Global Information Assurance Certification Paper

Alka Sharma
December 29, 2003

GIAC Security Essentials Certification (GSEC)
Practical Assignment
Version 1.4b – Option 1

Hacking People – How To Prevent It

Abstract

"Social engineering" is an under-estimated security risk that is rarely addressed in staff training programs or corporate security policies. This paper introduces the art of social engineering and briefly touches upon its various facets, like types of attacks, the underlying exploits, and ultimate impact of it to an organization. The paper's main focus however is on the most important and obvious question that follows any stated problem – what to do about it? The paper aims to direct an organization toward basic essential measures that it could take to prevent this non-technical but insidious attack. If carefully and dedicatedly followed, the organization can secure itself from the weakest link in security and the most vulnerable aspect of any organization's security infrastructure - people.

Table Of Contents

1.0 What is Social Engineering?

Security is about trust.

There is always someone somewhere who would have told us something they really shouldn't have because they believed we were somebody we weren't.

Social engineering exploits the natural human willingness to accept someone at his or her word. It is a hacker's clever manipulation of the natural human tendency to trust. It is the attempt to gain access to sensitive data (such as password, usernames and credit card numbers) by gaining human trust.

Social engineering is about using social interactions to obtain information, and tricking people into doing things they would not do if they knew the hacker's real identity and intentions.

It is an attack that plays upon an organization worker's sincere desire to get the job done and help others to do the same.

2.0 The Real Skill

According to Kevin Mitnick, "You try to make an emotional connection with the person on the other side to create a sense of trust. That is the whole idea: to create a sense of trust and then exploiting it."

Social engineering can involve a lot of 'groundwork' - information gathering and idle chitchat before an attempt at gaining information is ever made.

Typically, the social engineer creates a situation, makes up a likely story and ensures that the victim gets involved with the situation. Strong arguments in favor of helping out are presented that if the person would not help he might start feeling guilty. The victim eventually would feel the importance of helping out. The less competent a victim is, the more likely he is to agree to helping out.

A real social engineering attack would be accomplished over weeks, if not months.

3.0 Why Social Engineering?

A social engineer's goal is the same as that of any general hacker's - to obtain information that will allow him/her to gain unauthorized access to a system and the information that resides on it.

The objective is to gain unauthorized access to systems or information in order to commit either a typical attack like network intrusion or system/network disruption, or a large scale attack like fraud, industrial espionage, or identity theft.

Typical targets have included telephone companies and answering services, big-name corporations and financial institutions, military and government agencies, and hospitals.

4.0 Understanding the Threat

The human part of a security set-up is the most essential, and also the weakest. Almost every computer system relies on humans, which means that this security weakness is universal, independent of platform, software, network or age of equipment.

Anyone with access to any part of the system, physically or electronically is a potential security risk. Any information that can be gained may be used for social engineering further information. This means that even people not considered as part of a security policy can be used to cause a security breach.

Almost every human being has the tools to attempt a social engineering 'attack'; the only difference is the amount of skill used when using these tools. It's an issue of trust, and so every organization is subject to being successfully manipulated. All staff, not just hackers, are sometimes guilty of this type of manipulation.

The art of social engineering is not one that has just come to be known or used. It was in play in the late 60s, by Frank Abagnale Jr., as depicted in the 2002 movie *Catch Me If You Can*. Abagnale is known to have used his prematurely gray hair, charming looks and personality to fool millions into believing that he was an assistant attorney general, physician, professor and airline pilot.

However, the concern is more pressing now because information is the most priced item today. It can be transferred more quickly than at any other time in history. One slip by only one individual in an organization can release the equivalent of reams of sensitive data in mere seconds. There simply isn't time to respond unless all are prepared!

5.0 What is the Impact?

The impact of a social engineering attack is similar to that of a regular or known hacking technique.

The pieces of information gathered over a period of time can easily be combined with other small bits to produce a detailed and dangerous roadmap to the organizational treasures.

Computer systems and networks are compromised, and business is affected.

A social engineer can get an unsuspecting insider to install and run malicious software on the organization's system(s).

Intruders may exercise remote control over an organization's system(s), including the network.

Confidential data of the organization is exposed, erased or maliciously modified.

Reputation is the most intangible loss, and financial the obvious.

6.0 Attack Examples

An unsuspecting customer might be asked to call a phone number, where the very official sounding person on the other end, a social engineer really, will just want to verify that the customer's account is indeed his by getting his credit card data.

According to Winkler and Dealy in their paper on Social Engineering, "Masters of Deception, who significantly penetrated the United States' telecommunications system, were only able to do so after obtaining information found in the garbage of the New York Telephone Company(Slatalla & Quittner, 1995)."

Wes Vernon of NewsMax.com reported:

> A Revelation at a recent CMR (Center for Military Readiness) briefing [was] that in the recent past, unique access to Pentagon 'insider' discussions has been accorded a Democrat presidential candidate (apparently retired Gen. Wesley Clark), a 2000 military strategist for Al Gore, and a gay activist who contributed to Gore's recount campaign in 2000." Elaine Donnelly, president of the CMR, told NewsMax.com, "I'm a big admirer of Mr. [Defense Secretary Donald] Rumsfeld, but I wish he would be a little more careful with the people with whom he shares private information, or strategic information that person can turn around and use against the administration."

7.0 Types of Attacks

Social engineering attacks take place on two levels:

1. The physical
2. The psychological

7.1 The Physical

The physical setting includes the workplace, phone, trashcan, and on-line.

7.1.1 The Workplace

A hacker pretends to be a maintenance worker and walks about the workplace in search of information for authentication that could be used for attack later. Shoulder surfing by an outsider at the workplace is a tool as well.

7.1.2 By Phone

Hackers pretend they are calling from inside the corporation by playing tricks on the PBX or the company operator. Hence caller-ID does not prove to be the best defense. Help desks are particularly prone to this type of attack.

7.1.3 Dumpster Diving

Dumpster diving, or trashing, could contain potential security leaks: organization phone books, organizational charts, memos, organization policy manuals, calendars of meetings, events and vacations, system manuals, printouts of sensitive data or login names and passwords, printouts of source code, disks and tapes, organization letterhead and memo forms, and outdated hardware.

7.1.4 On-line

This type of attack involves use of the computer system, or the online communication infrastructure or the Internet, or all these. For example, it exploits the fact that many users often repeat one simple password on every online account, and so a hack into one account is a hack into all. A social engineer may pretend to be the network administrator trying to help a user fix an account-related problem and hence requests the user's password. Email attachments sent from someone of authenticity can carry viruses, worms and Trojan horses. (One of AOL's technical support staff opened an email attachment that executed a backdoor exploit that opened a connection out from AOL through the firewall.)

CERT® Incident Note IN-2002-03 states the following on Social Engineering Attacks via IRC and Instant Messaging:

> The CERT/CC has received reports of social engineering attacks on users of Internet Relay Chat (IRC) and Instant Messaging (IM) services. Intruders trick unsuspecting users into downloading and executing malicious software, which allows the intruders to use the systems as attack platforms for launching distributed denial-of-service (DDoS) attacks. Intruders are using automated tools to post messages to unsuspecting users of IRC or IM services. These messages typically offer the opportunity to download software of some value to the user, including improved music downloads, anti-virus protection, or pornography. Once the user downloads and executes the software, though, their system is co-

opted by the attacker for use as an agent in a distributed denial-of-service (DDoS) network. Other reports indicate that Trojan horse and backdoor programs are being propagated via similar techniques.

7.2 The Psychological

The psychological refers to the manner in which the attack is carried out.

7.2.1 Conformity

This psychological factor involves a person's desire not to offend other people. Psychologists refer to it as 'demand characteristics', i.e., having strong social constraints on how one should act. The social pressure is constructed by the social engineer by creating a believable situation in which the victim feels immersed. The victims give in when they believe that they are not solely responsible for their actions, or feel that it is their moral duty to. The guilt factor is exploited - people prefer to avoid guilt feelings and so help out.

7.2.2 Personal Persuasion

A victim's voluntary compliance with the social engineer's request is enhanced.
It involves guiding the victim down the intended path. The victims believe that they have control of the situation and are exercising their power to help out for a small loss of their time and energy.

7.2.3 Co-operation

Conflict with the victim is avoided, and softness is a handy tool. A positive history of co-operation, where things have gone well in the past, greatly increases the chances of co-operation.

7.2.4 Sensory Information

Sensory information is important for a victim. Sight and sound could lead the victim into letting out information more easily than, say, an IRC style chat.

7.2.5 Involvement

Low involvement means that the victim has very little interest in the social engineer's request, e.g. cleaners or receptionists. They are not directly affected by the request, and hence do not analyze the request or the persuasion. They solely comply based on arguments like the status of the person calling.

8.0 Preventing the Attack

An attack is not always about obtaining passwords. Successfully obtaining sensitive personal and organization information is as great a breach in security and needs to be addressed.

Organizations need to focus on and improve the security of their "human factor" in an attempt to prepare for a social engineering attack.

The defenses against an attack involve work in the following areas:

8.1 Study and Understand the Art

Know thy enemy!
In the case of a social engineering attack, it involves a study of the methodologies, tactics, and strategies of the art.

It is fundamental to understand the human characteristics that social engineers prey upon as well as the dynamics of it - why the approach of social engineering tends to work so well, and why defense is so hard to teach.

Differentiate types of social engineering manipulations, and know what methods may be used.

Identify the key indicators in a social engineering attack.

Realize that social engineers really exploit poor security awareness, from both an information and operational security perspective. A social engineering attack reveals vulnerabilities in security policies and awareness that cannot be detected through other means.

8.2 Identify the Threat and Vulnerability

Begin with a solid understanding of the organization's vulnerability to social engineering attacks.

Determine how social engineering can impact the organization’s business and the serious threat this attack poses.

Predict the target areas in the organization where a social engineering attack may occur.

Analyze public and semi-public sources of information, and the extent of information leakage involved.

Determine how vulnerable the organization is to a social engineering attack by conducting an enterprise-wide survey, with questions like:

1. Would you give your password to someone who told you in person, over the phone or in an e-mail message that he was fixing a problem with your computer or network? Or would you notify your computer security personnel immediately?
2. Do you lock your workstation before you leave your desk, or do you leave it up to your password-protected screensaver to activate on its own?
3. Do you challenge strangers you come across in restricted areas who don't display proper badges or identification, or do you assume that they are likely authorized to be there (and perhaps are too important to be questioned -- possibly because they're dressed in nice suits)?
4. Would you decline to participate in a phone survey that asks a multitude of questions about your organization's computer systems, or would you be likely to participate if offered a "free gift"?
5. Would you stop a clean-cut uniformed delivery person carrying packages who flashes a smile and asks where the mailroom is as he attempts to tailgate into a secure building with you, or would you politely hold the door open for him and point him toward the mailroom?
6. Do you leave work discussions at work or do you continue discussing business over meals at local restaurants or in other public places?
7. Do you shred your old phone lists, or do you simply dump them in the trash?

Consider the security weaknesses around systems, such as:

1. Telephone and Voicemail system
2. Intercom, Paging and Radio System surveillance
3. Bypassing mechanical and electronic lock/control systems
4. Video Surveillance
5. Dumpster Diving
6. Document and Authorization Forgery

Help desks are vulnerable because those personnel are trained to be friendly and to give out information. They are in place specifically to help, and hence may be exploited by people who are trying to gain illicit information.

The security model for Internet chat applications, such as instant messaging applications and Internet Relay Chat (IRC) networks, relies on each end-user to make independent security decisions rather than relying on a central enforceable security policy, thereby increasing the threat involved, as observed by CERT.

8.3 Focus on the Human Factor

Each social engineering attack yields problems that are specific to the organization being examined.

The defenses for a social engineering attack involve non-technical aspects of computer security along with technical measures.

The first step would be to make computer security part of everyone's job, whether they use a computer or not. This will help make staff more vigilant.

Integrate multiple techniques for incorporating effective social engineering defense into the organization's security program. Change ways to augment the security of the organization, while still remaining helpful and befitting the organizational culture.

According to Warren Moore, senior director of information security at Convergys Corp. in Cincinnati, "With human firewalling . . . really what you're talking about is changing corporate cultures. People want to be helpful, but that's the way intruders can get inside. You need to establish policies and educate employees."

Organizations in the service industry need to teach staff how to be helpful without giving away the store, and how to serve legitimate customers without appearing paranoid.

Focus on receptionists, security guards, technical support, customer service and help desk staff, since they are more vulnerable to a social engineering attack.

Emphasize a "trust but verify" mentality.

Determine and discuss ways of changing staff attitudes and behavior to recognize and reject attempts to steal information.

Innovate methods for handling inquiries that are helpful and professional, but that verify the requester's identity before disseminating potentially valuable or damaging information.

The techniques for making defense against social engineering should be made a normal part of the organizational culture.

Some convenient but effective procedures are:

Implement a call back procedure when disclosing protected information: Have staff verify the caller's identity by calling him/her back at their proper telephone number, as listed in the organization telephone directory. This is because hackers are able to pretend they are calling from inside the corporation by playing tricks on the PBX or the company operator. The caller-ID would not help in this case.

Identify direct computer support analysts: Every staff of an organization must be personally familiar with computer analysts, who should be the only people to directly contact users.

Create a security alert system: Devise a way for a staff to alert other staff members of a possible attack, especially while in the attack or right after.

Develop an incident response plan and set up a response team.

Set up a data classification system.

Train security guards to check on visitors if they hand their admittance badge over to someone else.

Confirm the visit of a utility worker before allowing into the building to do any work.

Cover general security guidelines with all new hires.

Conduct annual checks to make sure staff know the policies.

Have the System Administrator send an occasional reminder to not transmit passwords in clear. Even better, system administrators might want to warn their users against disclosing their passwords in any fashion other than a face-to-face conversation with a staff who is known to be authorized and trusted.

Report an attack or attempt to the manager or security official.

The Nonproliferation and National Security Institute offers the following tips:

1. Do not provide information if the identify of a caller who asks for personal information cannot be personally established.
2. ONLY the owner of an account should know the password. If a system administrator or maintenance technician asks for a password, it is reason for suspicion.
3. The local site administrator (who is known) should accompany systems maintenance technicians from outside vendors who come on site. If the site administrator is not familiar, or if the technician comes alone, it is wise to give a call to the known site administrator to check if the technician should be there.

8.4 Limit the Loss

Security directors should work with human resources and individual functional areas of the organization to decide how much data access each staff should get. Limit the amount of access a staff has to sensitive data to the bare minimum. This limits the information a social engineer can trick out of a single weak link.

Avoid displaying sensitive information on terminals and application programs used by the front-end staff like customer service representatives. This approach is already in use at VoiceStream and Amazon.com where systems do not reveal

a stored credit card number to either the customer or a customer service representative.

Treat phone lists, org charts, technical procedure manuals and other information as highly confidential. Adopt procedures and technology to minimize the impact that such confidential information loss can have.

8.5 Policies

Establishing policies and following through with training and education are key.

It is important to know how to develop, implement, and effectively communicate anti-social engineering security policies.

Some of the clauses that an organization might want to consider for inclusion in the policy could focus on the following points. The organization should thoroughly analyze, expand and tailor them to its needs and culture.

1. Reporting attempted social engineering incidents to the corporate security group. Companies should then attempt to hack staff at random and see what gets reported.
2. Destroying sensitive data
3. Handling Information media, e.g., backup tapes.
4. Use of computer terminals - locking it when walking away from desk, shutting it down when leaving for the day.
5. Dealings of internal staff with external staff like janitors, the mailman, e.g. letting the mailman into the premise.
6. Use of sensitive information in public places like pay phone or ATM. Hackers stand around phone booths at airports and shoulder surf to obtain credit card numbers.
7. Handling routine office paperwork, like
    a. Phone books - contain names and numbers of people to target and impersonate
    b. Organizational charts - contain information about people who are in positions of authority within the organization
    c. Memos - provide small tidbits of useful information for creating authenticity.
    d. Policy manuals - show how secure (or insecure) the organization really is.
    e. Calendars – tell which staff is out of town at a particular time.
    f. System manuals, sensitive data, and other sources of technical information - give hackers the exact keys needed to unlock the network.
8. Disposing hardware, like hard drives, that can be restored to obtain information.
9. Policies for the home and mobile user
10. Conducting staff background checks

11. System and network configuration
12. Password characteristics, resets
13. PBX system
14. Physical security features

8.6 Awareness and Education

According to Kevin Mitnick, “On the corporate side, as an employee, it all comes down to user awareness and education."

The best defense against social engineering is education.

Institute a staff training and security awareness program that effectively addresses the issues and threats of social engineering.

Training should include self-assertion, stress management and self-confidence to reduce the chances of an individual being socially engineered.

Formal courses, briefings, bulletins, training videos, role-playing sessions, case studies, lectures, training sessions, awareness briefings, penetration tests are some of the on-going programs that go a long way in maintaining the levels of awareness.

Staff should be educated in the risks involved with an attack.

Simple forewarning of possible attacks to people is often enough to make them alert enough to spot them.

Educate staff against

1. Disclosing their passwords in any fashion other than a face-to-face conversation with a staff member who is known to be authorized and trusted.
2. Running programs of unknown origin.
3. Downloading, installing or running a program unless it is trustworthy.
4. Readily releasing information.

8.7 Technical Solutions

Though the fight against the attack of social engineering involves concentrating on the human factor, technical measures still contribute in their own ways.

According to Robert Richardson, the Computer Security Institute's editorial director, “The ways to combat war mumbling are ‘training combined with technology’. Voice recognition technology can be used to require a caller to repeat a series of random numbers that are matched to a voice print so that

intruders can't anticipate a pattern or trick the system."

Run and maintain an anti-virus program to prevent staff from running malicious software. Good anti-virus systems prevent Trojans from being downloaded over the Web or by e-mail, or being copied onto a user's hard drive from a floppy, or being run if the software has been downloaded. It is important that the anti-virus software be kept up-to-date. Automatic updates when available are recommended.

Deploy log servers, computers that record log events from elsewhere on the network but don't allow any remote access. Firewalls can be configured to log all files that are transferred in or out of an organization.

Use strong encryption to secure sensitive communications.

Use strong authentication to establish trusted communications.

Software flaws and insecure configurations in client software could prove fatal. E.g. the configuration of chat software should be reviewed; security settings should be checked; patches should be installed.

Disable all services that are not needed, like chat client functionality on the network.

Do not rely upon common internal identifiers: Have separate identifiers for computer support activities and personnel functions. Augment with additional security to both personnel and computer activities.

9.0 Are the Efforts Paying?

"Penetration test" the staff – repeatedly hit them with actual social engineering attacks to teach the techniques to resist social engineering.

Only qualified and trustworthy people should perform the penetration attacks.

New staff should receive several social engineering attacks during their probationary period, since they are exceedingly vulnerable to attacks.

Appendix A

References

Vernon, Wes. “Clinton-Era Social Engineering Still Plagues the Military”.
October 28, 2003.
URL: http://www.newsmax.com/archives/articles/2003/10/27/163539.shtml

Granger, Sarah. “Social Engineering Fundamentals Part I: Hacker Tactics”.
December 18, 2001.
URL: http://www.securityfocus.com/infocus/1527

Granger, Sarah. “Social Engineering Fundamentals, Part II: Combat Strategies”.
January 9, 2002.
URL: http://www.securityfocus.com/infocus/1533

Harl. “People Hacking: The Psychology of Social Engineering”.
May 07, 1997.
URL: http://packetstormsecurity.nl/docs/social-engineering/aaatalk.html

Briney, Andrew and Prince, Frank. “Security Survey: Disciplined Security”.
October 2003.
URL:
http://infosecuritymag.techtarget.com/ss/0,295796,sid6_iss143_art294,00.html

Huston, Brent. “Social engineering in practice – a real world example”.
October 21, 2003.
URL: http://security.itworld.com/nl/security_strat/10212003/

CERT® Incident Note IN-2002-03.
“Social Engineering Attacks via IRC and Instant Messaging”
Release Date: March 19, 2002.
URL: http://www.cert.org/incident_notes/IN-2002-03.html

CERT® Advisory CA-1991-04: “Social Engineering”.
Original issue date: April 18, 1991. Last revised: September 18, 1997.
URL: http://www.cert.org/advisories/CA-1991-04.html

Gulati, Radha. “The Threat of Social Engineering and Your Defense Against It”
October 31, 2003.
URL: http://www.sans.org/rr/papers/index.php?id=1232

Khan, Ayesha. “How to deal with Social Engineering”.
December 30, 2002.
URL: http://www.giac.org/practical/GSEC/Ayesha_Khan_GSEC.pdf

Mitnick, Kevin D. and Simon, William L.
“The Art of Deception: Controlling the Human Element of Security“.
Wiley, John & Sons, Incorporated. October 2002

Christopher, Abby. “The human firewall “
October 28, 2003.
URL:
http://cio.co.nz/cio.nsf/0/CD50373FD1A06BD3CC256DCD00015C68?OpenDocument

Winkler, Ira S. and Dealy, Brian.
“Information Security Technology?...Don't Rely on It.”.
URL:
http://www.google.com/search?q=cache:uMgo5TgL0NwJ:www.usenix.org/publications/library/proceedings/security95/full_papers/winkler.ps+%22social+engineering%22&hl=en&ie=UTF-8

Slatalla, Michele and Quittner, Joshua.
“The Masters of Deception: The Gang That Ruled Cyberspace”.
HARPER. 1995