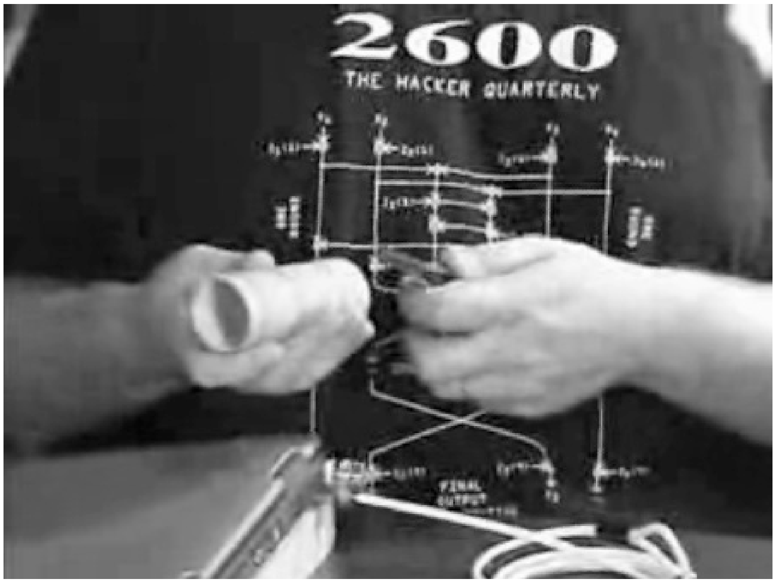
Several Web sites—listed at the end of this chapter—discuss this vulnerability in great detail. However, there's a decent amount of math and memorization involved in determining the first and second digits of the combination. Tim "Thor" Mullen presents a shortcut he worked out in his book *Stealing the Network: How to Own A Shadow* by Syngress Publishing. The story, co-authored by Tim, Ryan "Blue boar" Russell, and myself, tells a gripping tale of what hackers are capable of in the real world. By all accounts, the story is fiction, but the techniques, like the Master Lock brute force, are not. Check out the entire *Stealing* series to see what you might be up against when the hackers take the gloves off!

Picking Locks with Toilet Paper?

In 1992, the BBC reported that certain cylindrical axial pin tumbler locks were vulnerable to bypass by unskilled thieves. Twelve years later, in August of 2004, Marc Tobias, author of *Locks, Safes, and Security,* found that Kensington and Targus were using similar cylindrical axial designs in their laptop lock products. His report suggested that the locks could be easily bypassed with a pen or a toilet paper tube. In September of 2004, Chris Brennan described on his forums (www.bikeforums.net) how an expensive Kryptonite bike lock (which used the same cylindrical axial design) could be bypassed with a Bic pen. Chris posted videos to www.bikeforums.net/video and a media frenzy ensued.

Enter Barry Wels of Toool. While presenting at a hacker conference, Barry created a video (http://www.toool.nl/kensington623.wmv) showing how to apply the bypass technique to a specific Kensington laptop lock system. The hacker community found the video interesting, but the public in general was awed by the fact that he accomplished the bypass in mere moments using the cardboard from a toilet paper roll. (See Figure 8.19.)

Figure 8.19



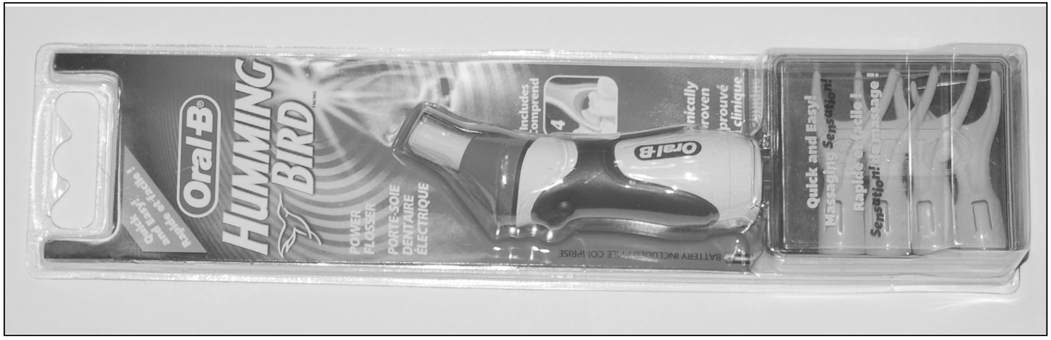
While there is always speculation about who thought of what first, nearly one million people have downloaded the video from Barry's site, and countless others have downloaded it from sites like Youtube.com. I love Barry's video because it is so accessible and it clearly demonstrates what I'm trying to show in this chapter: even the most complex security systems are at risk from simple attacks. If you have sensitive data on a laptop, and you rely on a single locking device to protect that data, you'll probably get burned whether or not the lock is vulnerable to this attack. Whenever you rely on a single layer of security, odds are you'll get burned. A laptop lock isn't a bad idea, but if you're concerned about losing sensitive data on the machine, consider some sort of crypto solution as well. Above all, try to think like a hacker. In that frame of mind, is a spindly cable the best solution?

Electric Flossers: A Low-Tech Classic

Lock picking is a real skill. To do it right, you've got to have a working knowledge of how locks operate and you need to practice. With the advent of newer devices, lock picking seems more accessible than ever. Still, lock-picking guns and electric devices are not foolproof. They require a decent amount of skill to successfully operate. In addition, these electric devices are expensive. Most amateurs would not consider investing a small fortune in a specialized device that's not foolproof.

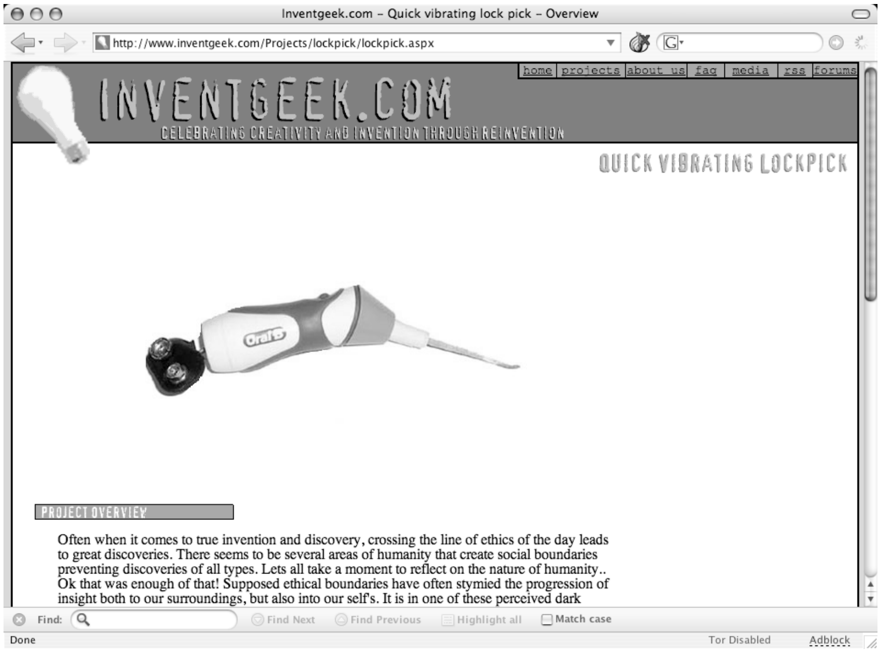
I can just imagine the look on some hacker's face when he or she strolled down the dental care aisle in the local Wal-Mart and spied this new-fangled electronic flossing device. (See Figure 8.20.)

Figure 8.20



I'm not sure who came up with the idea of hacking this innocent-looking thing, but someone did. The result was a tiny, inexpensive electric lock-picking system. According to Jared Bouck over at Inventgeek.com, this little device, when combined with even a makeshift tension wrench, will open most padlocks in a matter of seconds. (See Figure 8.21.)

Figure 8.21


Inventgeek.com – Quick vibrating lock pick – Overview
http://www.inventgeek.com/Projects/lockpick/lockpick.aspx
home
projects
about us
faq
media
rss
forums
INVENTGEEK.COM
CELEBRATING CREATIVITY AND INVENTION THROUGH REINVENTION
Oral-B
Find:
Find Next
Find Previous
Highlight all
Match case
Done
Tor Disabled
Adblock

QUICK VIBRATING LOCKPICK

PROJECT OVERVIEW

Often when it comes to true invention and discovery, crossing the line of ethics of the day leads to great discoveries. There seems to be several areas of humanity that create social boundaries preventing discoveries of all types. Lets all take a moment to reflect on the nature of humanity.. Ok that was enough of that! Supposed ethical boundaries have often stymied the progression of insight both to our surroundings, but also into our self's. It is in one of these perceived dark

The Web site demonstrating the technique is located at inventgeek.com/Projects/lockpick/lockpick.aspx, and the video demonstrating the technique in action can be found at inventgeek.com/Projects/lockpick/lockpick.avi. This might be a good time to revisit the no-modified-electric-flossers-in-the-workplace policy.

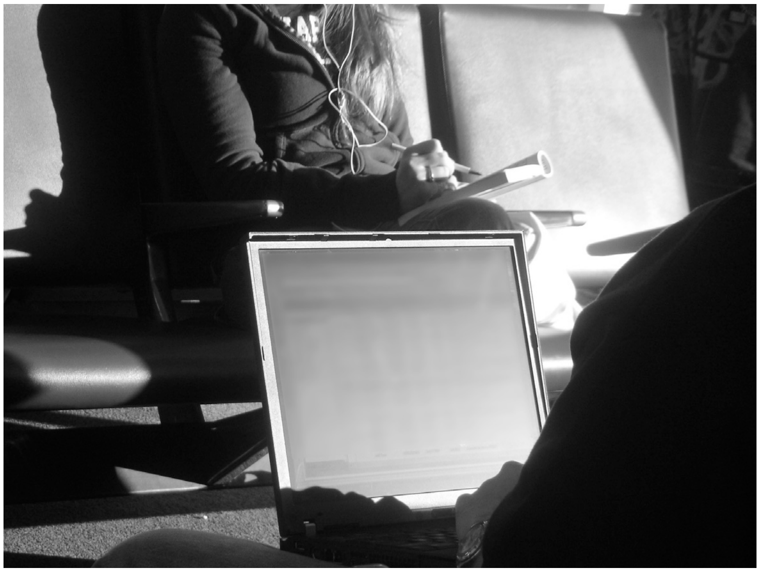
Information Security

A physical vulnerability can certainly put your information at risk, but there are quite a few no-tech hacks that can place your information at risk directly. In this section, I'll share a few of the more popular no-tech hacks I've relied on over the years.

Shoulder Surfing

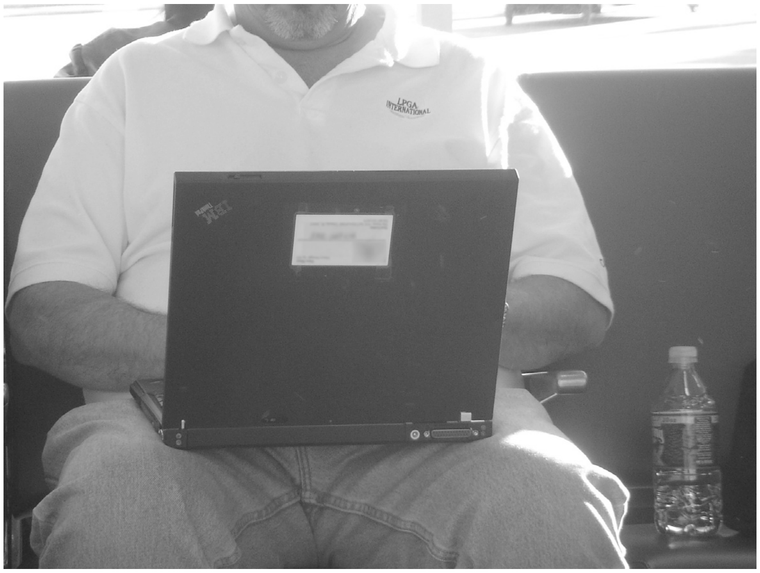
Shoulder surfing is a classic no-tech attack in which an adversary peers over the shoulder of a victim with the intention of gleaning sensitive information like usernames or passwords. Although the technique has been around since the invention of the computer itself, the attack is still amazingly effective thanks to the proliferation of portable computers and wireless public access points. (See Figure 8.22.)

Figure 8.22



Although I will primarily focus on information that can be gleaned from simply looking at the screen, I have come to realize that a great deal of information can be determined by looking at the machine itself. (See Figure 8.23.)

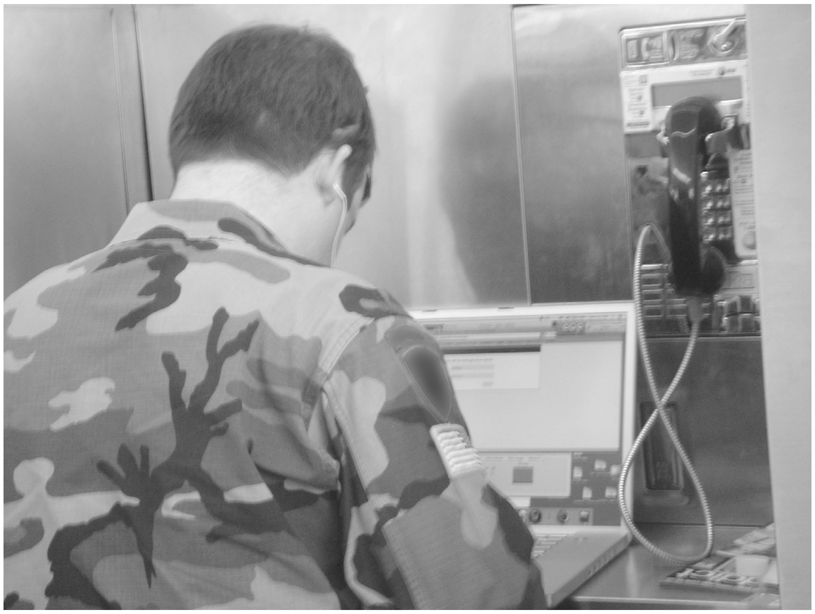
Figure 8.23



The business card attached to this machine not only highlights the name of the company this gentleman works for but also his name, job title, address, home phone, and cell phone numbers. As an adversary, I could perform my initial reconnaissance on him without even glancing at his screen. In many cases, I see property stickers, property passes, barcodes, and even stencil paintings on machines. An adversary can use this information to profile and perhaps even target an individual.

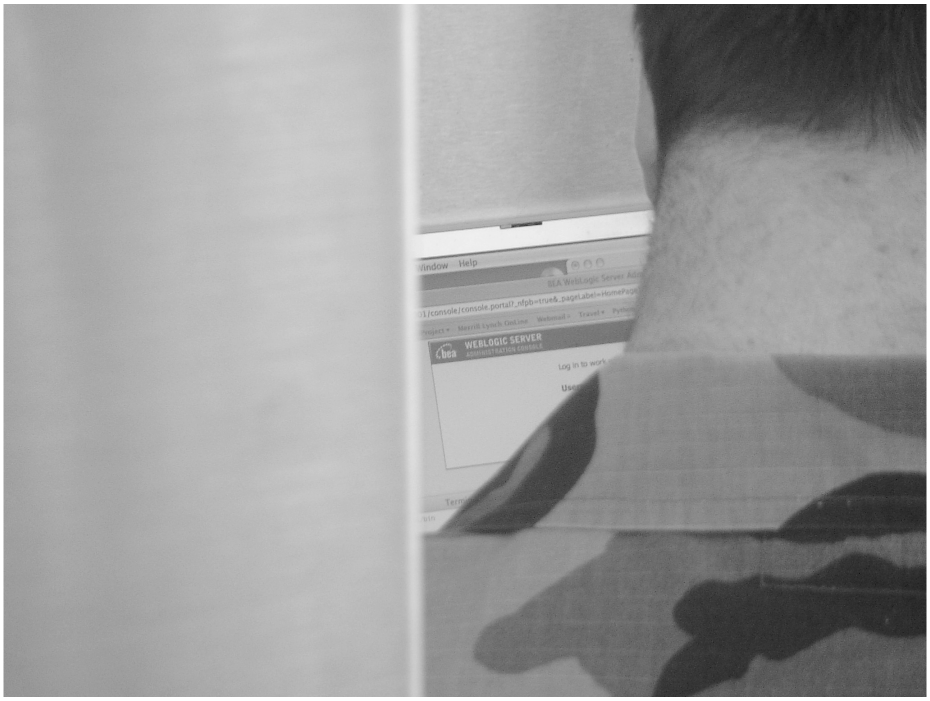
Some individuals, like members of the military, are extremely conspicuous when seen in public. I don't need to see a business card to realize that the gentleman in Figure 8.24 is a member of the United States military.

Figure 8.24



It's not hard to tell that he is a fan of Apple products. The Mac Addict magazine, the Mac laptop, and the iPod headphones all confirm this. If I were to start a conversation with him in order to glean sensitive information, I could use his love (and my knowledge) of Macs to naturally engage him. In this situation though, social engineering was not necessary. With the headphones on and his back turned, he was oblivious to my approach. I was able to take several pictures of him as he worked and I eventually approached to within inches of him. I snapped the photo in Figure 8.25 that revealed in stark detail not only the dermatologic properties of his neck but also his laptop screen.

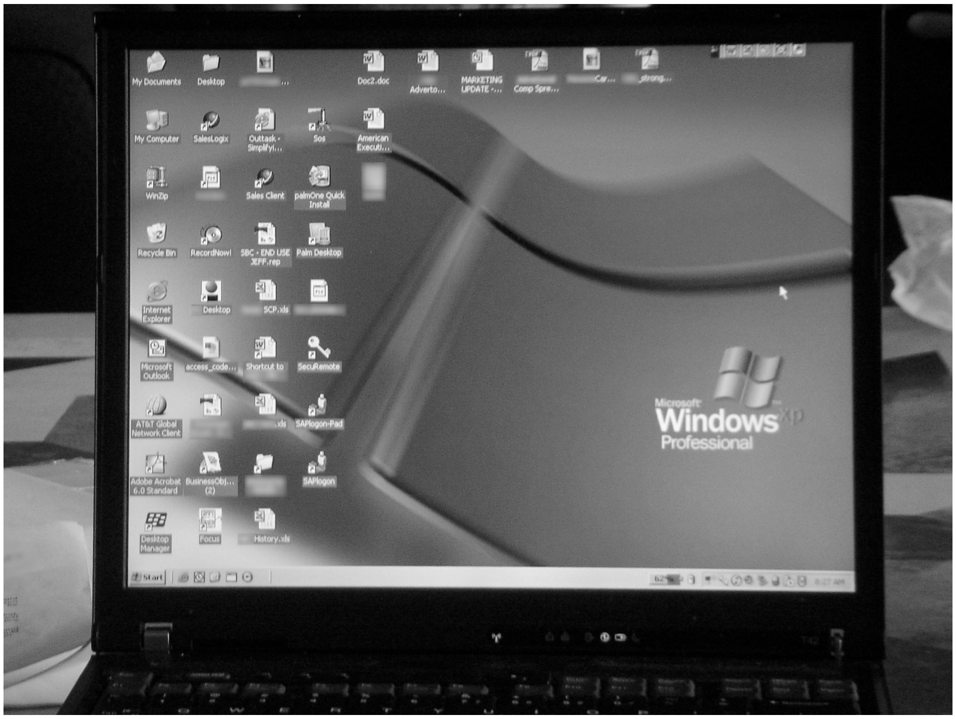
Figure 8.25


Window Help
BEA WebLogic Server Adm
01/console/console.portal?_nfpb=true&_pageLabel=HomePage
Project ▾ Merrill Lynch OnLine Webmail ▸ Travel ▾ Python
bea
WEBLOGIC SERVER
ADMINISTRATION CONSOLE
Log in to work
User
Termi
/bin

As it turned out, he was not casually surfing the Web, but was logging into the administrative console of a BEA WebLogic server. I watched as he typed in his credentials, made a quick adjustment to my camera and took another photo. The flash fired as I had instructed it to, and he turned around sharply, finally noticing me. I quickly pointed the camera towards myself and rubbed my eyes. He shrugged and returned to his work, convinced, I assume, that I was some kind of digital camera newbie just figuring out the ropes. This is common behavior. Most users of portable computers have grown accustomed to blocking out the world around them. This makes the job of an adversary even easier.

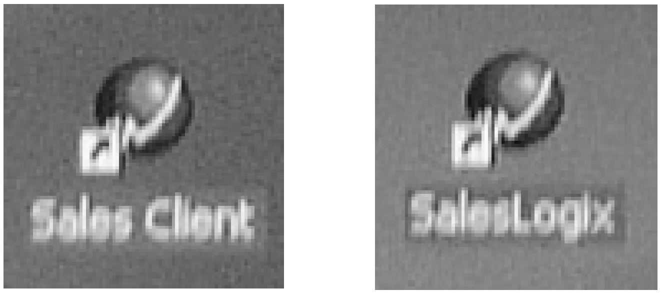
However, there's a bit more to shoulder surfing than simply reading a login page. Often, an adversary can piece together a startling amount of information from what seems like very little. Take, for example, the photo in Figure 8.26 of a temporarily unattended laptop I spotted in a coffee shop.

Figure 8.26



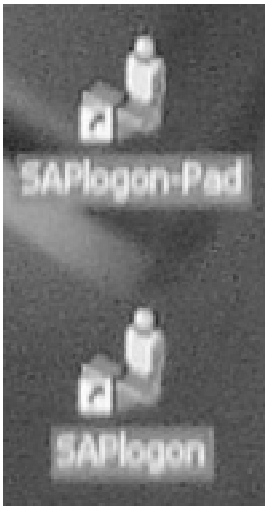
I have altered the image to keep the owner's company name confidential, but by using the information on the screen, an accomplished no-tech hacker can glean an awful lot of information. For starters, the desktop background indicates that the laptop is running Windows XP Professional. Other aesthetic clues such as the Start button configuration back this up. The operating system of a machine is a necessary piece of information a technical attacker can use to determine the type of attack to launch. Generally, an attacker would need to analyze a series of network packet responses to determine this information, but in this case that is probably unnecessary; it is unlikely the laptop's owner has installed another operating system's desktop background. Although they are a bit blurry since they were captured in the field, the desktop icons reveal more information. (See Figure 8.27.)

Figure 8.27



This is obviously some sort of sales software, but a Google search reveals that SalesLogix is the leader in mid-market CRM (customer relationship management) software. The search goes on to say that SalesLogix is "the most powerful sales tool on the Web." Another pair of icons (shown in Figure 8.28) refers to *SAP*, a common business software solution provider.

Figure 8.28



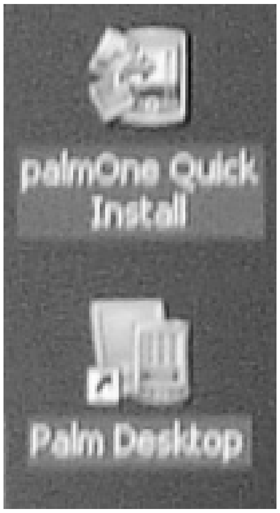
The existence of the SAP logon client indicates the logon credentials for the service may be installed on the laptop as well. Another similarly interesting icon reads *SecuRemote*. (See Figure 8.29.)

Figure 8.29

A Google search reveals that *SecuRemote* is a virtual private network (VPN) client. As with the SAP logon software, all or part of the VPN credentials may reside on the laptop. This could grant an adversary access to services inside the corporate network. At the very least, the mere existence of a particular brand of VPN is valuable information to a technical attacker.

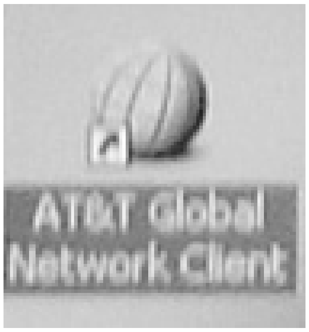
Two more icons on the desktop reveal that *Palm* personal digital assistant (PDA) software has been installed on the machine. (See Figure 8.30.) The existence of this software on the laptop suggests the owner is most likely in possession of a Palm PDA device.

Figure 8.30



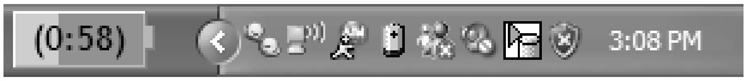
These icons also suggest that the Palm device is backed up onto the machine. If an adversary gains access to the laptop, they may also gain access to the data stored on the Palm. Another icon (shown in Figure 8.31) reveals the existence of the AT&T Global Network Client.

Figure 8.31



The icons provide a great deal of information, but a technically savvy attacker can learn even more by looking at other details on the screen. For example, what information can you determine by looking at the taskbar shown in Figure 8.32?

Figure 8.32

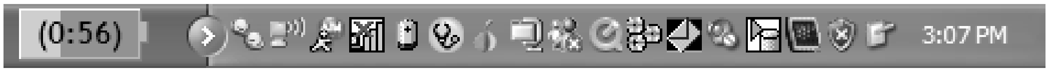


The taskbar itself reveals that the operating system of the machine is a modern version of Windows. The battery indicator shows this machine is most likely a laptop, and that there are 58 minutes of battery power remaining. We can tell that the system is currently unplugged from a power source because there is no electrical plug icon next to the battery. The icons reveal a great deal of information about the system as well. Starting from the left, the first icon is for Trillian, an instant messaging aggregator. The color and style of the icon reveal that the application is currently connected. The next icon shows the machine is connected to a wireless access point. The ever-popular AIM (AOL Instant Messaging) icon is next, and the style indicates it is also connected to a server and that the user is logged in. The battery icon is self-explanatory. The MSN instant messenger icon is next. It shows the service is disconnected and thus the user is not logged in. The speakers are muted, as revealed by the next icon. The white rectangular icon belongs to the IBM Hard Drive Active Protection icon, which indicates that an IBM hard drive is installed in the machine and that no shocks have been detected. The last icon, the Microsoft Security Center, is an indicator that the operating system of the machine is Windows XP or later. Last but not least, the system clock is set to 3:08 P.M. This information can be correlated with the current local time to help determine the time zone the owner originated in.

This is a great deal of technical information, but it also reveals quite a bit about the owner. We know, for example, that he or she is a heavy instant messenger user, as evidenced by the number of clients installed. It also appears, at first glance, that the user is non-technical since the running applications are simple in nature—other than the IBM software, which may have been installed by default.

A busier task bar reveals even more. What can you tell from looking at the expanded version of the taskbar in Figure 8.32? What judgments can you make about the user based on the taskbar revealed in Figure 8.33?

Figure 8.33



Many of the icons look the same, but some are different, and they change the profile of the user slightly, uncovering more specific information about the machine being used. The icon to the left of the battery indicates the laptop has an Intel Pro/Wireless 2200BG wireless network adapter. The icon to the right of the battery icon indicates that Norton Anti-Virus is running and that auto-protect has been enabled to protect against virus threats. The next icon, the one that looks like a green onion, would raise a technical user's eyebrows and would make the owner of the laptop a very interesting target. The onion is an icon for Vidalia, a package that incorporates Tor (The Onion router) and privoxy, two tools used to anonymize a user's Internet activity. A user surfing the Web with Tor enabled surfs in complete and utter anonymity. Remote Web sites can't tell where they are coming from, and anyone sniffing the local network traffic can't see where they are going. The blue envelope icon belongs to the IBM Message Center, which confirms that the laptop was most likely manufactured by IBM. The last icon on the right belongs to the Windows Tablet and Pen Settings Control Panel item. This reveals that the machine is a tablet PC.

Again, this information is very interesting to a technical attacker, but when pulled together it can be used to paint a very clear picture of what type of information the machine might contain and the technical ability of the machine's owner.

So what can you do? The best defense is to remain aware when traveling. Don't put yourself in situations that invite shoulder surfers. Position your back to the wall when using your machine, and never leave your machine unattended. Don't wear company logos and remove extraneous markings and information from your mobile computing devices, especially if your company name might entice an adversary. The tech support folks in your organization can probably provide you a long list of tech things to avoid when traveling. Follow their advice.

Security Alert…

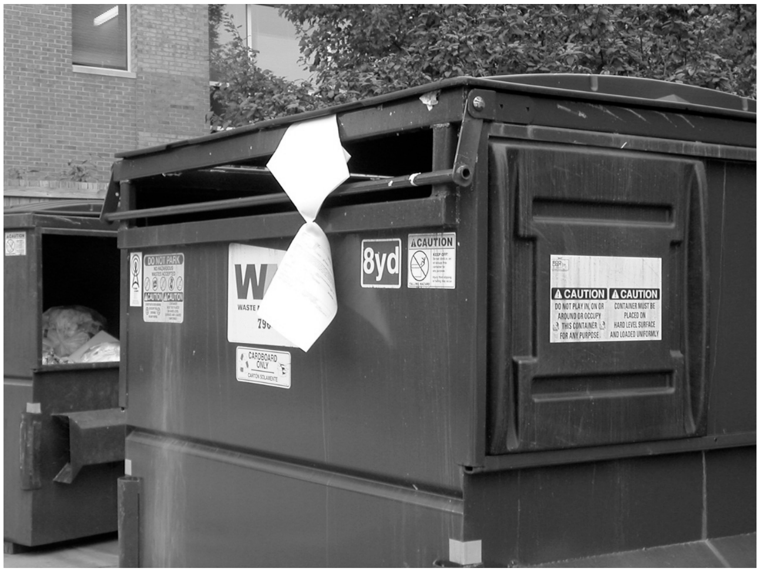
Taskbars?

StankDawg (please don't call him "Mr. Stank") wrote a terrific paper called "The Art of Electronic Deduction," which formed the basis for this section. Many hackers like myself always know to pay attention to the smallest details, but the idea of unpacking a taskbar is quite interesting and unique. His paper can be downloaded from http://www.docdroppers.org/wiki/index.php?title=The_Art_of_Electronic_Deduction, and StankDawg's Web site is located at www.stankdawg.com.

Dumpster Diving

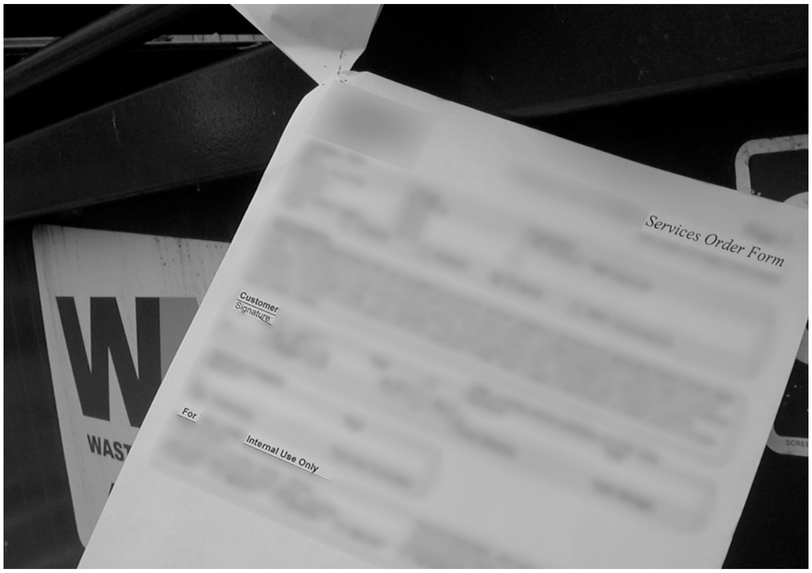
Another favorite hacker sport, *dumpster diving* describes the act of slogging through the trash in search of valuable tidbits of information. This might sound messy, but it doesn't have to be. Many times, interesting stuff is just hanging out there, waiting to be grabbed, as shown in Figure 8.34.

Figure 8.34


DO NOT PARK
CAUTION
WASTE
8yd
CAUTION
CARDBOARD ONLY
CAUTION
DO NOT PLAY IN, ON OR AROUND OR OCCUPY THIS CONTAINER FOR ANY PURPOSE
CAUTION
CONTAINER MUST BE PLACED ON HARD LEVEL SURFACE AND LOADED UNIFORMLY

Many times, trash is just trash, but in this case, this dumpster dangling document is labeled *for internal use only.* For this particular company, the phrase seems to have lost its meaning. (See Figure 8.35.)

Figure 8.35



Services Order Form

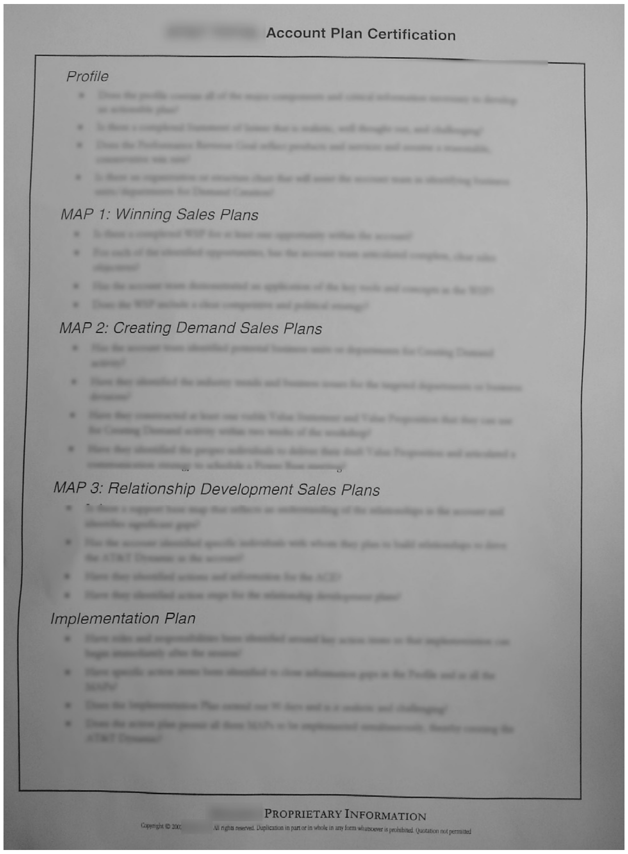
Customer Signature

For

Internal Use Only

I've found similar documents—such as the one in Figure 8.36 revealing proprietary information—lying *outside* of dumpsters.

Figure 8.36



[redacted] Account Plan Certification

Profile

- [illegible]
- [illegible]
- [illegible]
- [illegible]

MAP 1: Winning Sales Plans

- [illegible]
- [illegible]
- [illegible]
- [illegible]

MAP 2: Creating Demand Sales Plans

- [illegible]
- [illegible]
- [illegible]
- [illegible]

MAP 3: Relationship Development Sales Plans

- [illegible]
- [illegible]
- [illegible]
- [illegible]

Implementation Plan

- [illegible]
- [illegible]
- [illegible]
- [illegible]

[redacted] Proprietary Information

Copyright © 200[redacted] All rights reserved. Duplication in part or in whole in any form whatsoever is prohibited. Quotation not permitted

Admittedly, I've only seen a handful of cases that were this blatant. More often, I have to actually stick my head into the dumpster and peer inside. I discovered the document in Figure 8.37 in a dumpster on top of an open box of similar papers. It contains client, sales, and account information along with the Social Security numbers of the sales staff that received incentive payments on a particular contract.

Although this dumpster first appeared empty, the white envelopes littering the bottom of the container caught my eye. This particular health care invoice (See Figure 8.38) appears to have been opened and discarded, as if the recipient were finished with it. If this were my healthcare invoice, I would have certainly shredded it, or at least put it in the cat litter bag to deter even the most dedicated snoop.

Figure 8.37

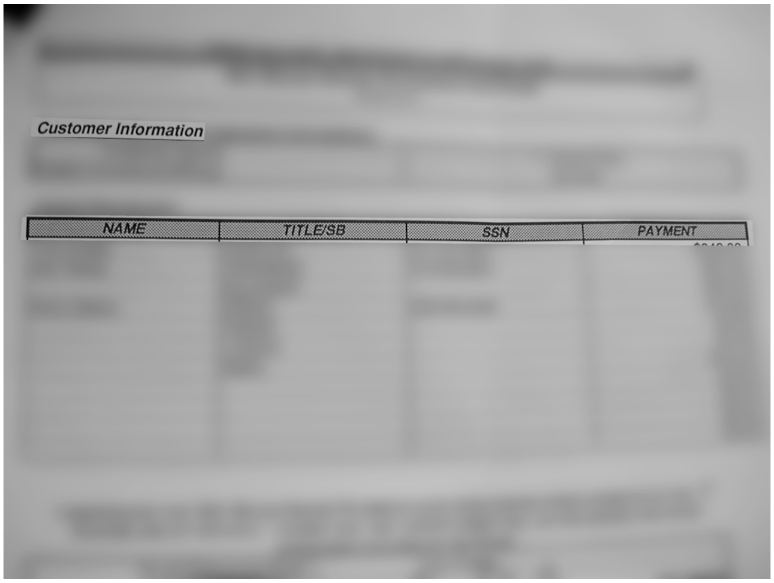
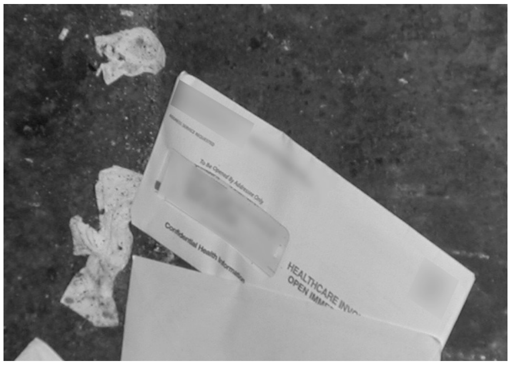
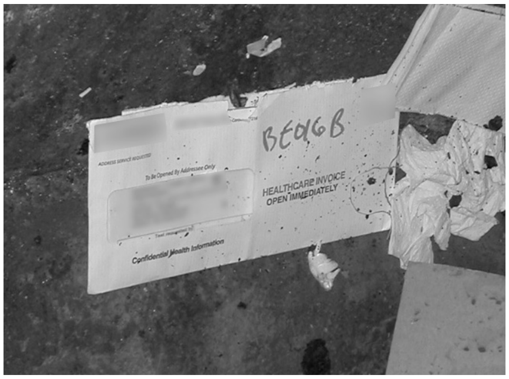


Figure 8.38


To Be Opened By Addressee Only
Confidential Health Information
HEALTHCARE INVO
OPEN IMME

The invoice in Figure 8.39, addressed to someone else, was discarded even before it was opened.

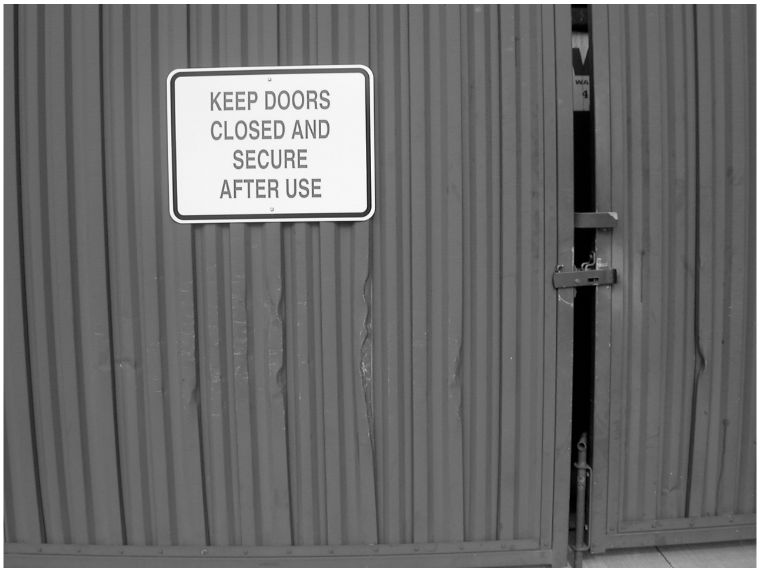
Figure 8.39


BE96B
HEALTHCARE INVOICE
OPEN IMMEDIATELY
To Be Opened By Addressee Only
Confidential Health Information

Further examination of the dumpster revealed other similar unopened envelopes. Examination of the address information on other envelopes in the dumpster revealed that these invoices were not discarded by the patient, but rather by the health care provider. In this case, it appears the patients had no control over how their confidential health information was handled. Obviously, this particular health care provider thought HIPAA had something to do with large thick-skinned semi-aquatic African mammals.

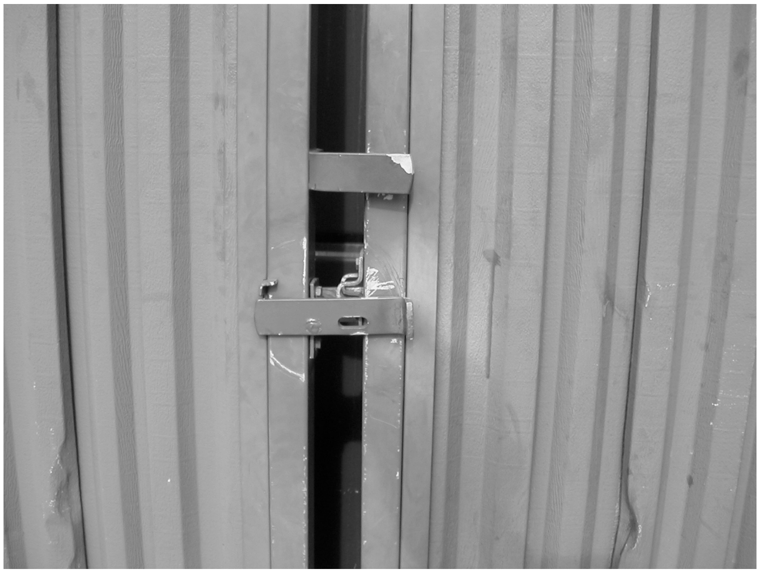
So what's the solution? It's to keep an eye on your trash. If I can grab all this without so much as touching a single piece of refuse, you should be able to get a feel for things by glancing at your dumpster every now and again. Signs like that in Figure 8.40 are a nice idea and serve as a great reminder.

Figure 8.40



Of course a nice sign is no replacement for an actual lock. (See Figure 8.41.)

Figure 8.41



The bottom line is that you should know what's in your trash before the bad guys do. If you find stuff in your trash that doesn't belong, you have a policy problem, or more likely an enforcement problem. If you deal with sensitive data (and who doesn't, really) it's in your best interest to keep a tight reign on what ends up in that big green box outside.

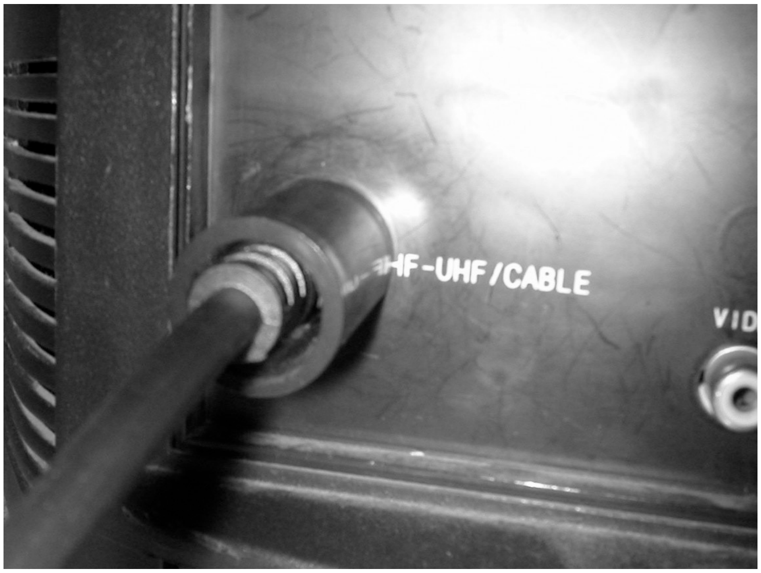
Watching TV, Hacker Style

So far, we've seen some interesting low-tech hacking techniques, but each of them requires some work. Shoulder surfing and dumpster diving takes a bit of walking, and God forbid, sometimes a bit of lifting. I know some of you (particularly the ones sitting on the couch, about ready to put this book down and grab for the remote) are thinking there must be something easier. Well, this section is for you. It's possible to be a full-fledged no-tech hacker from the comfort of a couch. In fact, this technique *requires* that you actually chill out for a while, put your feet up, and watch TV. You heard me right. The catch is that you have to be at a hotel, preferably a nice one. Isn't it amazing the tortuous lengths a dedicated hacker will go to?

After years of playing road warrior as I bounced from gig to gig, the hotel room became my home away from home. I never had cable TV as an adult, so flipping through the channels was a nice treat. Eventually, the thrill wore off and I found myself wanting something more. I knew better than to travel down the road of the $13-an-hour adult channels (don't get hooked, it'll wreck your life) but the technology behind the hotel TV system intrigued me. I began by fiddling with the TV controls, trying to access anything other than channel 3. I used the channel control buttons on the front of the TV as well as the remote, but the result was always the same: the TV had been locked down, allowing access to only seven or eight channels, which were odd channels showing nothing but static. Playing with the pay-per-view buttons on the remote got me nowhere. Everything I did gave me the distinct feeling I was pounding on the front gate of the castle. The system had been designed to deter this kind of fiddling.

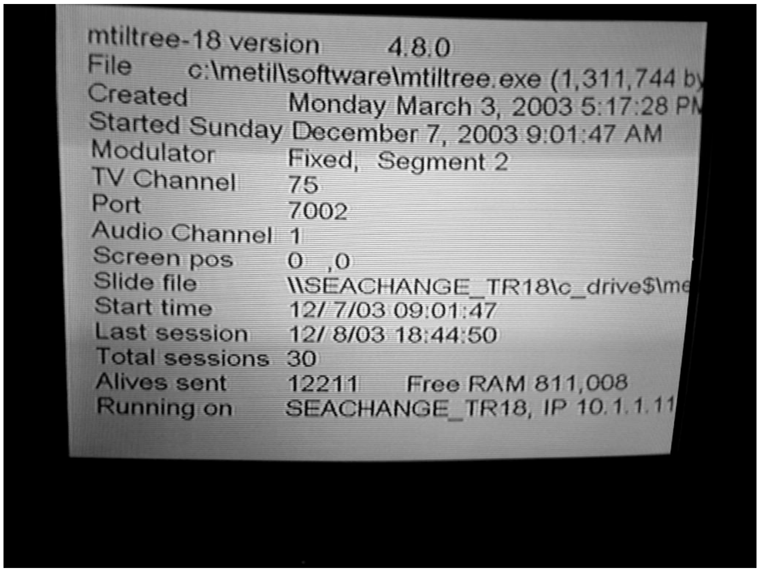
I tossed aside the remote and pulled out the TV to check the rear connections. I found a standard coax cable coming from the wall, connecting to a funny box on the back of the TV. Another coax cable ran from the box to the back of the TV. My first thought was to unplug all the cables and bypass the magic box. Closer inspection revealed something I didn't expect. (See Figure 8.42.)

Figure 8.42



Hard plastic sleeves secured the cable ends. Removing the cables required a special tool that slipped inside the sleeve and allowed access to the cable's collar. After considering the problem for a few moments, I rummaged through my bag and found my car keys. I jammed my ignition key down inside one of the protective collars and cranked it counter-clockwise. The cable turned inside the collar. I kept at it, and the cable rotated with each turn of the key. After several full rotations, the cable was a twisted mess, but eventually it came free and untangled, flailing around like an injured snake. I unscrewed each of the remaining cables and connected one of them from the wall directly into the back of the TV. I grabbed the remote and began flipping through the few channels the TV allowed. Each of them came in clearly; the static I had seen previously was gone. This was a sign that the hotel's raw cable feed was displaying cleanly through the TV's tuner, exactly as I had hoped. It was an interesting find, but not nearly as interesting as what I found on channel 75. (See Figure 8.43.)

Figure 8.43



```
mtiltree-18 version      4.8.0
File         c:\metil\software\mtiltree.exe (1,311,744 by
Created              Monday March 3, 2003 5:17:28 PM
Started Sunday December 7, 2003 9:01:47 AM
Modulator        Fixed,  Segment 2
TV Channel       75
Port             7002
Audio Channel  1
Screen pos       0   ,0
Slide file       \\SEACHANGE_TR18\c_drive$\me
Start time       12/ 7/03 09:01:47
Last session     12/ 8/03 18:44:50
Total sessions  30
Alives sent      12211     Free RAM 811,008
Running on       SEACHANGE_TR18, IP 10.1.1.11
```

As I read the information on the screen, the geek in me was delighted to see an IP address (10.1.1.11), a port number (7500), a pathname to a Windows or DOS executable (c:\metil\software\mtiltree.exe), and a universal naming convention (UNC) link to a machine share (*\\SEACHANGE_TR18\c_drive$*). I plopped down on the bed and gawked at the screen. My mind spun with the possibilities. Servers were running on the hotel's cable system, each connected by an IP network. The hacker in me wanted to jump in and start port scanning or sniffing, or *something*, but it was late, and I hadn't exactly been authorized to poke about the hotel's network. I snapped a few photos and reassembled the TV and the black box, silently cursing the TV for not allowing me access to more channels. There was interesting stuff on the blocked TV channels, I was sure of that.

When I returned from my gig, I couldn't get the hotel network out of my mind. I fruitlessly searched the Internet for a way to unlock the channels on the TV[3] and had just about given up on the prospect when I came upon an interesting device in a thrift shop. (See Figure 8.44.)

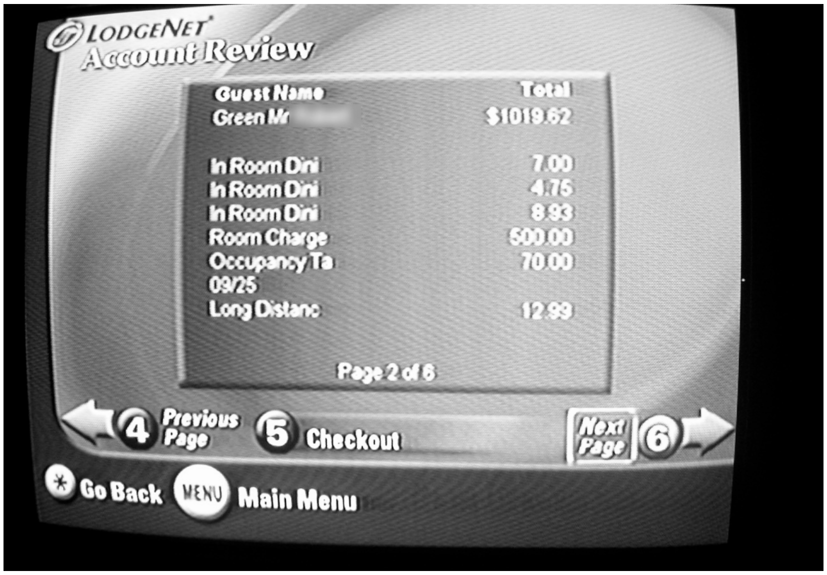
Figure 8.44

The device was an ancient cable box—a tuner, basically—that connected between a cable feed and a television. I paid less than three dollars for it, and brought it along on my next gig.

The moment I walked into my hotel room, I removed the cables from the back of the TV (making short work of the annoying sleeves) and connected my cable box between the cable feed and the TV. I turned on the TV, set it to channel 3, and began flipping through channels on the cable box. Just as I had suspected, I could view all the standard cable channels. However, as the numbers climbed I hit more of the interesting *Seachange* channels. Then, suddenly, I found one channel that wasn't like the others. (See Figure 8.45.)

I had to read the information on the screen several times before I realized I was looking at someone else's room bill. The screen flashed briefly and the next page displayed. I watched as Mr. Green flipped through his account information. Thanks to a $3 device, I was snooping on the hotel's customers. This technique works because certain channels are unlocked and distributed on an as-needed basis. If I were to use my remote to view my room bill, a channel would be allocated and unlocked, and the requested information would be shown on my TV. The cable box gave me the ability to see every channel, including the channels currently allocated to other customers. If a customer activated a custom feature on the TV, I could see what was happening if I viewed the same channel. Of course, the majority of customers used the system to view on-demand movies. If a customer paid for a movie, I could tune in as well and the hotel wouldn't know I'd watched it without paying. (See Figure 8.46.)

Figure 8.45

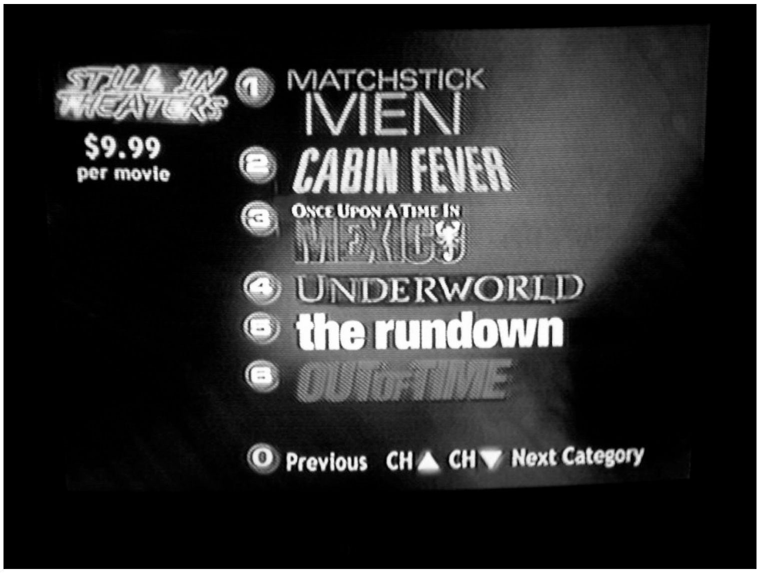


LodgeNet
Account Review

Guest Name	Total
Green Mr [redacted]	$1019.62
In Room Dini	7.00
In Room Dini	4.75
In Room Dini	8.93
Room Charge	500.00
Occupancy Ta	70.00
09/25	
Long Distanc	12.99

Page 2 of 6

Figure 8.46

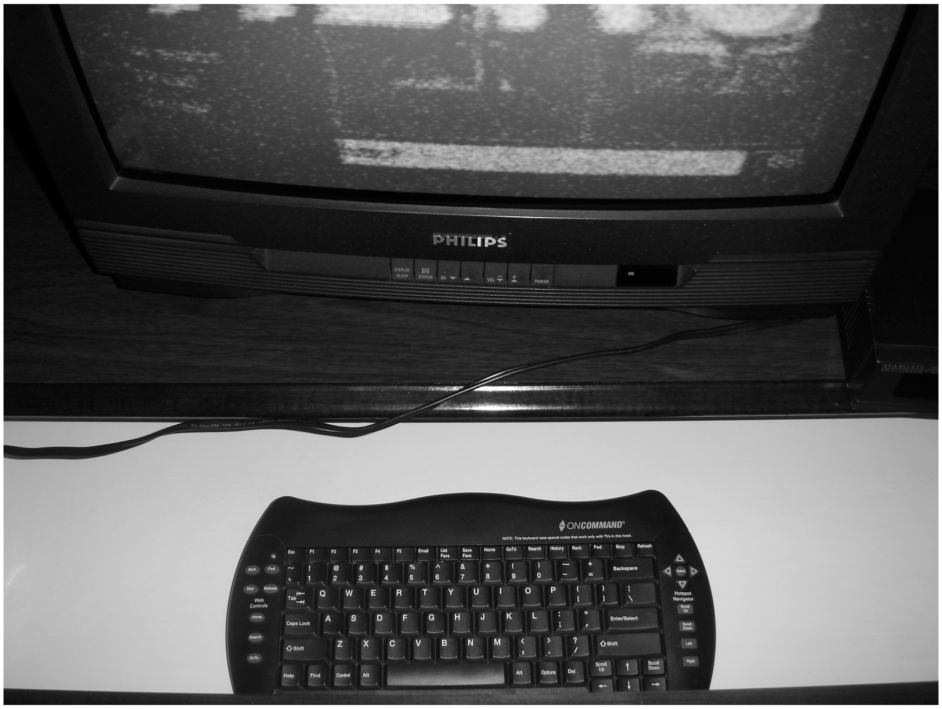


STILL IN THEATERS
$9.99 per movie

1 MATCHSTICK MEN
2 CABIN FEVER
3 ONCE UPON A TIME IN MEXICO
4 UNDERWORLD
5 the rundown
6 OUT of TIME

Some hotels have adopted more robust systems that allow customers to use the in-room TV as an Internet terminal. A wireless keyboard often accompanies this type of system. (See Figure 8.47.)

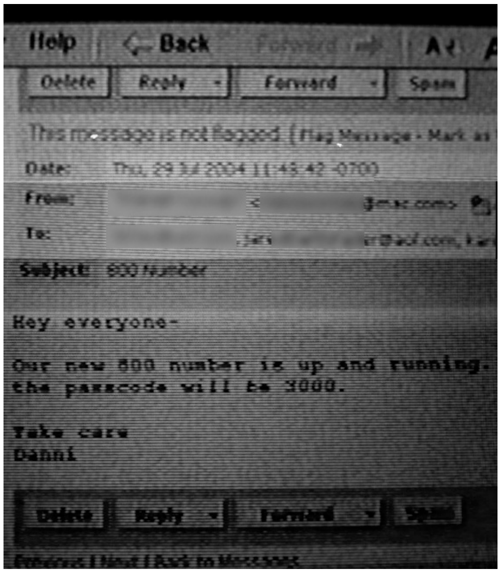
Figure 8.47



I've caught customers surfing the Web and checking their e-mail. The e-mail in Figure 8.48 reveals the passcode for a new 800 number. The number itself was sent in the previous e-mail.

The photo in Figure 8.49 shows a customer logging in to their American Express account. If I were an adversary, there's no telling what I could do with this information.

Figure 8.48



This message is not flagged. [Flag Message - Mark as

Date: Thu, 29 Jul 2004 11:45:42 -0700

From: [redacted] <[redacted]@mac.com>

To: [redacted], jan[redacted]r@aol.com, kar

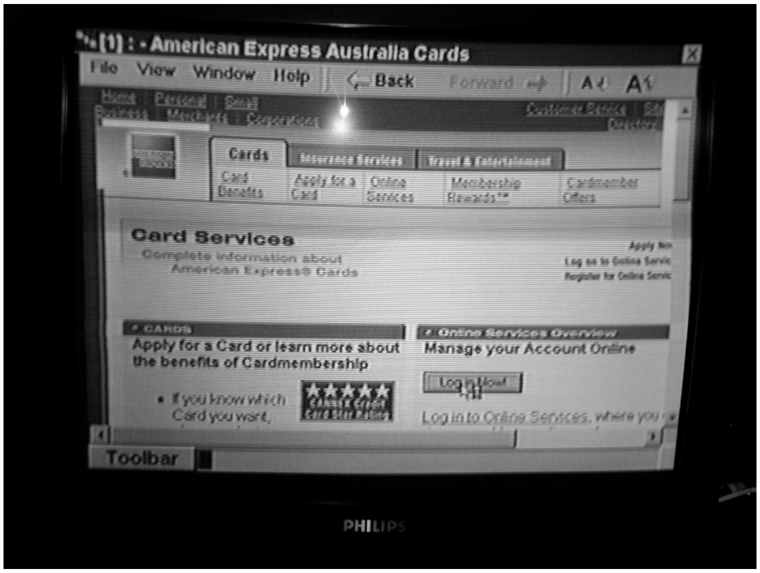
Subject: 800 Number

```
Hey everyone-

Our new 800 number is up and running.
the passcode will be 3000.

Take care
Danni
```

Figure 8.49



Card Services

Complete information about American Express® Cards

Apply for a Card or learn more about the benefits of Cardmembership

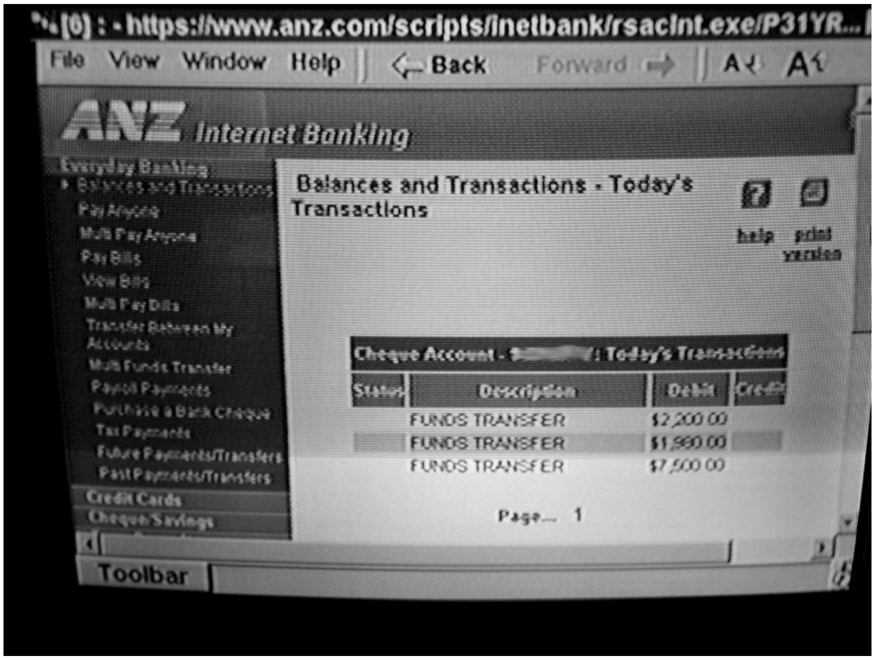
- If you know which Card you want,

Manage your Account Online

Log in to Online Services, where you

Figure 8.50 shows a customer logging in to their Internet banking site. The balances shown in this account were rather large. An adversary might decide to target this individual based on their income level.

Figure 8.50



Balances and Transactions - Today's Transactions

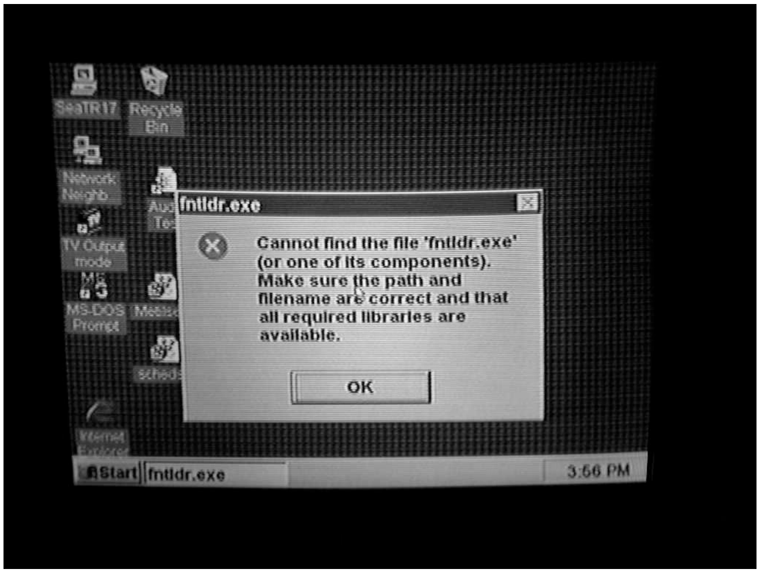
Cheque Account - [redacted]: Today's Transactions

Status	Description	Debit	Credit
	FUNDS TRANSFER	$2,200.00	
	FUNDS TRANSFER	$1,980.00	
	FUNDS TRANSFER	$7,500.00	

Page... 1

Adam Laurie, a.k.a, Major Malfunction, has discovered that hotel cable systems can be even further abused. By toying around with a PC-controlled IR (infrared) device, Adam found that he could reprogram the hotel television directly to allow him access to all the restricted channels, without a special tuner. Not only was he able to view channels already in use, he could change the ID embedded in his television to appear to be another hotel patron. After changing the code, he found it was possible to review their room charges, order items like room service, change the status of the room, learn who was staying in the room and for how long, and more. Adam even discovered he could take control of the administrative systems like these through the use of the in-room wireless keyboard. (See Figure 8.51.)

Figure 8.51



fntldr.exe

Cannot find the file 'fntldr.exe' (or one of its components). Make sure the path and filename are correct and that all required libraries are available.

This functionality was made possible by the black box I disconnected to hook up my tuner. For more information about Adam's work, see his presentation at www.alcrypto.co.uk/MMIrDA/mmirda_syscan05.pdf.

Keep these vulnerabilities in mind as you travel, and encourage your employees to do the same. Hotel TV–based Internet systems are never considered safe for any purpose, and your personal information may be at risk if an adversary is staying in the same hotel. And remember, those $13 charges for in-room entertainment that are so anonymous. Anyone in the hotel can see them, and how many $13 in-room entertainment possibilities are there, exactly?

Checklist

Links to sites:

- www.toool.nl/kensington623.wmv
- http://connect.waag.org/toool/:
  Toool—The Open Organization of Lockpickers; barry@toool.nl, rop@toool.nl
- http://connectmedia.waag.org/toool/whatthebump.wmv: Toool's lock bumping video

- www.bikeforums.net/video: One of the founding sites for the U-Lock bypass videos
- http://security.org/dial-90/alerts.htm: Marc Tobias's alerts page
- http://security.org: Marc Tobias's Web site
- www.fusor.us/lockpick.html: Master Lock brute forcing
- www.everything2.com/index.pl?node_id=1304470&lastnode_id=0: Master Lock brute forcing
- www.toool.nl/bumping.pdf: "Bumping Locks" by Barry Wels and Rop Gonggrijp
- http://cq.cx/prox.pl: Jonathan Westhues's Proximity Card cloner
- http://en.wikipedia.org/wiki/Van_Eck_phreaking: Van Eck Phreaking
- www.docdroppers.org/wiki/index.php?title=The_Art_of_Electronic_Deduction: StankDawg's great paper on electronic deduction (used for the shoulder surfing section)
- www.hidcorp.com: HID corporation, world class manufacturer of site security products
- www.toool.nl/bumping.pdf: Toool's great lock bumping whitepaper
- www.toool.nl/kensington623.wmv: Toool's great video showing Kensington Lock picking with a roll of toilet paper
- www.wired.com/news/privacy/0,1848,68370,00.html: A Wired article about Adam Laurie's Hotel TV bypass/snooping work

Summary

Hackers are certainly a technical bunch, but in this day and age, it pays to think simply. No-tech attacks are simple to pull off, but the effects can be devastating to your facility's security posture. Learning to think like a hacker is not necessarily as difficult as it may seem. Pay attention to the little things, and keep a vigilant watch for opportunities you are offering the no-tech hacker.

Notes

1. http://en.wikipedia.org/wiki/Van_Eck_phreaking
2. Of course, the phone company I emulated had no part in this. I have no affiliation with them, and this attack in no way reflects a security problem with that particular phone company. Neither my company nor I endorses this kind of behavior except in conjunction with an authorized security test. And please don't full-body tackle every poor phone technician you spot in the hallway.
3. I didn't know about Adam Laurie's awesome work and talk at www.wired.com/news/privacy/0,1848,68370,00.html. I'm not entirely sure his work was public back when I tried this.