Global Information Assurance Certification Paper

Social Engineering – Attacking the Weakest Link

Abstract

Much of the focus within the information security field centers on technical attacks and corresponding technical defenses. However, many successful information security penetrations are non-technical in nature. They involve targeting humans, often the weakest link in the information security chain. This form of attack is commonly referred to as social engineering.

Social engineering exploits a number of human traits and tendencies; with the goal of inducing the target to provide information or access that otherwise is not available. Just as social engineering attacks elude technical countermeasures, non-technical countermeasures may prove effective in mitigating these attacks. Well defined an enforced policies and procedures are critical to protecting any organization. Finally, user awareness training is imperative to educate and inform users of such threat vectors. Social engineering is a real and often realized threat in the information security world. With the appropriate countermeasures and due diligence, social engineering attacks can be easily thwarted.

Introduction

A junior systems administrator, recently hired to assist with the implementation of a new financial accounting system, receives a phone call from a frantic executive. The executive is currently at a client site and has forgotten his password to the new accounting system. He explains to the systems administrator that unless he gets access to the system, he will not be able to complete the client reports. A multi-million dollar contract is in jeopardy. The executive demands that the systems administrator reset his password so he can access the system. The systems administrator is clearly in a dilemma: if he resets the executive's password, he may be violating corporate policy. However, if he fails to fulfill the request, he may very well lose his job.

The scenario is completely plausible, as many companies have experienced similar, if not exactly the same, situations. The executive on the phone is not really an employee of the company, but an imposter looking to obtain privileged information about the company. Through careful reconnaissance, the attacker knows for a fact that the executive is out of town. If the attacker is successful, a systems administrator who is simply trying to be helpful will grant the attacker access to the system. The attacker will have bypassed all the firewalls, intrusion detection and other technical security devices. This is one illustration of a social engineering attack. This paper will discuss social engineering, a common tactic used by attackers to gain access to information and systems. This paper will cover the different kinds of social engineering attacks as well as countermeasures companies can implement to mitigate these attacks.

Definition

The information security industry defines social engineering as an attack that breaches an organization's security defenses by manipulating people and the human tendency to trust. The object of social engineering is the same as technical hacker* attacks: "to gain unauthorized access to systems or information in order to commit fraud, network intrusion, industrial espionage, identity theft, or simply to disrupt the system or network."[1] While the goals are the same as traditional hacker attacks, social engineering attacks are traditionally non-technical. These attacks leverage social skills and are implemented through human interaction.

The weakest link: humans

Social engineering is effective for several reasons. First, social engineering is relatively easy to execute. Social engineering attacks can compromise the most extensive security system with a simple question. It is amazing how much information people are willing to provide if they are simply asked. As "Mom" always taught, "you're never going to get something unless you ask for it." After all, we know that the worst that can happen is the person refuses. Asking for something is a cornerstone of social engineering because it is easy to do and is cost free.

* This paper uses the term "hacker" generically. A hacker is a person who attempts to gain unauthorized access to a system. This paper makes no distinction between a white-hat or black-hat hacker, cracker, or script kiddies. That debate is beyond the scope of this discussion.

However, social engineering isn't necessarily that simple. Social engineering requires levels of preparation similar to those of any other technical hacker attack. Social engineering is so effective simply because they target the weakest link in the information security universe: humans.

As Harl describes in "People Hacking," the weakest link in any system is the user. Recognizing that all information systems rely on humans, it becomes clear that users are a universal vulnerability, "independent of platform, software, network or age of equipment."[2] Below is a selection of psychological and behavioral traits that makes humans susceptible to social engineering attacks. Social engineering attackers exploit these traits to gain compliance from their targets.

Persuasion

Persuasion is an art and science employed throughout society. The advertising and marketing industries are experts in persuasion, producing campaigns that are designed to elicit certain responses. Like these industries, hackers have also discovered that "humans have certain behavioral tendencies that are exploitable through careful manipulation."[3] Hackers employing social engineering attacks are often skilled in persuasion and capable of getting targets to reveal information.

The foot-in-the-door technique is one common method of persuasion. The foot-in-the-door technique involves an attacker making a series of small, seemingly innocuous requests. Since these requests are small, they are likely to be granted. As more inconsequential requests are made and granted, the attacker creates a relationship wherein larger requests follow the natural sequence of the exchange. He increases the probability of compliance because the previous requests that have been granted were harmless.

Tendency to be helpful

Humans have a tendency to be helpful, to observe common courtesy. One example is holding an elevator for someone or opening a door for someone whose hands are full. Someone posing as a service technician, carrying a boxful of tools and equipment will often have a secured door held open for them. An appropriately dressed professional may claim that he left his access key in the other coat and request someone to give them elevator access. These common courtesies circumvent physical security and give attackers free reign throughout an office.

Diffusion of responsibility

Diffusion of responsibility is the concept whereby an individual believes that he or she is not solely responsible for his/her actions. Social engineering attackers skillfully create illusions whereby the individual does not have to bear the full burden of responsibility. This is often done by notifying the target that a supervisor has authorized such a request or that others, familiar to the target, are also involved. As a result, the attacker is then able to more easily coax information from the target.

Ingratiation

Ingratiation is a human behavior that increases compliance. Ingratiation involves the use of praise, flattery or friendly/helpful behavior in order to gain influence. It can work two ways. Often an attacker will curry favor with a target through ingratiation, slowly setting the target up for a request. The attacker creates a trust relationship through ingratiation. The goal of the trust relationship is to put the target in a position where the target will be more likely to grant a request.

Ingratiation also occurs when the attacker creates the environment wherein the target will want to ingratiate himself with the attacker. For example, the attacker is able to name drop and create the illusion of being able to help the target out in future situations. In this scenario, the attacker's request is more likely to be granted because the target believes that he will be making a deposit in the favor bank.

Moral duty

The concepts of right and wrong, good and bad are instilled into all human beings, often from an early age. These concepts serve to form one's morals, which guide behaviors and actions. Moral duty is a concept whereby one feels compelled to take action based on one's convictions and beliefs. Social engineering attackers exploit this by creating a situation whereby a target complies with a request because it is the their moral duty to do so.

Harl ties the concept of moral duty to guilt, noting that people prefer to avoid guilty feelings.[4] Attackers can also exploit this aversion by creating scenarios where failing to comply will result in guilt for the target. An example of this is when a requestor (read: attacker) tells the target that if the request is not granted, then the requestor may lose his job.

Other traits

The traits and behaviors described above is only a small list. Humans are naturally social with a host of other traits and behaviors that ensure a positive social environment. Other traits include:[5]

- the desire to be helpful – people tend to help out others often because we would appreciate similar assistance in our times of need.
- the desire to avoid unpleasant events for ourselves and others – people are compassionate and will not subject others to pain or discomfort.
- the desire to appear competent in our profession – no one wants to appear inept, especially in one's field of expertise.
- the desire to trust others, the tendency to accept what other say as being truthful unless proven otherwise – people tend to give others the "benefit of the doubt."
- the desire to advance our own cause and career – people are opportunistic and will try to help themselves if and when possible.
- the desire to be attractive to those whom we admire or desire – people want to be accepted in general, and even more so by those we look up to. We often believe that compliance will result in acceptance.

- the desire to believe that those we deal with are honorable – again, giving others the "benefit of the doubt."
- the desire to be perceived as a team member – teamwork is a common core value throughout many organizations. It is widely expected and not being a team player may even have career hampering repercussions.

As one can see, all these traits make humans extremely vulnerable to social engineering attacks. Yet with any vulnerability, there are countermeasures and steps an organization can take to mitigate these vulnerabilities.

Threat vectors

Social engineering attacks can come from all directions. These various attack points are known as threat vectors. Before information security professionals can properly develop countermeasures to social engineering attacks, it is important to understand the threat vectors and how exactly attackers transform interpersonal communication vehicles into entryways to an organization's privileged information and systems.

Dumpster diving

Dumpster diving is the practice of searching through a company's trash in hopes of finding useful information. While dumpster diving is not necessary an attack itself, it can provide would be attackers with important information about the company.

This information is used as part of the footprinting process. *Hacking Exposed* defines footprinting as "the fine art of gathering target information."[6] It goes on to point out that while "footprinting is the most arduous task of trying to determine the security posture of an entity…it is one of the most important."[7] Just as with a technical attack, they key to a successful campaign lies more in the preparation than the actual execution. Dumpster diving may yield any of the following items:[8]

- Company phone lists or phone books
- Organizational charts
- Memos
- Calendars of meetings, events and vacations
- Company letterhead
- Company policy manuals
- System manuals
- Printouts of source code
- Printouts of sensitive data (including login names and passwords)
- Outdated hardware, disks, tapes

These items reveal a wealth of information about the target organization. They provide legitimate names and titles of individuals that can be impersonated. Company letterhead can be used to forge a formal request. System manuals give the attacker an idea as to what systems are running and therefore be able to specifically refer to them when making a request.

Phone

One of the most common social engineering threat vectors is the telephone. The telephone is a widely accepted method of interpersonal communication used by society. Business is often conducted over the telephone. People have become accustomed to making and granting requests through the phone. Since telephone communication is so common, it becomes difficult for a target to determine which requests are legitimate and which may be social engineering attacks.

Social engineering attacks through the phone often involve impersonation. The caller will have done the proper footprinting, which provides the attacker with the necessary information to pull off a successful impersonation. Information such as the organization's management structure (with specific names and titles of important individuals), current and pending projects, and other detailed, but not necessarily privileged, information will help an attacker convince a target that he is making a legitimate request.

In addition to the scenario described in the introduction, another example is an attacker calling a target, posing as a technician from the help desk. The target is informed that the technical staff is performing some upgrades and needs the target's username and password to complete the process. An unknowing user may very well provide comply with the request.

Email

Emails are another form of interpersonal communication that attackers can leverage. Most email applications allow users to change the sent-from and reply-to fields in an email. Attackers can manipulate these settings and impersonate someone making a legitimate request.

Email attachments are also a major concern. Since emails routinely pass through firewalls unnoticed, destructive programs have a free pass into the system. Users unleash these programs when they blindly open attachments with little regard to the potentially damaging effects, especially if the email is sent from someone that the target recognizes. These attachments may be viruses, worms, or Trojan horses and are often disguised in a way that entices a user to execute the application. Any one of these types of attachments can wreak havoc on a system.

IRC/Instant messaging

Instant messaging (IM) has quickly grown in popularity. Businesses are slowly accepting IM as a yet another form of business communication (often as a workgroup collaboration tool). As these tools become more prevalent in the office, information security professionals need to be aware of the potential vulnerabilities.

The Computer Emergency Response Team (CERT) at Carnegie Mellon University recently issued an incident notice detailing social engineering attacks via Internet Relay Chat (IRC) and IM. In this notice, CERT warns of attacks that "trick unsuspecting users into downloading and executing malicious software."[9] The malicious software is

disguised as applications that offer improved download speeds, anti-virus protection, or pornography. As the CERT notice points out, this is a classic social engineering attack since the success of the attempt depends entirely on whether or not the user downloads and runs the program.

Countermeasures

While the various social engineering attacks outlined above are daunting, there are plenty of countermeasures an organization can implement to detect and prevent these types of attacks. Below is a discussion of the countermeasures that will mitigate the human factor.

Physical security

Physical security is one countermeasure that must be implemented, regardless of the types of threats an organization may face. Physical security starts by allowing only authorized personnel into and out of the organization's premises. Many organizations have security guards that monitor who enters and exits buildings. In addition, offices often have a receptionist responsible for assisting visitors.

In addition to posting guards physical security also calls for locking doors, cabinets, and drawers. This will limit access to those who have gotten past the initial layer. Another good practice is to shred documents that contain sensitive information. As discussed earlier, dumpster diving reveals a wealth of information. Shredding and properly disposing documents are effective countermeasures to dumpster divers.

Security policies

A well-defined security policy is a critical element in protecting against social engineering attacks. Policies can "remove the responsibility of employees [in making] judgment calls regarding a hacker's request. If the action is prohibited by policy, the employee has no choice but to deny the hacker's request."[10] Below are a few security practices recommended by the Gartner Group:[11]

- Establish procedures that eliminate any exchange of passwords. A system administrator should never ask a user for his or her password, nor even be able to view any password on the system.
- Promote strong passwords and avoid using passwords or authentication questions an attacker can easily discern.
- Delete email and system accounts for recently terminated employees. Disable these accounts for employees on extended leave.

A security policy should provide employees with acceptable rules of behavior and strict guidelines on what practices are allowed and restricted. They can either be general or specific, but should always be clear and easy to understand. In addition, policies should also enumerate enforcement mechanisms such as consequences for noncompliance.

A security policy must have complete support from management in order to be effective. As Granger points out, "management must understand that all of the money they spend on software patches, security hardware, and audits will be a waste without adequate

prevention of social engineering attacks."[12] Employees need to be ensured. Management buy-in is critical in ensuring that a security policy is implemented and enforced.

Awareness training

In addition to security policies, the other critical element in protecting against social engineering is a well-educated employee. Security policies are only effective if employees are familiar with them. Awareness training includes reviewing the security policy and the goals and motivations behind each of the directives. Employees need to understand the risks and what is at stake in case of a security breach.

An effective awareness program will not only educate employees about security threats, but also make them a part of the security process. Employees should be given specific roles and responsibilities in ensuring that the organization stays secure. Gartner states that, "if users understand these issues, they are more likely to comply with them or note suspicious behavior. The single strongest defense against social engineering attacks is an educated employee." As discussed above, social engineering threat vectors are all around; employees need to be aware of what they are, and be able to spot as well as disarm them.

Incident Response

An organization needs to have efficient incident response protocols that allow educated users to report suspect behavior. User awareness training has educated employees in how to spot a social engineering attack. They now need to have defined means of reporting these incidents. This empowers employees and makes them part of the security process.

Even more importantly, the organization needs to have feedback controls that let employees know that incidents are being addressed. Incident reports need to be treated with respect and followed through. Otherwise, "employees will be discouraged from noticing or reporting suspected social-engineering attacks."[13]

Access controls

Access controls implement the principle of least privileges. The principle of least privileges calls for a user or system to be provided with only the necessary access required to complete its tasks. Access controls limit the damage a novice user can cause. For example, a receptionist, who may be more susceptible to a social engineering attack, may be asked to email confidential files. However, if proper controls exist, the receptionist should not be able to access these files because that privilege is not necessary for the receptionist role.

Access controls can also prevent users from downloading and installing malicious software, as well as creating, modifying or deleting accounts. In case a target is compromised through a social engineering attack, access controls can limit the amount of damage the attacker can cause. Again, if the attacker compromises a receptionist's login and password, the attacker will be limited to the receptionist's restricted privileges.

Anti-virus

Anti-virus is a common layer of defense that many organizations implement. This layer of protection is an excellent countermeasure against social engineering attacks that request users to download and install files (e.g. email, IRC, and instant messaging attacks). Anti-virus software should be able to recognize threat signatures of malicious software and prevent them from being installed. Of course, anti-virus software is only as good as its definition file, so updating anti-virus software is also part of the countermeasure equation.

Conclusion

Last year corporations spent millions of dollars on security. Most of the money was spent on technical solutions, such as firewalls, border routers, intrusion detection systems, etc. Many companies believe that the information security problem is best addressed through money; protection is directly correlated to the amount of hardware and software erected to hold back attackers. However, experienced security professionals know that this is not the case.

While technical solutions are important components in the information security chain, social engineering attacks the weakest link: humans. Since humans interact with all information systems the result is a widespread vulnerability. As with any vulnerability, the best solution requires defense in depth. These layers begin at the physical level and include technical layers (access control, anti-virus) as well as management layers (upper level management buy-in, security policy, user awareness, incident response). As with most information security problems, the solution focuses on management. Organizations can strengthen their overall security posture as long as they take the time (and money) required to properly secure themselves not just from a technical perspective, but also a human perspective.

Bibliography

Allen, Malcolm. "The Use of Social Engineering as a Means of Violating Computer Systems." Oct. 21, 2001. http://rr.sans.org/social/violating.php. Visited Feb. 19, 2002.

Arthurs, Wendy. "A Proactive Defense to Social Engineering." Aug. 2, 2001. http://rr.sans.org/social/defence.php. Visited Feb. 19, 2002.

Berg, Al. "Cracking a Social Engineer." *LAN Times*. Nov. 6, 1995. http://packetstorm.decpticons.org/docs/social-engineering/soc_eng2.html. Visited Mar. 19, 2002.

Bernz. "The Complete Social Engineering FAQ!" http://packetstorm.decepticons.org/docs/social-engineering/socialen.txt. Visited Mar. 19, 2002.

CERT/CC. "CERT Advisory CA-1991-04 Social Engineering." Sept. 18, 1997. http://www.cert.org/advisories/CA-1991-04.html. Visited Mar. 19, 2002.

CERT/CC. "Social Engineering Attacks via IRC and Instant Messaging." Mar. 19, 2002. http://www.cert.org/incident_notes/IN-2002-03.html. Visited Mar. 19, 2002.

Gartner. "There Are No Secrets: Social Engineering and Privacy." *Social Engineering: Exposing the Danger Within.* Feb. 2002. http://www3.gartner.com/gc/webletter/security/issue1/index.html. Visited Mar. 15, 2002.

Gartner. "Protecting Against Social Engineering Attacks." *Social Engineering: Exposing the Danger Within.* Feb. 2002. http://www3.gartner.com/gc/webletter/security/issue1/article2.html. Visited Mar. 15, 2002.

Gartner. "Unmasking Social-Engineering Attacks." *Social Engineering: Exposing the Danger Within.* Feb. 2002. http://www3.gartner.com/gc/webletter/security/issue1/article1.html. Visited Mar. 15, 2002.

Granger, Sarah. "Social Engineering Fundamentals, Part I: Hacker Tactics." Dec. 18, 2001. http://www.securityfocus.com/infocus/1527. Visited Feb. 18, 2002.

Granger, Sarah. "Social Engineering Fundamentals, Part II: Combat Strategies." Jan. 9, 2002. http://www.securityfocus.com/cgi-bin/infocus.pl?id=1533. Visited Feb. 18, 2002.

Harl. "People Hacking: The Psychology of Social Engineering." Mar. 7, 1997. http://packetstorm.decepticons.org/docs/social-engineering/aaatalk.html. Visited Mar. 19, 2002.

Hisey, Patty. "Computer Security Awareness Training…Do you need it?" Dec. 20, 2000. http://www.sans.org/infosecFAQ/securitybasics/training.htm. Visited Oct. 15, 2001.

Nelson, Rick. "Methods of Hacking: Social Engineering." www.isr.umd.edu/gemstone/infosec/ver2/papers/socialeng.html. Visited Feb. 19, 2002.

Nichol, Kelly. "Implementing a Security Awareness Training Program in Your Environment for Every Day Computer Users." Dec. 8, 2000. http://www.sans.org/infosecFAQ/start/awareness.htm. Visited Oct. 15, 2001.

Paradowski, Christopher. "The Cyber Con Game – Social Engineering." Feb. 18, 2001. http://rr.sans.org/hackers/cyber_con.php. Visited Feb. 19, 2002.

Reuters. "Mitnick Meets His Pigeon." Feb. 21, 2002. http://www.wired.com/news/culture/0,1284,50585,00.html. Visited Feb. 24, 2002.

Stevens, George. "Enhancing Defenses Against Social Engineering." Mar. 26, 2001. http://rr.sans.org/social/defense_social.php. Visited Feb. 19, 2002.

---

[1] Granger. "Social Engineering Fundamentals Part I."
[2] Harl.
[3] Gartner. "There Are No Secrets."
[4] Harl.
[5] Stevens.
[6] *Hacking Exposed*. p. 6.
[7] *Hacking Exposed*. p. 6.
[8] Berg.
[9] CERT Incident Note IN-2002-03.
[10] Granger. "Social Engineering Fundamentals Part II."
[11] Gartner. "Protecting Against Social Engineering Attacks."
[12] Granger. "Social Engineering Fundamentals Part II."
[13] Gartner. "Unmasking Social-Engineering Attacks."

Last Updated: July 27th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event