Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

A Multi-Level Defense Against Social Engineering

Social engineering, the process of deceiving people into giving away access or confidential information, is a formidable threat to most secured networks. While there is plenty of information on social engineering, the threat is considered very real and not easily defended. This paper will discuss the basics of social engineering by giving a general overview. It will then discuss the psychological triggers that make social engineering so successful. These triggers include strong affect, overloading, reciprocation, decep...

Copyright SANS Institute
Author Retains Full Rights

AD

A Multi-Level Defense Against Social Engineering

© SANS Institute 2003, Author retains full rights

David Gragg
GSEC Option 1 version 1.4b
December 2002

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Abstract
Social engineering, the process of deceiving people into giving away access or confidential information, is a formidable threat to most secured networks. While there is plenty of information on social engineering, the threat is considered very real and not easily defended. This paper will discuss the basics of social engineering by giving a general overview of social engineering. It will then discuss the psychological triggers that make social engineering so successful. These triggers include strong affect, overloading, reciprocation, deceptive relationships, diffusion of responsibility and moral duty, authority, and integrity and consistency. Finally, this paper will define a multi-level defense that will address these psychological triggers. The levels of defense that are defined are security policy, security awareness training, resistance training, ongoing reminders, social engineering land mines and incident response. Social engineering land mines (SELM) are procedures or policies that, when implemented, act as an intrusion detection system for social engineering.

It is expected that this paper will add value to the security community in three ways: by incorporating the current social psychological research into the discussion of understanding and resisting social engineering, by using the psychological literature to provide a multi-level defensive strategy for hardening employees to social engineering threats, and by developing the concept of "social engineering land mines" as a part of the multi-level defense against social engineering.

Table of Contents

Abstract.....2
Introduction.....4
Background on Social Engineering.....4
Some Social Engineering Basics.....5
  Developing Trust.....5
  Reverse Social Engineering.....5
  Avenues and Media.....6
Psychological Triggers Behind Social Engineering.....6
  Strong Affect.....6
  Overloading.....7
  Reciprocation.....7
  Deceptive Relationships.....8
  Diffusion of Responsibility and Moral Duty.....8
  Authority.....9
  Integrity and Consistency.....9
A Multi-layered defense against Social Engineering.....10
  Foundational Level: Security Policy addressing social engineering.....10
  Parameter Level: Security Awareness Training for all users.....11
  Fortress Level: Resistance Training for Key Personnel.....12
  Persistence Level: Ongoing Reminders.....15

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Gotcha Level: Social Engineering Land Mines (SELM)..... 15
Offensive level: Incident Response 18
Conclusion..... 19
References 20

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Introduction

A system administrator must guard his or her network's confidentiality, integrity, and availability. In order to do this, he/she must determine what the threats and vulnerabilities of a specific network really are. This will help determine the network's risks. Along with this understanding, a determination must be made and agreed upon regarding the level of risk allowable for the network.

Confidentiality, integrity and availability can all be compromised directly or indirectly by the risk of social engineering. Security awareness training is usually offered as the primary defense against social engineering. However, current research in social psychology demonstrates that security awareness training alone will not equip employees to resist the persuasion of a social engineer.

A defense against social engineering must take into account what is known about the psychology of persuasion and develop that knowledge to understand the persuasive attack and the dynamics of building resistance. Social engineering is diverse and complex enough that a multi-layer defense is necessary as a compliment to the security administrators' defense-in-depth model.

Background on Social Engineering

In general, social engineering is the process of deceiving people into giving confidential, private or privileged information or access to a hacker. There is really not a lot of difference between the techniques used for social engineering and the techniques used to carry out a traditional fraud (Rusch, p. 4).

Keith A. Rhodes, chief technologist at the U.S. General Accounting Office believes that social engineering is very effective. He notes, "Very few companies are worried about this. Every one of them should be." Others have noted that "…incidents of social engineering are quite high" (Gaudin, p. 2).

Security consultants certainly understand that social engineering is a serious vulnerability. When doing a risk assessment for a corporate client, there is no question that the consultants will be able to compromise a network if they use social engineering. "It's never been much of an effort to exploit social engineering and get in," says Brain Dunphy, a director of analysis of operations at RipTech Inc., a security analyst and consulting firm. "Companies may request that we use social engineering. We really only do it for the non-believers" (Gaudin, p. 4).

System administrators and security professionals must understand the limitations of hardware and software to provide a truly secure environment. There is a real need for us to think with "greater clarity and precision about what else can be

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

done to develop a truly comprehensive means of fostering [a secure] environment" (Rusch, p. 2).

Some Social Engineering Basics

There are a number of basic methods that are used to get employees to give out information or access. Some of the basic methods include pretending to be an employee, exchange of favors, convincing the target that the request is normal, assuring the target that he or she will not be held responsible for what he or she is doing and plain old friendliness (Harl, p. 2-4).

The technology to change one's voice on the phone is inexpensive, fairly effective and discussed in hacking literature. It is believed that most hackers are male. However, since females are believed to be more successful at persuasion, the hacker might change his voice to a female voice for a telephone conversation (Bernz, p. 3).

Developing Trust

The first objective is to establish trust. Once trust is established, the hacker will be able to start acquiring sensitive information and access necessary to break into a system. The skilled hacker will gain information very slowly asking only for small favors or gaining information through seemingly innocent conversations. The hacker will work hard to maintain an apparently innocent relationship, while learning company lingo, names of key personnel, names of important servers and applications, and a host of other valuable information (Granger, "Hacker Tactics", p. 5).

Social engineering is generally successful because people are naturally helpful. Most people, especially in departments like Customer Service, Help Desk or in positions of service like business assistants and secretaries are already trying to help. These jobs require helping people all day long and it is not natural to question the validity of every call.

Reverse Social Engineering

Hackers also use a technique known as reverse social engineering. This is when the hacker causes a problem on the target's network or computer and then makes himself/herself available to fix the problem. Once the hacker has fixed the "problem," he or she is perceived as a hero and has thus gained the confidence and trust of the target. In order for reverse for social engineering to work, the hacker has to be able to get onto a computer or system ahead of time or send a file to cause the originating problem. This requires a good deal of preparation and research to pull off, but can be very successful (Granger, "Hacker Tactics", p. 5).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Avenues and Media

Social engineering is often done with a phone call, but it may also take any of a number of different avenues. One avenue might be physically visiting the office. Few employees question a personal visit from a repairman, IS support person, a contractor, or a cleaning person. However, each of these ruses has been used in the past as a disguise to gain physical access. A great deal of information can be gleaned from the tops of desks, the trash or even phone directories and nameplates.

Another avenue a hacker may take is to write a program (or edit one that is already written) to request usernames and passwords in exchange for a "grand prize." These can be sent to the target by email and be programmed to send the information to a place where the hacker can pick it up. IM messages, chat rooms and bulletin boards have also been used to target and carry out social engineering attacks.

Websites can be used for a more technical form of social engineering. A sweepstake offer or promise of something for "nothing" if the user only gives an email (often including the login id) and a password (sometimes the same password that is used on the network). With this much information, there is a lot that a hacker can do (Orr, p. 2).

Psychological Triggers Behind Social Engineering

Since social engineering is a social and psychological exercise, it makes since to try to understand the psychology behind social engineering before seeking to develop a multi-level defense against it. In order to do this, it is necessary to understand the psychological triggers that take effect during a social engineering attack. Triggers are psychological principles that exhibit some kind of power to influence or persuade people. Understanding the psychological triggers behind social engineering will help to set the stage for an effective multi-level defense.

Strong Affect

Strong affect is a trigger that uses a heightened emotional state to enable a hacker to get away with more than what would be reasonable. If the victim is feeling a strong sense of surprise, anticipation or anger, then the victim will be less likely to think through the arguments that are being presented. Strong affect is introduced when the social engineer makes some statement at the outset of the interaction that triggers strong emotions. The strong affect includes, but is not limited to fear, excitement or panic. This could be the promise of a substantial prize worth hundreds or thousands of dollars or the panic of having an employee's job dependent on one decision. The surge of strong emotions works as a powerful distraction and interferes with the victim's ability to evaluate, think logically or develop a counterargument (Rusch, p. 4).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Counterfactual thinking is a phenomena related to strong affect. Counterfactual thinking is when the anticipation of possibilities like that of winning a big prize short-circuits a person's reasonable thinking. The person ignores the fact that the likelihood of winning is actually very remote, leading the person to risk real and valuable goods (information or access) for the possibility of a prize. It is as if the person is under a spell that has been brought on by the rush of emotions (Landman, p. 299).

Hacker web sites emphasize the use of surprise. Surprise can be accomplished by calling early in the morning or by coming up with very unusual circumstances or arguments. Surprise can also be obtained by the use of emotionally loaded words or images (A&T, p. 4).

Overloading

Mistaken premises go unchallenged when they are heard rapidly and are sandwiched between convincing truisms. This is the psychological trigger of overloading. Having to deal with a lot of information quickly affects logical functioning and can produce "sensory overload." With too much information to process, people become "mentally passive – they absorb information rather than evaluate it" (Burtner, p. 2).

Arguing from an unexpected perspective can also trigger overloading. The target needs time to process the new perspective but that time is not available. This leaves the target with too much information and not enough time to think it through, reducing the target's ability to process or scrutinize the argument. The target is then more willing to accept arguments that should have been challenged (Petty, p. 2).

Reciprocation

There is a well-recognized rule in social interactions that if someone gives us something or promises us something, we should return the favor. This tends to be true even if the original gift was not requested or even if what is requested in return is far more valuable than what was originally given. This truth is known as reciprocation (Rusch, p. 6).

This psychological trigger has seen a good deal of usage. Kevin Mitnick, a well-known hacker, describes the reactions he has seen, "In the corporate environment, people are unlikely to evaluate a request thoroughly, so they take a mental shortcut…" The reasoning follows that if someone calls and is helping with a problem, that person is on my side and means me no harm (Farber, p. 1).

Reverse social engineering makes use of the reciprocation trigger. The hacker appears as a hero ready, willing and able to fix the target's problems. Even before the problem is resolved, the target feels indebted to the hacker. This is, of course, an ideal situation for the hacker (Nelson, p. 3).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Another way that reciprocation can be used has been demonstrated by behavioral experiments. These experiments show that when two people are in disagreement, if one will yield on some point – no matter how small – the other will feel compelled to yield as well. For a hacker this is fairly easy. He or she needs only to make more than one request, yield in understanding on one, then the target will feel pressure to yield on the other (Cialdini, p. 38).

Reciprocation is seen constantly in the corporate environment. One employee will help out another with the expectation that, eventually, the favor will be returned. It is an unwritten bartering system that is considered invaluable if one wants to be successful. However, the social engineer exploits this system because his or her motives are dishonest and he or she is seeking something that should not be given at any cost.

Deceptive Relationships

Another psychological trigger is building a relationship with the purpose of exploiting the other person. One way of doing this is sharing information and discussing a common enemy. Kevin Mitnick describes that his favorite con was when he was conning an employee who had already become suspicious of him in a different context. This time Mitnick was establishing a relationship with the employee through email by sharing information and technology without asking for anything in return. He also helped bond the relationship by talking negatively about "Kevin Mitnick" whom the employee did not realize was authoring the emails. After the relationship was established, Kevin was able to obtain all kinds of information about the target's system (Farber, p. 1).

Once a relationship has developed, there are a number of ways in which it can be exploited. A good example of this was a recent AOL attack, documented by VIGILANTe. The hacker called and talked to a technical support person with AOL for over an hour. At some point during the call the hacker mentioned that his car was for sale. The technician was interested, so the hacker sent an email attachment with a picture of the car. The attachment included a backdoor exploit that opened a connection though AOL's firewall (Vigilante, p. 2).

Another way a hacker can build a quick relationship by appearing to the target as if they are very much alike. The idea is for the victim to feel like he and the caller think alike, have the same interests or want the same things out of life. Believing that someone has characteristics identical or similar to our own provides a strong incentive to deal with that person favorably even trusting that person without legitimate motivation (Rusch, p. 6).

Diffusion of Responsibility and Moral Duty

Diffusion of responsibility is when the target is made to feel that he or she will not be held solely responsible for his or her actions. Ironically, this trigger can work very well with the use of moral duty as a motivation for the persuasion. Moral

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

duty comes into play when the target feels like he or she is doing something to save an employee, to help out the company, or, at least, to avoid feeling guilt (Nelson, p. 4).

The target is made to feel that he or she is making decisions that will be the difference between the success or failure of the company or of the "employee" who is calling, implying that the caller may lose their job based on his or her decision. This is a very difficult decision for many people to make and the employee will more easily comply if he or she believes that he or she will not be held responsible for the action.

Authority

People are conditioned to respond to authority. One recent study dramatically illustrates this tendency. Nurses in 22 different nurses' stations were asked to give a dosage of a non-authorized prescription drug to patients based on the orders given over the phone (against policy) from a physician whom they had never met and at a dosage that was twice the maximum daily dosage. These orders clearly should have been questioned; yet, in 95 percent of the cases the nurses actually procured the dosage and were on their way to administer the drug before being intercepted by the observers (Rusch, p. 6).

This dramatic example shows that people will do a great deal for someone they think is in authority. Consider the impact a fake director or vice-president may have on an employee who has not been prepared. This trigger is made more powerful by the reality that it is considered a challenge to even verify the legitimacy of the authority. This lack of perspective leaves this trigger wide open for exploitation by anyone willing to misrepresent him or herself as an authority figure.

Integrity and Consistency

People have a tendency to follow through with commitments in the workplace even though those commitments may not have been very wise in the first place. For some it is a matter of integrity to "do what you say you are going to do" even after one is suspicious that the request may not have been legitimate. This tendency is so strong that people will even carry out the commitments that they believe were made by their fellow employees. If a hacker gets a hold of a vacation schedule, the employee's absence can be exploited using this trigger.

Another aspect of the Integrity and Consistency trigger is that people have a tendency to believe that others are expressing their true attitudes when they make a statement. Unless there is strong evidence to the contrary, people will believe that the person with whom they are talking is telling the truth about what they feel or need. This tendency to believe others is based primarily on their own honesty in expressing feelings (Rusch, p. 7).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

A Multi-layered defense against Social Engineering

Building a defense against social engineering is similar to building any strong defense. The key is to determine what the vulnerabilities and threats are and then defend against those risks. The defense must have several layers of protection so that even if a hacker were able to penetrate one level, there would be other levels at which he or she would be stopped. Since social engineering has proven to be so successful, a multi-layered strategy is critical. At some point, the strategy must be more than a defense. Given unlimited tries, the social engineering predator will eventually find or create a weak spot. This is why the network must fight back or at least recognize that it is under attack.

The concept of Social Engineering Land Mines planted throughout the network provides this opportunity to fight back. SELM's, as will be described later in this paper, are designed to do more than just prevent a social engineer from getting in. They are designed to expose the hacker.

Foundational Level: Security Policy addressing social engineering

No fortress will stand without a strong and stable foundation. The foundation of information security is its policy. The security policy sets the standards and level of security a network will have. It also gives the network a known state that can be adjusted as necessary. This foundation is even more critical when the security policy is protecting the network from social engineering. Social engineering targets people who need to know how to respond to questionable requests. The established policy helps end-users feel as if they have no choice but to resist the hacker's pleas. End users should not be in a position where they have to consider whether or not certain information can be given out. It should be well defined beforehand by people who have thought seriously about the information's value.

An interesting line of study in persuasion theory is in metacognition. Metacognition is people's "awareness of and thoughts about their own or others' thoughts or thought processes." From the studies of metacognition in persuasion theory, researchers have discovered that one way to build resistance to persuasion is to develop the target's thought confidence. Increasing employee confidence by laying out clear policies decreases the chance that the persuader will have undue influence on an employee (Petty "Thought", p. 722).

The security policy must address a number of areas in order to be a foundation for social engineering resistance. It should address information access controls, setting up accounts, access approval and password changes. It should also deal with locks, ID's, paper shredding, and escorting of visitors. The policy must have discipline built in and, above all, it must be enforced (Granger, "Combat Strategies", p. 2)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The Security Policy level of defense in relationship to social engineering will help an employee defend against the psychological triggers of Authority and Diffusion of Responsibility / Moral Duty. The policies have a balancing effect on the authority that a person may assume when they call on the phone. The policy also sets responsibility for information or access that is given out so that there is no question as to the employee's own risk when giving away privileged information or access.

Parameter Level: Security Awareness Training for all users

Once the foundation of a security policy has been established and approved, all employees should be trained in security awareness. The security policy will provide guidelines for the training as well as motivation. Policies that are well thought out and then taught to employees can make a difference in how employees respond to requests.

Security awareness is more complicated than just telling people not to give their password away. In fact, a well-known hacker Kevin Mitnick stated in a talk "I have never asked anyone for his or her password." His goal was much more complex than that. It was "to create a sense of trust and then [to] exploit it" (Lemos, p. 2-3).

Employees must know what kind of information a social engineer can use and what kinds of conversations are suspect. Employees should know how to identify confidential information and should understand their responsibility to protect it. They also need to know how to say "no" when it is appropriate and have the backing of their management on the occasion where it might offend (Granger, "Combat Strategies", p. 3).

All employees should be aware of the basic signs present in a social engineering attack. Some of these signs include a refusal by the caller to give contact information, rushing, name-dropping, intimidation, misspellings, odd questions, and requesting forbidden information. Employees must be willing to question the caller and withhold information when it looks like things don't add up (Granger, "Combat Strategies", p. 3).

Employees should be aware that a good social engineer will first try to set up a trusted relationship. The social engineer will then exploit the trusted relationship to gain all kinds of valuable information. A great deal of information can be gained through casual conversation such as company lingo, names and positions of important people in the company, significant events, overall organizational structure and the names of significant servers (Lemos, p. 2-3).

The training curriculum should basically follow the security policies, but there are some key points that all users need to remember.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- ***Know what has value*** – Most people undervalue their data and access before being hacked or having a harddrive fail. They should consider what they would do if they suddenly could not access their computer at all. This should at least help them understand that what they have been working on for the last five years has some value.

- ***Friends are not always friends*** – Friends that are made over the phone or who, for any reason, are asking questions concerning privileged information may not be friends at all. Social engineers will often make friends with their victims long before they ask for anything. All users should be aware that just because someone seems to be a friend does not mean that they can be trusted with privileged data or access. Depending on the value of the data and the level of security required on a network, social engineers may go through elaborate measures to convince a target that he or she is a friend. This could potentially take place over a period of time including days, weeks or even years.

- ***Passwords are personal*** – Although some hackers will never ask for a password, others will come up with very convincing reasons why an employee should give his or her password to a complete stranger. Unfortunately, without training, people tend to give their passwords away without much thought.

  Passwords can be shared in a number of electronic ways as well. Web pages and emails can claim great prizes for signing up on their site or through an application. The usernames and passwords that many people use on these sites are often the same as the one used on the network. If the site or application requires an email address, the hacker may also have obtained the victim's domain. Instant messenger and chat rooms can also be fertile ground for a social engineer to gain valuable access, information or password compromises.

- ***Uniforms are cheap*** – A social engineer may show up at an office building and pretend that he or she has a legitimate reason to be there. In many offices, simply donning a uniform will win acceptance. It is important to train employees not to just accept a uniform as a reason for someone to be somewhere. Uniforms are cheap and readily available. Keep in mind that almost any information is valuable to someone trying to break into a computer system and thirty seconds of access on a computer can set up a perfect reverse social engineering ploy.

Fortress Level: Resistance Training for Key Personnel

Not only should all employees be trained in security awareness, but a part of a multi-level defense should also include resistance training for key personnel. Key personnel include Help Desk personnel, Customer Service, business assistants, secretaries and receptionists and system administrators/engineers.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Basically, it should include anyone whose job is to help others especially the general public and those whose job includes escalated rights.

Good resistance training will help prevent employees from being persuaded to give information away that the hacker might need. Recent studies have demonstrated that resistance training can be effective at hardening people to persuasion. Several resistance-training techniques can be used from the field of social psychology to help adequately prepare employees to resist the persuasion techniques of a social engineer.

- **Inoculation** – Inoculation is when employees are given weakened arguments that will be used by the social engineer. It works on the same principle as preventing the spread of a disease by giving the subject a weakened form of the disease. Employees would be exposed to the arguments that a social engineer might use along with strong refutational arguments that could be used by the employee. Studies indicate that this is an effective and long-lasting resistance building technique. The problem comes in that it presupposes that the trainer will be able to anticipate the arguments of the social engineer (Sagarin, p. 527).

- **Forewarning** – Forewarning is another resistance-building technique that has been tested by social psychologists. Psychologists have tested warning subjects both of the content of an upcoming message and the persuasive intent of an upcoming message. Forewarning of the content caused greater resistance than forewarning of persuasive intent. The practical application for resistance training is to warn that not only will the social engineer attempt to persuade the target, but more importantly, that the arguments they use will be manipulative, deceptive, and insincere. Employees must be told that the hacker's intent is criminal and that they are intent on stealing from them. This black and white terminology is necessary if forewarning is to be effective (Sagarin, p. 527).

  Other studies have shown that resistance to persuasion may be increased if the target has prior knowledge concerning the message or if the target at least perceives himself/herself as knowledgeable. This additional resistance is caused by the need for cognitive closure (Kruglanski, p. 874). The practical application of these studies is that the more informed your employees are, and the more confident they are in their need to protect privileged information and access, the less likely they will be to allow themselves to be persuaded.

- **Reality check** – One of the reasons why security awareness training fails is that people tend to have an unrealistic optimism about their own invulnerability. This perception leads many to ignore legitimate risks and fail to take measures to offset those risks. However, once they are fooled

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

and it is demonstrated to them that they are indeed vulnerable, the training is much more effective (Sagarin, p. 536).

There are three stages of perceived susceptibility to risk. The first is awareness – knowing a risk is out there. (This is where most security awareness training stops.) The second is general susceptibility, which is the belief in the likelihood of the risk for others. The third stage is personal susceptibility, which is achieved when one acknowledges one's own personal vulnerability. Security awareness training and resistance training will have limited value if one does not reach the personal susceptibility stage (Sagarin, p. 540).

Dispelling the perception of personal invulnerability is not a cognitive exercise but an experiential exercise. Just telling an employee that a social engineer can fool them is not sufficient to counter the attitude of invulnerability.

The implications of this study are that resistance training would ideally give participants a chance to actually be fooled before the class even starts. The possibilities are limited only by one's imagination. One idea is to have a persuasive person come in or call some time before the class in order to gain as much information as possible using social engineering techniques from those who will be participants in the class. Then the teacher would let this person come in to the class and reveal how much he or she has been able to find out from each member in the class. That way people would realize that they are vulnerable to this sort of attack. Another way to expose the participant's vulnerability is to have an application that will pop up and request the username and password of the target. It would say something like "Your connection has been lost. Please reenter your username and password." This application then returns a message that lets that target know that he or she had been fooled. Either way, security training related to social engineering should include a strategy allowing participants to see how easy it is for ***them*** to be fooled. This is really the only effective way to decrease the invulnerability complex so that employees will personalize the training and watch for social engineering tactics.

Overall, current studies demonstrate that attempts to train people to be resistant to persuasive attacks are likely to be successful to the extent that they install two essential features. The first is that the employee must realize that the caller is trying to manipulate them. The second and most critical feature is that employees must realize that they are personally vulnerable to such manipulation (Sagarin, 540).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Persistence Level: Ongoing Reminders
A multi-level defense will need to include regular reminders of the necessity of security consciousness. One shot at training people to resist the social engineer will be effective for only a very short period of time. Regular and creative reminders are necessary to keep people aware of the dangers that may lurk on the other end of a friendly call.

A good example of the need for regular reminders is a typical police department tactic. Many police departments give regular reports to their force of those recently killed in action. This is intended to be a constant reminder that the job is dangerous and they need to stay on their guard. It is also done so that they will be on their guard against those specific dangers that other officers had faced. In the same way, employees need to be regularly reminded of the possibility of a hacker attempting to steal information from them and specifically informed of any recent attempts.

Gotcha Level: Social Engineering Land Mines (SELM)
Social Engineering Land Mines are traps that are set up in the system to actually expose and stop an attack. Just like a land mine in a battlefield, this trap is set to "explode" in the face of an attacker. It will destroy the secrecy, perhaps "cripple" the attacker and stop the attack. The SELM will alert the victim and the victim's security that an attack is in progress and should be either addressed or a heightened security posture should be engaged. Several ideas are listed below, but the ideas are really endless and limited only by the security engineers' creativity.

- **The Justified Know-it-all –** A bold social engineer will not hesitate to walk right into a company and start looking around. Once inside the building, there are endless possibilities for the hacker to find valuable information. Passwords may be written out, company phone lists may be posted, confidential information might be laying around in filing cabinets or even on people's desks and printers. The Justified Know-it-all is a person who makes it his or her business to know everyone who is on the floor or walking around in a department. Many departments already have someone who does this naturally. For this to be a SELM, that person should be briefed on the security risks of the physical presence of a social engineer and should have the power to do something quickly to address an unescorted visitor. This land mine would be useful even if badges are used for security as hackers will often forge a badge and expect not to be confronted.

- **Centralized Security Log** – Having a centralized log of security events that is being monitored by information security personnel can help prevent an effective attack. Any time an employee is asked to give out information or reset a password or even has a suspicious call, it should be logged in this central log file. If a hacker is getting information from one employee

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

and using it to talk to another employee, the patterns could be noticed in the log. As soon as the pattern is noticed, security personal can take action to stop the attack by warning employees of the attacker. Employees who are trained and know that they must report all security-related requests will be less likely to give out confidential information without taking time to think it through first. This will help offset the Reciprocation psychological trigger as the logging will remind the employee that there is more involved than a single relationship.

The well-known foot-in-the-door (FITD) technique teaches that people are more likely to comply with a request if they have already agreed to a smaller, related request. Studies have shown that an inadequate delay between the requests can produce resistance and can significantly reduce the effect. Given this research, logging requests can help bring requests together (even if the requests have occurred over a period of days or weeks) reducing the FITD effect and increasing resistance (Guadagno, p. 38).

Updates to the centralized security log must be monitored in real time so this SELM would need to take advantage of whatever notification options the company has available. Email notification to a special account that will cause the security administrator to be paged is one way to do this. Depending on the frequency of the logging and the size of the company, a groupware package or dynamic database option might work better.

For the central log to be an effective SELM all security events must be logged and employees – especially Help Desk and Customer Service positions – must be evaluated in part by their adherence to this policy. The log must be centralized and monitored so that the attacker cannot just bounce to different people in the organization

- **Call Backs by Policy** – A fairly well known procedure that would make for an effective land mine is a policy that requires Help Desk personnel and system administrators to call back anyone requesting a password reset or questionable information. The call back will verify the phone number and should be the phone number listed in the directory for the person who is calling. This is a procedure that will defeat the trickery of using a PBX system and transferring around to try to make an unsuspecting target think that the caller is calling internally when the distinctive ring only indicates a local transfer. If the caller tries to explain why the call back cannot be done or if the phone number is not the number expected for that employee, the Help Desk personnel should have the freedom of not having to grant the request and a security log entry should be generated.

  In an interview, Kevin Mitnick was asked what the most common con that companies fell prey to was. His answer was giving out internal phone

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

numbers. People have a tendency to help people who are perceived to be in the company because the victim fears reprimand. This SELM will help prevent this con from being effective (Farber, p. 1).

- **Key Questions –** Another SELM is for a number of questions to be used to verify the identity of anyone who is calling for internal information or trying to get a password reset.

  The Three Questions Rule is a good one to use, but must be set up with all employees in advance. This rule provides a list of questions and answers that the Help Desk personnel can use to verify identity. The questions should be obvious for the employee but not for others. An example would be "What model was your first car?" Each user would provide answers for the list of questions when their account is set up. The questions and answers are available for the Help Desk personnel to verify identity when a caller is asking for a password reset. A variation of this would be to use information that is available in the authenticating database, if available. However, this information may be public enough that the hacker may also have access to it.

  Bogus Question - If none of these systems are setup, a bogus question could work as well. The bogus question is a question that implies false information and gives the caller a chance to set the record straight or build on the false information. This would give the social engineer an opportunity to do the best extemporaneous responding a conman can muster. Of course, it doesn't matter how well it's done, the conman has already been conned. An example would be "Oh Mr. Smith, how is you daughter? Is she getting better from the accident?" If the caller says, "My daughter wasn't in an accident." or "I don't have a daughter," the caller has passed a single test. At this point the employee would apologize and explain that he or she must be mistaken. However, if the caller starts talking about the accident or lets the target talk about the accident, then the hacker has been hooked. The target should immediately notify security.

  This SELM is still useful even if PIN numbers are used for verification. If PIN numbers are verbal they can be over-heard. If they are punched in the phone, they can be overseen.

  This social engineering land mine procedure is much like magic. The one who uses it cannot tell what he/she has done no matter what the answer is. The procedure also cannot be done so frequently that others start to pick up on what is being done. This

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

must be a secret that is kept among the Help Desk employees and appropriate security personnel.

- **"Please hold" by policy** – The psychological literature is clear that people are more easily persuaded to do something questionable when there is pressure, surprise, or overloading. An SELM to defeat this is a policy that requires that any suspicious call or any call asking for a password reset or privileged information should be put on hold. This will stop the action and give the employee a chance to think. During the hold, the employee can log the request, discuss the request with a co-worker, or decide how to verify the identification. The real key here is to take a minute and process the information that is being given to determine if it is legitimate, needs further verification or should be denied.

These are just a few ideas. SELM's must be taken seriously if a defensive posture is to have any hope of being effective. Strict defense without any offensive or reverse espionage leaves the network a open for any and every continued attack. If the target is not at least learning about the attacker while being attacked, eventually the hacker will win.

Offensive level: Incident Response

The final level of defense is incident response. This is critical so that the network is not just waiting for the social engineer to finally get a hold of someone in the company who does not know or care about security. There needs to be a well-defined process that an employee can begin as soon as he or she suspects something is wrong. This process should aggressively go after the hacker and proactively inform other potential victims.

If there is no incident response, every employee that deals with a hacker is fighting a new battle. In the meantime the hacker is getting better at understanding the organization's defenses. The incident response procedures stop that process. As soon as a social engineer is discovered in any part of the organization, the attack is characterized and the employees are alerted that he or she is there and what to expect in an encounter.

It is important to have one person or a department working very closely tracking these incidents so that the attack can be characterized quickly and effectively. This should be the same person that is watching the journal logs from anyone who is receiving suspicious requests.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Conclusion

Social engineering is a very real threat and one that currently has fairly free reign. This will not always be true. Once businesses start taking social engineering seriously and applying the social sciences to protect against this threat with a multi-layered defense, social engineering will become a much more difficult, if not impossible, avenue for a hacker to employ.

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

References

A&T (author's "name"). "An Example of social engineering: One of the easiest ways to gather information." June 1999
URL: www.searchlores.org/social_1.htm.

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

Bernz (author's "name"). "The Complete Social Engineering FAQ." (No date)
URL: http://www.mjones.multiservers.com/soceng.htm

Burtner, William Kent. "Hidden Pressures." Notre Dame Magazine, Winter 1991-92 p29-32.

Cialdini, Robert B.; Green, Beth L.,; Rusch, Anthony J. "When Tactical Pronouncements of Change Become Real Change: The Case of Reciprocal Persuasion" Journal of Personality and Social Psychology: Vol. 62(1), 1992, 30-40.

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

Farber, Dan. "Mitnick on Mitnick: 'Why I'm going legit' (Part Two) Interview with Dan Farber." ZDNet. October 8, 2002.
http://www.silicon.com/public/door?6004REQEVENT=&REQINT=55863&REQSTRI1

Granger, Sarah. "Social Engineering Fundamental, Part I: Hacker Tactics." Security Focus Online. URL: http://online.securityfocus.com/infocus/1527.

Granger, Sarah. "Social Engineering Fundamental, Part II: Combat Strategies." Security Focus Online. URL: http://online.securityfocus.com/infocus/1533.

Guadagno, Rosanna E.; Cialdini, Robert B. "Online Persuasion: An Examination of Gender Differences in Computer-Mediated Interpersonal Influence." Group Dynamics: Theory, Research, and Practice: Vol. 6(1), March 2002, 38-51.

Harl. "People Hacking: The Psychology of Social Engineering" Text of Harl's Talk at Access All Areas III 05/07/97
URL: http://packetstorm.decepticons.org/docs/social-engineering/aaatalk.html

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Kruglanski, Arie W.; Webster, Donna M.; Klem, Adena. "Motivated Resistance and Openness to Persuasion in the Presence or Absence of Prior Information" Journal of Personality and Social Psychology: Vol. 65(5), 2002, 861-876.

Landman, Janet; Petty, Ross, "It Could Have Been You: How States Exploit Counterfactual Thought to Market Lotteries," Psychology & Marketing Special Issue: Counterfactual thinking. Vol. 17(4), April 2000, 299-321

Lemos, Robert. "Mitnick teaches 'Social Engineering'." July 17, 2000. ZDNet News. URL: http://zdnet.com.com/2100-11-522261.html?legacy=zdnn

Lewis, Edge. "Spyware – Identification and Defense." December 14, 2001. URL: http://rr.sans.org/privacy/spyware.php

Nelson, Rick. "Methods of Hacking: Social Engineering." URL: http://www.isr.umd.edu/gemstone/infosec/ver2/papers/socialeng.html

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

Petty, Richard E; Brinol, Pablo; Tormala, Zakary L. "Thought Confidence as a Determinant of Persuasion: The Self-Validation Hypothesis. Journal of Personality & Social Psychology: Vol. 82(5), May 2002, 722-741.

Petty, Richard E.; Fleming, Monique A.; Priester, Joseph R.; Feinstein, Amy Harasty. "Individual versus group interest violation: Surprise as a determinant of argument scrutiny and persuasion." Social Cognition: Vol. 19(4), Aug 2001, 418-442.

Rusch, Jonathan J. "The 'Social Engineering' of Internet Fraud." United States Department of Justice (no date). http://www.isoc.org/isoc/conferences/inet/99/proceedings/3g/3g_2.htm.

Sagarin, Brad J.; Cialdini, Robert B.; Rice, William E.; Serna, Sherman B. "Dispelling the illusion of invulnerability: The motivations and mechanisms of resistance to persuasion." The Journal of Personality & Social Psychology: Vol. 83(3), Sept 2002, 526-541.

Sharon Gaudin. Social Engineering: The Human Side Of Hacking. IT Management. May 10, 2002. www.itmanagement.earthweb.com/secu/print/0,,11953_1040881,00.html

Vigilante. "Social Engineering." Security Resources. No date. URL: http://www.vigilante.com/inetsecurity/socialengineering.htm.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: June 20th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**