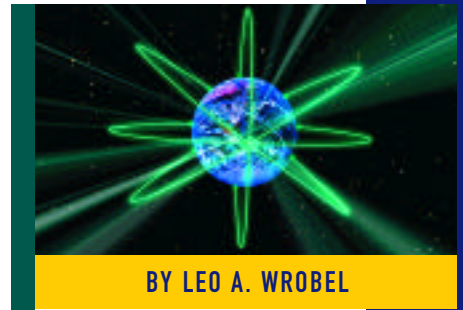


Security Issues for Common Work Tools: Part II — Voice Mail Systems and Cellular Phones



PART I (*Technical Support*, July 1997) examined security issues surrounding some of the most common office tools, namely fax machines and electronic mail. I stressed that the exposure of these systems can often far outweigh the value of the system itself since they frequently exchange information of a most proprietary or confidential nature. This month I will continue in the same vein, this time addressing a few more systems that are often overlooked, but equally prone to abuse or outright fraud: voice mail and cellular phones. Let's start with voice mail.

"Hello, this is Bob. I'm away from the phone right now or on the other line, but if you will leave your name and number, I'll return your call as soon as I can. If your call is urgent, press '0' for the operator."

Sounds familiar enough, doesn't it? Just suppose a hacker exercises the "press-0" option and when the operator answers, he does this:

"Where the hell is Bob! I've been trying him all day and he's supposed to be at his desk! That lowlife is in big trouble! Where is he! Oh, the hell with it, just give me an outside line so I can track him down!"

Excuse the colorful language, but it's to illustrate a point. The objective is to intimidate and frazzle the operator, so the more intimidating the better. The operator has a tough enough job, often answering 300 calls a day, most of which come from people who don't know where the person they are calling is, what their extension is, or whatever. Now the operator has one more hostile caller, who appears to be calling from inside the building — after all, who's number is lighting up on her switchboard? Why Bob's of course! (Remember, the hacker

transferred from Bob's line so that's what the operator sees!) So what happens? She almost always will give the caller an outside line. Once connected to the local Bell operator, and the company operator has disconnected and moved on to the next caller, the hacker continues:

Hacker: *"Operator, I would like to place a call to Islamabad, Pakistan please."*

Operator: *"How would you like to pay for that call?"*

Hacker: *"Oh, just bill it to this number."*

Unless your company is paying for line screening, which is generally used to tip the operator off that the call is coming from a hotel or pay phone, the hacker calls for free and your company gets the bill.

You have just been presented with one of the easiest and most common ways a hacker can compromise your voice mail system. And compared to some of the more sophisticated hackers out there, my technique is the technological equivalent of stone knives and bear claws. Line screening, which is what keeps people using hotel and pay phones from pulling this little trick, is rarely ordered or used by corporations. When it happens to them, they get stuck!

OTHER COMPROMISES OF VOICE MAIL SECURITY

Did you know that an astute hacker can tell from the tone of the automated lady's voice on your voice mail system what kind of system it is? That can be disastrous, since the hacker will also undoubtedly know what the factory default codes are for the system, allowing him to dial into the operating system itself. That could mean he could make outgoing international calls

Whether you're a technologist or the telecom manager, it's important for you to know the nuts and bolts safeguards behind the security of voice mail systems and cellular phones.

such as in the previous example. It also makes for some other interesting situations. For example:

One user I met at a seminar said his voice mail system was used several months to run a "Call Girl" operation! It seems that the hackers were able to break in, then set up special voice mailboxes (using the authorized users boxes) after hours. They were always careful to delete all of these messages before the real employees came in at 8 a.m. One day however, the operation was either raided, moved, or just lost interest in the voice mail system. And all the messages to the "clients" were still there when the shifts came in on Monday morning! The content of these messages was not elaborated upon by the telecom manager, but I am told many of the "surprising" messages found that morning are still legendary within the company. This is really kind of comical, especially since there was no real cost to the company other than to raise the office gossip a notch or two. It was unsettling, however, for everyone involved that it went on for so long undetected.

A second company was not so lucky. This company had a formal policy in place to block all operator transfers from voice mail to outside lines, except for 911. The operators were trained, and signed off on the new procedure. Everything was fine until Thanksgiving weekend last year. At that time the operators were off for the holiday, so the phones rolled to the security guard's desk — who was not trained. The guard answered an after hours call that went like this:

Hacker: *Hello, this is Jack at AT&T.*

We are testing the phones and need you to help us.

Guard: *Sure, no problem, what do you want me to do?*

Hacker: *Well, start by telling me what kind of phone you have.*

Guard: *It's green, it has several gray buttons, and it says "NEC" on it.*

Hacker: *Super, do you see the button marked "Transfer?"*

Guard: *Yes.*

Hacker: *Press that button, then dial 9, wait for the second dial tone, then dial "0" and hang up. Think you can handle that OK?*

Guard: *Sure, no problem. Here goes!*

You know from the previous example what happened next. This happened all day Thanksgiving, and the subsequent three days. Each time the guard made an entry in the log "Assisted AT&T." On Monday morning a security supervisor saw dozens of entries, got suspicious, and called the telecom manager who promptly had a cow. The result? A five-digit telephone bill for calls made to Pakistan!

**You have just been presented
with one of the easiest,
and most common ways
a hacker can compromise
your voice mail system.
And compared to some
of the more sophisticated
hackers out there, my technique
is the technological equivalent
of stone knives and bear claws.**

PREVENTATIVE MEASURES

So what can a user do to protect against abuse on these systems? Look at the following checklist and verify that your company does all of the following:

1. Have a policy which prohibits transfers to outside lines in all cases, except for the possible exception of a "911" emergency transfer. Remember, 911 emergency personnel are not necessarily dispatched to where the emergency is; they are often dispatched to where a PBX is, since the address which lights up on the 911 console (called the ALI or automatic location identifier) is where the circuits terminate. This can be a big deal in campus environments, and is often reason enough to prohibit outside operator transfers altogether. If you do allow them, train your after hours security people too!
2. Disconnect your Direct Inward System Access (DISA). It is used by nomadic or homebound workers to access PBX dial-tone from a remote location. The caller dials in, gets a dial-tone back,

enters an access code, then completes a call on the company switch. These systems literally cry out to the world, "Please HACK ME!" When a hacker stumbles upon such a number, they can't resist calling back in to crack it, often with the aid of computerized programs. If you must have it, use long, complicated access codes, and consider having it answer with silence, not a dial tone, until after the caller enters his code,

3. Monitor systems for suspicious activity. If you had 300 unsuccessful attempts on your DISA last night would your company know it? What about those dial-in ports to your multiple xers, routers, and PBX? Do you monitor these for suspicious activity? Do you change the original factory codes?
4. Watch for dumpster divers. Do you know how many people go through your company's trash looking for credit card receipts and long distance access codes? Do you know who your cleaning crews are? Do you instruct your users not to leave sensitive access codes out on their desks where these crews can find them? One client of mine actually had a high end fax machine ripped off — from a 17th floor office! They only thing we could figure is that the cleaning crew wheeled it out with the trash. (It was found in a nearby pawn shop a few days later.)

OTHER PRECAUTIONS

As I mentioned last month, a Policy on Telecommunications Privacy should be in place. It should be broad enough in scope to cover not only email, but voice mail and other mediums. Sample verbiage might be as follows:

"ABC Company is committed to absolute privacy of communications, and each employee has the right to not have their communications monitored. However, if in the course of normal maintenance activity we inadvertently discover illegal activity, we reserve the right to report this activity to the responsible authorities."

This would give you some recourse if you ever had to monitor a situation, such as the one that was accidentally discovered by a manufacturing company I once had contact with. They came in on a Monday morning

after a holiday (do you see the timing pattern here — hackers love long weekends) to find three T1's worth of traffic into US Sprint, all filled with people speaking Spanish. The problem was, the company had no Spanish speaking clients, employees, or overseas branches. But there it was, 72 channels of people speaking a foreign tongue to a far-away land — on the company's nickel, of course. Most of the people on the calls probably didn't even know it was illegal. Scam artists constantly work the immigrant communities, and lines of new immigrants at pay phones waiting for "discount calls" from disreputable thieves are an all-too-common sight in many cities.

CELLULAR PHONES

Another armament of the road warrior which is often abused is the cellular phone. One client we worked with, a multi-billion manufacturing company was arranging financing for the company, a very sensitive matter. Each day the CEO would park in 5 p.m. traffic discussing the most intimate details of the transaction on his cellular phone. Only as the deal neared a close did he think to ask, "Hey, can someone monitor these things?"

Luckily things went OK. Nonetheless, the CEO was shocked to learn that anyone with a \$200 bear scanner could have monitored his entire conversation with ease — start to finish.

"CLONING" CELLULAR PHONES

Thieves have also become very fond of cloning bogus authorization numbers into cellular phones. In years past, cellular providers have been hit hard by hackers cloning phones, then calling overseas. Most now block calls of this type unless they are certain it is an authorized user.

This can often mean inconvenience for an authorized user who happens to be "roaming" in another service area, where his identity cannot always be guaranteed with certainty. And not only overseas calls. I was recently in an area of New York City (which has the dubious distinction of being the telephone fraud capital of the world) where I could not roam with my cell phone at all. All calls were directed to an operator, who would only complete a telephone credit card call. I found this preposterous, since hundreds of hackers were probably standing by using their \$200 bear scanners, just waiting for me to read my credit card number to the operator so they could steal it and beat it to death calling Tahiti, Sri Lanka, and the Magnetic North Pole. I chose instead to find a pay phone and not roam.

PRECAUTIONS FOR CELLULAR PHONES

1. Never give a credit card or telephone credit card number over a cellular phone.
2. Never say anything over any wireless phone that you would not mind the whole world knowing.
3. Try dialing 800 numbers whenever possible when on the road rather than making credit card calls. An astute hacker can capture your touch-tone digits when you make an automated credit card call, even if you don't read the number to an operator.
4. Monitor your cellular bill closely and report any unusual calling activity (indicating your number may have been cloned) to your cellular provider immediately.

5. Consider upgrading to digital cellular service. Although not foolproof, digital technologies require more sophisticated equipment to monitor and are thus more difficult to intercept by hackers.

This is by no means an exhaustive dissertation on all the areas where your company can pay a significant financial penalty for lack of vigilance. It pays to keep an eye on even the most ho-hum systems, to assure that these minor conveniences of the office place do not become a major strain on another important system — your cardiovascular system. Good luck in your endeavors!

ts



Leo A. Wrobel is an active author and lecturer. He has nearly two decades of industry experience, including assignments in government and the banking, brokerage, heavy manufacturing, and telecommunications industries. He is president and CEO of Dallas-based Premiere Network Services, Inc. Contact Premiere's web site at www.dallas.net/~premiere or (972) 515-5000 for more information.

©1997 Technical Enterprises, Inc. Reprinted with permission of *Technical Support* magazine. For subscription information, email mbrship@naspa.net or call 414-768-8000, Ext. 116.