GATHERING SENSITIVE HEALTHCARE INFORMATION USING SOCIAL ENGINEERING TECHNIQUES

B. Dawn Medlin
Appalachian State University
John A. Walker College of Business
Department of Computer Information Systems
Boone, North Carolina 28608
Phone: 828.262.2411

Joseph A. Cazier
Appalachian State University
John A. Walker College of Business
Department of Computer Information Systems
Boone, NC 28608
Phone: 828.262.6184

ABSTRACT

Social engineering can be viewed as a low-tech attack method or acknowledged as one of the most effective and easily perpetrated forms of attack. Hackers can use this method to gather personal information such as passwords or access codes or even more innocently seeming a birthday or pet's name. With the predominance of mass media’s coverage of hackers and security intrusions, the prevailing question becomes whether or not the general population is aware of the damage that may occur should they or their health care organization be subjected to a social engineering attack? This research in progress study will attempt to identify the personal information that employees will supply as they enter into their place of employment. The results of our study will be provided at the conference. In addition to the results, the authors will also make recommendations that health care companies can incorporate into their policies in order to protect their employees as well as systems from intrusion-based social engineering attacks.

INTRODUCTION

Most hackers rely on employees to inadvertently help them to attack company networks and systems. Today, most health care agencies have intrusion detection/prevention systems that can be used to alert organizations in the event of a security incident, firewalls to protect their internal network, and virtual private networks to ensure individuals connecting from the outside are authorized and have a secure connection. Username and passwords can be provided by the organization as a security method, and is the most common form of authentication [2]. But with all of these methods in place, the question still remains of how much information might an employee provide to a stranger?
Organizational controls, such as processes and procedures, are put in place by an organization to control or protect its assets which can include physical goods, buildings, and money or intangible assets such as a firm’s reputation and image. Of the many types of controls, one of the most fundamental is access control. Access controls are put in place to allow or restrict access to only those authorized personnel who should have the authority to view or work within that system.

Passwords for most health care organizations are one of the most prevalent types of access controls. One weakness of passwords is the difficulty to remember long and complicated passwords thus leading people to create passwords that are easy for them to remember [1]. Individuals due to their short-term memory also tend to reuse their passwords for multiple accounts, making the danger of a weak password greater as it can compromise multiple systems [3].

Currently, most networked systems rely on the username/password combination to grant access. As such, obtaining this information is the equivalent of hitting the jackpot for a hacker. When a hacker is attempting to break into a system, they want to find the quickest and easiest point of entry. This is why many hackers rely on social engineering techniques [4], to gain access to a target, since in many cases it is a lot easier to exploit a human than a system [6].

The social engineer can and often does utilize an arsenal of methods allowing him or her to leverage the emotions of a victim in aiding in an attack. The social engineer can flirt with the victim in an attempt to get him or her to release information; make the victim feel guilty so they divulge information they would not have otherwise; or even convince the victim that their job could depend on giving the attacker the requested information [6]. No matter the type of scenario employed, if relevant and meaningful information is supplied the entire network along with all of its information is placed at risk.

METHODOLOGY

A survey was created and will be administered in Fall 2007 to gather data and to establish how many people would disclose personal types of information to a stranger. As close as possible, we will attempt to simulate the type of information a social engineer would attempt to gather in order to gain entrance into a system (whether personal or within the organization). Shown in Appendix A is the survey we plan to use.

The first section of the survey was designed to gather personal non-identifying information, such as a favorite movie, television show, place of birth, or pet. These categories were chosen based on research performed by Medlin et al. [5]. In their research, they found 19.3% of passwords gathered were based on family, 2.1% were based on being a fan, 5.7% were based on faith, and 1.3% was based on places.

Some personal demographics will also be gathered for informative purposes in order to support the research. This type of information can be used to create a personal profile of the employee that can be used to guess or use password cracking software to determine the strength of their password.

The last piece of information that will be gathered is related to the employees own password. This is especially important in the event of a true social engineering attack. This would give an attacker the company’s name, possible login information from the email address, and the password in the event it was provided by the employee.

The survey and demographics will be kept separate for two reasons. The first is to protect the respondents as well as the researchers from possible privacy breaches. The second reason is to put them at ease with filling out the survey to facilitate a greater percentage of respondents disclosing their
password by giving the impression the survey was truly anonymous. For ethical reasons, the researchers will keep everyone anonymous exactly as promised, however it would be a simple matter for a social engineer to combine the data.

Survey Implementation

In order to assess the current awareness of information security within today’s health care climate, the survey is aimed at employees within a health care setting. However, in order to better represent what a social engineer might be able to accomplish, we will set up a survey booth outside the entrance of a major hospital, rather than have the hospital ask their employees to participate. The employees were targeted due to the sensitive information about patients and the organization to which they have access such as medical history, social security numbers, drugs administered and next of kin. Additionally, they may have access to the intellectual property of their employer.

Individuals will be asked to fill out a survey in exchange for candy and the opportunity to win a free gift card to a local restaurant from a drawing. All personal information for the drawing will be filled out on a separate piece of paper in order to protect and provide anonymity to all persons involved.

Results, future discussion, recommendations, and future research will be discussed at the time of presentation.

CONCLUSION

If a single piece of information such as an employees name and their department or a password can be gathered or information combined to guess or crack a password from social engineering techniques, a hacker has done the first step of their job. With this information the hacker has been doors opened to them.

Employees, in order to be the first line of defense must be educated in social engineering attacks, and have the knowledge to spot and protect against these attacks. Even if a single password could be gathered that should indicate to health care organizations the distinct need for more training and awareness among its employees.

As more and more information becomes digitalized, there needs to be a greater increase in security awareness for both the protection of the organization as well as the employee personally. This awareness on the part of the organization and its employees can be the difference between an organization falling victim to an attack or ensuring the security of their information. This potential weakness in guarding health information is a critical ethical issue the public sector should address.

REFERENCES


Communications of the ACM, 47 (4), 75-78.


In M. Khosrow-Pour (Ed.), Encyclopedia of E-Commerce, E-Government, and Mobile Commerce. 
Hershey, PA: Idea Group Reference.

In: Wiley Publishing.
APPENDIX A - Condensed Survey

Gender: [ ] Male  [ ] Female  Place of Birth: ______________________________
Favorite TV Show: __________________  Favorite Movie: __________________
Favorite Sport and Team: ___________________________  Favorite Singer/Band: ________________
Favorite Song: ___________________________  Favorite Type of Pet: ________________________
Pet Name(s): ___________________________
Do you have kids: [ ] Yes  [ ] No

Please list the first names of the one (or two) most important person (or people) in your life:
______________________________________________________________________________

To help with our research study, please tell us a little about your organizations security

How often do you use a password to access systems?

How often do you change your passwords?

Most people use the same password on multiple accounts. How often do you do this?

Does your employer offer password security training?
[ 1 ] Yes  [ 0 ] No

Does your employer offer any other security awareness training?
[ 1 ] Yes  [ 0 ] No

When was the last time you participated in either a password or another security awareness training program?

On average, do you choose your own password or have one assigned?
[ 1 ] Choose Own  [ 0 ] Assigned

Most passwords fall into the following categories, please mark if yours fits in any of these (select all that apply):

- □ Family
- □ Cryptic
- □ Numbers
- □ Fan
- □ Faith
- □ School
- □ Fantasy
- □ Place
- □ Other

How many characters are in your most commonly used password?

Do your passwords contain any numbers?
[ 1 ] Yes  [ 0 ] No

Do your passwords have any special characters in them (@, #, %, &, etc…)?
[ 1 ] Yes  [ 0 ] No

In order to facilitate creation of solid data, we would appreciate if you would provide one of your passwords. This information will be held in the strictest of confidence, and will be used only to generate a number that describes the characteristics of your password and then destroyed.

My Home/Work/Both password is: ___________________________

Comments: