Social Engineering – The Attempt of Deceive

Matt Guidry & Daniel Gomez
guidry@cs.fsu.edu gomez@cs.fsu.edu

1 INTRODUCTION

Cryptography has come a long way over the past years. Breaking into a server from a remote machine is becoming more and more difficult. System administrators make it so that most systems require strong passwords and will reject weak passwords. Current security measures such as Triple DES and DSA do a good job of maintaining the confidentiality, integrity and availability of a given system. These are all examples of how security methods have been built over the years to protect data. However, an often overlooked flaw in the system is that John Doe can easily bypass these thorough security measures by befriending the secretary at the front desk and asking her for her talented help. Yes, years of security research beaten by a friendly smile.

This devious art is commonly referred to as Social Engineering, or more commonly known as conning. A social engineer is a hacker who uses "physical tactics on legitimate users of a computer system in order to obtain information"[1] he/she needs to gain access to a system. This form of engineering poses a serious threat to the security world specifically because it abuses security's weakest link; the human factor. "Social Engineering is a hacker's clever manipulation of the human willingness to trust"[2]. There are several methods and tactics that are used by social engineers many of which go unnoticed.

The second section of this paper describes the various methods that are commonly used to manipulate a system. In contrast, the third section depicts measures that can be taken to flag these malicious attacks. Conclusively, a few historical attacks will be mentioned and a brief summary will be given.

2 CURRENT METHODS

From a high level perspective the goal of a social engineer is quite simple; he/she simply needs to master the three areas: Identification, Authentication and Authorization (IAA). The IAA is a commonly used test for maintaining the confidentiality, integrity, and availability of a system [3] .

To bypass the first area of the test, Identification, the hacker must attempt to disguise him/herself. There are numerous examples of attempted and achieved impersonations. These usually involve assuming vulnerable or trusted authority characters. The hacker may pose as an actual member of a given organization, a vendor, an IT member or supervisor, a service representative, etc... These roles initiate the trust factor that targets are so susceptible to. A target, a group or individual who is to be attacked, is more likely to comply or assist people depending on who they actually claim to be. In other words, assuming one of the roles mentioned above does not guarantee the hacker will be successful in retrieving unauthorized information. The selected impersonation must be suitable to the attack at hand; if the hacker impersonated a car salesman asking for your credit card number because they needed it for record purposes, this may seem

suspicious. However, the hacker could disguise him/herself as a manager of a store calling to ask for credit card details because of a robbery that happened at that store resulting in numerous credit card numbers stolen. If this person wanted to get some information about your card to see if yours was one of the exposed cards, one might be more inclined to give out the information.

Having picked a suiting role, the hacker must now sell him/herself; they must convince the target they are who they claim to be. This step is called the Authentication Step. The hacker must use various methods to gain information and to play their character as accurately as possible. Becoming familiar with organizational jargon is a useful step. Similarly, learning the lingo of the character; Doctor or IT terminology for example. The hacker could also learn the names of people within the organization and/or the names of other companies that work with the organization. He/she sometimes may use some form of identification that the target is usually not able to readily look up. It is evident, the more the hacker is familiar with the way the target's organization works, the more likely the target is convinced and thus more willing to mentally sign off on their credibility.

Nonetheless, if the target believes the hacker, are they going to comply with the perhaps unlikely request of the hacker? This leads into the last step of the process; Authorization. The social engineer must convince the target they are eligible to the unauthorized information. It is common for the hacker to use a play on emotions to seep into the targets mind and lock their trust with them. The hacker may use the target's pride; simulate an event where them helping advisory boosts their moral and give them a feeling of accomplishment for being able help the hacker. Similarly, if the advisory assumes a position of authority they may inflict fear in the target by threatening them with their job[4].

One tactic that could help to accomplish these three tasks easily is reverse social engineering. Reverse Social Engineering is the tactic where instead of initially asking for help the attacker initially offers the help [5]. The hacker lets the target know that their might be problem in the future and to call them if the problem ever does arise. Then the hacker purposely causes the problem to happen and waits for the victim to call for help. While 'helping' the victim the advisory tries to extract pieces of information that may be useful for future attacks. The advisory is more likely to gain unauthorized access because the victim sees the advisory as a helpful authority. An example of a problem that the advisory could control; say he/she found a network switch they could tamper with to force a network failure, they could then play the role of a network administrator.

In an attempt to bypass the IAA tests, hackers sometimes resort to a another method, psychological convincing. Essentially, the social engineer attempts to cause mental shortcuts in the minds of their target. A tactic to achieve this is referred to as social proof[6]. One instance of social proof is the bandwagon trap. The target is convinced to allow the hacker to bypass usual standards because others seem to have allowed him to as well. Another instance is finding common interests between themselves and the target and in doing so making the individual feel comforted and at ease [7]. Thus, more likely to be helpful in leaking unauthorized information.

3 CURRENT DEFENSES

To properly defend against social engineering attacks it is important that you thoroughly understand your opponent, the attacker. For corporations it is important to understand that sometimes seemingly meaningless information can be a crucial clue to someone looking for it. It is important for employees to share as little information with others as possible when it is not needed.

Once a company or organization has analyzed its important information and how to keep that information safely guarded, it is time to meet with the members that work with that organization to better prepare them to safeguard against these attacks. For instance in World War II the United States government took a very proactive approach to safeguarding information. They displayed posters saying "Loose Lips Sink Ships" a term that gives insight to the era. The US government was afraid of citizens talking about small bits of information that they knew and that information getting into the wrong hands; thus sinking ships. This is the same approach corporations should take with their employees.

Common methods for training employees include making them aware of social engineering constructs. One could also supply them with a model of security procedures, this is especially helpful because it gives them a "credible" reason to deny information or passage. They will have a rulebook that they can site and this will make it more difficult for a social engineer to take advantage of social bullying. Another technique is to limit access to larger or more powerful duties for newer employees. It is important to restrain misuse of vital tools within an organization by ensuring that employees fully understand the power of that tool before they take control over it.

Other important tactic is to train employees to use are the principles of the IAA Test mentioned previously. It is important that employee properly identify unknown persons by asking them for proper identification given the different circumstances where they could encounter these people. Next, it is important that the identification is properly authenticated. If this person supplies some sort of ID badge, it is important that the employee can ensure its validity and that it was not printed out the night before. Also if the unknown person says he is a here to see a manager or some employee, it is important that this fact is properly verified before they are allowed to go on. This leads us to the next part of the test, authorization. Properly authorizing someone is important to the previous tests because social engineers will attempt to find the most difficult disguise to authorize. Such as being the new help desk employee here to help with a computer failure or the janitor that was scheduled for that night at the last second.

4 FAMOUS SOCIAL ENGINEERS

There are a few lists of famous and publicly known social engineers, although it is important to mention that potentially the most dangerous social engineers remain unknown and possibly could still be practicing their deceitful trade. One such person who was eventually caught was Kevin Mitnick. Kevin Mitnick began his career in Los Angeles after he persuaded a friendly bus driver to tell him where he could buy his own ticket punch as a young child. He was then able to ride the public transportation for free by stamping his own tickets. [8] He later led on to a highly successful fraudulent career hacking cell

phones and even some IBM systems. They have since written a movie about his capture and he has released a book The Art of Deception which is widely used as a counter-tool against social engineering. Some of the techniques in this paper are derived from that very book.

Another successful and highly recognized social engineer was Frank Abagnale. Mr. Abagnale did various impersonations beginning with an airline pilot and spanning to positions such as a doctor and an attorney. Surprisingly enough he did not go to college before his exploits! He was just a master at reading people and determining how to say the right things to persuade them to trust him. His exploits were depicted in the popular modern movie Catch Me If You Can.

5 CONCLUSION

It is evident, social engineering is one of the many problematic areas in the field of security. As Kevin Mitnick puts it best, "You could spend a fortune purchasing technology and services...and your network infrastructure could still remain vulnerable to old-fashioned manipulation."[9] Individuals and organizations must familiarize themselves with the various methods social engineers may use. Furthermore, they must learn that divulging bits of information could lead to the attacker forming a greater attack. In lieu of the situation, individuals and organizations must instantiate 'rule books' and/or protocols that secure the confidentiality, integrity and availability of their organization/company [3]. These measures will help to ensure that all of their secret information stays only within the confines of their corporation.

6 REFERENCES

[1] Virus Awareness (June 2009) *"Phishing"* Retrieved on 30 March 2010 <http://www.austincc.edu/hr/profdev/eworkshops/virus/virus7.php>

[2] Peikari, Cyrus & Chuvakin, Anton "*Security Warrior"*, Gravenstein Highway North, Sebastopol CA, O'Reilly Media Inc.

[3] Thornburgh, Tim " *Social Engineering: The "Dark A*rt" "Kennesaw State University, GA.

[4] Mitnick, K & Simon, W (2002) *The art of Deception: Controlling the human element of security*. Indianapolis, Indiana: Wily Publishing, Inc

[5] Meunier, Pascal (March 2007) *"ITaP Presentation: Social* Engineering" Retrieved on 03 April 2010 <http://www.purdue.edu/securepurdue/docs/socialEngineering.pdf>

[6] Buetler, Ivan Compass Security (June 2009) *"Social Engineering Test Cases"* Retrieved on 05 April <http://www.hacking-lab.com/misc/downloads/Social_Engineering_V2.0.pdf>

[7] Rusch, J *The "social engineering" of Internet fraud."* Published on Internet Society. Retrieved March 30th 2010 from <http://www.isoc.org/inet99/proceedings/3g/3g_2.htm>

[8] Greene, Thomas C. (13 January 2003). *"Chapter One: Kevin Mitnick's story"*. The Register. Retrieved on April 10 2010 <http://www.theregister.co.uk/2003/01/13/chapter_one_kevin_mitnicks_story/>

[9] Granger, Sarah (December 2001) "*Social Engineering Fundamentals, Part I: Hacker Tactics"* Retrieved on 01 April 2010 <http://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics>

[10] McDowell, Mindi "*Avoiding Social Engineering and Phishing Attacks"* US-CERT. Retrieved on 31 March 2010 from <http://www.us-cert.gov/cas/tips/ST04-014.html>

[11] David Gragg (December 2002) *"A multi-Level Defense Against Social Engineering"* SANS Institute. Retrieved on 01 April 2010 from <http://www.sans.org/reading_room/whitepapers/engineering/multi-level-defense-social-engineering_920>

[12] CNN (October 13th 2005) "*A convicted hacker debunks some myths"* CNN Website. Retrieved on 02 April 2010 <http://www.cnn.com/2005/TECH/internet/10/07/kevin.mitnick.cnna/>

[13] National Consumers League, Press Release, (Feb. 10, 1998) *"NCL Releases Top Ten Internet Scams,"* Retrieved on April 06 2010 <http://www.natlconsumersleague.org/top10net.htm>