Chapter XXIII
Social Engineering

B. Bhagyavati
DeSales University, USA

ABSTRACT

This chapter will present a detailed view of social engineering and why it is important for users to beware of hackers using this technique. What social engineering is, what techniques can be employed by social engineers and what kinds of information can be gathered by these techniques will form the core of the chapter. We will also present case studies of notorious social engineers such as Kevin Mitnick. Different modes of social engineering attacks will be described. Such attacks could occur in person, via the telephone, or via the Internet. An in-depth presentation of the consequences of a successful social engineering attack will be presented. A series of steps users can take in order to avoid becoming a victim of the social engineer are explored, along with examples. We will also present strategies for training employees and users so that there is minimal risk of a successful social engineering attack. Finally, we caution against ignoring the training and awareness program for front-line employees such as secretaries. Since social engineers often try to bypass front-line employees, there is a critical need to train front-liners to recognize and repel such attacks.

INTRODUCTION

Social engineering is the process by which one gets others to do one's wishes. It is the term used to describe techniques and methods used by people who wish to indirectly obtain sensitive information (usually) without having legal access to the information. These people are referred to as social engineers, and they typically induce other people with legitimate access to information to divulge it to them. In political science, the term social engineering refers to a concept that involves methods used by governments or individuals to manage the social behavior of people on a large scale, as in a society (*Wikipedia,* 2006a).

In the realm of computer security, the term social engineering is used to describe the malicious intent of

people who are trying to gain access to sensitive data and information through illegal means. The process of obtaining information through social engineering techniques implies a lack of technical skills but places a strong emphasis on social skills. However, a skilled social engineer can spend a lot of time gathering publicly available information about the targeted data and talking to eventual victims before directly requesting access to the desired information.

Harl (1997) says of social engineering: "Like hacking, most of the work is in the preparation, rather than the attempt itself". For example, a social engineer may gain knowledge of an organization's chain of command and hierarchical structure by studying internal documents of the organization through dumpster diving or other means. By means of a telephone call, the social engineer may then determine that the employee's supervisor is out of town and not easily reachable. Finally, the social engineer may pose as a guest of the supervisor and ask a particular employee for sensitive information, knowing that the employee's supervisor is currently not reachable for verification of the social engineer's identity.

BACKGROUND

Human beings manage computers and information systems, and they are vulnerable to social engineering attack techniques. People can be persuaded by skilled social engineers to divulge confidential information even against their better judgment. This weakness is universal among human beings and does not depend on the platform, operating system, hardware, software, or type of equipment that the information system uses. Social engineering is, therefore, a powerful tool in the cyber terrorist's arsenal, and defenders would do well to consider countermeasures against social engineering attacks.

According to Harl (1997), even people who are not considered as part of the security policy may unknowingly contribute to increasing a social engineer's knowledge of the overall organization's policies and procedures; a skilled social engineer can then cause a security breach and losses to the organization by exploiting such sources that are traditionally outside the security-policy loop. Therefore, training and awareness must be addressed as critical challenges in defending against social engineering attacks. Any human being who has knowledge of the physical and/or electronic set up of the information system should be considered as an attractive target for potential social engineers.

The techniques used by social engineers can vary depending on several factors, such as the response time required, preparation time needed, the circumstances of the attack, the awareness (or lack thereof) among the people who manage the data, and the sensitivity of the information. Social engineering attacks typically use a combination of methods, such as the desire to trust and the helpfulness of the victims; use of publicly available information; informed guesses about or actual knowledge of internal processes; and the use of authority or any other ruse to gain the reluctant victims' cooperation. If social engineers are skilled, they often have the technical knowledge to gain access to part of the system and need other people's knowledge and access for the remainder of the system.

Generally, social engineers use several miniattacks and integrate knowledge gained from these seemingly innocuous requests for information into a large pool of sensitive data and reach their goal of compromising the organization. As Dolan (2004) states, "Social engineering is all about taking advantage of others to gather information and infiltrate an attack". In today's post-Sept. 11, 2001, world, social engineering can be part of a well-orchestrated cyber attack that is timed to cause panic in conjunction with a physical attack on critical infrastructure and facilities, such as utilities, water supplies, and energy systems. The need to be aware of and guard against social engineering tactics is compelling in light of the interconnectivity between current systems.

The *Wikipedia* (2006) encyclopedia defines social engineering as "the practice of obtaining confidential information by manipulation of legitimate users".