GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Psychological Based Social Engineering

© SANS Institute 2004, Author retains full rights.

Charles E. Lively, Jr.
GSEC Option 1 version 1.4b
December 2003

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Abstract:

This paper discusses the dangerous, often-overlooked aspects regarding the underlying psychology of social engineering. When done well against those unprepared, internal accesses to systems can be gained without ever trying to bypass the firewall because the attacker is already sitting in front of his/her target.

Social Engineering is a technique used by computer hackers based on getting people to unknowingly assist the hacker in successfully accomplishing his/her attack.

This paper focuses solely on the psychological dimensions of these attacks, categorizing them into four distinct psychological attack vectors:

- Careless Attack Vector
- Comfort Zone Attack Vector
- Helpful Attack Vector
- Fear Attack Vector

As the causes and threats of these four attack vectors are discussed, a Defense in Depth Strategy is suggested to effectively defend against them.

Before discussing the four psychological attack vectors, a moment should be given to take a look at how social engineers study people. I recently spent an evening that turned into a late night listening in on a hacker chat session. I learned a lot about how they acquire their social engineering skills before I took a plunge and posted my questions. What I learned in their replies helped me to realize how serious and skillful these people are.

The Mindset behind Social Engineering

Social engineers study people. Truly committed social engineers are better equated to actors and actresses rather than computer nerds. They read books about body language, voice control, vocal indicators and group dynamics. They study individual personality types that come out through body language and vocal cues, they practice observing these conscious and sub-conscious traits in others and themselves.

One individual mentioned how he used clubs and bars to practice his social engineering skills. Another mentioned using his high school and one even said how he used dating to help hone his social engineering skills. Over time and practice they learn how to recognize how other people are feeling by observing what they say and do. This is very important since bluffing and gaining trust through deception means is imperative to their success. As social engineers

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

progress they learn how to alter these feelings in others by simply changing their own vocal cues and body language. As one individual in the chat room put it, it is only at this point that they consider themselves to be actual social engineers. It is their goal to be able to blend in or gain trust at will.

In "Hack Attacks Denied" by John Chirillo[1], he includes a social engineering tip list that he acquired at a hacker gathering. The "tip list" included among others: "Be professional", "be calm", "know your mark", meaning that one should become an expert in how the target thinks and reacts before ever engaging the target. The list went on to include team-oriented social engineering and suggested, among other things, to "manipulate the less fortunate and the stupid." The ultimate goal of social engineering psychologically is to make the victim want to give the attacker the information the attacker needs because doing so will benefit the victim.

With this understanding of the psychology of social engineers and of social engineering, we can now look at the four psychological attack vectors that they prey on. Social Engineering is as much an art as a technical skill. While there are more common techniques, the variation and execution of these are limited only by the attacker's imagination. However, due to the psychological basis of these attacks, almost all can be broken down into four psychological attack vectors. All four attack vectors become extremely more complex if the attacker is inside the target organization.

The Careless Attack Vector

The careless attack vector is made exploitable due to the indifference of implementing, using, or enforcing proper defensive countermeasures. It is often the first phase of a more complex overall attack. The attack escalates as the attacker's knowledge expands about the target. Reconnaissance is often seen in this vector.

Dumpster Diving

One common technique used is called "Dumpster Diving". Dumpster diving is the act of taking trash from commercial dumpsters outside of office buildings. This is often done at night by entering the dumpster, putting the trash into bags, and later analyzing the trash for useful information about the target. While this does sound bizarre and extreme, intelligence agencies have been using this technique for decades. In 1991, a consul general from a European country was questioned as to why he and another individual in an unmarked van picked up someone's trash bags that had been left outside for the real trash man. The trash bags turned out to be from the home of a senior executive that worked for a U.S. defense contractor. This European country has had a history of economic spying against the United States.[2] An example that particularly brought out the damaging potential of carelessly discarded trash was given by Bob Hillary at the

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

SANS Conference I attended in July 2003. [3] He asked the class a simple question, "What would I find in your trash if I picked it up for a couple of weeks?" I immediately remembered the unwanted credit card applications, bank advertisements, and other mail. I now own a crosscut shredder. Indeed, crosscut shredders are one of the most recommended practices against this threat. Keeping the dumpsters locked is suggested as well. It is also necessary to have a clear and enforced policy regarding shredding in order to drastically reduce this risk

Password Theft

A common vulnerability found within the careless vector is passwords written down and left out in the open. Anything from a sticky note on the monitor to a note stuck under the desk drawer is an obvious security risk. Regardless of what object the password is under, behind or in, the chances are that since it has not been memorized but is used regularly, it is somewhere within arms reach of the user's chair. A quick look under and around the monitor, keyboard, mouse-pad, mouse, the front and underside of the desk, along with any personal items will usually reveal any hidden passwords in under five minutes. This vulnerability is very prolific due to the innate sense of security many users feel in their office space. The false sense of security is the very foundation for the next group of attacks. A strictly enforced password policy could reduce the likelihood of many of the aforementioned potential compromises. The reasons for the policy should also be a part of user awareness training.

Comfort Zone Attack Vector

The next psychological attack vector could be called the "Comfort Zone Attack Vector". Exploits often occur here because the user is in an environment they feel comfortable in, therefore, their level of threat perception is lower. Typical examples of the comfort zone could be a user's office, floor, cafeteria, etc. To gain access to this attack vector usually requires exploiting one or more of the other attack vectors. This is why we as security professionals must work hard to maintain a constant multi-layered defense, because hackers often attack in depth.

Impersonation

A common attack employed here is technical support impersonation. Hackers have been known to impersonate everything from janitors and utility repairmen to fellow co-workers from a user's own IT staff. Most people will assume that the guy in overalls or the lady wearing the company's IT polo shirt is exactly who he/she says he/she is. While this situation usually turns out to be legitimate, the user should try to verify the person's legitimacy. A call to the IT Staff would be most prudent before giving the friendly lady your user name and password, as would be a call to the maintenance desk before opening the door to the nice guy

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

in overalls. This is also where gleaning information through improperly disposed of trash occurs. Rather than diving into a dumpster, the attacker will dive into a trash can for the same reason. This usually occurs after business hours. Often the attacker either is impersonating a janitor or is legitimately employed and selling the gleaned trash for profit. Again, having a cross-cut shredder and a clear and enforced policy on shredding will drastically reduce this risk.

Shoulder Surfing

A common technique used in the Comfort Zone is known as shoulder surfing. This often occurs after exploiting one or more of the other three psychological attack vectors discussed later in this paper. Shoulder surfing is the act of looking over a user's shoulder to observe the entries to the keyboard as the username and password are being typed. With practice the use of shoulder surfing can become quite effective at acquiring another user's credentials and can be employed from any angle at which the keystrokes can be observed. User awareness and education to shoulder surfing along with discretely placed keyboards would be an effective countermeasure against this technique.

Direct Approach - Theft

One of the least discussed, but extremely dangerous type of attack vector is a special type of direct approach. The direct approach is a technique where the attacker makes direct contact with the user usually in person or over the telephone. This specialized type of direct approach, however, targets the user outside of the office and often outside of his/her building. Most users work in a team or group of some sort. Often these teams will frequent a favorite restaurant or go out at the end of the workweek for a few drinks. Computer hackers use this frequency to observe these interactions (reconnaissance) and learn the group's behavior to calculate the best time and way to make their direct approach. Since the user is in a comfort zone his/her threat perception is still lowered and depending on the number of drinks maybe slightly diminished. After the direct approach has been executed someone is usually missing a wallet or purse. If it was executed very well, only an ID badge. It will probably go unnoticed until next Monday morning. Which is, of course, the whole idea.

Physical Security

Another vulnerability in this attack vector lies within the realm of physical security. A common example would be the designated smoking areas within organizations. Due to the difficulty in securing these areas, they provide an easy point of physical entry into an otherwise secure facility. Doors are often propped open to avoid the hassle of swiping ID badges or of the insider threat of keys being needed to re-enter the facility. Also, many organizations have more than one smoking area designated with no access control whatsoever. This vulnerability could be then effectively exploited by a seasoned social engineer.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The Insider Threat

While not a technique, in any analysis of the comfort zone, the social engineering threat posed by someone within the organization should be discussed. This is commonly referred to as "The Insider Threat" and almost always involves multiple elements of social engineering. This threat is especially hard to defend against because the attacker is already inside the workplace and if he/she uses a computer, the attacker is also inside the organization's network. The attacker could employ most of the social engineering techniques mentioned in this paper. After all, if you are reading this paper what is to keep the disgruntled employee that you may be working beside from reading it also? This type of threat, especially in regards to information access, requires a written policy along with user awareness. Many employees can often probe how much of the network they have access to by "accidentally" double clicking on that folder or network share. In this case reconnaissance is especially hard to identify and false positives are very common.

Another social engineering technique used by the malicious insider is asking for favors from the IT help staff. The insider will often indirectly ask about logical (and sometimes physical) information regarding the network, security systems, as well as IT policies. Often the questions are spread out over the span of a long time frame and posed to different personnel within the organization. In this way a lot of dangerous information can be leaked out. The leaks are usually expensive. A CSI statistic that Jarvis Robinson noted in "Internal Threat - Risks and Counter Measures"[4] illustrates the potential damage from successful social engineering when committed by an insider, "the average attack costs the target enterprise $2.7 million, compared with $57,000 for the average outside attack."

Employees and users will only be able to help their IT staff if they are properly trained to identify social engineering attempts and the threat from malicious insiders. Again, employees must know that the policy exists and is enforced, so that the user doesn't feel awkward in saying that certain information is considered sensitive and can not be given out. An easy way to make sure that the policy is publicly known and enforced could be in the form of a "top ten" list in tactics employed by social engineers and malicious insiders.

Helpful Attack Vector

The Helpful Attack Vector is used on the premise that people generally will try to be helpful, even if they do not know whom they are helping. There are two main direct attack types here.

Direct Approach - Piggybacking

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

A simple example given by Bob Hillary at the SANS Conference illustrated this quite well. [5] It is called the Big Box technique. The attacker approaches secured doors that he/she needs to get through in order to gain access to the target. To get in they will carry a big heavy looking box. The attacker begins his/her act when he/she spots a probable employee approaching the doors. As the attacker struggles to carry the box to the doors the employee sees this and tries to help the attacker by letting him/her in. The employee unknowingly just gave the total stranger access to the premises.

Another less dramatic way of doing the same thing is when the attacker pretends to be only a few steps behind another employee entering the same secured door that a legitimate employee just unlocked. The employee usually will hold the door for the next person, which in this case is the attacker. Both techniques are most often used when many employees are going through the doors at once. Examples would be the company starting time for work in the morning or re-entering a building after a fire drill.

Direct Approach - Impersonation

A popular way to gain information is to call organizational numbers and simply ask to be connected to the IT helpdesk or ask, "Who can help me?" These numbers have usually been the result of dumpster diving and other previously mentioned techniques. Calling the help desk or IT support and simply pleading or pressuring to have a password on a user's account changed has become more difficult over the past five years as IT and helpdesk training has put more emphasis on past successful exploits. This approach is still being successfully used though, therefore, it shouldn't be left out.
Again, a solid security policy and user awareness training would be very effective in minimizing these attacks. Both of the aforementioned hacker techniques can be easily defeated by a policy that required all employees to provide identification to a security guard prior to any further access to the building. The policy could also include securing any doors prior to the guard station.

Employees that were made aware of these type of attacks would feel less uncomfortable letting the security guard know that someone immediately took a different door or stairwell just after entering the building, rather than heading to the guard station like everyone else.

Help desk personnel can be very venerable to helpful based attacks. Since IT support and Help Desk jobs can often involve customer relations as much as technical support it is especially important that all help desk staff have a policy plan already in place. They should be completely familiar with the policy plan and also know that management will support them when they follow it.

Often after gaining a user's name a hacker will call technical support claiming to have lost or forgotten his/her password and request a new one. This common

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

hacker technique has been used successfully against AOL employees and created a real headache for the Internet service provider. Kim Hu, a staff writer for CNET News.com, wrote the interesting article "AOL boosts email security after attack"[6] on how AOL was exploited technically as well as socially. Mr. Hu had a unique perspective on AOL's predicament since he himself had been hacked while on AOL just a couple of years beforehand. However, a few years before CERT[7] had already released an advisory in specific regards to social engineering in which it emphasized user awareness to both the technical and social aspects of social engineering. AOL's hardships might have been avoided had the CERT advisory been followed.

One of the most significant reasons for clear policy and management support for users is because the helpful attack is often used asymmetrically with the fear-based attack.

The Fear Attack Vector

"The Fear Attack Vector" is often the most aggressive type of psychological attack. Its foundation is based on attacking the user in such a way that the user provides the attacker with the information or access needed due to putting the user in a state of anxiety, pressure, stress and fear. This attack often uses impersonation, blending elements from all of the previous attack vectors.

One common technique is to pretend to be an individual of high importance within the user's organization. There are many techniques employed within this attack vector, but most if not all employ persuasion reinforced by fear.

Impersonation & Conformity

An example of a fear-based attack is employing the conformity technique.[8] Here the attacker puts the user in the uncomfortable position of being the only user to not help them out as the others have in the past. This type of peer pressure is often used to get a password reset or a username altered. This occurs when the user feels that, since this behavior has occurred in the past, his/her personal responsibility is diffused, or spread out amongst all of the other users that have done this before him/her. This helps alleviate the stress that the user is under and provides the user with the justification for granting the attacker's request.

Impersonation & Time Frame

A more aggressive technique is a time frame attack. This attack uses a fictitious deadline in order to obtain user compliance from a Helpdesk Operator. An example of this technique would be an attacker impersonating a legitimate user from the accounting division. The "payroll bookkeeper" is in need of assistance ten minutes before the close of business on a Friday evening in order to make sure that all of the staff receives their paychecks on time. The bookkeeper could

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

increase the pressure by complaining about the IT staff's latest system change as being the source of their password dilemma. The Help Desk operator now has been placed under two significant pressures. The time of the attack combined with the chosen day potentially reduces the chance of the operator's ability to confer with a superior. If a well-defined and enforced password policy is not already in place, there is a good chance that the attack will succeed.

Impersonation & Importance

A technique employing impersonation is one in which the attacker pretends to be someone important or acting on behalf of someone important. "The director forgot her password again and would like it to be changed to her son's name. She wants to know how long it will take?"

Another technique would be to utilize the comfort zone vector and to show up in the Bell Atlantic polo shirt during a particularly sever thunderstorm. "This storm has been causing a number of our PBX's to overload due to an improper ground. Can I check yours to make sure it has the proper setting?"[9]

Conclusion

As was discussed earlier, the use of Social Engineering can be quite effective when one leverages and interweaves these four psychological attack vectors. A Defense-in-Depth strategy to counter this threat should begin with a properly written security policy. It would need to be written in such a way that management agrees with it and supports it. It should be able to be updated as necessary. It also needs to be inclusive of the multiple aspects of physical security, i.e. security guard check points, as well as technical security.

Since the social engineer relies often on fear based attacks it is absolutely critical that any defensive policy take this into account. Help desk staff should be fully confident in management backing up their decision not to change a VIP's password if that situation should escalate into a complaint. Public acknowledgement and other rewards should be given to those users that have demonstratively taken the threat of social engineering and other security issues seriously. These rewards would show that management treats security just as seriously as they expect their subordinates too.

However well conceived, all plans (and policies) have unknown flaws. A good security policy will always incorporate a Defense in Depth strategy. It would, therefore, be prudent to test the policy from time-to-time. Aside from making it known that the policy is taken seriously, periodic testing will also bring out any weak spots and non-compliant areas.

It is often said that computer security is part of everyone's job and that users are often a security specialist's first line of defense. However, users cannot defend

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

against what they do not know. Therefore, user awareness and user rewards are essential parts in any complex strategy against social engineering. User awareness to the threat of social engineering should go beyond just discussing pop-up logins and callers requesting confidential information. It should include thorough sampling of the wide array of techniques used by Social Engineers as well as a good look at their training and acquired talents.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

[1] Chirillo, John. "Hack Attacks Denied" A Complete Guide to Network Lockdowns for UNIX, Windows, and Linux, Second Edition". Second Edition". John Wiley & Sons, Inc. 2002.

[2] Heur, Richard. "Theft and Dumpster diving". Defense Security Service Academy. March 1996. URL: http://www.mbay.net/~heuer/T3method/Theft.htm

[3]Hillary, Bob. "SANs Security Essentials". SANS Conference. July 2003.

[4] Robinson, Jarvis. "Internal Threat-Risks and Countermeasures". Version 1.0. November 15, 2001. URL: http://www.sans.org/rr/papers/60/475.pdf

[5] Hillary, Bob. "SANs Security Essentials". SANS Conference. July 2003.

[6]Hu, Jim. "AOL boosts email security after attack." CNET News. September 21, 2000. URL: http://news.com.com/2102-1023_3-242092.html?tag=st_util_print

[7] CERT Coordination Center. "CERT Advisory CA=1991-04 Social Engineering". September 18, 1997. URL: http://www.cert.org/advisories/CA-1991-04.html

[8] Granger, Sarah. "Social Engineering Fundamentals, Part II: Combat Strategies". Security Focus. January 9,2002. URL: http://www.securityfocus.com/printable/infocus/1533

[9] Granger, Sarah. "Social Engineering Fundamentals, Part I: Hacker Tactics". December 18, 2001. URL: http://www.securityfocus.com/printable/infocus/1527

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.