The following paper was originally published in the
Proceedings of the Fifth USENIX UNIX Security Symposium
Salt Lake City, Utah, June 1995.

Information Security Technology?...Don’t Rely on It
A Case Study in Social Engineering

Ira S. Winkler and Brian Dealy
Science Applications International Corporation

Information Security Technology?...Don't Rely on It
A Case Study in Social Engineering

Ira S. Winkler
Brian Dealy
Science Applications International Corporation
200 Harry S Truman Parkway
Annapolis, Maryland 21401

Author Contact Information

Ira S. Winkler
E-mail: winkler@c3i.saic.com
Telephone: (301) 261-8424
Fax: (301) 261-8427

Brian Dealy
E-mail: bdealy@c3i.saic.com
Telephone: (301) 261-8424
Fax: (301) 261-8427

ABSTRACT

Many companies spend hundreds of thousands of dollars to ensure corporate computer security. The security protects company secrets, assists in compliance with federal laws, and enforces privacy of company clients. Unfortunately, even the best security mechanisms can be bypassed through Social Engineering. Social Engineering uses very low cost and low technology means to overcome impediments posed by information security measures. This paper details a Social Engineering attack performed against a company with their permission. The attack yielded sensitive company information and numerous user passwords, from many areas within the company, giving the attackers the ability to cripple the company despite extremely good technical information security measures. The results would have been similar with almost any other company. The paper concludes with recommendations for minimizing the Social Engineering threat.

1.0 INTRODUCTION

There are millions of dollars spent on both Information Security measures and research and development in this area. These measures are designed to prevent unauthorized people from gaining access to computer systems, as well as preventing authorized users from gaining additional privileges. The proper technical security measures can effectively combat almost any technical threat posed by an outsider. Unfortunately, the most serious attack may not be technical in nature.

Social Engineering is the term the hacker community associates with the process of using social interactions to obtain information about a "victim's" computer system. In many cases, a hacker will randomly call a company and ask people for their passwords. In more elaborate circumstances, a hacker may go through the garbage or pose as a security guard to obtain critical information. A recent edition of 2600: The Hacker's Quarterly detailed methods for obtaining a job as a janitor within a company (Voyager, 1994). While these methods appear to be ridiculous, and possibly even comical, they are extremely effective. Social Engineering provides hackers with efficient short cuts, and in many cases facilitates attacks that would not be possible through other means. For example, the Masters of Deception, who significantly penetrated the United States' telecommunications system, were only able to do so after obtaining information found in the garbage of the New York Telephone Company (Slatalla & Quittner, 1995).

The case study described in this paper does not represent a single operation. To protect the authors' clients, the case study represents a compilation of several real attacks against large financial institutions. These attacks were conducted as part of a comprehensive vulnerability analysis for the organizations. While the corporate officers were aware of a potential attack, the remainder of the companies' employees were not. Everything described in the case study has occurred on multiple occassions.

The "attackers" were restricted to gathering information over the telephone, and were specifically instructed not to exploit the system with the information. The attack was limited to four man-days of effort, requiring the attackers to be more "bold" than is normally required. A real Social Engineering attack would be accomplished over weeks, if not months. Since the potential reward for an attacker would be very great, a real attack would have included several physical visits to the company's offices and possibly even obtaining a job at the company.

2.0 THE ATTACK

Initially, the attackers performed a search on Internet library resources to obtain an initial perspective on the organization. Miscellaneous databases, revealed the names of numerous company employees and officials. A search of a local telephone directory provided the telephone number of a company office in the vicinity of the attackers. A call to the office obtained a copy of the company's annual report as well as the company's toll free telephone number. No justification was needed to obtain this information.

Combining the data from the annual report with the data that was obtained from the Internet provided the attackers with names and positions of many senior officials, along with information on the projects they are working on. The next logical step was to obtain a corporate telephone directory, which revealed the names of additional employees and a comprehensive view of the company's corporate structure.

Using the toll free telephone number, a call was placed to the main telephone number to contact the Mail Room. The caller stated that they were a new employee and needed to know what information was required to ship packages both within the United States and abroad. It was learned that there were generally two numbers required to perform a transaction within the company; an Employee Number and a Cost Center Number. A call to obtain similar information from the Graphics department confirmed the importance of the numbers.

The attackers determined which executive they knew the most about. Calling through the main telephone number, the executive's secretary was contacted by an attacker claiming to be from the company's Public Relations Department. Within a series of basic and harmless questions about the executive's background, the attacker asked for, and obtained, the executive's Employee Number. A later call to the secretary, by another attacker, obtained the Cost Center of the executive through the impersonation of an auditor confirming appropriate computer charging.

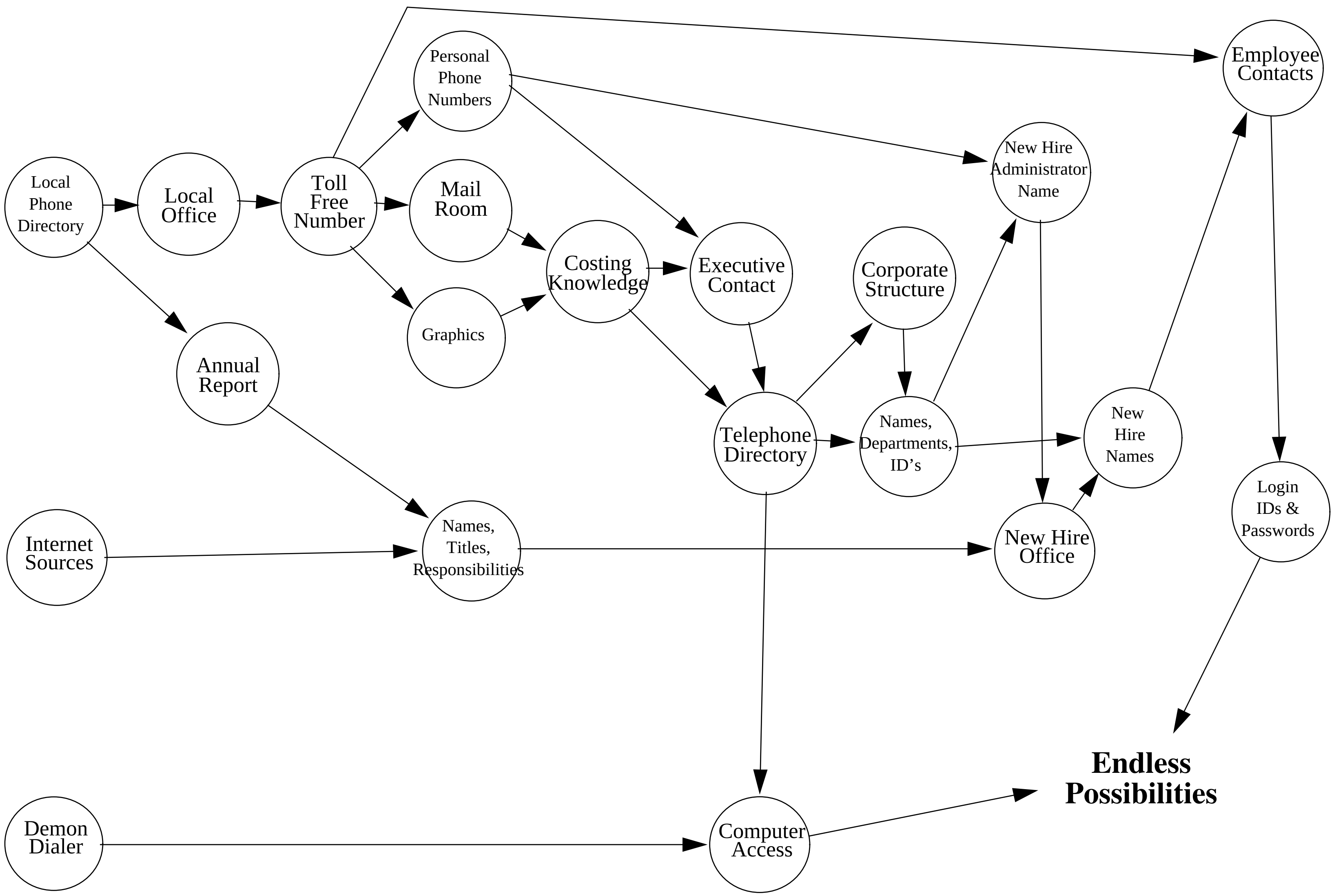
Another call, through the main telephone number, connected the attackers with the department responsible for distributing corporate telephone directories. By impersonating the executive, it was requested that a telephone directory be sent to a "subcontractor". The executive's Employee Number and Cost Center were provided, and the directory was shipped via overnight courier to the subcontractor.

Using the telephone directory, the attackers contacted dozens of employees in various departments to obtain additional Employee Numbers that could be used for additional attacks. The numbers were usually obtained by impersonating a Human Resources employee who accidentally contacted the wrong employee, and needed the employees Employee Number to clear up the "confusion".

The attackers then determined that they would attempt to obtain the names of new employees, who were probably least aware of any threats to the company. Using the information obtained from the initial phase of the attack, the name of a very senior company executive was identified. The telephone directory revealed the name of an employee who most likely worked for the executive. At this time it was determined that the best method to obtain the names of the new employees was to claim that the executive wanted to personally welcome new employees to the company. The attacker would claim to work for the executive, and that the executive was extremely upset, because the information was overdue.

As luck would have it, an initial call to the New Hire Administration Office was answered by an answering machine. The message on the machine revealed: 1) the office had moved, 2) the name of the person assigned to the telephone number, and 3) the new telephone number. The name of the person was critical, because knowledge of a specific name increases the legitimacy of the caller. It was late in the day and the specific person had left. This allowed the attacker to indicate that the absent person usually provides the information. The attacker also claimed that a very prominent executive was extremely upset. The "pleas" of the attacker encouraged the person that answered the telephone to provide the requested information. The names of all of the employees that began employment during the current week were obtained, along with the departments of many of the employees.

It was then determined that the attackers should avoid contacting Information Systems employees, because they were more likely to be aware of the importance of protecting passwords. The attackers impersonated an Information Systems employee and contacted the new hires under the guise of providing new employees with a telephone "Computer Security Awareness Briefing". During the briefing, the attacker obtained "basic" information, including the types of computer systems used, the software applications used, the Employee Number, the employee's computer ID, and the password. In one case, the attacker suggested that the new



Anatomy of an Attack

Figure 1.

employee change their password, because it was easy to guess.

A Demon Dialer and a call to the Information Systems Help Desk obtained the telephone numbers of the company's modems. The modem numbers provided the attackers with the capability to exploit the compromised user accounts. Obtaining the modem information effectively circumvented a very sophisticated Firewall system and rendered it useless. During a later attack, the attackers used similar methods to have the company provide them with their own computer account. The attackers also were able to convince company employees to send them communications software that accessed a "secure" connection.

3.0 LESSONS LEARNED

Despite strong security measures, the attackers were extremely successful in a very short period of time. While the attack might have seemed very complicated and time consuming, it was accomplished in less than three days and cost very little. Many of the weaknesses exploited by the attackers are common to most companies. Expanding upon these weaknesses will assist companies in overcoming many weaknesses posed by Social Engineers.

3.1 Do Not Rely Upon Common Internal Identifiers

The attackers were occasionally asked to authenticate themselves as real employees by providing their Employee Numbers. Fortunately for the attackers, the Employee Numbers were used commonly and were easily obtained from real employees. The attackers had a list of Employee Numbers, and were ready for any challenge. Many companies rely upon similar identifiers. Companies should have a separate identifier for their computer support activities. Having a separate identifier for computer related activities would separate personnel functions from support functions and provide additional security to both personnel and computer activities.

3.2 Implement a Call Back Procedure When Disclosing Protected Information

Many of the attacks could have been prevented if the company employees verified the callers identity by calling them back at their proper telephone number, as listed in the company telephone directory. This procedure creates a minimal inconvenience to legitimate activities, however when compared to the scope of the potential losses, the inconvenience is greatly justified. If employees are required to call back anyone asking for personal or proprietary information, compromises of all natures will be minimized. Caller ID services might also be acceptable for this purpose.

3.3 Implement a Security Awareness Program

While giving out your password to a stranger might seem ridiculous to the reader of this paper, it seems innocuous to many computer users. Companies spend millions of dollars acquiring state of the art hardware and software security devices, yet a general awareness program is ignored. Computer professionals cannot assume that basic security practices are basic to non-computer professionals. A good security awareness program can be implemented for minimal cost and can save a company millions of dollars of losses.

3.4 Identify Direct Computer Support Analysts

Every employee of a company must be personally familiar with a computer analyst. There should be one analyst for no more than 60 users. The analysts should be a focal point for all computer support, and should be the only people to directly contact users. Users should be instructed to immediately contact their analyst, if they are contacted by someone else claiming to be from computer support.

3.5 Create a Security Alert System

During the attacks, the attackers realized that even if they were detected, there did not seem to be a way for a employee to alert other employees of a possible attack. This indicates that even if there was a compromise in the attack, the attack could continue with minimal changes. Essentially, a compromise would have only improved the attack, because the attackers would have learned what does not work.

3.6 Social Engineering to Test Security Policies

Social Engineering is the only conceivable method for testing security policies and their effectiveness. While many security assessments test the physical and electronical vulnerabilities, few vulnerability analyses study the human vulnerabilities inherint in users. It must be noted that only qulaified and trust worthy people should perform these attacks. The above attack was accomplished by people trained within the U.S. Intelligence Community who were very familiar with computer security measures and countermeasures.

4.0 CONCLUSION

Even the best technical mechanisms could not have prevented the attack. Only the use of one time password mechanisms could have minimized the effects of the Social Engineering attacks. The attackers exploited poor security awareness, from both a information and operational security perspective. Even if the attackers were unable to "obtain" computer passwords, they successfully obtained sensitive personal and company information.

A Social Engineering attack reveals vulnerabilities in security policies and awareness that cannot be detected through other means. In general, Social Engineering attacks will uncover similar problems in many organizations. However, each attack will yield problems that are specific to the organization being examined. It is for this reason that every threat assessment should include a thorough Social Engineering effort performed by qualified and trusted individuals.

Security officers must consider the non-technical aspects of computer security along with technical measures. All too often computer professionals believe that basic computer security principles are known to everyone. That is a dangerous assumption, and is all too often very incorrect. There must be a comprehensive program of ensuring information security, which includes a continual security awareness program.

BIBILIOGRAPHY

Slatalla, M. and J. Quittner (1995), *Masters of Deception: The Gang that Ruled Cyberspace*, New York: HarperCollins, 1995.

Voyager (1994), Janitor Privileges, *2600: The Hacker's Quarterly,* 11(4).