https://doi.org/10.48009/2_iis_2010_162-167

COMPUTER SECURITY IN COMPUTER LITERACY EDUCATION

Rob Barton, Utah State University, rob.barton@usu.edu

ABSTRACT

Computers are a pervasive part of society, even more so on college campuses. Among other skills, it is important that students have a base of understanding related to computer networking and security in order to protect themselves from online threats. Students who study for and pass tests that show their understanding of these topics appear to have a lower rate of computer security related issues. Since user education does appear to be an effective tool in affecting computer security practices, and security threats seem to be getting worse all the time, it is worth the effort to focus more energy on teaching network and security basics to all undergraduate students in both technical and non-technical majors as part of their degree programs. Given that security issues affect full time faculty and staff at the university, in addition to students, it is recommended that the computer security training developed for students be extended to all university employees.

Keywords: Computer Security, Computer Literacy, Education, Internet

INTRODUCTION

As the number of Internet users around the world approaches 1.5 billion at astounding growth rates [8], the importance of keeping computers protected against a multitude of threats grows as well. The Internet is used for more purposes by more people all the time, making users more vulnerable to a host of potential problems. With many novice users joining the networked ranks, it is important that these new users have a set of basic computer literacy skills to help them work efficiently and to keep their computer and data secure [4, 3, 12].

On college campuses, it is practically required to have a computer. With the speed that technology is changing, the skills that need to be taught in computer literacy courses are also changing [5, 6, 2]. Although students often come to campus already proficient in the use of many computer applications, they lack a real understanding of how technology works. Most importantly, they often lack a thorough understanding of computer and network security [9, 11].

Teer [11] lists computer security topics that should be understood by computer users: antivirus software, firewalls, opening email attachments, passwords, and patching the operating system. She found that among the users surveyed, 28% do not know if their antivirus software is up to date, 73% do not verify the sender before opening an email attachment, 30% do not know if their operating system is patched, 28% do not have a password set on their computer, and 47% have given out their passwords to other people. There did not appear to be a large difference between students with technical and nontechnical majors, although a more comprehensive study with a wider cross section of students than that used in Teer's study might show significant correlations between selected major and secure practices.

On the Utah State University (USU) campus, IT security recently started weekly scans of known computer vulnerabilities to find and educate users or shut down computers that have not been secured properly before hackers, who are also scanning the campus network, take them over. Since the results of these security scans are easily accessible, we can look at those whose computers are flagged for improperly securing their machines to identify patterns among computer users' behavior and knowledge.

As part of the USU general education program, students are required to pass a series of Computer & Information Literacy (CIL) tests. The Computer Systems CIL test covers computer security topics and other knowledge about how computers work and common applications necessary for students to work efficiently in their studies. With similar programs and courses in place at most higher education institutions and the pace at which technology changes, it is important to keep computer literacy training up to date. This paper serves as a pilot study to determine whether there is a practically significant correlation with users who have had security problems with their computers and their knowledge of computer security. To measure computer security knowledge, we can look at whether students have passed the Computer Systems test, which is designed to show understanding of basic computer security practices, plus basics of connecting to a network, parts of a computer, size and speed measurements, and operating system functions. Although an understanding of secure computing techniques does

not necessarily mean students put those techniques into practice [7], it may be postulated that a lack of knowledge will lead to unsecured and eventually compromised machines. By verifying the linkage between computer security knowledge and secure computing practices, we may justify a more full scale analysis of which topics would benefit from additional training.

The most common issues for which computers are flagged by IT security are vulnerable versions of software or operating systems that have not been recently updated and blank or easily guessed passwords. Both of those issues are directly addressed in the Computer Systems test and study materials. Faculty and staff are not required to obtain any special computer literacy training in order to be issued a campus computer, although many faculty and staff computers are managed by an IT professional in the department or college.

METHOD

The IT security team publishes the results of its weekly security audits on a wiki site accessible to the entire campus community. These results include the owner of each computer and the issue for which each is being flagged. As a large residential school, the security issues faced by USU are likely similar to those faced by other higher education institutions around the country. By comparing the list of users with vulnerable computers to the CIL test score database, the author was able to determine which users had or had not passed the CIL Computer Systems test. Although this only tells us limited information about the users whose lax security practices were enough to get them caught by the security scans, it may be enough to justify a study of the larger campus population to determine the extent to which preparing for the CIL Computer Systems test or other resources have contributed to user computer security practices.

Once the list of users and test scores is compiled, users will be broken out into their main role as either staff or student at the university. There is some overlap with staff that are also working on a degree, but it is largely insignificant. By comparing the proportion of students who have passed the CIL Computer Systems test to the proportion of students whose computers have been flagged for security issues in spite of having passed the test, it will be possible to determine whether there is a significant difference in the practices of those who have and have not passed the test. According to a recent nationwide study [10], three-quarters of students at four year universities have laptops and almost all respondents to their survey had a computer of some kind. 85% prefer communicating electronically with the university. With an 11% response rate, it is unclear the extent to which the survey results may be generalizable to the entire population of college students or to the students at USU specifically, but it is likely that the majority of USU students own a computer of some kind. Between students living on campus and those bringing their laptops to campus, the majority of those owning computers are likely to have registered for campus network access on their computers as well.

To determine whether there is a significant difference between the two proportions, all students who have passed the test and students whose computers have been flagged for security problems and have passed the test, a 99% confidence interval for the difference between the proportions will be used. The null hypothesis, that there is no difference between the two proportions, will be accepted if the calculated confidence interval includes the value 0, as there would be a chance that the difference between the proportions is 0. The null hypothesis will be rejected if the 99% confidence interval does not include 0. A 99% confidence interval is being used rather than the more standard 95% confidence interval, to counteract the possible over-estimation of the number of students on campus with computers.

In addition to measuring the relative effectiveness of the current Computer Systems test, it will be useful to analyze the issues for which computers on campus are flagged for security problems. Doing so may provide areas on which a new version of the test may be focused to address common problems. The issue for which each computer is flagged is included in IT's weekly report, so coding those reasons will help determine the most pressing issues, based on the percentage of computers that are flagged with each issue. All of the issues that have been collected so far may be reduced down to one of three main categories: outdated or unpatched operating system, vulnerable versions of application software, and poor passwords or other weak user-defined configurations.

Given that no security training is currently done for faculty and staff on campus and that faculty and staff use their computers for different reasons than the students, it may be useful to compare the security problems for which faculty/staff and student computers are flagged by the security team. If these groups turn out to be similar in their behaviors and practices, it may be worth providing training to faculty and staff, similar to that received by the

students. If there are major differences, a custom training for faculty and staff may prove to be beneficial by meeting their specific needs.

RESULTS

There are over 28,000 computers registered on campus (Mike Fotes, personal correspondence), but it is unknown how many are owned by students and how many are managed by trained or untrained university staff. For the Fall 2008 semester, there were approximately 13,394 undergraduate students on the main campus and 20,289 students total, including distance education sites. Of all students including main campus and distance sites, 13,542 have passed the Computer Systems test. There are approximately 2,800 faculty and staff at USU [1].

The confidence interval is calculated by multiplying the z value for the 99% confidence level by the square root of the sum of the squares of the standard errors of the two proportions. That value is then added to and subtracted from the actual difference in the two proportions to give the interval.

The proportion of students who have passed the CIL Computer Systems test is 13,542/20,289, or 67% with a standard error of .003. The proportion of students whose computers have been flagged by IT security and who have passed the test is 27 out of 187 with a standard error of .025. Thus, the confidence interval is .52 +/- 2.576(sqrt(.003^2+.025^2)) or .455 to .585, which is more than enough to reject the null hypothesis.

When it comes to what particular practices are not being followed, by dividing the number of students and faculty/staff that have each security problem by the total number of computers disabled over the study period, we can see which issues cause the most problems for each. For faculty and staff, 51% had issues with not keeping their operating system up to date, 36% had vulnerable versions of software installed, and 12% had password issues. For students, 73% had unpatched operating systems, 17% had issues with vulnerable software, and 10% had bad password policies.

Since all these issues are important to teach, it matters more whether there is a practical difference between faculty/staff and student computing practices and not as much whether there is a statistically significant difference. The password issues appear to be relatively the same proportion of 10-12% of all those flagged for security issues. The main practical difference comes in the proportion of issues with unpatched operating systems versus unpatched application software. Students have relatively fewer problems with out of date software and a considerably higher percentage of computers with unpatched operating systems, compared to faculty/staff machines.

DISCUSSION

We can conclude that there is a significant difference in the proportion of students who have passed the CIL Computer Systems test for students whose computers have been flagged by the IT security team for insecure computing practices compared to the university population as a whole. If there had not been a significant difference, we would have to assume that passing of test showing computer security knowledge is not related in any meaningful way to student behavior. Since a significant difference does exist, we can conclude that it would be valuable to further research this issue to determine the extent to which preparation for a test or participating in a training course affects student computing practices and what changes to tests and instructional materials should be made to further contribute to proper user security practices.

The first question is what differences, if any, exist in the behavior of faculty and staff at the university, compared to the students? Each department is different in terms of the technical expertise expected of faculty and staff and the level of support provided by dedicated IT personnel. Approximately the same number of computers managed by university employees and personal student machines were flagged for security vulnerabilities, but since there are so many more students than employees, the percent of employees whose computers have security issues is much higher than that of the students. It is likely caused by several reasons, depending on the department, including lack of a dedicated IT support person, lack of communication between faculty and IT personnel, an inflated number of vulnerable computers due to one vulnerable configuration being copied to many computers in a computer lab, lack of basic computer skills for older employees that are not digital natives like many of the students, and the higher likelihood that staff computers will be on and connected to the university network when security scans are performed. When looking at the particular reasons for which computers are flagged for security issues, the difference becomes more apparent. While there is little difference between faculty/staff and student practices when it comes to secure passwords, there is an obvious difference in the number of issues dealing with operating systems updates compared to

software updates. Part of this difference may be due to a larger variety of applications installed on faculty/staff computers than on student computers, as students will be less likely to install expensive, specialized client applications or any type of server applications. Students are often more likely to run cloud-based applications over the internet, where no software is actually directly installed on the computer than are staff. Although these differences mean students may not be as likely to run into problems with keeping their software applications properly patched, these numbers draw attention to the fact that understanding this concept will be even more important when students graduate and enter the workforce.

Werner [12] asserts that a computer security component of a computer literacy requirement should influence users' future behavior and attitude. Topics she recommends that students should learn include security scanning tools, operating system security, firewalls, antivirus software, spyware, inherent insecurity of email, social engineering, backups, and encrypting files. In order to cover all these materials, Werner claims that security should take up a large amount of the time dedicated to computer literacy, possibly up to 1 credit of a 3 or 4 credit class. Because security concepts are often dependent on an understanding of the networking concepts that accompany them, any security education requires at least a basic understanding of networking.

Providing students required instruction as part of their coursework is relatively straight forward, with the support of faculty curriculum committees. Adjusting this training for students is relatively straight forward to implement and may greatly improve the security practices of students at this and other universities. Faculty and staff are many schools are generally not required to demonstrate any competency or skill to be issued a computer by their department. While instituting any kind of mandatory university-wide training will meet considerable resistance at many levels, it is nonetheless important to consider such an action. In working towards such training for faculty and staff, a good way to start may be to provide the training developed for students to faculty and staff on a volunteer basis to individuals and/or to departments who choose to implement the training. This could be done in conjunction with a university IT department who often look to provide such training materials for the campus community. Providing the same training to faculty and staff may also help reinforce to students that what they are learning is relevant to them.

RECOMMENDATION

Based on the preliminary security scan results and literature on the topic [11, 12], it is recommended that the following topics be included in further analysis to determine the extent to which they are problematic for students and staff. The outline, in no particular order, is as follows.

Phishing, Spamming, Scams, and Social Engineering

Phishing and spamming and other social engineering methods are threats that have been around as long as the Internet but continue to grow as threats. It is important to determine whether these topics need to be covered more in depth, going into not only the definition of the terms, but the specific threats both to the security of the computer involved and the privacy of the person receiving these scam messages, as well as techniques to filter out spam and other unwanted email or to avoid spam harvesters from obtaining email addresses to begin with.

Malicious Software

Users often know generally what a virus is but may not understand the various types of malicious software and how they are categorized, including viruses, trojans, worms, and spyware. More specific analysis of user understanding of these topics is important. Skills that may be useful to ensure students know include how to avoid being infected with these threats or to remove them once infected, running the computer with a non-administrator account without permissions to install software, how to check what processes are running on a machine, available virus removal tools, and using system restore to roll back a computer's configuration to an uninfected state. It is also important to gauge user understanding of another category of new threats in this realm, browser based attacks such as plugins and ActiveX controls that can be major security problems if a user installs certain programs in their browser that can then read information from their hard drive or install additional programs on their computer.

Network Basics

Much of this information is core to users' daily tasks but without giving it much thought. The underlying structure of how our networks are structured should lead to better security behaviors. Information on IP addresses and URLs may be used a way of identifying where information came from so a user can assess its reliability based on who published it.

This will help users understand what sites they may or may not want to trust when downloading and installing new software. Another core competency that may not be at the highest level is user understanding of how the Internet was set up to be fully redundant, without centralized control, and to allow everyone to communicate equally, along with the benefits and drawbacks of this model.

Wireless Networks

With the increasing proliferation of wireless networking, whether through cell phone networks, wifi access points, or bluetooth, it is becoming more important for users to understand what information they may be broadcasting to the world and how to keep their own networks safe. It is unclear the extent to which users understand that wireless networks are less secure, so users need to be more careful, employing specific steps to ensure wireless network traffic is encrypted and not to fully trust a network just because its traffic is encrypted but that it is recommended to always take additional steps to encrypt sensitive data separately before transmitting.

Firewalls

A big problem for computers running the Mac operating system is that although the operating system includes a firewall, it is turned off by default, and that is clear from the security scan results. It may be important in security education courses to provide more operating system specific information to users and take a little more time explaining how users need to expect that enabling extra security features like a firewall will make their computer harder to use. Security is always a tradeoff with usability, so patience is necessary in taking the time to properly set up a computer to allow or block what it is supposed to.

Operating System and Software Updates

As mentioned in the firewalls section, more operating system specific information may need to be provided. Operating system patches were the largest problem identified by far with the scans performed by the IT security team, so that particular issue deserves more attention. With the large number of applications that are currently out there, it is not practical to have instructions on every piece of software one could possibly install. However, some basic tips on how most applications may be recommended, including how to tell whether an application has the ability to notify the user that updates are available or if the user will be expected to manually check for updates.

Passwords

Passwords are often the most visible part of any security initiative and often lead to frustration. Initial security scan results show this is the case with the large number of both students and staff users having password security problems. A potential additional training topics to be provided may include the basic rules of a good password, that is, specific techniques on creating a password that is long and complex to anyone else but simple to the user who created it.

Backups

Few computer security courses spend much time on backups as a security issue. Although backing up data may not always be thought of as a security issue, it actually is. A user losing data to a virus that deletes everything off the hard drive is not much different in its effect than losing data to a hard drive that crashes or even accidentally saving a file in place of another one. Having backups of data is an important practice to follow. Various ways of backing up data either to online repositories, which are becoming much more widely available, or to external devices like flash drives or even to a second hard drive within the same computer may be useful to cover with students and staff, if it is seen that they lack this knowledge.

FUTURE RESEARCH

The issue of operating systems is an important one to consider. Approximately half of the computers flagged for vulnerabilities have been Macs, yet they make up a relatively small percentage of the computers on the USU campus (Miles Johnson, personal correspondence). Macs are traditionally considered to be more secure, but the recent number of Mac vulnerabilities is catching up as they have become more common. It is unknown, however, the number of computers with each operating system, so that would be important to collect.

Werner [12] points out that it is unfortunate when many students wait until they are seniors to take a required computer literacy course. That is not inconsistent with student behavior at USU or at many other universities. It is not known how many students wait until the end of their college careers, but it is not uncommon for students to do so. It could be possible that students who put off fulfilling academic requirements like CIL until they are absolutely required to are also likely to ignore common practices that will make their computer safe,

not because they do not know better, but because they are simply failing to prepare themselves. A survey of student attitudes towards CIL, their other classes at the university, and computer security may shed some light into whether failure to complete computer security training is a cause of their failing to secure their computer or a symptom of student apathy and procrastination.

Further study into student and faculty perceptions, attitudes, knowledge, and behaviors regarding computer literacy in general and computer security specifically will contribute to the field by giving computer literacy programs more leverage to maintain or even expand their training for both students and faculty. This will improve the quality of graduates being sent into the workforce as well as improve security on campus networks as both students and faculty are motivated to follow proper security practices.

REFERENCES

1. Analysis, Assessment, & Accreditation (2008). "Facts and figures about USU." Retrieved from http://aaa.usu.edu.
2. Childers S. (2003). "Computer literacy: Necessity or buzzword?" Information Technology and Libraries, 22(3), pp. 100-104.
3. Duffy, T. J. & Walstrom, K. A. (2003). "Changes in student computer technology attitudes over time," Journal of Computer Information Systems, 43(3), pp. 27-33.
4. Gordon, L.A., Loeb, M.P., Lucyshyn, W., & Richardson, R. (2004). "2004 CSI/rai Computer crime and security survey," CSI Publications.
5. Hoffman M., & Blake, J. (2003). "Computer literacy today and tomorrow," Journal of Computing Sciences in Colleges, 18(5), pp. 221-233.
6. Hoffman M., Blake, J., McKeon, J., Leone, S., Schorr, M. (2005). "A critical computer literacy course," Journal of Computing Sciences in Colleges, 20(5), pp. 221-233.
7. Lee, S.M., Yoon, S.N., & Kim, J. (2008). "The role of pluralistic ignorance in internet abuse," Journal of Computer Information Systems, 48(3), pp. 38-43.
8. Miniwatts Marketing Group (2008). "The Internet Big Picture: World Internet Users and Population Stats," Internet Usage Statistics Retrieved from http://www.internetworldstats.com/stats.htm.
9. Robila, S.A., & Ragucci, J.W. (2006). "Don't be a phish: Steps in user education," Proceedings of the 11th annual ACM SIGCSE conference on Innovation and technology in computer science education, 38(3), pp. 237-241.
10. Salaway, G. & Caruso, J.B. (2007). "The ECAR study of undergraduate students and information technology, 2007," Educause Connect, 6. Retrieved from http://connect.educause.edu/library/abstract/TheECARStudyofUnderg/45075.
11. Teer, F.P., Kruck, S.E., & Kruck, G.P. (2007). "Empirical study of students computer security practices and perceptions," Journal of Computer Information Systems, 47(3), pp. 105-110.
12. Werner, L. (2005). "Redefining computer literacy in the age of ubiquitous computing," Proceedings of the 6th ACM SIGITE conference on Information Technology Education, pp. 95-99.