Helping the Hacker? Library Information, Security, and Social Engineering

Samuel T. C. Thompson

Social engineering is the use of nontechnical means to gain unauthorized access to information or computer systems. While this method is recognized as a major security threat in the computer industry, little has been done to address it in the library field. This is of particular concern because libraries increasingly have access to databases of both proprietary and personal information. This tutorial is designed to increase the awareness of library staff in regard to the issue of social engineering.

One morning the phone rings at the circulation desk; the assistant, Joyce, answers. "Seashore Branch Public Library, how may we help you?" she asks, smiling. "My wife and I recently moved and I wanted to confirm that you had our current address," a pleasant male voice responds.

"Could you give me your name please?"

"The card is in my wife's name, Jennifer Greene. We've been so busy with the move that she hasn't had a chance to catch up with everything."

"Okay, I have her information here. 123 Main Street, Apartment 2B. Is that correct?"

"Thank you so much, that's it. Do you have our new number or is it still 555-555-1234 in your records?"

"Let me see . . . no, I think we have your new number."

"Could you read it back to me?"

"Sure . . . 555-555-6789, is that right?"

"555-555-6789 . . . that's right. Thank you very much, you've been very helpful.'

"No problem, that's what we're here for."

<click>

What just happened?

What happened to Joyce may have been exactly what it appeared to be—a conscientious spouse trying to make sure information was updated after a move. But what else could it have been—research for an identity theft, or a stalker trying to get personal information? We have no way of knowing. All reasons except for the first, innocent, reason are covered by the term *social engineering.*

In the language of computer hackers, social engineering is a nontechnical hack. It is the use of trickery, persuasion, impersonation, emotional manipulation, and abuse of trust to gain information or computer-system access through the human interface. Regardless of an institution's commitment to computer security through technology, it is vulnerable to social engineering.

Recently, the Institute of Management and Administration (IOMA) reported social engineering as the number-one security threat for 2005. According to IOMA, this method of security violation is on the rise due to continued improvements in technical protections against hackers.[1]

Why and how does social engineering work?

The first thing to keep in mind about social engineering is that it does work. Kevin Mitnick, possibly the best known hacker of recent decades, carried out most of his questionable activities through the medium of social engineering.[2] He did not need to use his technical expertise because it was easier to just ask for the information he wanted. He discovered that people, when questioned appropriately, would give him the information he wanted.

Social engineering succeeds because most people work under the assumption that others are essentially honest. As a pure matter of probability, this is true; the vast majority of communications that we receive during the day are completely innocent in character. This fact allows the social engineer to be effective. By making seemingly innocuous requests for information, or making requests in a way that seems reasonable at the time, the social engineer can gather the information that he or she is looking for.

Methods of social engineering

The arsenal of the social engineer is large and very well established. This is mainly because social engineering amounts to a variation on confidence trickery, an art that goes back as far as human history can recall. One might argue that Homer's *Iliad* contains the first record of a social engineering attack in the form of the Trojan Horse.

Direct requests

Many social-engineering methods are complex and require significant planning. However, there is a simple and effective method that is often just as effective. The social engineer contacts his or her target and simply asks for the information.

Preying on trust and emotion

Social engineering is a method of gaining information through the persuasion of human sources, based on the abuse of trust and the manipulation of emotion. In his book, *The Art of Deception,* Mitnick makes the argument that once a social engineer has established the trust of a contact, then all security is effectively voided and

Samuel T. C. Thompson (sthompson@collier-lib.org), is a public service librarian at the Collier County Public Library, Naples, Florida.

the social engineer can gather whatever information is required.

The most common method of targeting computer end-users is through the manipulation of gratitude. In these cases, a social engineer, usually impersonating a technician, contacts a user and states that there is something wrong on the victim's end, and that the social engineer needs a few pieces of information to "help" the user. Appreciative of the assistance, the victim provides the necessary information to the helpful caller or carries out the requested actions. Predictably, no problem ever existed and the victim has now provided the social engineer either access to a computer system or with the information needed to gain that access.

A counterpoint to the manipulation of gratitude is the manipulation of sympathy. This method is most often used on information providers such as help-desk personnel, technicians, and library staff members. In this scenario, a social engineer contacts a victim and claims to have either lost information, is out of contact with a normal source, or is simply ignorant of something that he or she should know. As anyone can empathize with this plea, the victim is often all too willing to provide the information sought by the social engineer.

Using these methods—taking advantage of the gratitude, sympathy, and empathy of their victims—social engineers are able to achieve their aims.

Impersonation

Because forming trust relationships with their victims is critical to a social-engineering attack, it is not surprising that social engineers often pretend to be someone or something that they are not. Two of the major tools of impersonation are (1) speaking the language of the victim institution and (2) knowledge of personnel and policy.

To allay suspicion, a social engineer needs to know and be able to use an institution's terminology. Being unable to do so would cause the victim to suspect, rather than trust, the social engineer. With a working knowledge of an organization's particular vocabulary, a social engineer can phrase his or her request in terms that will not rouse alarm with the intended victim.

The other major goal of a social engineer in preparing a successful impersonation is to develop a familiarity with the "lay of the land," i.e., the specifics of and personnel within an organization. For instance, a social engineer needs to discover who has what authority within an organization so as to understand for whom he or she needs to claim to speak.

Research

To establish trust in their victims, social engineers use research as a tool. This comes in two forms, background research and cumulative research.

Background research is the process by which a social engineer uses publicly available resources to learn what to ask for, how to ask for it, and whom to ask it of. While the intent and goal of this research differs from the techniques used by students, librarians, and other members of the population, the actual process is the same.

Cumulative research is the process by which a social engineer gathers the information that he or she needs to make more critical requests of their victims. The facts that a social engineer seeks through cumulative research may seem without value to the casual observer, but put together properly, they are anything but that. Questions can include names of staff, internal phone numbers, procedures, or seemingly minor technical details about the library's network (e.g., what operating system are you running?).

Late in the afternoon the phone at the reference desk rings. Marcy, the librarian on duty answers, "Reference desk."

"Hi there, this is Dave Simpson calling from information services at the main branch. Sorry about the echo, I'm working in the cabling closet at the moment, so I'm calling you on my cell phone."

"No problem, I can hear you fine. What can I do for you?"

"Thanks. A lot of the branches have been having network problems over the last few days. Has everything been okay at the Seashore Branch reference desk?"

"I think so."

"Okay, that's good. I'm running a test right now on the network and needed to find a terminal that was behaving itself. Could you log off and let me know if any messages come up?"

"No problem." Marcy logs off of the reference computer; nothing strange happens. "Just the usual messages."

"Good. Now start logging back on. What user are you going in as? I mean which login name are you using?"

"Searef. Okay, I'm logged on now."

"No strange messages?"

"Nothing."

"That's great. Look, our problem might be kids hacking into the system so I need you to change the password. Do you know how to do that?"

"I think so."

"Well, let me walk you through it." Dave spends a couple of minutes walking Marcy through changing the system password. The password is now changed to 5eaR3f, a moderately secure password. "Thanks, Marcy. You've been a great help. We have your new password logged into the system. Could you pass on the new password to the other reference personnel?"

"Sure."

"Wonderful. Just remember not to give the password out to anyone who doesn't need it, and don't write it down where anyone who shouldn't have it can get at it. Have a great day."

"You too."

<click>

or she needs to violate the library's internal information systems.

Why are libraries vulnerable?

Libraries are vulnerable to social-engineering attacks for two major reasons: (1) ignorance and (2) institutional psychology. The first of these difficulties is the easiest to address. The ignorance of library professionals in this matter is easily explained—there is very little literature to date about the issue of social engineering directed at library personnel. What exists is usually mixed in larger articles on general security issues and receives little focus.

This lack of concern about social engineering can also be seen in computer professional literature, where it is dwarfed by the volume of articles concerning technical security issues. This is a curious gap, considering the high rate of occurrence of this kind of attack. Is it because many technical professionals are less comfortable with a social issue—that can only be solved through people—than with a technical security issue that can be solved through the development or implementation of proper software?[3]

Unfortunately, not knowing about a method of security violation leaves one vulnerable to that method. It is incumbent on librarians, computer administrations, and security professionals to be aware of these issues.

The second factor is harder to address but equally important. Unlike almost any other profession, librarians are expected to fulfill their patrons' informational needs without question or bias. This laudable goal makes librarians vulnerable to social-engineering attacks because the inquiries made by a social engineer about the information resources available at a library may be used for nefarious purposes. A reference interview over these issues may be very successful from the point of view of both parties involved, as the librarian fills the open-ended inquiries of the social engineer, and the social engineer receives much, if not all, of the information that he or she needs to violate the library's internal information systems.

Why libraries can be targets

At this point, it is relevant to ask why security violators would even bother with library computer networks. What do libraries have that is worth possibly committing a crime to get?

Personal information is probably the most tempting target in a library computer system. Libraries possess databases of names, addresses, and other personal data about library cardholders. This information is valuable, and not all of it is easily available from public sources. As may be seen in the section of this article on techniques, such information could be used as an end unto itself or as a stepping stone to security violations in other systems.

Subscriptions to proprietary databases are quite expensive, as any acquisitions librarian will explain. Given the high prices and limited licensing, a hacker may want to gain access to these information resources. This could be a casual hacker who wants to have access to a library-only resource from his or her home computer, or this may be a criminal who wishes to steal intellectual properties from a database provider.

Libraries often have broadband access designed for a large network (e.g., T1). As these lines are very expensive, few individuals can afford them. At the same time, it has been observed that these broadband lines have immense capabilities for downloading information from other networks. There are many reasons why a hacker would seek to illicitly use such a resource.

For instance, a casual hacker may want to download a large number of bootlegged movie files, or a criminal may wish to download a corporate database. With access to a library's high bandwith internet line, these actions can be carried out quickly and with a minimized chance of detection.

Libraries possess large numbers of computers due to their increasing automation. These computer resources can, if compromised, be used as anonymous remote computers by hackers. Called "zombies," compromised computers could be used to deliver illegal spam, distributed denial of service (DDoS) attacks, or as servers to distribute illegal materials. If library computers are used in this way, there is a potential for a library to face legal responsibility for the actions of its computers or for the questionable materials found on them.

Prevention

The tools needed to prevent social engineering from succeeding are awareness, policy, and training. These tools feed into one another—we become aware of the possibility of social-engineering attacks, develop policy to communicate these concerns to others, and then train others in these policies to protect them and their libraries from social engineering.

Libraries should have a simple set of policies to help prevent social engineering from affecting them. This policy need not be long; ideally, it should be a small page of bullet points that are easy to remember or to post near telephones. What is important is that it is easy to remember and implement when a call or e-mail comes in.[4]

Basic guidelines for protection against social engineering

- Be suspicious of unsolicited communications asking about employees, technical information, or other internal details.
- Do not provide passwords or login names over the phone or

via e-mail no matter who claims to be asking.

- Do not provide patron information to anyone but the patron in person and only upon presentation of the patron's library card or other proper identification.
- If you are not sure if a request is legitimate, contact the appropriate authorities.
- Trust your instincts. If you feel suspicious about a question or communication, there is probably a good reason.
- Document and report suspicious communications.

In closing

Social engineering is an immensely effective method of breaching computer and network security. It is, however, entirely dependent on the ability of the social engineer to persuade staff members into providing information or access that they should not provide. With care and good information policies, we can prevent social engineering from working. After all, do we really want to be helping the hacker?

The circulation desk phone rings. Joyce answers, "Seashore Branch Public Library, how may we help you?"

"Hi there, I'm worried that I haven't turned in all the books I have out, and I really don't want to get stuck with a fine. Could you tell me what I have out?"

"No problem. What is you name?"

"Sean Grey."

Joyce brings up Sean Grey's circulation records, and then remembers about the library's information policy and decides to ask another question, "Could you give me your library card number?"

"I don't have that with me. I really don't want to get stuck with those fines."

"I'm sorry. Mr. Grey, to preserve patron privacy we can only give out circulation information if you give us your card number or if you are here in person with your card or ID."

"But I just want to avoid a fine. Can't you help?"

"Don't worry; if you are late by accident on occasion, we are willing to forgive a fine."

"So you can't give me my records?"

"I'm sorry but we have to protect patron privacy. I'm sure you understand."

"I guess so. Goodbye."

"Have a good day."

<click> ■

References

1. Institute of Management & Administration, "Six Security Threats That Will Make Headlines in '05," *IOMA's Security Director's Report* 5, no. 1 (2004): 1–14.

2. K. Manske, "An Introduction to Social Engineering," *Security Management Practices (*Nov./Dec. 2000): 53–59.

3. M. McDowell, "Cyber-Security Tip ST04-014," (2005), http://www.us.cert.gov/cas/tips/ST04-014.html (accessed June 5, 2005).

4. K. Mitnick and W. Simon, *The Art of Deception* (Indianapolis: Wiley, 2002).

Index to Advertisers