Social Engineering: The “Dark Art”

Tim Thornburgh
Kennesaw State University
Department of Computer Science and Information Systems
1000 Chastain Road, MS 1101
Kennesaw, GA 30144
+1 770-423-6005
tat6214@students.kennesaw.edu

ABSTRACT

The key to maintaining the confidentiality, integrity, and availability of an organizations information and information systems is controlling who accesses what information. This is accomplished by being able to identify the requestor, verifying the requestor is not an impostor, and ensuring that the requestor has the proper level of clearance to access a given resource. There have always been those that attempt to by-pass this security mechanism through brute force or guile. In the past, those who use guile have been called confidence men and con artists. Today, these people are called social engineers, but the tactics remain the same even if the objectives have changed.

Categories and Subject Descriptors

C.2.0 [**Computer Communications Networks**]: General – *Security and protection*
K.4.1, .2 & .4 [**Computers And Society**] - .1 Public Policy Issues - *Abuse and crime involving computers, Computer-related health issues, Ethics, Intellectual property rights, Privacy. .2 -* Social Issues - *Abuse and crime involving computers.* .4 Electronic Commerce - *Security*
K.6.5 [**Management Of Computing And Information Systems]** - Security and Protection – *Authentication, Invasive software, Unauthorized access.*

General Terms

Management, Security, Human Factors.

Keywords

Information Security, Information Assurance, Social Engineering.

INTRODUCTION

The security of this intellectual property and the systems that contain it from unwanted access relies on a three step process—identification, authentication, and authorization (IAA). Identification asks the question, “do I know you?” Authentication asks the question, “are you who you say you are?” And authorization asks, “are you supposed to be here?” If this process is subjugated or by-passed, the confidentiality of the information or information system is compromised and the integrity and availability of the system is subject to compromise as well. Those who attempt to by-pass IAA use misrepresentation of themselves and their situations as well as the emotions of their victims to accomplish their goal and are the topic of this paper.

THE “DARK ART”

Throughout history, humans have sought to secure themselves against all types of threats to their well being and their property. Our prehistoric ancestors had to worry about predators (including same-species predators), disease, and the weather. Today, we only have to worry about predators, disease and the weather. That is not to say that technological advances over the years, especially the last 20 years, have not allowed us to mitigate the impact of many of the specific threats we face. Advanced weather satellites and computer-aided prediction models certainly give us some advanced warning and time for preparation. Modern medicine has extended our life expectancy. Yet, the more we advance, the more threatening we become to ourselves. The jawbone of an ass really pales in comparison to surface-to-air missiles not to mention nuclear warheads. Destruction aside, we also seek to protect ourselves from the theft of our belongings and trespass on our property. Our concept of property has changed as well: in the past two hundred years we have expanded realm of property rights to include not only land and the possessions thereon, but also to our ideas, our artistic works, and our information.

Access control, whether physical (such as a guardhouse with personnel lists, challenges, and passwords) or digital (using login, password, and access lists), is still limited in its effectiveness by individuals and the degree to which they can be persuaded to circumvent standard operating procedures. In the military, stories abound of privates (the lowest ranking members and typically the ones placed on guard duty) who admit unauthorized personnel of high rank without the proper authentication (password) because they fear reprisals. For the stories that are true, the result for the private was much worse than the reprisal they feared.

InfoSecCD Conference'04, October 8, 2004, Kennesaw, GA, USA.
Copyright 2005 ACM 1-59593-048-5/04/0010…$5.00.

THE “DARK ART” DEFINED

The term “social engineering” (SE) has gained wide acceptance in the Information Technology (IT) and Information Systems (IS) communities as a social/psychological process by which an individual can gain information from an individual about a targeted organization. This information may be used immediately to by-pass IAA or as part of a further SE event. For example, someone calls claiming to be from computer support and says, “Hey, this Chuck from support and we need to check the network’s connectivity. What’s your login and password?” While this is an extreme exaggeration, but the basic framework is set: “Hi, I’m someone you should trust and I sound like I know what I’m talking about and I’m working on something you probably do not understand. For those reasons, I need you to give me a piece of information that you normally wouldn’t give to a stranger, but hey, I’m legit.” Social engineers are not hackers by definition, but hacker-enablers. With regard to information systems, the ultimate goal of the social engineer is to gain direct access (either physical or digital) to an organization’s information or information system. This is roughly the equivalent to trespassing and, perhaps, even breaking and entering depending on the methods used. The social engineer can then enable a hacker to penetrate the system in order extract, corrupt, or delete information as well as disrupt services. Of course, the social engineer may be the hacker as well.

The profile of a SE attack is much like the software development life cycle (SDLC) and Mitnick identifies 4 distinct stages of “The Social Engineering Cycle:” research, developing rapport and trust, exploiting trust, and utilizing information [1]. A single cycle may produce only one piece of information that is then added to the research for the next cycle. The process continues until the ultimate objective is reached. Research consists of gathering as much information about the organization as possible. Anything that might describe the organizational structure, financial strength, current business plans or marketing campaigns is of use to the social engineer and much of this information is available on the organization’s web-site. Mitnick includes Dumpster diving as a research tool and not a SE attack type [2]. Erlanger and Granger also include Dumpster diving in their discussions of SE [3,4]. Manske submits that both shoulder surfing and Dumpster diving are types of SE attacks, but in both situations, there is no social interaction or persuasion involved [5]. The fact that useful information can be found in an organization’s trash is an indicator of poor operations security, not SE. Shoulder surfing falls in line with pick pocketing or theft.

In a common ploy for developing rapport and trust, the social engineer will make contact via telephone posing as another member of the organization, a service provided, vendor, or customer. Then, she will use name-dropping of verifiable employees or organizational jargon to lull the victim into believing the caller is, indeed, who she says she is. If e-mail is the medium of attack, the social engineer combines identification and authentication by composing official-looking correspondence from another organization with which the victim does business. Often, the counterfeit correspondence is nearly indistinguishable from that of the actual organization. Once the social engineer has established herself as authentic, she will exploit trust by weaving a story that plays upon the emotions of the victim and leads to a request for information, action, or both. Strong emotions such as fear, empathy, or greed along with the belief that the attacker is authentic often compel the victim to make a “judgement call” that results in fulfilling the attacker’s request. Utilizing the information means that the attacker can either implement the technical attack or penetration or use the new information as research for the next SE attack. User names, network architecture, and applications that run on specific servers are a few of the more technical details that social engineers seek. More mundane information about the systems “wetware” (that is, the people who use the system) can also be useful to the social engineer: the names of children, spouses, and pets are often the ill-selected passwords of less security savvy computer users. Knowing when a person is away on vacation can also prove valuable.

SPELLS, CHARMS, AND POTIONS

Individuals can be persuaded to act either through sound analytical processing of the facts or through emotions and Rusch refers to these paths as the “central route to persuasion” and “peripheral route to persuasion,” respectively [6]. Because the social engineer’s entire approach is based on misrepresentation and dissembling, the central route is really not an option. In order for a SE attack to succeed, the targeted person must feel compelled to proffer the information requested and this feeling must elicit strong enough emotions in the target to make them willing to forego established procedures or their “gut” instinct. Rusch refers to the reaction by the target as a “mental shortcut;” meaning that the exploited person knows better, but has been able to justify their actions to themselves [7]. Several factors are employed to evoke these strong emotions, but the most common are authority and empathy. Authority represents the power to reward or punish and the emotions evoked could be pride, fear or even greed. Everyone has been new to an organization at least once and may have felt disoriented, confused, or helpless. Knowing this, the social engineer seeks to solicit empathy from the victim to spark these strong feelings. Mitnick gives some examples of the methods used by social engineers [8]:

- Posing as someone in authority
- Posing as a new employee requesting help
- Offering help if a problem occurs, then making the problem occur, thereby manipulating the victim to call them for help
- Using insider lingo and terminology to gain trust

THE IMPACT OF SOCIAL ENGINEERING

A single event in which a social engineer gets what she wants can be considered as a successful attach even if the information, on its own, is not sufficient for the attacker to perform a penetration of the targeted organization. Every bit of information gathered by the attacker increases the possibility of a successful penetration. The impact of successful SE attacks varies widely. In instances where the information gained cannot augment a further attack or where subsequent attacks have been stifled, the impact is minimal or even non-existent. A successful attack that has been discovered may still lead to a system penetration, but with effective incident response, subsequent attacks may be prevented. The attack that has not been detected can be very dangerous especially depending on the information being sought. Since SE is cyclical in nature, the social engineer can repeatedly use an individual to penetrate a system over and again for different goals. For this reason, social engineers take care not to "burn" their sources. That is, they remain anonymous and cover their trails as best they can to prevent detection.

While the effects above pertain more to SE attacks, it bears stating that the penetration attacks resulting from the knowledge gained in a SE attack can make a serious impact. Manske offers [9]:

> Successful social engineering attacks give the attacker the means to bypass millions of dollars invested in technical and nontechnical [sic] protection mechanisms and consulting, completely nullifying security investment, Firewalls, secure routers, PKI, e-mail…and security guards are all down the drain.

DEFENSE AGAINST THE DARK ARTS

A multi-faceted approach must be employed to secure an organization against successful SE attacks using policy, procedures, training, awareness programs, and incident response plans. Well-defined policy should establish an information classification system that clearly defines not only what information can be disclosed but also to whom and by whom. The previous implies that the organization also assign a security clearance level to individuals both inside and outside of the institution. Policy takes decision-making out of the hands of the employee and gives them justification for not "helping out." Education on what information a social engineer can use, how he gains it, and how it can be used is very important, especially for the non-technical (read "most") employees of an organization. Training on how to recognize and react to a SE attack empowers employees and removes doubt. Mitnick also gives tips on recognizing a SE attack [10]:

- Refusal to give a callback number
- Out-of-ordinary request
- Claim of authority
- Stresses urgency
- Threatens negative consequences of noncompliance
- Show discomfort when questioned
- Name dropping

The development of effective awareness campaigns help to "jog" the memory of the employees. During World War II, the United States government undertook an awareness campaign to aid in operations security. "Loose Lips Sink Ships" was the slogan on one of the awareness posters. While very simple, it accurately conveys the importance of not openly discussing information of a sensitive nature because of the potential disastrous results. Whitman and Mattord identify four factors for a poster campaign: vary the content of each poster and keep them current, do not make the posters overly elaborate while keeping them eye-catching, the message should be concise and easy to understand, and information on who to contact if a violation is observed [11]. Posters alone are not enough, however, bulletins or newsletters, web sites, and "awareness days" should also be developed to keep the members of an organization constantly informed and focused on security. Employees are at a distinct disadvantage because their exposure to SE is infrequent and without constant vigilance they may facilitate a successful attack. The social engineers, on the other hand, practice their trade daily.

CONCLUSION

Social engineering, by any name, has existed in many forms throughout history and will continue to exist because it relies on human nature. Because of this, organizations and individuals alike must arm themselves with the knowledge of what information can be used, how information divulged could precipitate further attacks or actual compromise of their systems, how the attacker develops the attack, and in what forms the attack may appear. In reaction to that knowledge, policy, procedures, training, and response plans must be formulated to address both the general threat and the specific delivery methods of attack. And finally, because the threat will not abate, organizations must maintain constant vigilance through the implementation of effective awareness programs that keep security from SE at the forefront of its employees' minds.

REFERENCES

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

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

[3] Erianger, L. (2004) The weakest link. *PC Magazine, 23, 58-59*. Retrieved June 13, 2004 from EBSCOhost database.

[4] Granger, S. (2001, December 18) Social engineering fundamentals, part I: Hacker tactics. Retrieved June15, 2004 from http://www.securityfocus.com/infocus/1527

[5] Manske, K. (November 2000) An introduction to social engineering. *Information Systems Security 9, 53-59*. Retrieved June 7, 2004 from GALILEO: Computer Source database.

[6] Rusch, J. (1999, June 24) *The "social engineering" of Internet fraud*. Paper presented at the 1999 Internet Society's INET'99 conference. Retrieved June 6, 2004 from http://www.isoc.org/isoc/ conferences/inet/99/ proceedings/3g/3g_2.htm

[7] Rusch, J. (1999, June 24) *The "social engineering" of Internet fraud*. Paper presented at the 1999 Internet Society's INET'99 conference. Retrieved June 6, 2004 from http://www.isoc.org/isoc/ conferences/inet/99/ proceedings/3g/3g_2.htm

[8] Mitnick, K. & Simon, W. (2002) *The art of deception: Controlling the human element of security*. Indianapolis, Indiana: Wiley Publishing, Inc. p. 332.

[9] Manske, K. (November 2000) An introduction to social engineering. *Information Systems Security 9, 53-59*. Retrieved June 7, 2004 from GALILEO: Computer Source database.

[10] Mitnick, K. & Simon, W. (2002) *The art of deception: Controlling the human element of security*. Indianapolis, Indiana: Wiley Publishing, Inc. p. 333.

[11] Whitman, M. & Mattord, H. (2004). *Management of information security*. Boston: Thomson Course Technology.