Chapter XXIV
Social Engineering

Michael Aiello
Polytechnic University, USA

ABSTRACT

Traditionally, "social engineering" is a term describing "efforts to systematically manage popular attitudes and social behavior on a large scale" (Wikipedia, 2006). In this context, the practice of social engineering is the application of perception management techniques to a large populous. As it relates to terrorism, social engineering is a tool used by terrorists whose actions are intended to cause the loss of confidence in a social institution's ability to protect the security of its citizens and assets.

INTRODUCTION

Traditionally, "social engineering" is a term describing "efforts to systematically manage popular attitudes and social behavior on a large scale" (Wikipedia, 2006). In this context, the practice of social engineering is the application of perception management techniques to a large populous. As it relates to terrorism, social engineering is a tool used by terrorists whose actions are intended to cause the loss of confidence in a social institution's ability to protect the security of its citizens and assets.

In the context of cyber security, social engineering is the process of manipulating individuals to perform actions or reveal privileged information that benefits the engineering party. This is usually accomplished by forming a trust with a victim and later transitioning their psychological state to one which renders them more vulnerable to the attacker's instruction. In the simplest case, an attacker may call an employee of an organization, claim to be a help-desk technician, and ask the user to reveal password information for maintenance purposes. However, social engineering attacks take place over many mediums and are not limited to persuasive phone calls.

SOCIAL ENGINEERING

The practice of social engineering as a method to exploit computer systems was popularized by Mitnick, a cracker turned security professional, describes his techniques in *The Art of Deception* (Mitnick, 2002). Mitnick used these techniques to successfully convince several technology organizations to release proprietary source code, which he then used to exploit systems.

On a large scale, it is difficult to describe the threat of social engineering attacks. This is due to its broad definition, the complexity of the attacks in which social engineering is used, and the general difficulty of producing statistics on "hacking events." However, examples of social engineering vulnerabilities and attacks on government systems have been made public.

1. In a March 15, 2005, U.S. Treasury report, it was shown that out of 100 employees auditors were "able to convince 35 managers and employees to provide their username and to change their password." This figure is "about a 50 percent improvement over the previous test conducted in 2001" (United States Department of Treasury, 2005).
2. In early 2006, after a recent image-handling exploit was released for the Microsoft Windows operating system, attackers attempted to send UK government e-mail addresses malicious software that would enable them "to see classified government passwords." "The attack occurred on the morning of 2 January, before Microsoft's official patch was available. The hackers tried to send e-mails that used a social-engineering technique to lure users into opening an attachment containing the WMF/Setabortproc Trojan" (Espiner, 2006).

Furthermore, Mitnick (2002) claims that "companies that conduct security penetration tests report that their attempts to break into client company computer systems by social engineering methods are nearly 100 percent successful" (p. 245).

TYPES OF SOCIAL ENGINEERING

In *A Proactive Defense to Social Engineering*, Arthurs (2001) breaks social engineering down into two main attack avenues: human based and computer based. In human-based attacks, attackers directly interact with their victims (in person, by phone, via e-mail, snail mail, etc.) and persuade them to comply with their requests. In computer-based attacks, computer systems persuade victims to reveal information or perform actions. E-mail phishing, for example, is a computer-based social engineering attack, where attackers send e-mail messages to victims, claiming to be another trusted entity and direct them to submit their authorization credentials or install software.

THE SOCIAL ENGINEERING PROCESS

Social engineering attacks tend to follow a simple process that contains three broad steps: information gathering, relationship establishment, and social exploitation.

In the information gathering step, the social engineer will mine public intelligence sources for information. This includes organization Web sites, quarterly reports, newsgroup postings, publicly available legal documents, vendor advertisements, and other public descriptions of the people, operations, and systems that the organization houses. The goal of the information gathering step is to heighten the attacker's ability to be able to give the impression that the he or she is part of the victim organization. The successfulness of this step is directly proportional to the amount of publicly availability information pertaining to the victim organization (i.e., acronyms, organizational charts, and other organization specific information).

In the relationship establishment step, social engineers feign a relationship with the victim. The depth and nature of this attempted relationship is dependent on the type of attack. This step can vary from a simple statement in which the attacker claims to be a technician