The Non-Technical Threat to Computing Systems

Ira S. Winkler

Science Applications International Corporation

ABSTRACT: Many companies spend millions 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. Introduction

Typically, many organizations have information that has value that justifies expensive protection mechanisms. Critical information may include patient records, corporate financial data, electronic funds transfers, access to financial assets, and personal information about clients or employees. The compromise of critical information can have serious consequences, including the loss of customers, criminal actions being brought against corporate executives, civil law cases against the organization, loss of funds, loss of trust in the organization, and the collapse of the organization. To respond to the threats, organizations implement Information Security Plans to establish control of information assets.

Information Security Plans specify protection mechanisms for organizational information. There is usually a heavy reliance upon technical security mechanisms, such as firewalls, user passwords, closed networks, and operating system protection mechanisms. There is usually a discussion about physical protection mechanisms and other operational security issues. There appears to be a belief within the computer and information security profession that everyone understands the Operational Security requirements for protecting information. For this reason, most funding for Information Security is funneled to technical mechanisms, and little, if any, funding is designated for security awareness and operational security training. Unfortunately within non-Defense related organizations, the assumptions about the level of security awareness of the organization's employees are incorrect.

The disclosure of information through non-technical means can and will occur. This type of disclosure can bypass millions of dollars of technical protection mechanisms. In many cases, if an impending attacker wants to gain access to a computer system, all they have to do is ask for it. While this might seem ridiculous, the author's personal experiences in performing vulnerability analyses for large, commercial organizations confirms that many people with computer access do not understand the value of the information to which they have access. Users have disclosed a variety of sensitive information, including the names of employees, organizational costing information, telephone numbers to organizational modems, and customer data. Surprisingly, user identifiers and passwords are

extremely easy to obtain. Combined with the telephone numbers of the modems, the passwords give the attackers access to all corporate information when combined with other technical intrusion methods. This paper assumes that the reader is aware of the devastating results that can occur if an attacker gains unauthorized access to an information system. The case study demonstrates how easily unauthorized access can be obtained.

2. *What is Social Engineering?*

Social Engineering is the term that hackers give to acquiring information about computer systems through non-technical means. Hackers usually consider Social Engineering to be calling people up within a targeted organization and asking them for information. The hackers usually use a variety of ruses to obtain information. Hackers may claim to be from the computer support staff and state that they need a user's password to correct a problem with the computer system. To the reader, Social Engineering might seem like a fancy word for lying. It is. It is also extremely effective.

Another type of Social Engineering involves obtaining a job at the targeted organization. By obtaining a job at the organization, an attacker might be given access to the information that they desire. Even if they are not given direct access to the information, they can possibly learn enough information to get additional access. A job as a janitor can be extremely valuable to a hacker. For example, a janitor is usually given access to areas of a building to which an average employee does not have access. Janitors can take their time to go through the garbage to obtain potentially valuable information. Additionally, janitors have the opportunity to go through a person's desk or belongings after they leave for the day. A recent edition of *2600: The Hacker's Quarterly* includes an article on how to obtain a *job* as a janitor [Voyager 1994].

Social Engineering attacks may also involve going through trash dumpsters. The term for going through trash dumpsters is "dumpster diving." Again, the tactic may seem to be almost comical, however it does provide very valuable information. It is well known that in the Defense Community there are classified materials destruction procedures. Burn bags and shredders are common throughout the U.S. Government, yet almost unheard of in private industry. The Masters of Deception, who compromised the U.S. telecommunications system to the point where they could have brought it down, were only able to do so after they obtained system passwords from the garbage of the New York Telephone Company [Slatalla & Quittner 1995].

There are other forms of Social Engineering that include criminal actions. There have been several cases cited that show that former Intelligence Operatives are now engaging in industrial espionage. These operatives are hired by foreign companies to gather economic intelligence. Actions performed by these people include theft of equipment and breaking into corporate facilities (Schweizer, 1993). Also actions used by thieves to collect credit card numbers, such as "Shoulder Surfing" where someone eavesdrops on someone else entering a password, are being used to collect computer passwords.

Social Engineering gives an outside attacker the knowledge and abilities of internal employees. It can also give an internal attacker more knowledge and abilities than they should have. Social Engineering can bypass all technical security mechanisms to allow an attacker to obtain the information of their choosing. In some cases, a Social Engineering attack may yield all the desired information without an attacker having to resort to technical means. This is an extremely important concept, because this indicates that a person who intends to obtain computer-based information does not need to know anything about computers.

There is an additional element to Social Engineering that must be considered. If a hacker breaks into a computer system and obtains information, then they are probably committing a crime. However, if a Social Engineer uses the telephone and asks someone for information, then there is definitely doubt as to if a crime has occurred. The person that gives out the information may be the person that is legally liable and may subject the organization to criminal or civil charges. For example, if a person calls up a hospital and asks for the name of all patients diagnosed with Acquired Immune Deficiency Syndrome (AIDS), and obtains the information by implying that they are from the Board of Health, the hospital could be sued by patients whose lives were damaged by the disclosure of the information. Essentially, Social Engineering attacks weaknesses in what is considered to be common sense.

3. What Enables Social Engineering?

Since Social Engineers attack non-technical weaknesses in security, there must be a discussion of what are the weaknesses in security. Basically, there are two types of weaknesses that allow Social Engineering to occur. A lack of Security Awareness facilitates most Social Engineering attacks. In other words, people do not know how to respond appropriately to compromising situations. Poor plans and procedures also facilitate an attack. In many cases, plans and procedures are designed to thwart a would-be attacker, however they are not tested by an independent source to determine their adequacy.

3.1. Poor Security Awareness

Organizational information security plans will usually address basic issues in computer security. These issues may include non-disclosure of passwords, not giving out sensitive data unless the identity of a caller is confirmed, etc. However, most plans do not include realistic procedures for making employees aware of the security procedures. Many security experts assume that the general population understands basic security issues, such as the importance of a password. These issues are considered to be common sense by computer and security personnel. However, before there can be common sense, there must be common knowledge.

There is very little common knowledge when it comes to computer security-related issues. The dissemination of computer passwords is one such issue. An extremely large percentage of users do not understand the importance of a password for authentication and access to a computer system. They do not realize that their account can be accessed from anywhere in the world, given the proper access point.

Users do not understand the lengths that people will go to to obtain the information that they have access to on a daily basis. Many people do not understand that throwing something in the garbage does not mean that the information is destroyed. What is garbage to a user might be extremely valuable to a hacker, and most people do not understand this concept.

3.2. Human Weaknesses

People will give out information for many reasons. In most cases, people just want to be helpful, because that is their job and/or nature. People can also be intimidated to release information, either by being made to believe that a superior wants the information or by just trying to make an annoying person go away. Corporate spies and many hackers understand that what is considered to be a positive personal attribute can easily be exploited and used against the individual.

3.3. Untested Plans and Procedures

While organizations might understand their threats and vulnerabilities, and attempt to address the vulnerabilities through proper operational procedures, it is difficult to determine if the procedures are adequate unless they are tested. A good example of an untested procedure is the reliance upon internal identifiers. Many organizations establish an internal identifier that is used to authenticate an employee to another employee. For example, many organizations rely upon the Social

Security Number to identify people. It takes very little effort for an outside attacker to obtain a Social Security Number before attempting to obtain the desired information.

A Social Engineering attack may be composed of several small attacks, which in and of themselves might be inconsequential. Unfortunately, the sum of a Social Engineering attack is greater than the sum of its parts. Small attacks will probably go unnoticed, and may occur over several months.

While an organization might establish a procedure that requires an authenticating mechanism, there must be procedures to protect authenticating mechanisms. This is where a large number of security plans fail. Many organizations may test a specific part of a security plan or procedure, however the security plans and procedures must be tested as a whole.

4. The Attack

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 occasions.

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.

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 were working on. The

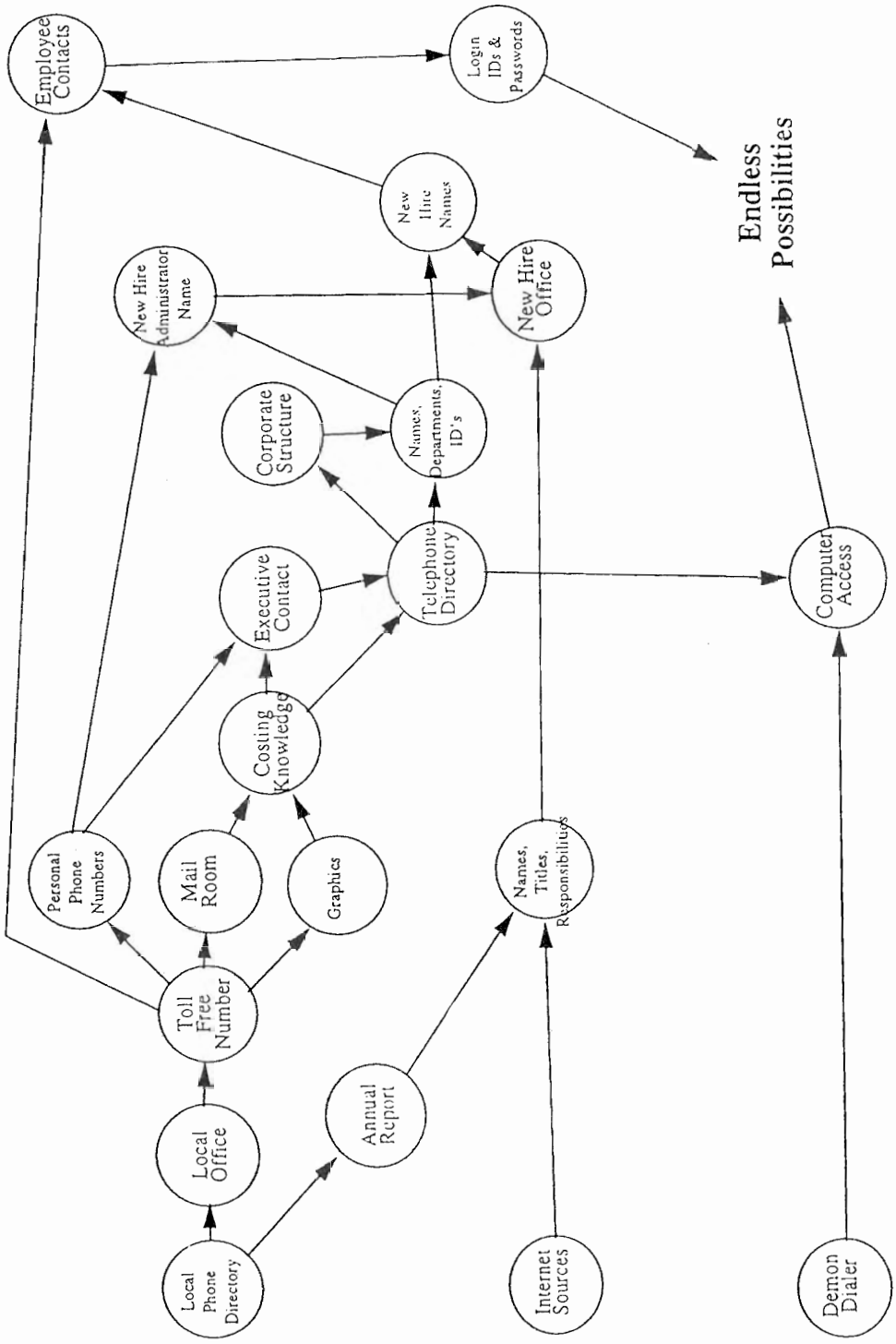

Figure 1. Anatomy of an Attack.

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 claimed to be a new employee needing 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 employee's 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 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.

5. 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 exploited by Social Engineers.

5.1. 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.

5.2. Implement a Call Back Procedure When Disclosing Protected Information

Many of the attacks could have been prevented if the company employees verified the caller's 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.

5.3. 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.

5.4. 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.

5.5. 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 an 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.

5.6. 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 inherent in users. It must be noted that only qualified and trustworthy 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.

6. 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 an 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.

References

1. P. Schweizer, Friendly Spies, New York: Atlantic Monthly Press, New York 1993.
2. M. Slatalla, and J. Quittner, *Masters of Deception: The Gang that Ruled Cyberspace*, New York: HarperCollins, 1995.
3. Voyager, Janitor Privileges, *2600: The Hacker's Quarterly, 11(4)*, 1994.