Global Information Assurance Certification Paper

GIAC Security Essentials Certification (GSEC) Practical Assignment

Name:	Thomas Miller
Assignment Version Number:	1.4b (amended 29 August 2002)
Descriptive Title:	Social Engineering – Emphasizing People
Transmitted:	10 February 2003

Abstract.

Social engineering is a real-world method of illegally obtaining access to information resources. Social engineering exploits a trust relationship with an individual. Social engineering happens and the results can range from minor to catastrophic. Social engineering is a potential backdoor into any computer, network, or information system. The main defense to social engineering is an informed, motivated individual supported by good security practices. Informed, motivated individuals need to be fostered. Without informed, motivated individuals, expensive and otherwise effective software and hardware controls monitored by information technology professionals can be circumvented.

Discussion.

What is social engineering?

In the information technology world, social engineering is a con game directed at an individual. A couple of definitions are provided to make this point. Social engineering "describes a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures" (searchSecurity.com Definitions). A social engineer "illegally enters computer systems by having persuaded an authorized person to reveal IDs, passwords, and other confidential information" (TechEncyclopedia). The Free Online Dictionary of Computing jargon file describes social engineering as "cracking techniques that rely on weaknesses in wetware [people] rather than software; the aim is to trick people into revealing passwords or other information that compromises a target system's security." A common element of these and other social engineering definitions is that it involves "a hacker's clever manipulation of the natural human tendency to trust" (Granger, "Social Engineering Fundamentals, Part I"). Social engineering depends on establishing a trust relationship between the social engineer and a target. The social engineer then abuses the trust relationship.

How is social engineering accomplished?

The key to social engineering is establishing that trust relationship. There are a number of ways to categorize social engineering techniques. The categories can overlap. Granger provides the following social engineering categories: (1) by dumpster diving (not really an attack on an individual), (2) by phone, (3) through on-line processes, (4) by persuasion, and (5) reverse social engineering ("Social Engineering Fundamentals, Part I"). The common thread in all but dumpster diving is apparent: an individual is tricked, cajoled, awed, persuaded, or otherwise convinced that providing the requested information is the appropriate course of action.

In an information technology environment, the goal of the social engineer could

be to gain unauthorized access to a technology system like a file server or a telephone exchange. Alternatively, social engineering may be used where accessing an information system to steal data is difficult; the opportunities to circumvent the information system are too easy to pass up. The goal of the social engineer could be personal or business. The effect on the target could be benign or catastrophic depending on what information or systems are compromised: email addresses, names, social security numbers, credit card numbers, family relationships, business plans, password files, war plans, unpublished news stories, state secrets, telephone systems, accounting systems, web pages, student information systems, on-line investing systems, and so on.

Dumpster diving is a technique used to gain information useful in generating information for a social engineering attack on an individual. Dumpster diving consists of literally sorting through trash for discarded documents that can provide information useful for a social engineering attack against an individual. Examples of useful information includes, but is not limited to, staff directory information, account information, internal telephone numbers, organization charts, correspondence (email, letters, and memos) and the like. Dumpster diving may provide sensitive information directly: social security numbers, credit card numbers and the like. The results of a successful dumpster diving session can provide tidbits of information that make the social engineer's line more believable. (Dumpster diving does not normally involve direct interaction with the target, but it is a common and frequently rewarding technique in preparing for a social engineering attack (Berg).)

Social engineering by phone consists of telephoning a target individual to obtain the desired information or action. The social engineer pretends to be a person with a legitimate need for the information requested. The target is persuaded to provide the information. The classic example is the social engineer impersonating a telephone employee who asks the target to dial "90" to assist in system testing. As the con goes, "9" frequently provides external access and "0" connects to the operator. From there, the social engineer can call anywhere.

On-line social engineering includes requests via email for information. Again, the social engineer sends an apparently-legitimate request based on a story plausible to the target and gains personal, business, or access information that provides benefit or utility for the social engineer. The ruse of having a fake logon error message pop up is another example of on-line social engineering. The target believes a keying error was made and is asked to re-enter desired information into a dialogue box which is then provided to the social engineer.

Social engineering by persuasion is inherent in all the forms of social engineering against an individual. The social engineer does not physically threaten the target individual with a weapon or physical harm. The social engineer, by various means, convinces the target that the social engineer has a legitimate need for the information requested. This can be by email, by phone,

or even in person.

Reverse social engineering is a form of social engineering in which the victim unwittingly contacts the social engineer in an attempt to communicate with a legitimate reference or help site. In the course of this interaction, the social engineer induces the target to provide the information or data the social engineer seeks. An example of reverse social engineering would be to establish a web site that purports to be an official site that the target would normally access. The web site could present itself as a bank or credit card application service and request that the target enter more than enough information to accomplish an identity theft. Another tack would be to entice the user to enroll in an apparently useful web site. The target would be asked to select a userid and password. The success of this scam is based on the habits of some people to use the same userid and password on different sites. Reverse social engineering can be a complex endeavor.

In addition to Granger's general framework above, there is also a potential for social engineering by regular mail. Bernz describes in some detail using regular mail to obtain personal information for use in executing other types of social engineering attacks, particularly by telephone. With information garnered from bogus mailings, it is possible for a social engineer obtain the information that will make a telephone request more believable (Bernz). According to Bernz, people can be more receptive to written requests for information than to verbal requests.

Is social engineering real?

Real-world examples of social engineering are rare because individuals and organizations do no like admitting to being tricked or to having weak or imperfect controls. The risk of litigation or loss of confidence probably works against reporting successful social engineering attacks. The real-world examples that are available are usually sanitized of identifying information.

Here are three sanitized but purportedly real-world, successful social engineering attacks.

Real World Example #1 (Small business)

A small engineering firm had a new product line stolen by a competitor using a social engineer acting as a consultant. The ersatz consultant was able to obtain blueprints from the engineers, cost and supplier information from the financial people, and product roll-out information from the marketing personnel. The social engineer attacked while the president of the small engineering firm was on vacation. The social engineer used a stereo-typical consultant image, flattery and other people skills to con select members of the firm. The competitor brought the new product to market first ("Social engineering: examples..."). (Note that this instance, as far as we know, did not involve compromising a

computer system or a telephone system at all. It demonstrates the potential effectiveness of a specific social engineer.)

Real World Example #2 (Individual consumer)

Several individuals were duped into providing credit card information. The individuals were contacted by email shortly after subscribing to an online computer service. The email indicated there were problems with the new account and requested that each new subscriber provide logon password, and bank or credit card data. This scam targeted new subscribers who were less likely to know that they should not respond to the email (Rusch). (This demonstrates the potential vulnerability of naïve users to a particular social engineer.)

Real World Example #3 (Telecommunications / information technology professional)

At a "Meet the Enemy" session of the Computer Security Institute (CSI), a hacker was challenged to demonstrate social engineering to facilitate a network intrusion. The hacker provided a live demonstration of social engineering techniques. The hacker convinced a telephone company duty supervisor, identified with the help of the help desk, that the supervisor's system was experiencing problems. The hacker, pretending to be troubleshooting the non-existent problem, caused enough concern that the duty supervisor provided the hacker her logon userid and password. The duty supervisor was about to provide the personal identification numbers of ten telephone company customers when the hacker terminated the call, having demonstrated the effectiveness of social engineering ("Social engineering: examples..."). (This instance illustrates a successful social engineering attack on an information system to the extent the social engineer obtained a valid userid and password and was about to obtain the personal identification numbers of several telephone customers. Again, this demonstrates how effective an expert social engineer can be.)

These examples demonstrate that social engineering occurs. It is apparent that there may not be much of a trail after such an attack. That plausible examples of social engineering are easy to imagine is another indicator that social engineering is a real threat.

Social engineering can be high-tech, but is frequently low-tech. Social engineering can be relatively cheap and appear to have little personal risk associated with it. Why would a hacker spend hours or days of trial and error with the possibility that an alert network administrator might detect the attack when the same end can be accomplished with a call to a mid-level manager or to a secretary, or to a help desk? If a target individual provides a legitimate userid and password, the attacker logs on as an authorized user and avoids a lot of wasted effort. Once logged on, the attacker can use freely available

network tools and established hacking techniques to exploit the initial access. Why would an attacker physically stalk a person, when the person's address and telephone number can be acquired by asking a helpful clerk or by asking the stalking target directly?

The degree of risk to an organization or individual depends on the type of information available. It could range from the minor irritation of spam to the loss of proprietary information, from the compromise of confidential personal information to a theft of assets (money, property, reputation).

Are you being or have you been exploited by a social engineer?

An organization may not be aware of a successful social engineering attack if tangible assets are not stolen, modified, or destroyed. Similarly, individuals may not be aware of an attack until the credit card statement or the bank statement reveals unauthorized charges. If the individual is lucky, the credit card company might notice and investigate unusual buying patterns before too much damage is done. If a social engineering event is not identified when it happens, there is a risk of damage to the target or the target's organization.

There are some common indicators that a contact (telephone call, email, instant message, or office visit) is a social engineering attack. SBC Ameritech, a telephone giant, provides a list of warning signs of social engineering fraud on its consumer information web page. The warning signs include **requests** for transfers to an operator, indications that a call is coming from outside the business, **requests** for outside lines during times when supervisory personnel are usually absent, and **unsolicited calls** requesting personal or proprietary information (SBC Ameritech, emphasis added). Other indicators that a contact is a social engineering attack include refusal to provide call-back contact information, rushing or a sense of haste, name-dropping, intimidation (aggressive persuasion), small mistakes that indicate an impersonator rather than an original, and requesting forbidden information ("Social engineering: examples..").

In a discussion of social engineering, these warning signs and red flags are obvious. In a work setting, in the fog of war, or with the alligators nipping at one's heals, the signs and red flags of social engineering may not be so obvious. A social engineer will make a concerted effort to distract, disorient, or cause an emotional impact on a target. Rusch describes the use of a "peripheral route to persuasion" while Bernz discusses the merits of impersonating a female voice when telephoning (male) information technology workers. An alert, aware responder is the key to thwarting a social engineering attack.

What can you do to defend against social engineering?

Kevin Mitnick, convicted felon and recently published author, described his

social engineering technique as creating a sense of trust with the target person and then exploiting it (Lemos).

Most organizations have people who want to do a good job and who are basically honest, helpful, and positive about their employers. Given this assumption, the key to preventing social engineering is to create an informed, motivated workforce. An informed workforce will have clear guidance on what work place information is restricted or confidential. They will have guidance on the appropriate ways to provide restricted or confidential information to customers or employees who have a need-to-know. They will be trained and periodically reminded about the risks and warning signs of social engineering in particular. Defending against social engineering is not rocket science; it is simple and prudent management. Practices and people are required to guard against social engineering.

Defending with practices –

Practices include: (1) Establishing security policies that are reasonable given the nature of the organization and the information at risk. (2) Ensuring physical security addresses visitor control, document control (confidential or restricted documents marked and properly stored), disposal methods (shred documents, wipe magnetic media, lock the dumpster), and protecting machines and networks with adequate access control features (passwords, tokens, biometrics, or combinations of the three). Establishing appropriate practices based on a current risk assessment (cost versus benefit) will allow individuals to be most effective in defending against social engineering (Granger, "Social Engineering Fundamentals, Part II").

The basic assumption here is that practices established will be put into effect and monitored from time to time. Management must support the security practices. Unsupported or paper practices will provide only a false sense of security to the trusting and a sense of cynicism in everyone else.

Defending with people –

In social engineering, an individual is the target and the individual is the first, if not only, line of defense. If there is a question about who should be trained or informed concerning social engineering, err on the side of a broader audience. It may not only be a receptionist or help desk representative that is the target of the social engineering attack. Depending on the nature of the organization's information, the target could be a health professional, an office administrator, a financial professional, a student worker, a clerk, a senior manager, or an on-line shopper: almost anybody can be a target.

Educate individuals about what is appropriate and what is not appropriate in the way of requests for information. This is where policies, procedures, and guidelines are very helpful. Is it company policy to reset a password based on a

telephone call or not? Is the caller authorized to receive the social security number, the credit card number, or the security administrator's home address? Is the responder authorized to provide that information if they have it? People need to know how to respond to inquires and who to call if there is a problem. Remember, the social engineer is going to provide a good line; the responder needs a good response.

Foster a professional skepticism in dealing with unknown and unsolicited callers or correspondents. This can be accomplished with courtesy and good humor. Sometimes signs and red flags are not indications of social engineering; there is no need to alienate a potential customer or constituent ("Social Engineering Fundamentals, Part II"). The proper mental attitude can be created by making employees aware of the red flags of social engineering and providing guidance on what is appropriate to communicate and what is not. The basic red flags of social engineering include a sudden sense of urgency and a request for inappropriate information. The basic guidance needs to address how to handle exceptions appropriately. The social engineer may try to create an apparent problem situation that the employee feels compelled to resolve. The employee needs to have a safety valve short of providing the information to the social engineer.

Provide an environment in which individuals feel safe in following established information security procedures. (This assumes the organization has established relevant guidelines or procedures.) This requires support up and down an organizations chain of command. Support ensures guidance is available and current. Support ensures that appropriate training and reminders are provided. Support tolerates reasonable mistakes while determining if the cause of the mistake can be prevented in the future. Support fosters consistency in applying established procedures.

Even with education, continuing reminders, written policies and procedures, and a supportive chain of command, individuals make decisions that are not consistent with organizational pronouncements or common sense. A serious social engineer may be able to compromise even normally alert, intelligent, loyal individuals. Individuals need to feel safe in reporting incidents and mistakes. If individuals do not feel safe, the organization will not learn of compromises until damage is noted.

By the nature of social engineering, there is very little that hardware and software can do to protect information. If the social engineer has the appropriate password, the appropriate combination, or can get the information desired without accessing an information system directly, then there is no trigger for the hardware or software countermeasure. Consider, for example, situations where the helpful clerk provides the password, the combination, the social security number, the credit card number, the confidential report, etc.

Measures to reduce the success of social engineering in an organization do not

have to be expensive. Such measures include providing individuals with examples of appropriate behavior, with continuing education, with reminders about information security in general and social engineering in particular, and with reporting processes for individuals who believe they may have encountered a social engineer.

Social engineering presents a clear risk to all organizations, but especially to organizations that are knowledge-based. It seems that more and more individuals, businesses, and governmental bodies are becoming knowledge-based entities.

Conclusion.

As long as people interact with information systems, social engineering will be a threat to those information systems.

Social engineering is a real threat. It comes in many guises: a telephone call, a fax, a visit, an email, a piece of mail. Both individuals and organizations have valuable information that others want to abuse or steal. As the attacker, the social engineer gets to pick the point of attack. Individuals and businesses need to arm themselves with knowledge and plan to protect their information.

Social engineering is capable of bypassing the patches, the firewalls, the administrators, and the logical and physical access controls. Hardware and software controls are vital to protecting information and systems. Preventing unauthorized access is a fundamental role of information systems professionals just as much as providing services and resources. The person, however, is the target of social engineering so the person is the key to preventing social engineering attacks that would nullify the hardware and software controls. If information and assets are worth protecting, then it is necessary to educate the work force to the tactics of social engineering. It is imperative that individuals are provided the procedures and the training to be effective against social engineering threats.

List of Works Cited

Berg, Al. "Cracking a Social Engineer," LAN Times, 6 Nov. 1995. Packet Storm. 24 Jan. 2003 <http://packetstorm.decepticons.org/docs/social-engineering/soc_eng2.html>.

Bernz. "The Complete Social Engineering FAQ!" Packet Storm. 24 Jan 2003 <http://packetstorm.decepticons.org/docs/social-engineering/socialen.txt>.

Granger, Sarah. "Social Engineering Fundamentals, Part I: Hacker Tactics." 18 Dec. 2001. Security Focus Online. Pt .1 of a 2-part series. 22 Jan 2003 <http://online.securityfocus.com/infocus/1527>.

Granger, Sarah. "Social Engineering Fundamentals, Part II: Combat Strategies." 9 Jan. 2002. Security Focus Online. Pt. 2 of a 2-part series. 22 Jan. 2003 <http://online.securityfocus.com/infocus/1533>.

Lemos, Robert, "Mitnick teaches "social engineering." 16 Jul. 2000. ZDNet News. 22 Jan. 2003 <http://sdnet.com.com/2102-11-522261.html>.

Rusch, Jonathan J. "The 'Social Engineering' of Internet Fraud." 1999. Proceedings of the Internet Society. 22 Jan. 2003 <http://www.isoc.org/isoc/conferences/inet/99/proceedings/3g/3g_2.htm> .

SBC Ameritech. "Consumer Information – Social Engineering Fraud." 2003. SBC Properties, L.P. 22 Jan. 2003 <http://www05.sbc.com/content/0,,257,00.html>.

"Social engineer." TechEncyclopedia. TechWeb. 22 Jan. 2003 <http://content.techweb.com/encyclopedia/defineterm?term=social+engineer&Define.x=29&Define.y=7>.

"Social engineering." Free On-Line Dictionary of Computing. 22 Jan 2003 <http://wombat.doc.ic.ac.uk/foldoc/foldoc.cgi?query=social+engineering> .

"Social engineering." searchSecurity.com Definitions. Tech Target. 22 Jan. 2003 <http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci531120,00.html>.

"Social engineering: examples and countermeasures from the real-world." Nov. 1999. Computer Security Institute. 22 Jan. 2003 <http://www.gocsi.com/soceng.htm>.

Works Consulted

Allen, Malcolm. "The Use of Social Engineering as a Means of Violating Computer Systems." SANS Reading Room. SANS Institute. 12 Oct. 2001. 22 Jan. 2003 <http://www.sans.org/rr/social/violating.php>.

Robinson, Shane W. "Corporate Espionage 101." 15 Feb. 2002. SANS Reading Room. SANS Institute. 22 Jan. 2003 <http://www.sans.org/rr/social/espionage.php retrieved 1/22/2003>.