IDEA GROUP PUBLISHING
701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com
ITB12701

This paper appears in the book, *Emerging Trends and Challenges in Information Technology Management, Volume 1 and Volume 2* edited by Mehdi Khosrow-Pour © 2006, Idea Group Inc.

An Investigation of Information Security Policies, Procedures, and Perceptions within University Campuses

Ramesh Subramanian & Robert Tordella
Quinnipiac University, School of Business, Mail code: SB-DNF, 275 Mount Carmel Avenue, Hamden, CT 06518,
P : 203-582-5276, F : 203-582-8664, {Ramesh.Subramanian, Robert.Tordella}@quinnipiac.edu

Minnie Yen, College of Business and Public Policy, University of Alaska Anchorage, 3211 Providence Drive, Anchorage, AK 99508,
P : 907-786-4117, F : 907-786-4115, afmyy@uaa.alaska.edu

ABSTRACT

We present the results of an investigation of university campus security policies, the perceptions of the students regarding such policies and the resulting implications for campus security implementation. Our study shows that there are significant gaps between the students and the security administrators with regards to the perceptions of students regarding IS security in general, and with regards to the policies implemented by security administrators. Significant communication gaps exist regarding the understanding and the significance of those policies amongst the students.

INTRODUCTION

The U.S. Health and Human Services Department warned in 2002 that bioterrorists could hack into university networks (Olsen, 2002). Unlike industry, universities are constrained by the extent to which computer security could be imposed and implemented. The constrains arise from unwired campuses (Intel, 2005), protecting the freedom of expression, providing an open and unrestricted learning environment and creating a culture of open inquiry and access to all forms of media (AAUP, 2003), (Fino, 2001), and the lack of resources for employing qualified security professionals, purchase highly priced security software, and providing security training (Foster, 2004). University communities also often oppose censorship. Despite all this, universities are pushing forward in implementing security for fear of legal and financial liabilities (Olsen, 2002). Many universities have hired Information Security Officers for planning and implementing security programs.

More recently, the security research community has come to recognize the importance of the human factor in security. The human factor is frequently described as the "weakest link" in the computer security chain (Schneier, 2000). Typically, user behavior facilitates security breaches. Adams and Sasse (1999) point out that security has largely failed to consider usability, and consequently, the demands that different security mechanisms place on users have been allowed to increase unchecked. In many environments, the demands that different security mechanisms place on users have become unattainable.

Given this context, this study's objectives were to (a) broadly identify the perceptions of students and security administrators concerning existing security policies and programs, and (b) identify a specific set of factors affecting security that could be studied further in a later study.

METHODOLOGY

After studying several user security behavior theories and security models, such as Social Cognitive Theory, Protection Motivation Theory and Reason's (1990) Generic Error Modeling system that identified and addressed security issues involving human behavior, we adopted a socio-technical approach using both qualitative and quantitative methods in this study. We used personal interviews and a survey to conduct the study.

Our study was restricted to two prominent universities in northeastern United States, namely Yale University and Quinnipiac University. The universities are one of the most 'wired' campuses in the U.S.A. (Micali, 2001).

We first studied the published information security policies of both Quinnipiac University (Quinnipiac, and Yale University. We then interviewed the information security officers of both universities. We then developed and administered a student survey to 50 residential undergraduate students from Quinnipiac University and 50 residential undergraduate students from Yale University (please see Appendix 1 for the survey questions). The survey questions were designed to gain an in depth look at different behaviors of students. The idea was to discover if the improper uses of a computer are due to the lack of computer knowledge, the lack of IT policy education, or strictly disobeying the IT policy. The questions also focused on specific applications, protocols and technologies commonly used by, with a view to gaining information of perceptions of students, vis-à-vis the associated security issues. Much of the analysis consisted of interpreting computation of percentages.

ANALYZING PUBLISHED CAMPUS SECURITY POLICIES AND PROCEDURES

We analyzed the published IT and security policies of both universities (Quinnipiac -http://www.quinnipiac.edu/x6336.xml & Yale http://www.yale.edu/policy/1607/1607.html).

An examination of the published policies shows that they attempt to convey the security-related policies in general, with varying levels of specificity. However, a deeper analysis reveals several statements that are difficult to interpret and understand even by experienced systems professionals. Several stated policies pertaining to computer security are very general or not specific enough that they often leave a very wide room for interpretation.

ANALYZING THE 'EVIDENCE' FROM INFORMATION SECURITY OFFICERS

We interviewed the information security officers of both Yale and Quinnipiac University. Our subjective summary and interpretation of the evidence gathered follows.

Yale University Information Security Officer – Interview

During the interview, the Information Security Officer mentioned that there were numerous problems arising from students not following the

IT policies. It is assumed that students might be confused with some of these policies, as discussed in an earlier section. For example, on the use Peer-to-Peer (P2P) applications such as Ares or Kazaa: the policies do not specifically indicate that students must not download files using P2P applications. They merely make a general statement that "…other behavior that may cause excessive network traffic or computing load is also prohibited" (Section 1607.1 C1 of the Yale IT Appropriate Use Policy). The guidelines are generally written in a broad sense that there is room for interpretation when an issue arises. In our analysis of the surveys of Yale students (Appendix 3), 22% of the students were admittedly downloading and sharing files through P2P programs during the period of the study. However, the Information Security Officer mentioned that Yale prevents this issue by implementing a "packeteer" which can be configured to limit the bandwidth allowed on such P2P programs. Although the packeteer will cause a nuisance to use P2P downloading, dedicated users will still disobey the policies and download files. Even though this policy is enforced on campus

and the IT policies are publicly available, it was apparent that students flouted the stated policies and worked around the defenses stated by the information security officer.

Quinnipiac University Information Security Officer - Interview

Quinnipiac University's Information Security Officer is responsible to develop, with a committee, the policies and procedures to enforce in order to keep the Quinnipiac University computing resources network stable and secure. In addition, once the policies and procedures are broadly framed, the actual implementation and enforcement of the policies falls under the security officer's purview. However, during the interview, the officer made it clear that it is increasingly hard for him to implement and maintain many of these policies because he is the only person controlling them; his view was that there needed to be additional help hired for implementing and enforcing the security policies. We learnt during the interview that the information security officer has to control all aspects of security: physical security (integrated with IT security), policy meetings, major student issues, network problems, IT administration meetings, and monitoring the network for illegal traffic. The implication of this situation is that the information security officer is often overloaded and understaffed, which by itself poses a major security problem to many universities that do not have the resources to hire additional security officers. This means that since there is less time spent on configuring the network and implementing policies, there are internal issues that can go undetected.

The evidence gathered from the interviews again point to the fact that policies are often misunderstood or not understood by students because they leave room for different interpretations. In addition, campuses sometimes suffer from inadequate security professional.

Analyzing the Student Surveys

Fifty undergraduate students from Yale University and fifty undergraduate students from Quinnipiac University were randomly selected to participate in the survey. The survey questions results are listed in Appendix 1. (Note: The survey *results* have been removed from Figure 1 and discussed in the body of the paper only, due to space constraints). The survey included questions that were designed to be general enough to gain an understanding of students' perceptions about campus security. In the following sub-sections we provide our analysis of the results. *For our analysis we combined the two sets of survey data (Yale and Quinnipiac).*

Analysis of the Survey Data

An analysis of the data revealed the following broad security categories: wireless security issues, operating system issues and email issues.

Wireless Access Vulnerabilities

The combined survey results showed that 85% of students own a laptop, and 16% of the students predominantly use wireless access, while 28% showed a preference for combined use (i.e. wired and wireless). This implies that up to 44% of the students could potentially use a wireless connection sometime or other. Although a wireless connection is more convenient, it has many more vulnerabilities than a wired connection. Being located in a city (New Haven, Connecticut), Yale is even more vulnerable to a random "war driving" attack against its wireless network. An attacker driving a car equipped with easily available wireless-hacking hardware and hacking software can actively sniff, attack, or gain access to the Yale network.

"War-driving" at Yale University: As part of our study of wireless access vulnerabilities, we performed a "war-driving" exercise around the Yale campus using NetStumbler (http://www.NetStumbler.org), a wireless-sniffing software. Even without an antenna, we were able to pick up various Yale wireless access points. We found connections from local students with an ad- hoc (peer) configuration, actual campus access points, or local residents/businesses (see Figure 2). Out of the 154 access points we discovered, 51% of them were not encrypted and were left open (unsecured). Most of these open access points were from the residential colleges within the Yale campus. Most of these access points were never configured and were taken "out of the box" and plugged in. Since most manufacturers do not enable encryption or require the user to change the password of the router by default, the wireless network could be wide open for an attacker. An attacker can thus easily access an open network by just being in the signal range of the router. While being in range, the router will automatically assign the attacker an internal IP address. This enables the attacker more access to further his/her attack on the network or the individual users connected to the same router.

Other attacks can also be done with wireless networks. Besides attacking access points, an attacker can connect to network users directly. Our "NetStumble report" of Yale (see Figure 3) shows 76% (20 out of 26) of peer connections were "open" during our war-drive. Any attacker can thus connect to an ad hoc (peer) connection within range. This will enable an attacker to access any network shares on the computer or use the computer as a gateway to access the Internet. Once an attacker is inside a network, there are numerous attacking methods that could be used against individual users or the network. Some of these methods will be discussed later in this paper.

"War-driving" at Quinnipiac University: Similar to our Yale war-driving study, we "war-drove" the campus of Quinnipiac University. Since Quinnipiac is a fairly secluded campus at the edge of a small town (Hamden in Connecticut,), we decided to use a different strategy for our war-drive. We walked around the campus covering a couple of dorms (student residences). Even scanning without an antenna, we were able to pick up various wireless access points configured by students (see Figure 3). Out of the 27 access points we "discovered", seven were not encrypted and left open (unsecured). As discussed in the discussion on the war-driving of Yale University, this makes it easy for an attacker to gain access. Attackers can also use this vulnerability to their advantage from an internal approach. Once they have the DHCP (Dynamic Host Configuration Protocol) address (192.168.1.X22) from the wireless router, the attacker could possibly run multiple attack methods. In addition, because of the use of the DHCP address, there will be a low risk of being traced because any attacks are conducted within the router's internal addresses, rather than the actual originating network.

Operating System Vulnerabilities

The survey results reveal that 29% of all the students surveyed never used Windows (or Mac) security updates. The updates are patches that are release periodically by vendors to fix certain problems or "holes" that are found in the operating systems. These "holes" could be ports that are accidentally opened by poorly written code, unnecessary services running, or loopholes within the operating system that leads to these

vulnerabilities. Malicious software ("malware") is able to exploit these vulnerabilities that are left open if a machine does not have the current updates. In some cases, these Trojans or worms could start to "ping" other computers on the network looking for the same vulnerability, so it can spread to other machines. With around one-third of students on the network not updating their systems, they all could be infected by the spread of malware. This would cause network traffic to become bogged down causing it to eventually slow down in performance due to the amount of bandwidth being used.

The survey also showed that 8% of the students continue to use older operating systems such as Windows 95 and Windows 98. These operating systems are only secure up to a certain extent as they weren't initially designed with a strong level of security. Malware can easily penetrate the older systems through known "computer exploits." Even though students continue to use these unsecured operating systems, about 8% of the surveyed students never used Anti-Virus software, and of the remaining, 9% never scanned their computer for viruses. Also, 29% of the students scanned their computer only once a month. This time lapse could be crucial for the individual's computer and the university's network. The longer a person is infected with certain types of malware, the more harm it can cause to the network and other users. A malicious attacker could destroy a network by deploying a virus or Trojan on a known vulnerable machine with the intent that it would spread to other machines.

E-mail Vulnerabilities

Through our survey we related the students' use of e-mail with online shopping. This relation is most common for "phishing" attacks, such as a spoofed e-mail which claims to offer the consumer a prize for re-entering their information on the company's website. When asked about what security signals they would look for when providing personal information on the web, we found that 14% of the students surveyed always checked for security signals, 45% sometimes did, and 41% rarely or never checked. Among the students who did check for security signals, 53% only checked for the yellow security lock icon on the bottom right corner of their browser. Since this icon is the main security method that a person looks for, they will believe that the site is legitimate and therefore will be comfortable providing any information. Because very few people check for any of the other signals such as SSL connection or digital certificates, an attacker could easily fool the user with just masking the yellow lock icon. When using the phishing technique, the attacker is able to send a link to a spurious web page (e.g. www.paypai.com) in order to make it look like the real web site (www.paypal.com). The attacker typically offers a benefit such as a $10 credit on a user's account for updating user information. When the student clicks on the link they are taken to a page that was copied and made to look exactly like the www.paypal.com login page. They will be asked to update all of their personal information including their credit card number, username, and password. This is when the attacker would spoof the security lock icon on the bottom of the browser. After they submit their information, they will be directed to a page that claims the prize or money will be included in their account soon. All of the information that the user had typed, falls into the attacker's possession, to be used for future attacks.

Of the students surveyed, 57% claimed that they use the same password for most applications. An attacker with experience in phishing attacks could easily use this to his/her advantage. Since the majority of students used sites such as amazon.com for their online shopping, an e-mail would be sent to random students asking them to update their amazon.com account. The web page would direct them to a masked amazon.com web page (with the security lock masked) and ask the users to login. After the login attempt, a web page will then provide them with an error claiming they are experiencing heavy traffic. For the user, they will think nothing of it and try again some other time. However, the attacker now has the student's username and password which was secretly stored in the background. The attacker can now attempt to log into Yale's or Quinnipiac's network by trying the student's amazon.com password.

"Internal" Network Vulnerabilities: Port Scanning

Once inside the local area network (LAN) of the campus wireless router, an attacker could easily "port-scan" another computer within the 192.168.1.X address scheme (Figure 4). The attacker can find open ports, computer names, MAC addresses, and open network shares. Having knowledge of which ports and network shares are open could be beneficial for an attacker in other attack methods. Our example in Figure 4 shows the telnet and certain NetBIOS ports open. Since this particular user has telnet services running (port 23 is shown open in Figure 4), the attacker can try to enter into the user's machine by a telnet connection. Also, knowing the user's MAC address and computer name is helpful for future identity theft attacks. An attacker is able to spoof his/her MAC address and computer name in order to mask his/her identity.

"Internal" Network Vulnerabilities: Address Resolution Protocol (ARP)-Domain Name Server (DNS)

Poisoning

Upon analyzing our survey results from both Yale and Quinnipiac universities, we noticed that students have similar behaviors that could cause the respective campus networks to become vulnerable to attacks. Using the Quinnipiac survey, we can associate similar behaviors for a phishing attack as compared to an ARP-DNS poisoning attack. Specifically on the Quinnipiac network, we could use an ARP-DNS poisoning attack for many different reasons, but in the example (see Figure 5) we attack the users on the same subnet trying to access Blackboard (the example is simulating this attack on a closed private network). According to the Quinnipiac survey, 72% of students feel secure on the campus network. This state of comfort could be exploited because those who feel secure would not expect the "trusted" Blackboard site to be tampered with. Freeware programs such as Cain & Abel (www.oxid.it/cain.html) can deploy ARP-DNS poisoning simply for an attacker. Plus, within the program, an attacker is able to spoof his/her MAC and IP address so he/she can be harder to trace. Specifically on the Quinnipiac network, ARP-DNS poisoning can be deployed to redirect the flow of traffic by poisoning the DNS cache to have Blackboard (http://blackboard.quinnipiac.edu/webapps/login) end up pointing to the IP address of a local Web server (e.g. 192.168.1.6) . This Web server can contain an installed version of the freeware Apache web server, which could run an exact replica of the Blackboard login page. Similar to the phishing attack example against paypal.com, this masked version would record usernames and passwords of the users.

CONCLUSIONS

Based on the study, we arrived at the following conclusions:

- The security of a campus network is very dependent on the hardware, software, network configurations and the people who use them.
- Security is very dependent on user behaviors.
- Campus security administrators are constantly fighting the tide of new exploits, combined with the over-confidence, indifference and apathy of the students who use the campus IT resources.
- There is inadequate training of users. Security policies are not well understood by users.

We propose to conduct further studies with more university campuses to further analyze the issue of students' perceptions of policies in campus networks. In addition, the studies will also compare and contrast industry practices with academic practices to see what, if any, can be learnt from industry. It is hoped that further studies will provide university administrators with a blue-print to frame and implement security policies.

REFERENCES

AAUP (2003) Academic Freedom and National Security in a Time of Crisis: Executive Summary. Retrieved February 25, 2005 from HTTP://WWW.AAUP.ORG/ISSUES/HOMELAND%20SECURITY/EXEC911.PDF

Adams, A. and Sasse, M. A. (1999) Users are not the enemy, *Communications of the ACM*, Vol. 42, No. 12, December, 1999.

Fino, J.J. (2001). Campus Software Regulations can threaten Academic Freedom. Retrieved February 25, 2005 from Footnotes (Fall 2001) HTTP://WWW.AAUP.ORG/PUBLICATIONS/FOOTNOTES/FN01/FN01JF.HTM

Foster, Andrea L. (2004) Colleges Brace for the Next Worm. The Chronicle of Higher Education (March 19, 2004). Retrieved February 25, 2005 from HTTP://CHRONICLE.COM/FREE/V50/I28/28A02901.HTM

Intel (2005) Most Unwired College Campuses. Retrieved February 25, 2005 from HTTP://WWW.INTEL.COM/PERSONAL/PRODUCTS/MOBILETECHNOLOGY/UNWIREDCOLLEGES.HTM

Micali, Lisa. (2001). Quinnipiac on most wired list. Business New Haven, November 26 2001. Retrieved February 26, 2005 from HTTP://WWW.CONNTACT.COM/ARCHIVE_INDEX/ARCHIVE_PAGES/435_BUSINESS_NEW_HAVEN.HTML

Olsen, Florence. (2002) The Growing Vulnerability of Campus Networks. The Chronicle of Higher Education (March 15, 2002). Retrieved February 25, 2005 from HTTP://CHRONICLE.COM/FREE/V48/I27/27A03501.HTM.

Reason, J. (1990) Human Error, Cambridge University Press. , Cambridge, UK

Schneier, B. (2000), Secrets and Lies, John Wiley & Sons, 2000.

Figure 1. Survey questions

University Security Survey - 100 Undergraduate Students from Yale University and Quinnipiac University		
	Surveyed	**Percentage**
Gender		
Computer Type They Owned		
Preferred Connection (wired, wireless, both)		
Current Operating System Used		
Do you use Anti-Virus software?		
How often do you use your Anti-Virus Updates?		
How often do you run Anti-Virus Scans?		
Do you use Windows Updates?		
How often do you run Windows Updates?		
Do you use P2P Programs?		
Which P2P programs do you use?		
How often do you use of P2P Programs?		
Which e-mail program do you use the most?		
How often do you check your e-mail?		
Do you take precaution with e-mail attachments?		
Do you use an application firewall?		
Do you use AIM?		
Do you share your own password?		
Do you use the same password for most applications?		
Do you change the default password to personal one?		
Do you feel safe on the school's network?		
Would you attend an information security seminar?		
How would you rank your computer knowledge?		
How Secure do you feel on the school's network?		
How concerned are you with privacy?		
What Security signals do you look for?		

Figure 2: Netstumbler report - Yale

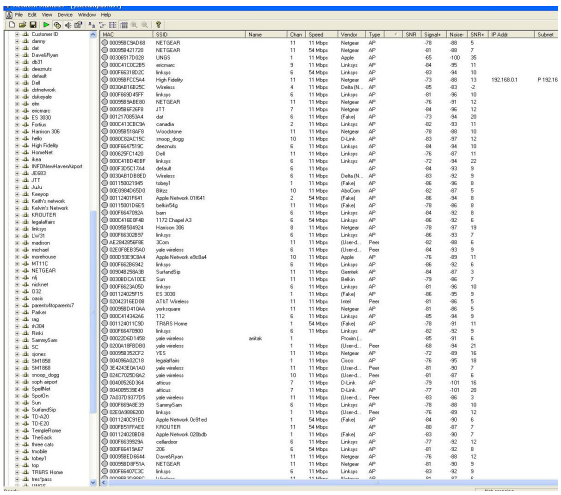

Figure 3: Netstumbler report - Quinnipiac

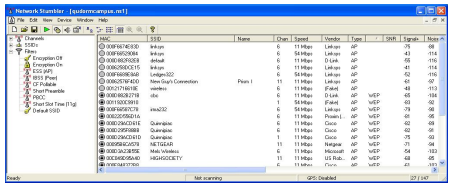

Figure 4: Port Scanning

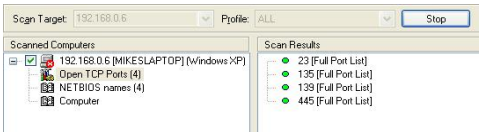

Figure 5: Cain and Abel ARP-DNS poinsoning