Global Information Assurance Certification Paper

How to deal with Social Engineering
By
Ayesha Khan
SANS GSEC Practical Assignment 1.4b

December 30, 2002

Abstract

This paper focuses on measures that can be taken to protect organizations from social engineering and to draw attention of IT security professionals towards social engineering. Case studies are included to demonstrate the threat, the intended goals of a social engineer are analyzed, and steps to preventing social engineering are reviewed. In addition, thoughts from Kevin Mitnick, a renowned convicted social engineer, are brought in to shed light on this topic, from a "reformed hacker's" point of view.

Introduction

Any meaningful discussion of social engineering should begin with a definition of it. Social Engineering is generally a hacker's clever manipulation of the natural human tendency to trust. The hacker's goal is to obtain information that will allow them to gain unauthorized access to a valued system and the information that resides on that system (Granger, 18 December 2001).

According to Teri Bidwell, social engineering is a term used for a variety of scams and con games involving tricking a victim into voluntarily giving up private information that's useful (Bidwell, 2002).

Note that, according to these definitions, social engineering is a non-technical way of hacking. The human factor, not technology, is under attack. The potential loss to an organization from a successful social engineering attack can be as substantial as the loss suffered by a traditional network hacking attack.

Aspects of Social Engineering

Social engineering attacks mainly have two different aspects: the physical aspect or the location of the attack, such as in the workplace, over the phone, dumpster diving, on-line, and the psychological aspect, which refers to the manner in which the attack is carried out, such as persuasion, impersonation, ingratiation, conformity, and friendliness (Granger, 9 January 2002).

Most attacks have physical and psychological aspects. Identifying these aspects will assist in designing a program to help prevent social engineering. These aspects are discussed with examples as follows:

Social Engineering at Workplace

At the workplace the social engineering attack can be done internally by the employees of the organization or from outside. Internally, an employee could be an industrial spy from a competitor company. They could be disgruntled employees, or employees who consider social engineering fun. Hackers could be spies either working from outside the company or individuals with malicious

intent. For example, suppose there is a marketing company working on some product which has not been introduced in the market yet. The competitor company hires a social engineer to obtain information regarding this product. This attacker may try to apply for employment in that company. The social engineer can also impersonate as a reporter, research student, or an auditor. This example has both physical and psychological aspects. Since in this example the attack occurs at a certain location as in this case it is a workplace, this is the physical aspect. In this case impersonation is the manner in which attack was carried out, this becomes the psychological aspect.

Social Engineering over the phone

Social engineering attacks over the phone are very common, and can occur at the workplace as well as at home. At work, a hacker may place a call and pose as an auditor or consultant and request a list of all applications or code. The social engineer may present himself as a LAN administrator over the phone and could request the employee to provide his or her user ID and password. At home, the attackers may present themselves as some marketing representatives and make very attractive offers. By offering free gifts, they may ask for personal information including credit card numbers, bank account numbers or even social security number. These examples again have both physical and psychological aspects. The attacker tried to obtain information over the phone and this can be considered the physical aspect and impersonation, persuasion, friendliness, and ingratiation are the psychological aspects in the above examples.

Social Engineering by Dumpster Diving

In this aspect of social engineering, the attacker actually looks for information in the dumpster or trash bins. For example, the attacker will look for any kind of information including the names of employees, contact numbers, e-mail addresses, or any kind of information that could be useful for them to stage social engineering attacks. Most individuals when throw away their credit card bills in the dumpster without properly shredding the paper. These bills have personal information including the name, address, account number, balance etc. Another example is when someone throws away old hardware like hard drives or floppy diskettes, without properly reformatting them. They can have plenty of useful and critical information which is very easily obtained by the attacker. In these examples, the physical aspects were trash cans and there was no psychological aspect.

Online Social Engineering

Here a victim receives an attractive e-mail, offering some valuable information or free gifts. There could be various websites hosted by the social engineers. These web sites would offer some really popular merchandise or free gifts and in return would ask for personal information such as name, address, social security

number, credit card information, employers name and address, contact numbers, job title etc. This example has physical and psychological aspects. Physical are the website or the e-mail and psychological aspects are persuasion, friendliness, impersonation, and ingratiation.

What follows are components of the previously discussed psychological aspects.

The Components of Psychological Aspects

There are some psychological tactics which Kevin Mitnick has pointed out in his book, The Art of Deception. According to Mitnick, there are six basic tendencies or weaknesses that social engineers use to manipulate people. These tendencies are:

- Authority

For example they can show themselves as a person in authority like a physician, an auditor, bank manager, or any executive employee. It is a natural tendency for the majority of employees to comply with a request if they believe the requestor is a person in authority.

- Liking

It is also possible that the attacker may try to show similar interests as their intended victim.

- Reciprocation

It is not unusual when someone either appears helpful or may even offer some gifts to gain favors in return.

- Consistency

Some clever social engineers may try to manipulate the procedure or policies already in place and usually new employees fall victim to this kind of exploitation. For example, the attacker may trick a person into revealing their password by showing up as a compliance person who is making sure that users password is in accordance with the company's policy.

- Social Validation

There is one more tendency among human beings, which is to follow what others are doing. It usually comes from team spirit and they do not want to look like a person who does not work along with other team members.

- Scarcity

If people find out that something is in short supply, there is a natural tendency to get it. For example, the attacker may send out e-mails telling people that if they register at some company's new web site, they will win free tickets for some popular new movie. That's how attackers trick users into obtaining sensitive information through web site registration processes (Mitnick, 2002).

Types of Social Engineering Attacks

The Gartner Group has identified four major types of social engineering attacks:

- Plausible Personal Request
- By just answering a few questions
- Using really interesting e-mail
- The Trojan Horse

The first and most common type is the "Plausible Personal Request". It means a request is presented to an individual and it also involves impersonation and lying. The attacker may pose as an employee and request a password change. They could pretend to be executives and would demand access to the real executive's account. They may say that they have left their physical access badges at home and really need to access their research lab in an emergency.

Another type is an attack in which the attacker directly solicits proprietary or confidential information. The perpetrators will try to patronize or flatter the employee and may identify themselves as reporters or students. These attacks range from gathering confidential or competitive information on behalf of the attacker's client. Just by answering a few questions, the attacker will have sufficient information to exploit the organization.

A third kind of social engineering is achieved through interesting and attractive e-mails which will try to catch an employee's attention. Such e-mails could offer friendship, gifts, or appear to contain useful information. Once the employee opens an e-mail, which usually contains viruses, worms, other uninvited programs, that employee's system or network could be compromised. Such e-mails or web sites could also be used to obtain personal information like social security number, names, and addresses.

What is a Trojan Horse attack? It is a seemingly innocent program which hides malicious code. It can happen in a number of ways. A user is prompted to log in to the network, but the login prompt is really a Trojan. The user logs in as usual and is automatically handed over to the real login program. The Trojan Horse in the meantime e-mails the logon information to the attacker. These attacks are far more dangerous technical attacks with social engineering component. There may be an electronic form the employee is asked to fill out for some worthy cause, but in reality it provides a full dossier of information to a social engineer (Gartner's Information Security Strategies Research Notes, December 2001).

Goals of Social Engineering

In order to prevent social engineering attacks, it is important to identify what are the goals of a social engineer. Now that all the aspects and types of social engineering have been discussed, it is time to find out what are actually the goals of social engineering.

- Financial Gain
- Network Intrusion (Anonymous, November1999)
- Identity Theft (Anonymous, November1999)
- Industrial Espionage (Anonymous, November1999)
- To Obtain Sensitive or Critical Information
- Just for Fun

Prevention

This section mainly focuses on the preventive measures that should be taken by organizations to protect themselves from these attacks.

Preventing social engineering

There are several ways to prevent social engineering in any organization. Most of the important ones are outlined below and discussed in detail with examples.

I. Security awareness

II. Hiring process

III Periodic audits

IV. Physical security

I Security awareness

It is extremely important for any organization to develop a well structured, well maintained training program for security awareness of all employees. Every

organization must make sure that their employees understand the social engineering aspects. This needs to include how social engineers deceive people and use various methods to gain physical access as well as access to confidential data. Employers need to recognize such attacks and how to handle them if they encounter one. Another training objective is where and how to report such attempts or successful attacks. The emphasis must be on challenging anyone who makes a suspicious request and to know what a suspicious request looks like. It needs to be stressed that employees should not implicitly trust anyone without proper verification. The training should include what is sensitive or critical data and how to safeguard it. The employees should be fully aware of the importance and the background of the security policies and procedures. It should be made an obligation of every employee to comply with the policies and procedures, and they should understand the consequences for noncompliance (Mitnick, 2002).

Regarding Kevin Mitnick…

> He earned notoriety in the 1980s and 1990s for his apparent ability to break into telephone and computer systems across the world at will. Arrested six times, his last capture resulted in a five-year jail term - the heaviest sentence ever handed down for a hacker. Now, 38 year old Mitnick has 'gone straight', offering a rare insight into how hackers really operate. Mitnick says that in addition to the usual technical security procedures - regular port scanning, for example - organizations need to more rigorously enforce security policies and train staff to be alert to the dangers posed by social engineers, particularly in companies that might be targeted by industrial spies (Graeme Burton, 4 September 2002).
>
> In testimony before Congress after Kevin Mitnick was released from jail, our country's most notorious computer hacker, he told the lawmakers that the weakest element in computer security is the human element. "I was so successful in [social engineering] that I rarely had to resort to a technical attack," Mitnick explained. He added that "employee training to recognize sophisticated social engineering attacks is of paramount importance (Author and Date unknown URL: http://rf-web.tamu.edu/security/SECGUIDE/V1comput/Social.htm#1)

Some of the critical issues that need to be addressed in training employees are very well outlined by Kevin Mitnick in his book, The Art of Deception. A security awareness training should cover some of these critical issues.

- Security policies related to computer and voice mail passwords.
- The procedures for disclosing sensitive information or materials.
- Email usage policy, including the safeguards to prevent malicious code attacks including viruses, worms, and Trojan Horses.
- Physical security requirements such as wearing a badge.
- The responsibility to challenge people on the premises who aren't wearing a badge.
- Best security practices of voice mail usage
- How to determine the classification of information, and the proper safeguards for protecting sensitive information.
- Proper disposal of sensitive documents and computer media that contain, or have at any time in the past contained, confidential materials (Mitnick, 2002).

II. Hiring process

Special stress must include educating new hires, and updating and providing more frequent security awareness training for current employees. The employers need to conduct frequent refresher courses for managers so that employees, when placed in such a position, will not be afraid to question the requestor's identity. Well trained employees will be able to handle such attacks with more confidence and caution.

> In the course of hiring process, the employers should run background checks. To some extent it plays an important role because that company may be hiring an industrial spy from a competitor company. There was a paper published at SANS Reading Room site by Shane W. Robinson entitled "Corporate Espionage 101." Robinson gives references in explaining how people obtain fake diplomas of prestigious universities. They also provide fake credentials and fictitious references to gain employment in a targeted company. That is why it is so important to verify credentials and references of the applicant for the job (Robinson, 15 February 2002).

III Periodic audits

It is also a good practice to run periodic audits by creating such attacks to find out the weaker areas, and then taking care in removing such weaknesses in security as soon as possible.

Besides security awareness training, it is recommended that the best way to prevent it from happening is to actually conduct social engineering attacks on a regular basis to find out the weaknesses in training and education. These kinds of audits can really help in preventing such incidents and thus saving corporation from all kinds of damaging effects (Mitnick, 2002).

IV. Physical security

Physical security is considered a very critical part of any security planning, and is a fundamental component to all security efforts. Without physical security, it is very difficult to provide information security, software security, user access security, and network security. The common concept regarding physical security is that it is provided by using locks, bars, alarm, and uniformed guards. According to National Cooperative Education Statistics task force,

> Physical security refers to the protection of building sites and equipment (and all information and software contained therein) from theft, vandalism, natural disaster, manmade catastrophes, and accidental damage (e.g., from electrical surges, extreme temperatures, and spilled coffee). It requires solid building construction, suitable emergency preparedness, reliable power supplies, adequate climate control, and appropriate protection from intruders (National Cooperative Education Statistics task force, 2002).

Some critical issues are emergency exit procedures, regulating any equipment placement and use, and valid vendor security agreements. The doors should be lockable, fireproof, solid, and observable by the assigned security staff. The secured room doors should never remain open. Besides keyhole locks, it is recommended to use window bars, anti-theft cabling, magnetic key cards, security cameras, and motion detectors. The access to these areas should be limited to authorized personnel only and it is a good practice to keep an updated list of personnel authorized to access them. Whenever the equipment is required to be moved or serviced, the task should be pre-authorized. The service representative should produce an authentic work order and their proper form of identification. Access to the equipment area, data center, or any restricted area should be monitored. The log reports of physical access and activity should also be reviewed and monitored (National Cooperative Education Statistics Systems task force, 2002).

According to Kevin Mitnick, physical security is not only the responsibility of the building security guard. Other employees need to be cautious and aware of security risks involved with physical security. For example, if somebody walks up to a receptionist and present themselves as an executive, an auditor, or consultant, requiring access to restricted area, the receptionist should be unafraid to take necessary action to verify their identity. There should also be a policy regarding wearing of identity badges and carrying physical access cards or tokens. Non-employees or delivery people who enter company premises almost daily should be given special badges or other form of identification per corporation security policy. Those who are non-employees and infrequent visitors should be escorted at all times. The visitors should also be required to

provide some valid form of identification before allowing them to enter the premises.

During an emergency evacuation or training drill, it is recommended that the security personnel should make sure that the entire building has been evacuated. This is suggested because an intruder can cause a diversion to gain access to a building or a restricted area. In addition to the preventive measures suggested in this section, it is always strongly suggested to install security cameras in the buildings. Besides the entrance or exit, the security cameras should be installed in all the sensitive areas like server rooms, data center, or any place which contains critical data and equipment. Those employees who are monitoring the cameras should be very well trained to observe and identify any suspicious activity (Mitnick, 2002).

Conclusion

It all comes down to education, and of course it will only be possible if the employer and individuals themselves are aware of the repercussions of social engineering and realize the extent of damage it can cause to the organizations and innocent persons. The good, strong, and updated security policies also have a crucial role to play in fighting against social engineering if they are enforced properly.

> "There's always the technical way to break into a network but sometimes it's easier to go through the people in the company. You just fool them into giving up their own security," says Keith A. Rhodes, chief technologist at the U.S. General Accounting Office, which has a Congressional mandate to test the network security at 24 different government agencies and departments. "Companies train their people to be helpful, but they rarely train them to be part of the security process. We use the social connection between people, their desire to be helpful. We call it social engineering. "It works every time," Rhodes says, adding that he performs 10 penetration tests a year on agencies such as the IRS and the Department of Agriculture. "Very few companies are worried about this. Every one of them should be." (Gaudin, 10 May 2002).

Social engineering is preventable. In order for an employer to protect their assets, they need to fully understand the repercussions of social engineering and take strong measures to train their employees. Education and awareness are an on-going process. As new employees are hired, they should be instructed as to how to recognize a possible social engineering attack and be given the companies security policy on how to deal with these situations.

Companies should evaluate their security policy on a yearly basis. Information should be added to the policy as they become aware of new potential problems.

Depending on an organization's resources a company should consider hiring a firm to attempt a social engineering attack. The company can use the information obtained to see if employees are following proper procedures and see if policies or training need to be addressed.

Social engineering is not going to disappear; it will continue to be a serious threat to companies. Those employers who understand these dangers and the potential damage of these attacks will be able to prevent a social engineering attack.

References:

Granger, Sarah. "Social Engineering Fundamentals, Part I: Hacker Tactics." 18 December 2001.
URL: http://www.securityfocus.com/infocus/1527 (11 March 2003)

Granger, Sarah. "Where to Begin? Security Policies" Social Engineering Fundamentals, Part II: Combat Strategies. 9 January 2002. URL: http://online.securityfocus.com/infocus/1533 (11 March 2003)

Anonymous. "Social Engineering: examples and countermeasures from the real world" Computer Security Institute newsletter. November 1999. URL: http://www.gocsi.com/soceng.htm (11 March 2003)

Gartner's Information Security Strategies Research Note TG-15-1287. 19 December 2001.
URL:http://www4.gartner.com/gc/webletter/security/issue1/article1.html (11 March 2003)

Burton, Graeme. "Companies exposed to 'social engineers' — Mitnick" 4 September 2002. URL: http://www.infoconomy.com/pages/news-and-gossip/group66338.adp (11 March 2003)

Robinson, Shane W. "Corporate Espionage 101" 15 February 2002. URL: http://www.sans.org/rr/social/espionage.php (12 March 2003)

Author and Date unknown. URL: http://rf-web.tamu.edu/security/SECGUIDE/V1comput/Social.htm#1 (11 March 2003)

Gaudin, Sharon. "How To Thwart The Social Engineers" 10 May 2002. URL: http://itmanagement.earthweb.com/secu/article.php/1041161
(11 March 2003)

Gaudin, Sharon. "Social Engineering: The Human Side Of Hacking" 10 May 2002.
URL: http://www.esecurityplanet.com/trends/article.php/10751_1040881
(11 March 2003)

National Cooperative Education Statistics Task Force. "Protecting Your System Physical Security" 2002. URL:
http://nces.ed.gov/pubs98/safetech/chapter5.asp (4 April 2003)

Bidwell, Teri. Hack Proofing Your Identity – In The Information Age. Rockland: Syngress Publishing, Inc., 2002.

Mitnick, Kevin. The Art of Deception – Controlling The Human Element Security. Indianapolis: Wiley Publishing Inc., 2002.