Global Information Assurance Certification Paper

YOU ARE THE WEAKEST LINK!

Social Engineering targets the most vulnerable component of a computer system—people

Brian Purcell

GSEC v 1.4, Option 1

May 6, 2002

Information security is one of the hottest topics in the IT field today. Organizations are pouring a record amount of resources into protecting their networks and computing systems from hackers and other intruders. Yet most have neglected to "secure" the weakest element of their enterprise systems—the human beings that use and operate these systems. Hackers and pseudo-hackers determined to get into to an organization's network often use deception to gain the access and information they desire. The techniques of this deception are known as "Social Engineering" and can range from the seemingly obvious to more illusory exploits. But there are simple and inexpensive ways to help guard against such attacks. Before we explore that, however, it is important to understand the scope and possible avenues of this threat.

WHAT IS SOCIAL ENGINEERING?

Social Engineering is one of the least known and yet one of the most dangerous threats to information security. The simplest definition of Social Engineering is "an outside hacker's use of psychological tricks on legitimate users of a computer system in order to gain the information (usernames and passwords) he needs to gain access to the system" (Palumbo). Social Engineering can also be used to gain other proprietary information about a target organization such as financial, personnel, product, customer, or research data. In short, Social Engineering is duping somebody into giving you information that they would not normally divulge, and doing so without arousing suspicion.

WHAT TECHNIQUES ARE USED?

A Social Engineering attack is the most difficult type of cyber attack to defend against. It cannot be detected or foiled by technology, and it can take on many seemingly harmless forms. The techniques used in Social Engineering are generally divided into two classifications based on the mode used to make contact with the victim: human and computer (Arthurs). Human-mode attacks are the most common and simplest and involve direct personal contact with the target. "It relies on interpersonal relations and deception, using the 'tools' of the trade such as flattery, intimidation, name-dropping, asserting authority and belittling" (Arthurs). Computer-mode attacks, on the other hand, use some form of technology to capture information willingly supplied by an unsuspecting target, usually without direct contact between the hacker and the victim.

Before beginning an actual Social Engineering attack, or even deciding which method to use, an experienced social engineer will first research the intended target institution to learn its organizational structure, names, phone numbers, and internal idiosyncrasies and jargon. This information is invaluable as it helps the intruder determine the path of least

resistance, the best source of the information and access he is seeking, and the best scheme to achieve his goal. This information will also help the intruder seem authentic if or when he approaches his victims. And yet, despite its extreme value to hackers, most of this information is readily obtainable from an organization's website, roster, building directory, trash, or by simply walking though their offices (Arthurs).

Once a hacker has these details, it is simply a matter of putting them to use. Let's take a detailed look at some of the most common attacks.

One of the most frequent targets of Social Engineering attacks is an organization's technical support Help Desk (Tims). A hacker can call the Help Desk claiming to be a VP or department head who has forgotten his password or whose password is not working. If he encounters resistance, some simple threats of reporting the technician to their boss or even having them fired will usually result in the hacker getting the desired password (Orr). Many times, the social engineer will add urgency to the request by stating that he needs some important data in the next 10 minutes to close a deal or to report to an even more important person (for instance, the company president.)

Another common method is the third-party approach. An intruder will call the Help Desk or another person who has authority to grant access to computing resources and claim that a VP or other important person gave them authorization to a certain system, such as a financial database (Tims). This is especially successful if the important person being referred to is out of the office and cannot be contacted easily to verify the request. Again, urgency can be added to the request by saying that the data is needed for an important meeting in a few minutes. Adding urgency increases the pressure on the technician to comply with the request without investigating it.

Yet another potential technique is to call a secretary or other employee with high-level clearance pretending to be a technician with the organization's IT department. One of several scenarios is then used to elicit that user's password. For instance, the hacker could claim to be troubleshooting a network problem or testing a new system and they need that user's password to complete their work. Most people would readily divulge this information so as to be helpful.

The previous examples have all been done over the phone. But in some cases, social engineers can actually do their dirty work in-person. A common method is to impersonate a contract or field service technician (Tims). The intruder simply shows-up at an unsuspecting employee's office claiming to be working on the company's network or mainframe, and they need to test the employee's workstation (Allen). They ask for (and usually readily get) the employee's user name and password, sit down and test it, and sure enough, it works! They now have known-good credentials and they disappear as quickly as they appeared. A variation of this technique is to approach an employee and pose as a temporary clerk in need of help connecting to that "financial program." The legitimate employee will likely believe the "temp" and help them out.

One of the simplest physical techniques is known as "shoulder-surfing." This is where an intruder merely watches over the shoulder of someone as they type-in their password (Tims). In many cases, this can be done without the victim even knowing that the intruder was even there.

Although it does not involve direct contact with anybody in the target organization, another "in-person" scheme is the rather unpleasant yet potentially rewarding practice of so-called "Dumpster diving." This involves simply digging through an organization's trash for documents that may give the social engineer the information they need (Arthurs). It could be something as simple as a Post-It Note with a user's user name and/or password to something as significant as server or software documentation. Other valuable information that could be found in the trash includes directories, organizational charts, memos, personnel records, invoices—even company newsletters.

In addition to human-based forms of Social Engineering attacks, technology can be used so that a social engineer can get the information he desires without ever directly contacting the victims. One common form is through the use of Java script pop-up windows that capture an employee's voluntarily-supplied user name and password. These "Spartan horses," as they are sometimes referred to as, emulate a password dialog box that the user is familiar with. For instance, a common ploy is a Java-based dialog box that looks very much like the Dial-Up Networking connection screen in Windows 9x. To any but the most experienced user, the dialog box appears authentic giving the appearance that the user was disconnected from their Internet Service Provider. The unsuspecting victim would supply their credentials in order to reconnect. However, what actually happens is that those credentials are sent to the hacker. Other forms of this include faked Windows NT and 2000 login windows, phony e-mail and website authentication screens, and bogus error messages (Gregoire). Programmers can easily write their code to check what platform the user has and present a spoofed dialog box appropriate for that platform, hence preventing any trepidation on the part of the average user.

Internet chat services can be a particular source of concern. Hackers can masquerade in chat rooms and solicit seemingly innocuous information from unwary victims. A recent Instant Messaging Social Engineering attack involved tricking users into installing hacker software on their computers. Users are coaxed into doing this by automated tools that posts messages offering software that the user would likely find valuable, such as an anti-virus tool, software to download music, and even pornography. Instead, a Distributed Denial-of-Service agent, Trojan horse, sniffer, or backdoor program is installed, thus compromising that workstation and possibly the network that it is connected to (CERT Incident Note IN-2002-03).

Another form of technology-based Social Engineering attack involves an e-mail sent by a hacker to the user of a machine on which the hacker has already installed a Trojan horse.

The message asks the user to run "test" or beta software as part of a pilot project for a phony company, usually a game or some other application that an average user would be more than happy to try. The message includes instructions for running the software and a blurb that because of this-or-that technical reason, the user will have to re-enter their password. When the user executes the program, it prompts them for their network credentials, which the user will more than likely provide. These are then sent to the hacker (CERT Advisory CA-1991-04).

Many people instinctively register for various sweepstakes that they come across while on the web. Social engineers have set-up bogus sweepstakes websites which require the user to enter a password to register. Since many users will use the same password on these sites as they use at work for their network access, hackers are able to easily get a plethora of passwords fairly quickly by simply sending a mass e-mail to the target company advertising the bogus sweepstakes site (Tims).

There is one other form of Social Engineering that, instead of resulting in an intruder gaining access to the network, causes varying degrees of lost productivity or disruption. This method is the ubiquitous virus hoax, urban legend, e-mail chain letter, or occasional actual e-mail worm virus (Tims). Depending on the volume of mail created by these, the damage caused can be as insignificant as the wasting of a minute of an employee's time, or as serious as the widespread congestion or even collapse of an organization's network.

WHO IS VULNERABLE?

Any and all organizations are vulnerable to Social Engineering attacks. If an organization has data or resources that a hacker wants, they are at risk. However, some institutions may be more susceptible than others for different reasons. For instance, larger companies are especially vulnerable because of the intrinsic anonymity created by a large number of employees. How would an employee in an organization with thousands of workers know that the person claiming to be from the IT department is really not who he says he is? Larger organizations also tend to have more desirable assets that attract hackers.

Still, small organizations can and are targets of Social Engineering attacks. Many small organizations lack permanent IT staff and often rely on contract support services. Consequently, this opens the door to infiltration from spurious technicians (actual or counterfeit) who walk in off the street and are automatically given complete administrative access to servers or the network simply by claiming to be from their support contractor. The lack of an IT staff also means that nobody is informing employees of potential security risks, writing security policies, or monitoring the network for suspicious activity. And, smaller organizations may be more trusting simply because they are small. They don't expect to be a target of hackers, and they usually have a more casual workplace atmosphere resulting in a more trusting attitude.

Because of its very nature, Social Engineering is a truly "platform independent" method of attack. As long as the attacker knows the basic functioning of the major network and server systems, they can use Social Engineering to attack them. Even if a hacker encounters a proprietary or custom application or system that he has difficulties getting into, he could use Social Engineering to get assistance by simply calling the organization's Help Desk and impersonating a bewildered new employee.

Organizations are the focus of Social Engineering for various reasons. The most common are corporate espionage, disgruntled employees and former employees, and the simple "fun-seeking" hacker. Corporate spies might use Social Engineering to gain customer or product data from a competitor. A disgruntled employee could use Social Engineering to cause harm to the organization in retaliation for some perceived wrong. And, inexplicably, there are those out there whose only goal is to break-in to networks just to do it.

HOW OFTEN DOES IT HAPPEN?

Because Social Engineering attacks are designed to cause no suspicion on the part of the victim, it is virtually impossible to determine how often these ploys occur. But hackers employ it enough that there are several websites and even FAQ (Frequently Asked Questions) pages dedicated to the subject. One such site is prefaced with the rather ominous quote, "there's a sucker born every minute" (Bernz). These sites include descriptions of the various methods of a Social Engineering attack, stories of successful scams, and even some scripts or other tools to accomplish certain objectives. The presence of these resources would seem to indicate that Social Engineering is employed regularly by hackers, and as a result, organizations should realize this threat is real.

WHAT ARE THE POSSIBLE IMPACTS?

The impact of Social Engineering attacks can range from benign to catastrophic. A small Social Engineering attack might compromise a limited amount of data, maybe resulting in a few lost sales or the leaking of some confidential or embarrassing information. More advanced attacks can result in the wholesale theft of an organization's trade secrets, financial figures, research data, customer lists, etc., resulting in incalculable financial losses. In some cases, a company may not even know that their data has been compromised. Social Engineering attacks can also have more obvious or tangible results, including the destruction or alteration of data.

WHAT CAN BE DONE TO PREVENT IT?

Generally, the best defenses against Social Engineering attacks are strong security policies and user education (Tims). A single, low-tech piece of hardware can also go a long way to defending against Social Engineering, that being a simple paper shredder (Dubin).

First, before any plan to guard against Social Engineering can be put into place, management must buy into the need for such a plan. Unfortunately, management often

relies on a strict dollar-and-cents analysis before they approve anything. The damage potential from Social Engineering is at best nebulous and certainly highly variable. So, convincing management of the need for specific Social Engineering countermeasures can be a chore. However, many managers and decision-makers today are aware of the need for information security, and many organizations have an existing "infrastructure" of information security policies and procedures that can be leveraged and adjusted to include Social Engineering prevention. Also, since the main components of Social Engineering prevention are simple policies and training, the costs of this form of information security can be substantially less than other more-conventional security projects. This can be a major selling point in getting such an effort approved.

Once management has bought-in to the concept and need for Social Engineering prevention, then implementation can begin. There are two main yet simple things an organization can do to "engineer" themselves against Social Engineering attacks: create or strengthen security policies, and educate their employees.

First, an organization must have a strong information security policy that all employees are aware of. Such a policy should address the following issues:

- *Employee responsibility:* Employees should be aware that they are the first-line of defense and that the responsibility for information security rests with each individual as part of their daily jobs. Yet, it should not be written so strictly that it causes excessive anxiety or fear among employees.
- *Passwords:* All users must have a password on their account and such passwords should meet a moderate level of complexity (such as the inclusion of numbers and special characters.) Passwords should not be so complex that employees will be tempted to write them down. A statement prohibiting writing passwords down and leaving them near workstations should also be included in this policy. In addition, passwords should be changed at reasonable regular intervals. Again, requiring passwords to be changed too often will prompt employees to write their passwords down. Prohibitions on sharing accounts and divulging passwords should also be written into the policy. One other component of a good password policy would be a statement prohibiting IT employees from asking for user's passwords.
- *Non-disclosure agreement:* Users must agree that the organization's data must and will be kept confidential.
- *Help Desk:* Specific policies to protect and direct Help Desk technicians are integral to maintaining strong information security. Help Desk personnel should be insulated from threats from anybody in the company to prevent intimidation. Additional measures can be implemented that require all password or account requests to be verified either through an established chain-of-command, callback procedure, or in-person requests with ID. Sanctioning specific trusted employees with the sole authority to request password changes for a given organizational unit

(i.e. a department) can also be an effective measure to prevent unauthorized password resets.

- *Access control:* Similar to password reset control, a set of procedures to verify requests for changes to data access permissions should be in place and enforced. Procedures to establish new accounts and ensure that accounts for terminated employees are deleted should also be enacted.
- *Internet and e-mail use:* A clearly delimited policy should be in place that defines what is considered acceptable use of the Internet and e-mail. It should include statements that prohibit accessing pornography, personal e-mail accounts, known hacker sites, and the use of company resources for personal gain. When establishing an acceptable use policy, a key point to keep in mind is reasonableness. If the policy is too restrictive (such as banning all personal use), it will be difficult to enforce and employees will be more likely to disregard the policy altogether, whereas if reasonable restrictions are placed with an explanation of their rationale, then employees will be more likely to "buy-into" the policy and cooperate. In essence, such policies are a matter of compromise or give-and-take. While this may seem to be contrary to an organization's need (and right) to control use of their resources, in the end, the goal is to protect the organization's assets, and a *reasonable* acceptable use policy that employees support is the best means to that end.
- *Visitor policy:* An organization should require that all visitors register at a central reception desk and obtain and wear a visitor tag for the duration of their stay, and that they be accompanied by an employee at all times. Special procedures and tags should be used for visiting repair technicians so that they can be distinguished from "regular" visitors. Also, employees should be required to wear company-issued ID and anyone not wearing ID should be challenged.
- *Physical security:* All server rooms, data centers, communications closets, and record storage areas should be secured under lock-and-key. Card access systems that log all entries are even better. Only personnel that need access to any of these facilities should be granted such access, and procedures to grant and revoke those rights should be in place. In addition to the above mentioned facilities, waste areas and Dumpsters should also be secured.
- *Destruction of data:* An appropriate schedule of data archiving should be created and implemented. Obsolete or expired data should be either destroyed (if allowable under law) or archived and stored in a secure location. Once such data is no longer required to be kept, those archives should be properly destroyed. A person or team should be designated to periodically perform the archival and destruction duties. In addition, this policy should also include requirements to degauss or otherwise erase hard drives and floppy disks before they are transferred, sold, or discarded.
- *Destruction of paper documents:* All official documents being disposed of by an organization should be shredded or incinerated. Even "regular" trash should be discarded in a controlled manner (such as a locked Dumpster). Many companies

participate in paper recycling programs—these can be continued, but the paper to be recycled should be shredded before it is turned-over to the recycling contractor, and the recycling contractor should be bound by a strict privacy or non-disclosure agreement.

- *Inventory management:* Strict control of all computing devices (including PCs, workstations, and laptops) must be kept to prevent unauthorized electronic data from "walking-out" of the organization on stolen equipment.
- *Telephone procedures:* All employees (except the Help Desk) should be informed not to act on unsolicited or unsubstantiated telephone requests and should be encouraged or required to forward any such requests to a central IT security team.

These are just a few fundamental security policies that all organizations should have. Additional custom policies should be implemented based on the specific desires or requirements of the organization.

Once the policies are in place, the next thing to do is to educate employees about those policies. Such training should include an ongoing security awareness program so that employees understand the possible dangers and receive contemporary information about emerging and continuing threats. In addition, all employees should receive basic and advanced technical training so that they better understand the systems they work with. This oftentimes removes the mystique of enterprise computing systems and gives employees a sense of ownership and understanding that can be helpful in thwarting Social Engineering attacks. Training and education programs should be offered continuously to employees and all new employees should be required to attend at least the basic level courses as a requirement of their jobs.

The security awareness training should use real-life examples of possible (or even actual) attacks that can occur and should demonstrate what the effects of such attacks are. It should be shown what the possible outcome can be for a seemingly innocent request (such as an IT technician's asking for a password.) But such training should also be sensitive so as to not make employees feel that they will be deemed "gullible" or naïve if they fall for such exploits. Instead, employees should be encouraged to report any suspicious activity, possibly through an incentive program.

In addition to personal training, information security policies and up-to-date information should be posted on a company intranet site. Login banners, periodic e-mail messages, videos, brochures and newsletters, and screen savers can all be used to disseminate timely security information (Arthurs). A key to keep in mind when employing these methods is to keep them current and to change them often so that they do not become "monotonous", and not to deploy them excessively lest they be ignored. Annual, bi-annual, or quarterly seminars on information security, especially for those in sensitive positions, should also be considered. But, personnel in positions that are not directly connected to technology (i.e. receptionists, mail room clerks, custodians, etc.) should also be included in information security training and policies as these workers oftentimes know enough

about an organization to be valuable to hackers. In short, every employee should feel they have responsibility and ownership for their organization's well-being.

CONCLUSION

As we have seen, the methods used by Social Engineers can run the gamut from various forms of human contact to impersonal technological exploits, and the dangers presented by such activities can be detrimental to an organization's data security. Unfortunately, Social Engineering is designed to prey upon the inherent weaknesses in the human personality, and as a result, will always be difficult to defend against. "Human nature, being what it is, will always be susceptible to social engineering" (Orr). But there are easy solutions to help prevent or mitigate such attacks, those being the implementation of sound and clear information security policies and the continuous training and education of users. The best aspect of these solutions is that they are relatively inexpensive and simple to implement, but the payoff can be tremendous. The old adage "an ounce of prevention is worth a pound of cure" certainly applies to the threat of Social Engineering.

SOURCES

Allen, Malcolm. "The Use of Social Engineering as a Means of Violating Computer Systems." October 12, 2001. URL: http://rr.sans.org/social/violating.php

Arthurs, Wendy. "A Proactive Defence to Social Engineering." August 2, 2001. URL: http://rr.sans.org/social/defence.php

Bernz. "The Complete Social Engineering FAQ!" Date unknown. URL: http://morehouse.org/hin/blckcrwl/hack/soceng.txt

Dubin, Lawrence. "The Enemy Within: A System Administrator's Look at Network Security." January 7, 2002. URL: http://rr.sans.org/social/within.php

Elliotte Rusty Harold. "User Security Issues and Social Engineering." June 15, 1998. URL: http://www.ibiblio.org/javafaq/course/week5/15.html

Gregoire, Dannie J. "The Spartan Horse: A Simple, Yet Effective Browser Based Trojan Horse." 1998. URL: http://www.thetopoftheworld.com/spartanhorse

Lyman, Jay. "'Social Engineering' Spreads New Plague of Web Chat Attacks." March 21, 2002. URL: http://www.newsfactor.com/perl/story/16870.html

Orr, Chris. "Social Engineering: A Backdoor to the Vault." September 5, 2000. URL: http://rr.sans.org/social/backdoor.php

Palumbo, John. "Social Engineering: What is it, why is so little said about it and what can be done." July 26, 2000. URL: http://rr.sans.org/social/social.php

Paradowski, Christopher. "The Cyber Con Game – Social Engineering." February 18, 2001. URL: http://rr.sans.org/social/cyber_con.php

Stevens, George. "Enhancing Defenses Against Social Engineering." March 26, 2001. URL: http://rr.sans.org/social/defense_social.php

Tims, Rick. "Social Engineering: Policies and Education a Must." February 16, 2001. URL: http://rr.sans.org/social/policies.php

CERT Coordination Center. "CERT Advisory CA-1991-04 Social Engineering." April 18, 1991 (Revised September 18, 1997). URL: http://www.cert.org/advisories/CA-1991-04.html

CERT Coordination Center. "CERT Incident Note IN-2002-03 Social Engineering Attacks via IRC and Instant Messaging." March 19, 2002. URL: http://www.cert.org/incident_notes/IN-2002-03.html

Last Updated: May 28th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event