Calhoun: The NPS Institutional Archive
DSpace Repository

Faculty and Researchers

Faculty and Researchers' Publications

2006-06

Analysis and Defensive Tools for Social-Engineering Attacks on Computer Systems

Laribee, Lena; Barnes, David S.; Rowe, Neil C.; Martell,
Craig H.

Monterey, California. Naval Postgraduate School

7th IEEE Workshop on Information Assurance, West Point, New York, June 2006
<https://hdl.handle.net/10945/35986>

Downloaded from NPS Archive: Calhoun

Calhoun is the Naval Postgraduate School's public access digital repository for research materials and institutional publications created by the NPS community. Calhoun is named for Professor of Mathematics Guy K. Calhoun, NPS's first appointed -- and published -- scholarly author.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

<http://www.nps.edu/library>

Analysis and Defensive Tools for Social-Engineering Attacks on Computer Systems

Lena Laribee, David S. Barnes, Neil C. Rowe, and Craig H. Martell

Extended Abstract

The weakest link in an information-security chain is often the user because people can be manipulated. Attacking computer systems with information gained from social interactions is one form of social engineering [1]. It can be much easier to do than targeting the complex technological protections of systems [2]. In an effort to formalize social engineering for cyberspace, we are building models of trust and attack. Models help in understanding the bewildering number of different tactics that can be employed. Social engineering attacks can be complex with multiple ploys and targets; our models function as subroutines that are called multiple times to accomplish attack goals in a coordinated plan. Models enable us to infer good countermeasures to social engineering.

A. Trust and Attack Models

Our Trust Model shows how a social engineer establishes a trustworthy relationship with a person that has needed information for a social engineering attack. Figure 1 provides an overview. Initially, an attacker obtains background information (freely available if possible) about the target. [3] cites three key characteristics of trust: ability, benevolence and integrity. Presenting some combination of these character traits, the attacker convinces the target that he or she is a trusted person that has a need to know or do [4]. Many ploys can be used to reach these goals [5].

Our Attack Model (Figure 2) explains how information-gathering social-engineering attacks are carried out. It includes the tactics of friendliness, confidence, persistence, quick-wittedness, impersonation, ingratiation, conformity, diffusion of responsibility, and distraction. Using some combination of these methods, the attacker tries to gain unauthorized access to systems or information in order to commit fraud, network intrusion, industrial espionage, identity theft, or simply to disrupt the system or network. Trust of the victim for the attacker, as grown by the ploys covered by the Trust-Building Model, is a catalyst for the operations of the Attack Model: It greatly increases their effectiveness but is not essential.

Figure 1: Social-Engineering Trust Model.

Figure 2: Social-Engineering Attack Model.

Countermeasures to social engineering are actions that interfere with any of the steps in any instantiation of the Trust and Attack models. For instance, in Trust Models the trust building can be foiled by providing accurate information about unknown people to their victims. In Attack Models, victims can be educated about particularly suspicious ploys or trained to follow precisely designed procedures to foil classic attacks. We are using the approach of [6] as a systematic way of finding ways to foil plans.

B. Phishing

We are particularly focusing on phishing [7], use of deceptive email to lure the recipient to a fraudulent website to obtain sensitive personal, financial, corporate or network information. Many attackers target financial or retail organizations, but military targets are increasing (especially highly targeted phishing called "spear fishing"). Phishing has increased in prevalence and severity lately [8].

We developed a model for phishing attacks as an application of the general social engineering model. A phishing attack is comprised of five phases: Target Determined, Attack Developed, Attack Performed, Data Accumulated, and Fraud. Goal Researched and Attack Planned in Figure 2 map to Target Determined; either Deception or Persuasion map to Attack Developed; Tactic Chosen applies maps to Attack Performed; Intelligence Obtained maps to Data Accumulated; and Security Hole Penetrated maps to Fraud.

Here is a typical phishing scenario:

Target Determined: The phisher gets an account with the target organization to understand their online procedures and to receive legitimate email from the organization. As an authorized user, the attacker can see the organization from the inside and start to find exploitable weaknesses in procedures.

Attack Developed: The phisher acquires a domain name, harvests addresses, and configures a bulk-mailing tool. Performing email tests to discover filtering techniques allows the phishers to circumvent spam filters and to reach a larger number of recipients. Mirroring the target Website to appear as the legitimate one is vital. The attacker may choose to host the website on a valid or a hacked server. To make the Website appear authentic, the site may have a fake security certificate. A database is established to collect the desired information.

Attack Performed: Spam email is sent to millions of potential victims providing a link to a fraudulent website. The fraudulent Website is used to collect victim credentials. The attack may also install malware or spyware when the victim visits to the fraudulent site.

Data Accumulated: Victims who fall prey to the attack divulge sensitive information in one of three ways. The spam email may suggest logging onto to the Website or responding to the email with requested information. The scam may require the victim to visit the fraudulent website and submit information in a web form. Lastly, malware may be installed and silently collect information for the attacker.

Fraud: Data that is collected may be sold to hackers or thieves; the phisher may use the information in another attack such as breaking into a network or hijacking a server; or the phisher may directly steal the victim's money or information.

The above model of phishing, and the general Trust and Attack Models, suggest quite a few places and methods that can be used to defend against a phishing attack in a "defense-in-depth" strategy.

- Organizations should ensure that their valid sites and their email should not look similar to those of scams (surprisingly, many organizations fail).
- They should monitor their Web servers to detect footprinting, copying of their graphics to create fake sites.
- They should watch for the assignment of similar domain names to theirs by checking domain-registration sites periodically.
- They should exploit "spam honeypots" that detect when the same email is sent to many recipients.

- They should exploit spam detectors developed to look specifically for phishing by looking for distinctive phrases and text features.
- They should educate users on scams and anti-phishing technology.

Using our systematic approach we hope to propose a detailed set of policy recommendations for defending against phishing. In addition, our general social-engineering models will be effective in understanding and foiling other kinds of attacks.

REFERENCES

- [1] Mitnick, K., and Simon, W., *The Art of Deception*. Indianapolis, IN: Wiley, 2002.
- [2] McDermott, J. "Social engineering – the weakest link in information security," retrieved March 16, 2006, from www.windowsecurity.com/whitepaper.
- [3] Mayer, R. C., and Davies, J. H., "An integrative model of organizational trust," *Academy of Management Review*, vol. 20, no. 3, pp. 709-734, 1995.
- [4] Cialdini, R. B., *Influence: Science and Practice*. Needham Heights, MA: Allyn and Bacon, 2001.
- [5] Granger, S., "Social engineering fundamentals," retrieved March 16, 2006 from www.securityfocus.com/infocus/1527 and 1533.
- [6] Rowe, N., "Counterplanning deceptions to foil cyber-attack plans," Proc. 2003 IEEE-SMC Workshop on Information Assurance, West Point, NY, pp. 203-211, June 2003.
- [7] James, L., *Phishing Exposed*. Rockland, MA: Syngress, 2005.
- [8] Krebs, B., "The new face of phishing," retrieved February 13, 2006 from blog.washingtonpost.com/securityfix/2006/02/the_new_face_of_phishing_1.html.

This paper appeared in the 7th IEEE Workshop on Information Assurance, West Point, New York, June 2006.

Manuscript received on May 3, 2006. This work was supported in part by NSF under the Cyber Trust Program and by the Chief of Naval Operations. Contact the authors at Code CS/Rp, 833 Dyer Road, U.S. Naval Postgraduate School, Monterey, CA 93943. Email: llarabee, dsbarnes, ncrowe, and cmartell at nps.edu. The opinions expressed are those of the authors and do not represent those of the U.S. Government.