Global Information Assurance Certification Paper

“Hacker on Line One”

Social Engineering and the Telephone

Veronica Byers
GSEC Version 1.2f

Abstract

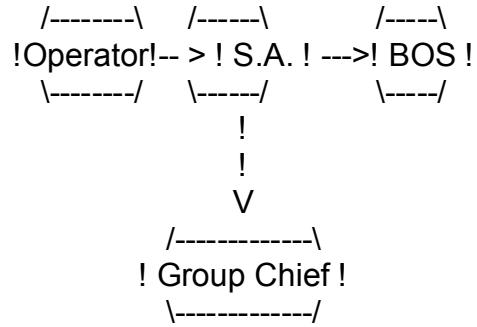
In the midst of today's focus on social engineering and identity theft through computers and the Internet, many people have forgotten that social engineering through the phone is alive and well in the 21st century. Although it may not be at the forefront of information security personnel's' minds, they need to know the tactics used to gather information over the phone and how to protect themselves against it. The effects can be equally or even more devastating than more "glamorous," high-tech methods of hacking.

In the Beginning

The telephone was one of the first tools used by hackers. In fact, hacking started on phones long before the Internet was a reality. Black boxes, beige boxes and shoulder surfing were the words of the day rather than spoofing, war dialers and denial of service. The aim was to steal long distance service rather than disk space or valuable information. Nowadays, instead of being a target, phones are a very useful and often underestimated tool used to get into any company's network.

The first telephone social engineering occurred when "phreakers" (phone system hackers and crackers) would call telephone service centers and attempt to gather information from the operators by claiming to be a lineman. This was effective because phreakers had carefully gathered insider information such as the lingo and organizational charts. In fact, the following archived document on the web from1985 detail this insider information for phreakers:

> *''Ever get an operator who gave you a hard time, and you didn't know what to do? Well if the operator hears you use a little Bell jargon, she might wise up. Here is a little diagram (excuse the artwork) of the structure of operators*



If a lineman (the guy who works out on the poles) or an installation man gives you the works ask to speak to the Installation Foreman, that works wonders.

Here is some other bell jargon that might come in handy if you are having trouble with the line. Or they can be used to lie your way out of situations...."

Guides like these were widely available on the Internet. By sounding confident and having internal information, they could get even more confidential information about the phone system. Since then, social engineering has become even more refined an "art."

The Threat the Phone Poses

Today the target of social engineering (phone and otherwise) is large companies with valuable information rather than the former "MaBell" and has become an even more complicated an "art." However, the inherent security weaknesses of the telephone system still make this a serious threat.

Some of the risks of telephone communications are:

1. **Lack of Authentication or Verification -** The principal problem with the telephone is that there is much less authentication than with electronic means, especially when the user doesn't have caller id. Consider the typical phone call. When someone calls and identifies himself or herself, do you ask them for any other proof of identification? Even if you do not know them and don't have caller id, I'd be willing to guess that your answer is "no." Most people have become so accustomed to using only verbal authentication over the phone that they do not even realize they are doing it. They will accept that a person is who they say they are, even if they don't recognize the name. Just imagine if this were common practice on network systems!

2. **Implicit Trust -** In general, people will give out information to an unknown source over the phone that they would never give to someone with an unknown e-mail address. Part of this is due to the lack of authentication. Since the person has been authenticated in the person's mind, they mentally assign them a certain level of "clearance." There is an unsafe amount of implicit trust associated with the phone. In addition, social engineers will use previously acquired insider information to enhance the target's trust.

3. **Ability to Disguise One's True Identity –** There are a multitude of devices on the market that allow the user to change their voice to sound like the opposite sex or older. This further damages the level of authentication over the telephone. Use of business jargon and knowledge of company organization completes the "transformation" into a believable fellow employee.

4. **The PBX is a Computer, as Hackable as Any Other –** PBX, a telephone system used by many large companies, is in essence a computer system, and therefore just as prone to hacking as any other computer. Once a social engineer has phreaked a PBX, they could social engineer company information by leaving voicemail messages. (e.g. "Phillis, this is Bob from the helpdesk. We're having trouble with your account and need to log in as you in order to fix it. If you could give me a call on my cell, we'll take care of the problem." One short "call-back" later, "Bob" has a valid username and id to get into the network.)

Although used casually by virtually everyone to conduct business on an everyday basis, the telephone is an insecure method of communication.

Examples of Social Engineering via the Phone

Most people believe that the stereotypical phone-hack consists of a conversation like this:

> *"Hi Bev, this is Sam from the IS department. We just got a new corporate screensaver and since you're the VP's secretary you will get it first. It's really cool wait 'till you see it. All I need is your password so I can log on to your PC from the computer center and install it."*
>
> *"Oh Great! My password is rover. I can't wait to see that new screen saver!" (http://www.sans.org/infosecFAQ/social/social.htm)*

While social engineering phone calls are sometimes this straightforward, more often, attempts are much more subtle. As famed social engineer Kevin Mitnick once said:

> *"I don't think I've ever – except on one or two occasions – asked someone for their password. That's a big red flag."(http://www.securityfocus.com/news/60)*

An excellent example of more intricate social engineering is evident in what happened at a HOPE (Hackers On Planet Earth) conference last year. In a demonstration of social engineering, Eric Corley, publisher of 2600 magazine called the AT&T's Information Security department and used a fictional name in an attempt to get a copy of a confidential document. He managed to engage the security personnel for over five minutes before they became suspicious despite that:

- The person he was talking to was a trained Information Security professional.
- He used a completely fictional name that wasn't even in the company's address book.

- The Information Security person he spoke with knew about the conference and that social engineering via the telephone would be attempted.

This endeavor, though technically a failure, shows how much information a hacker can get just by calling. In addition, the main reason he failed was because he gave a false name that didn't exist in the company and the employee became suspicious when he couldn't find him in the e-mail address book. If he had socially engineered the name of just one AT&T employee through dumpster diving or equally low-tech means, it is fair to speculate that he may have very well been successful.

Another technique that is used by social engineers is to find a high-ranking officer's name on the target's website and use that name to garner people into divulging information. ("I'm a new consultant working on a high-priority project for Bob but I don't have an account yet. I know that this isn't your usual procedure, but there's a strict deadline and you know how Bob can be. Would it be possible to create my account over the phone?") Other techniques used to improve the chances of successful engineering include learning the jargon of the company, gaining access to an organizational chart, and sifting through company garbage. The more internal information a social engineer has, the better chance he has of being successful.

How to Defend Yourself

Unfortunately, there is no firewall for the telephone. Guarding against telephone social engineering involves people rather than technology. Educating your users is absolutely essential. Some methods for protecting your company from this threat are:

- Discuss the topic of social engineering via the phone often through your company's information security awareness program. If your company doesn't have such a program, get management backing and begin one. This is probably the single most effective step in protecting against social engineers of all types.

- Hold seminars for your users showing live demonstrations of social engineering techniques. The demonstration given at HOPE 2000 (performing an actual attempt) may not be feasible, but role-playing can also be very effective.

- When instructing new employees on the phone system, be sure to also educate them on social engineering.

- Encourage employees to report all incidents of suspected social engineering, especially if it was successful. Many people are reluctant

to report successful social engineering attacks for fear of looking "stupid" or "ignorant." Stress that the safety of the company's information assets far outweighs any embarrassment they may feel from being "had."

- One technical step that you can take is to make sure that all employees have caller id installed. While this has become the rule rather than the exception for most medium and large corporations at the home office, be sure to consider field offices and subsidiaries as well.

- Ensure that all of your policies and procedures stress the utmost precaution with handing out passwords. Under NO circumstances should passwords ever be exchanged over the telephone. No exceptions. Tell users that they will never be asked for nor should they ever give out their password over the phone. This will prevent the "Helpdesk technician" ruse that less sophisticated social engineers will try to use.

- Shred all confidential documents and keep your recycle and garbage bins in a locked and secure area. Although "dumpster diving" is a separate type of social engineering, information gathered through it can be used to successfully use phone techniques.

- Performing your own periodic dumpster dives can give you great insight into what information is "leaking out" through the garbage and can be a great barometer to your users' "social engineering savvy."

  For example, at one major corporation, a dumpster dive revealed the social security number, addresses, and phone numbers of a CFO of an outside company, salary information for interns, and even the keys to a Lexus car! This was one week after a message about social engineering had been e-mailed to the entire company. Don't assume that your security awareness is getting through. Validate it!

- Keep up-to-date with the latest techniques by checking online sources such as CERT and industry magazines. Knowing the social engineers' tricks is very effective in foiling them.

Conclusion

Today's information security headlines are full of stories of various companies and people getting hacked and socially engineered through highly sophisticated and technical means. While attention-grabbing, they downplay the effectiveness of more "old school" techniques such as the telephone. It is very important to know the most often techniques that social engineers use over the

phone and how to protect your company against them. A couple technical and procedural changes and a lot of user education can go a long way towards winning the battle.

References

1. CERT, “CERT Advisory CA-1991-04 Social Engineering” April 1991 http://www.cert.org/advisories/CA-1991-04.html (10 November 2001)
2. Finley, Michelle, “Phone Phreaks to Rise Again?” May 2000 http://www.wired.com/news/business/0,1367,36309,00.html (11 November 2001)
3. “The Official Phreaker’s Manual” http://www.dopeman.com/g-files/hack/pkman.txt
4. Palumbo, John, “Social Engineering: What is it, why is so little said about it and what can be done?” July 2000 http://www.sans.org/infosecFAQ/social/social.htm (10 November 2001)
5. Poulsen, Kevin, “Hackers demo “Social” skills in NY” July 2000 http://www.securityfocus.com/news/60 (10 November 2001)
6. Vigilante, “Social Engineering” http://www.vigilante.com/inetsecurity/socialengineering.htm (10 November 2001)