

Mitigation of Social Engineering Attacks in Corporate America

Kevin C. Redmon, Graduate Student in Information Security, East Carolina University

Abstract—Information has become the most valued commodity in American companies, where physical possessions of businesses once held that title. Protecting this information has proven to be a much more daunting task than its physical counterpart as it can be stolen from afar and the landscape of the attack is so much greater.

In this paper, I will describe the enemy and his various methods and strategies of attack to access this information. Based on these attack modes, I will propose various methods to mitigate, or even eliminate, the impact of a social engineering assault on a corporate security system. As my conclusion, I will briefly discuss ongoing steps that a security team can take that will help to ensure continual compliance with security policy. Although titled and focused on Corporate America, the concepts discussed in this paper are universally applicable.

Index Terms— Hacking, Information Security, Security Policy, Social Engineering

I. INTRODUCTION

THE Merriam-Webster Online Dictionary defines social engineering as “management of human beings in accordance with their place and function in society : applied social science” [18]. This is the glorified, politically correct definition that seems to liken social engineers with chemists, doctors, and mathematicians. An alternative definition that many computer-centric websites reference is the *Jargon File* definition – “Term used among crackers for cracking techniques that rely on weaknesses in wetware rather than software; the aim is to trick people into revealing passwords or other information that compromises a target system’s security.” [19] This jargon-rich definition is difficult for the layman to understand. The layman’s definition, and by far the most succinct yet also the most accurate, is “old-fashioned manipulation” [4],[8]. Whatever definition is attached to the term, the result is the same - social engineering is one of the biggest security issues faced by corporations today.

II. CATEGORIES OF EXPLOITS

Social engineering is not a new concept. Odysseus and

Sinon used social engineering tactics to get the wooden horse behind the walls of Troy circa 1671 [20]. Police officers use social engineering to catch drug dealers, prostitutes, and other criminals. Children are often trained in social engineering when they are young – whining or crying as a ploy to get a toy, a bottle, or simply attention [12]. Whether the goal is an honorable one or not, the approach is the same - manipulate a person to reach your end goal. It could actually be one of the oldest arts around although its form has evolved over time.

The modern version of social engineering can be broken down into two main categories – computer-based and human-based attacks [5]. Computer-based attacks use a webpage, a computer program, or other technology in order to trick the victim into providing information. The computer-based deception is often performed by providing the user with a URL or an attachment, usually via email. This URL could be a location to provide key information for a survey (such as email address and password – providing the attacker with what is likely a valid username, domain name, and password), sometimes with the promise of a prize, or to download an application. The application, if it is downloaded, could be a Trojan horse (that will allow remote access for the victim) or a keylogger (which will send all keystrokes on the victim’s keyboard to the attacker - including login IDs and passwords). A similar approach could be employed via a counterfeit pop-up window, asking the victim to type his username and password to reauthenticate to the network. This data, once again, will be sent off to the attacker.

A human-based attack leverages human relationships to get the desired information. Human-based methods are still the most prevalent within social engineering attacks [13]. There are many ways to use human relationships in order to get what you want out of a victim. Some of the more common approaches are:

A. Impersonation

Impersonation is likely the most valuable tool of a social engineer. Using this tool, he may act as an authority figure or take on the identity of a lay user. In either case, the attacker has moved much of the risk away from himself – if someone were to expose the attacker, they will often lack the attacker’s real identity. Posing as an authority figure can help to intimidate the victim. If the victim does not provide the requested information, there could be consequences inflicted by the authority figure. As a lay user, the attacker can assume the identity of an everyday insider. Using this approach, the

Manuscript received November 29, 2005.

Kevin Redmon is a Graduate Student studying Information Security at East Carolina University, East Fifth Street, Greenville, NC 27858 USA (e-mail: kcr1116@mail.ecu.edu).

social engineer can stay comfortably under the radar while gathering valuable information for the next series of attacks.

One other facet of impersonation is to don a person's physical appearance. Impersonating a current employee in this fashion would be too risky. However, impersonating a service person (janitor, IT consultant, plumber) [9] would tend to be a more successful scenario. This approach is highly effective when physically visiting a victim's location for intelligence gathering. Some of the intelligence that is gained in this fashion may include gathering user passwords by browsing offices, stealing faxes, stealing valuable documents, among other possibilities. This could also yield an opportunity to plant a computer-based attack, putting a CD or pamphlet (with a hacked webpage) into each user's mailbox.

B. Trust

Trust has to be developed and does not happen over night. The social engineer in this situation will "visit" the same person several times, developing a rapport with that person. As Kevin Mitnick describes in his book [2], the "Social Engineering Cycle" is "Research, Developing rapport and trust, Exploiting trust, and Utilize Information". During these initial visits, an attacker would have several uneventful dialogues with the victim, not seeking anything of appreciable value. His key goal is to be trusted by the victim. The attacker may use common interests, work place experiences, or locations where he has lived or has been in order to identify with the victim. Once an acceptable level of trust has been established, the attacker will go after the "valuable" information. Moving too quickly when using the trust approach may "burn" [2] the victim, making him suspicious and not useful for future inquiries.

C. Diffusion

Diffusion is the ability to lessen the perceived impact of fulfilling a request [11]. The attacker may state that an authority figure would not have an issue with the attacker's request or make assertions that others have done the same task for the attacker in the past. The end goal is to relieve some of the stress that the victim may be feeling if they succumb to the attacker's request.

D. Overloading/Strong affect

Overloading is the act of rapidly providing a victim with so much information that they are unable to effectively process that information [16]. This is used by the social engineer to create mental shortcuts – leaps in logical thought - within the victim. The attacker will utilize this attack by hiding a rather obvious fallacy between two truths in his rapid-fire dialogue with the victim. The victim cannot mentally keep up and soon finds himself agreeing to the attacker's requests.

Similarly, strong affect utilizes the mental shortcut [16]. This mental shortcut is created slightly differently. Using strong affect, the social engineer promises the victim an opportunity to win a substantial prize. The victim's mind is often distracted at the potential to win the prize and will

sometimes forego logical thinking, giving in to the attacker's requests for information.

E. Moral Duty

People inherently want to do what is right[11]. They want to be a team player and help their co-workers. When the attacker makes a request that the victim could help with by breaking "a little rule", depending on the risk involved and the likelihood for punishment, the victim may comply with the attacker's requests.

F. Reciprocation

A victim will be more likely to accommodate an attacker's requests if the attacker will reciprocate [6]. When an attacker makes a small request and offers to pay back the favor immediately or at a later time, the victim is more likely to assist the attacker in his request. The initial offer of goods or services can come from either party in this case.

H. Urgency

An attacker may stress to a victim that if certain information isn't provided quickly, there could be negative consequences for the attacker and, often times, for the victim as well [7]. This approach, much like overloading and strong affect, can create a mental shortcut within the victim. The victim must make the right decision quickly – presumably the right decision is to comply with the attacker. If the victim does not comply, he may be forced to pay the consequences.

I. Direct Approach

This is probably the most risky and the most unsuccessful human-based attack [11]. The attacker in this scenario simply asks for what he wants. Sometimes, the victim will comply. However, this may also make the victim suspicious and remove him from future information seeking efforts.

III. SOCIAL ENGINEERING METHODS

There are many ways to utilize the social engineering exploit techniques mentioned above. That is what makes the attacks so difficult to combat – the battlefield is constantly changing. In this section, I will describe some of the more common approaches used by social engineers. The scenarios will hopefully serve to inoculate the reader, allowing them to see future instances of social engineering attacks.

One of the key steps in executing an attack is research, a process known as 'footprinting'[14]. In order to be affective in a social engineering attack and to get the most out of it, an attacker must know his victim. He must know about the processes used within the victim company, the lingo that is used, departments within the company, key personnel, and most importantly what information he will want to gain from the victim company.

There are many ways to gather information about your victim:

A. Corporate Website

There is a lot of good information available on corporate websites [12]. By reading the website of any company, an attacker can become educated on that company's business, cities and states where the company is located, phone numbers, and possibly even contact information about key personnel. Also, by reading the website information, he can become knowledgeable on key processes and terms (aka lingo) that is used within that branch of business. All of this information can prove to be useful fodder in executing an attack.

B. Google Search

Possibly even better than a review of the corporate website above, a Google search can provide information about the victim company from many different sources [3]. This information may include stock analysis and financial data, competitors, partnerships with other companies, etc. You can sculpt your search terms on Google to even show posts to public newsgroups by the victim company's employees. Reading through some of these articles or newsgroups from Google may help to develop an organizational chart or provide some user names and job functions to impersonate. If the attacker is extremely fortunate, he may find some of the information that he seeking already contained within the emails or newsgroup posts.

C. Job Sites

By searching the job listings available within the victim company, either directly on the corporate webpage or a jobfinder webpage (e.g. Monster.com), a social engineer can find out a lot about a company's current development, future development, and where they need to improve from the manpower standpoint [3]. Depending on the attack scenario that the social engineer is planning, this could possibly even provide him an opportunity to become employed at the victim company.

D. Public Venues

This could prove to be one of the most overlooked methods to gain information about a victim company. All too often, employees from a corporation will not practice good operational security and will openly discuss company processes, projects, or secrets in a public venue (e.g. Airport, restaurant). By simply overhearing conversations, an attacker can become familiar with organizational charts, projects, lingo, etc. – all good information to use on a future attack.

Furthermore, logging into company computer systems from a public kiosk is also a huge security risk. Many of these computers have been exploited by illicit users and will contain keyloggers or Trojan horses that will send login information to the hacker. Even if a public kiosk system does NOT contain a keylogger or Trojan horse, there is still a great opportunity for an illicit user to shoulder-surf – looking over a person's shoulder – to gain his login in credentials. In either case, with this information, the illicit user can log into the victim company remotely.

E. Dumpster Diving

Although this is not the cleanest aspect of social engineering, it can often prove to be the most useful. Dumpster diving, also known as “trashing”, is the act of going through someone's trash in order to find out important information. This information may include printed emails, faxes, pay stubs, phone bills, company directories, organizational charts, etc. [15] Per a 1988 Supreme Court ruling [13], all of this can be perfectly legal as long as the victim does not post “No Trespassing” signs.

There are still other ways to gather information, yet using one of these methods will mitigate a majority of the risk (excluding Dumpster Diving). Physically collecting data at the victim company site can be considered an additional method of information gathering, but it may be best used as part of the second and subsequent phases.

Now that much of the research is done, the attacker can now proceed to go after the information that he *really* wants. Using the exploit techniques mentioned in the previous section, the attacker can now build upon that information. Here are some exploit scenarios:

- Either using information found during the data gathering phase or cold-calling, the attacker may call up an employee within the victim company. He can then ask for the phone number of a particular person and/or department to further his research, eventually getting to the right people or getting the right information. Any names that are gained during this or previous steps in the attack may be used to establish identity (collecting the credentials to impersonate that user) and/or for establishing credibility and trust via name-dropping.
- After establishing a level of trust with a user, the attacker could ask the victim user to go to a website and fill out a survey or download a program. In either case, the goal could be the same – gather login information from the user via this hacked webpage or Trojan horse application. This login information could be used during future attacks to act as a legitimate system user. This login information could also be used to establish identity during a help desk call.
- Once the victim has access to the network as a legitimate user, he can then install other hacker tools onto the network. Either with the access alone or the installation of the hacker tools, the attacker could now have remote access to the network. He could attack the network from afar with little fear of ever being caught. Sometimes the first login account is immediately used to create several other accounts of equal security level. These additional accounts can serve as a “back door” if the attacker's actions have been detected and the initial account disabled.
- Using the company letterhead that was found during the dumpster-diving exercise, an attacker sneaks his way into a mailroom at the victim company. The attacker places the drafted letters or surveys into every user's mailbox. Even if a small percentage of the users complete the survey, the opportunity for gathering

useful information can be very high – possibly gathering login information that can be used for future covert attacks.

- After finding a map of the offices in the victim company’s garbage, the attacker knows the floor layout well enough to deflect suspicion if he were to sneak into the building. A week later, the attacker “tailgates” (following someone into the building without providing proper credentials) and installs a keylogger (either hardware or software keylogger) onto several of the computers in a particular department. He also installs software that will disrupt the user’s normal computer use, resulting in a call for IT support. The IT guy, unknowing about the existence of the keylogger, attempts to login as administrator on the victim’s computer, now exposing his password to the attacker. This keylogger will send the data, including the IT administrator’s credentials, to an anonymous email account in China. This administrator password can then be used for all kinds of nefarious future activities. Kevin Mitnick once stated that he had never asked for a password [10] – why ask for a password if you can create one for yourself.

These are just some examples of attacks that a social engineer may invoke. However, this list is by no means exhaustive. Every new piece of data that is gathered can open up twenty new opportunities for exploiting the victim’s information security systems. “Security solutions have a technological component, but security is fundamentally a people problem.” [1]

IV. MITIGATION

I have described several attack scenarios above but there are still several thousand more to be considered. All is not lost – there are routes that you can take to help mitigate these risks or eliminate some of them altogether.

A. Policy

Policy is *key* to a good information security policy. Document all security policies and post them in a central location for all users to see. A common approach is to make them available via a central download webpage. As an annual process, ask that each user review the policy and accept the conditions of the policy.

This policy should be a condition of employment, agreed to by the employee prior to starting the job [5]. If he declines to accept this agreement, he will not be allowed to work for the company. Annual reviews of the security policy/policies should be given the same consideration – if the user fails to accept the new rules, he will not be allowed to continue employment. In order for this to be affective, the company management must support this stance and be willing to enforce it.

Keep security training fresh. Constantly iterate a single message, yet use different wording and different images to

keep the users interested. If a company uses the same slogan the same way every time, it will serve to dilute the message.

To be more effective in the dissemination of security training and materials, institute a test system that helps confirm that every person has read and is familiar with his role in security. Otherwise, the user may simply click “I agree” to the security policy while not having read it.

B. Physical Security

Physical security is the first line of defense. Proper access controls must be in place to allow the proper people into the company with ease while keeping all others out.

One key component to physical security is identification. Everyone who is given legitimate access to a company should wear a picture badge in a visible location on their person. Depending on the employee’s status (employee, temporary employee, etc), the identification will utilize a different background color and/or formatting. Also, all visitors should be assigned a temporary badge that clearly shows that they are visitors. The visitor badge, assigned to a specific person upon entry into the building, will allow him default access to some resources, yet deny him access to all others. This badge should help to curtail any other people, such as an attacker, from roaming the halls and going into areas where they should not be.

The badges that are used should also contain some sort of access control mechanism. This could be an RFID device and/or a magnetic strip. The access control mechanism should be used whenever entering into controlled areas such as laboratories or restricted floors. When a visitor must be escorted into a controlled area, he should also scan in. This may likely create a failure record within the access system log, but the failure would indicate his access to that portion of the building.

In controlled access areas, implement a multi-factor identification/authorization system such as biometric verification. This system will use something that you are (e.g. fingerprint), something that you have (e.g. your ID badge), and something that you know (e.g. a PIN number). This will help to prevent unauthorized access.

When an employee sees someone tailgating them into the building, the employee should ask the tailgate person to show his badge. If it is a restricted access area, due care must be taken in order to verify that the user is not only an employee but also has proper authorization to this area. This can sometimes be accomplished by asking the person to “swipe” their ID – if the light is green, they are OK to enter. Otherwise, the security office or superior should be notified of the attempt at an attack.

C. Acceptable Use

Acceptable use is a term that describes what is considered acceptable in using the company computers and other electronic resources. Some companies hold a strict policy that business resources can *never* be used for personal use, while other companies are much more lenient. Whichever stance is taken by a company will depend on the company culture and the amount of liability that the company is willing to accept.

The acceptable use policy may also lay out some rules and/or regulations that will define password guidelines, password reset rules, etc. One key example of this is to disallow writing of passwords onto a piece of paper and to also choose strong passwords. Sometimes this seems like a mutually exclusive requirement as the stronger a password is, the harder it can be to remember. In this case, encourage the use of password keyring software, asking that the user remember one strong password to “unlock the keyring”. The user will put all of his passwords onto this keyring and whenever needed, he can open the keyring with his single strong password to access all other passwords.

D. Help Desk

The help desk within a company is the most prone to social engineering attacks. The help desk personnel have the ability to reset passwords, to configure accounts, to turn on or turn off access, etc. Extra care must be taken by the help desk team to ensure that the user is who they say they are. This can be done via a PIN number, a series of questions, doing a callback, etc. Even if the user is able to prove who they say that they are, the help desk must ensure that the password or account information still does not get into the wrong hands. If at any point during the help desk phone call, if things do not seem “right”, the help desk employee should be empowered to deny access if he sees fit. Whenever a social engineering attempt is detected, the help desk employee should enter all relevant data into a central logging system. Administrators can review this logging system and detect any patterns that individual users may not see. [16]

E. Improvements

Continual review and improvements should be made to any security policy. All employees should be empowered to provide their input into this security policy. By personalizing the security policy for the individual users, compliance with the policy will be much better received. Any suggested changes to the security policy should be reviewed by a committee for applicability and to ensure that they don't unnecessarily reduce employee efficiency.

V. AUDIT

Performing an audit is a task that should not be taken lightly. There are security companies that specialize in audits and can offer sound advice on how to proceed if an audit is what is needed. If an audit is needed, be sure to get the signoff of upper level management. If the audit is not handled correctly, legal implications and drops in employee moral could result. If a company still insists on an internally driven audit, some things to consider are:

- Get upper management blessing FIRST! There are many impacts that a social engineering audit could have on an organization, including a drop in employee morale, legal issues, etc.
- If an outside 3rd party is the desired approach at performing a security audit, use a trustworthy resource

who is endorsed or certified by a reputable security organization [4].

- Audit the physical security of your company by attempting tailgating, entering into areas where you are not authorized, and removing hardware from the building.
- DO NOT attempt to access any employee's personal effects during the audit. Although this could be a likely scenario for a true social engineer, this would likely be received poorly by the employee and could result in unneeded legal action.
- To verify the proper use of strong passwords and the misuse of unencrypted passwords on the company intranet, use password cracking and sniffing tools. These tools, such as Cain and Able, can help you to find and fix a security hole before someone else does.
- Establish a data classification scheme for the various data elements within your company and limit data dissemination on a “Need to Know” basis. This will help to limit the exposure of the data to attackers. [17]

VI. CONCLUSION

Social engineering is a difficult field to teach in a few short pages. Over the last five sections, we have only begun to scratch the surface of this dynamic art of manipulating human relationships. One thing is for sure – it is a *real* risk to every corporation's information systems. Every corporation should take it upon themselves to implement all reasonable controls to effectively mitigate the attacks of a social engineer.

REFERENCES

- [1] B. Schneier, *Secrets & Lies: Digital Security in a Networked World*, Indianapolis, Indiana: Wiley Publishing, 2000, pp. xii
- [2] K. Mitnick, W. Simon, *The Art of Deception: Controlling the Human Element of Security*, Indianapolis, Indiana: Wiley Publishing, 2002, pp. 330
- [3] C. Jones, “Social Engineering: Understanding and Auditing”, *GSEC Practical Assignment*, February 2004
- [4] G. L. Orgill, G. W. Romney, M. G. Bailey, P. M. Orgill, “The Urgency for Effective User Privacy-education to Counter Social engineering Attacks on Secure Computer Systems”, in *October 2004 Proceedings of the 5th Conference on Information Technology Education*
- [5] R. Gulati, “The Threat of Social Engineering and Your Defense Against It”, *GSEC Practical Assignment*, SANS, 2003
- [6] J. Rusch, “The ‘Social engineering’ of Internet Fraud”, *INET'99 Proceedings*, Retrieved on November 27, 2005 from http://ftp.isoc.org/inet99/proceedings/3g/3g_2.htm
- [7] S. Granger, *Social Engineering Fundamentals, Part I: Hacker Tactics*, Retrieved on November 27, 2005 from <http://www.securityfocus.com/infocus/1527>
- [8] S. Granger, *Social Engineering Fundamentals, Part II: Combat Strategies*, Retrieved on November 27, 2005 from <http://www.securityfocus.com/infocus/1533>

- [9] I. S. Winkler, "Information Security Technology?...Don't Rely on It A Case Study in Social Engineering", *Proceedings of the Fifth USENIX UNIX Security Symposium*, Salt Lake City, UT, June 1995
- [10] R. Lemos, *Mitnick teaches 'social engineering'*, Retrieved on November 24, 2005 from http://news.zdnet.com/2100-9595_22-522261.html
- [11] G. Stevens, "Enhancing Defenses Against Social Engineering", *GSEC Practical Assignment*, SANS, 2000-2002
- [12] A. Dolan, "Social Engineering", *GSEC Practical Assignment*, SANS, February 10, 2004
- [13] W. Arthurs, "A Proactive Defence to Social Engineering", *GSEC Practical Assignment*, SANS, August 2, 2001
- [14] M. Allen, "The Use of 'Social Engineering' as a means of Violating Computer Systems", *GSEC Practical Assignment*, SANS, August 13, 2001
- [15] S. W. Robinson, "Corporate Espionage 101", *GSEC Practical Assignment*, SANS, February 15, 2002
- [16] D. Gragg, "A Multi-Level Defense Against Social Engineering", *GSEC Practical Assignment*, SANS, December 2002
- [17] T. Thornburgh, "Social Engineering: The 'Dark Art'", *October 2004 Proceedings of the 1st Annual Conference on Information Security Curriculum Development*, October 8, 2004
- [18] Definition of "social engineering", Meriam-Webster Online Dictionary, Retrieved from <http://www.webster.com/dictionary/social%20engineering>
- [19] Definition of "social engineering", Jargon File, Retrieved from <http://jargon.watson-net.com/jargon.asp?w=social+engineering>
- [20] "History of the Trojan War", Retrieved from <http://www.stanford.edu/~plomio/history.html>