INTEGRATING A SECURITY AWARENESS PROGRAM INTO AN INFORMATION SECURITY COURSE

Frank H. Katz
Department of Information Technology
Armstrong Atlantic State University
Savannah, GA 31419
912 921-5608
katzfran@mail.armstrong.edu

ABSTRACT
As Armstrong Atlantic State University (AASU) enters the wireless world during the Spring 2007 semester, it is important that those connecting to the university’s network use notebook computers that are free from viruses and malware. In order to help secure this network, Information Technology students were given practical experience by organizing and performing virus and malware scan sessions on student notebook computers. This paper describes the effects of the outcome of this project on using similar hands-on activities in the teaching of Information Security.

INTRODUCTION
As more and more students at AASU use their notebook computers to connect the Internet, they and the university run increased risks of exposure to dangerous viruses and spyware. Wireless connectivity escalates the threat of the university’s network being compromised by a notebook computer. Indeed, “the threats against wireless networks reflect the variety of users on the network.”[4] Unlike a corporation, which represents “a single point of trust for their employees,” the university environment lends itself to many different users on the network using a wide variety of notebook computers, not all of which will be free from viruses and malware. It is possible for mobile users “who leave a network and open their machines to files that could contain malicious payloads such as viruses, worms, and Trojan horses and then infect the network when they log back on.”[5] To alleviate these threats, students should not only be made aware of them, but should have their notebook computers scanned for viruses and malware and be taught the best practices for maintaining the integrity of their computers.

In order to accomplish these goals, during the Spring 2006 semester, students majoring in Information Technology and taking Information Security (ITEC 3100) designed and executed a series of virus/malware scan sessions for the AASU general student population. Performed for the first-time ever at AASU, this project enabled the IT students to put theory learned in their Information Security course into practice.

The results and findings of this project were documented in a paper entitled Campus-Wide Spyware and Virus Removal as a Method of Teaching Information Security at the Information Security Curriculum Development 2006 Conference (InfoSec CD 2006) at Kennesaw State University in September, 2006 [3]. Like many first-time programs, it was not completed without its share of issues requiring improvement. Considering that it was going to be incorporated in the future as part of this course’s curriculum, it is important to review the first instance of this project, the conclusions drawn from it, and how they can be used to improve the project for subsequent Information Security classes.
THE 2006 PROJECT

The virus/malware scan project executed during the Spring 2006 semester was originally conceived as a submission to Armstrong’s Faculty Development Committee for consideration to be awarded a Teaching and Learning Grant. Upon approval, the grant was used to purchase flash memory jump drives to be given to the general student population as an incentive to participate in the sessions. Such incentives are often an important component of a “security awareness program designed to keep information security at the forefront of users’ minds as they work day to day.”[6] The drives contained the anti-virus/anti-spyware software used to conduct the sessions. The funds were also used to pay two student assistants majoring in IT up to $200.00 each to help with the design and implementation of the project, instruct the student participants in security best practices, perform the scans, and to collect scan data.

Expected outcomes – anticipated improvement in teaching and learning

The two target populations of this project were the student participants who had their notebook computers analyzed and the IT students performing the analysis. It was expected that the project would provide a benefit to student participants by ensuring that their computers were virus and malware-free, and that it would improve information security awareness on campus.

For the IT student assistants, it was anticipated that the practical experience gained would include the ability to identify and assess risk, plan and conduct a security education, training and awareness (SETA) program, work with different security technologies, and instruct students in various security best practices, thus translating the theory of the classroom into action.

Execution

On the basis of their technical expertise and interest in the project, the two student assistants were selected from my ITEC 3100, Information Security class. In order to keep the project on schedule, the assigned tasks were entered into MS Project, thus simulating a real work environment. Based on their academic and work schedules, several dates were chosen for the scans and a location was selected.

The assistants were assigned to write a list of approved practices to be distributed to the participants at the evaluation sessions; a list of statistics to be collected and survey questions that the participants would answer; and a list of software to be loaded on the flash memory drives. In order to “spread the word about mobile device security weaknesses”[2] and our scan sessions, they created the advertising and ensured that it was distributed throughout the campus. Designing the various elements of the plan gave them realistic experience in systems design, necessary for the installation of an information system of any size.

Three different two-hour scan sessions were held during the Spring 2006 semester. Twenty-five student notebook computers were evaluated during these sessions.

Upon arrival, each student was required to fill out a liability waiver. The assistants recorded technical information about each participant’s computer. The student assistants and I loaded the security software onto the participant’s notebook PC from the flash memory drive. When the scans were completed, each participant was given the
flash drive. In each case, if a participant had up-to-date antivirus or anti-spyware software, those programs were used to perform the scans. Otherwise, we used the programs that were downloaded to their computer. Viruses and malware were removed from those computers that were infected and statistics were recorded. We also checked to determine if the students were performing regular Microsoft security updates.

The student assistants taught the participants various different ways of protecting the data on their notebook computers. These included: instruction in the utilization of “strong passwords containing alpha-numeric characters that are at least eight characters long and are unique”[2]; instruction in how to update their anti-virus software; the proper execution of the security software given to them; how to perform Microsoft security functions; and instruction in the use of a mobile firewall.

Lessons Learned
1. We needed more student assistants, as there was too much work to be done by only two assistants and myself. The project was funded to provide stipends for two assistants. Using students who were being paid and students who were not being paid might have caused conflict throughout the duration of the project. Since future sessions will not involve student stipends, budgetary constraints will not be an issue. The solution to this is that the entire Information Security class should be involved, not just two student assistants. Working the students in shifts should alleviate any scheduling problems. More assistants will also facilitate a more accurate recording of scan statistics and provide the student participants with more one-on-one instruction.

2. Not enough time was given to thoroughly scan each student’s notebook computer. A normal virus scan may often run for one hour or more. The longest session was only two hours long. Some of the scans had to be aborted before they had completed. Some students who showed up an hour into the sessions had to be turned away. Provided that we have enough student assistants, we should schedule each session for a minimum of four hours, and perhaps an entire school day. An increase in the number of student assistants should make it easier to offer longer sessions.

3. We used the university’s faculty dining room for the scan sessions. While the room provided ample enough space to accommodate all of the student participants, with only two network jacks, the location was not conducive to downloading updates to the software. Use of another location with wireless access or more network jacks that was more readily accessible to the general student population would be preferable for future scan sessions.

SPRING 2007 – IMPLEMENTING THE RECOMMENDATIONS
At the beginning of the Spring 2007 semester, the entire ITEC 3100 class was charged with preparing and executing the semester’s campus-wide virus/malware scan activity. Implemented as an integral, graded component of the course, the students were tasked with:

- Electing a group leader to manage the project and a group scribe to document the project.
- Keeping track of the progress of the project either in project management or spreadsheet software, and submitting updates and meeting documentation for my review.
Taking into consideration the schedules of the class members and my teaching schedule, determining the date and time period of the scan session, as well as the project member shift work schedules on those days.

Taking into consideration room size, physical layout, student accessibility, and wired or wireless connectivity, determining various appropriate locations on campus and then making their recommendations to me so I could reserve the room.

Determining and obtaining the software to be used to perform the scans.

Determining the data to be collected from the scan of each student’s computer.

Acquiring or creating the necessary liability/security waivers.

Creating the advertising and ensuring that it was properly posted on information boards throughout campus and in the student newspaper.

Requiring the entire class to be involved had two advantages. It ensured that all of the students in the class would receive the maximum benefit of this practical exercise. It also ensured that, working in shifts, we would have enough students to perform the scans.

The class group determined that six hours would be long enough to scan an optimum number of student participant laptops. This would mitigate the problem of incomplete scans that occurred during the 2006 sessions. It would also give student participants more time to take advantage of this service. The problem of students showing up with only an hour left in the session was one that could not be resolved. The class group determined that those who showed up late into the session would be provided the software, taught how to use it, and be instructed to perform the scans on their own at home. It was expected that some student participants would have to leave their laptops with the project team to receive the full benefit of the scans. This and the possibility of the corruption or damage to any files or computers required the acquisition of a thorough liability waiver. After attempting to find such a waiver online, the team was provided the same waiver used during the 2006 sessions.

After researching various university venues for suitability, the students selected a student organizational boardroom adjacent to the student cafeteria. This room had several advantages over last year’s venue: while smaller in size, it was still large enough to accommodate a dozen participants at one time; it’s proximity to a large number of students as opposed to a room that was not readily apparent to most students; and its wireless connectivity, allowing the group members to download the latest updates to the software that they would be downloading onto the participant laptops.

As opposed to the 2006 project, the students in the 2007 cohort created impressive, professional-looking advertising to post throughout the campus. Considering that the 2006 flyers were effective in inducing students to participate, it was expected that these advertisements would be even more successful in convincing the general student population to have their laptops scanned. In addition, the students passed out the flyers to various professors in the School of Computing so that they might give them to their students.
Spring 2007 project results

Each student in the class participated fully in the design phase of the project, completing all of their assigned tasks in time for the scan session, which was held in early April.

Twelve students participated in the scan session, which was less than we had expected. Upon arrival, each student was required to fill out an information form and sign the liability waiver. Specific technical specifications about their computers, such as the operating system and processor, were recorded. Before picking up their computers, each student was instructed in the utilization of strong passwords, the correct use of their virus / spyware protection software, and the need to perform regular security software updates.

Nearly all of the student notebook computers were virus-free, and those that were infected had no more than ten virus objects. The quantity of spyware removed from the machines varied. Some notebook computers did not contain any spyware, while others had as many as 500 spyware objects that were deleted when the software was executed.

Of greater significance were the results of the surveys given to the student participants and the students in the project group. When asked if they understood what was being done to their computers, 80% of the student participants responded yes. 100% of the participants felt that the IT students were helpful and 90% of the participants would recommend the service to other students.

The students in the project group were surveyed after the completion of the project. Their responses are given in the table below.

<table>
<thead>
<tr>
<th>Question</th>
<th>Strongly Agree</th>
<th>Agree</th>
<th>Neither</th>
<th>Disagree</th>
<th>Strongly Disagree</th>
</tr>
</thead>
<tbody>
<tr>
<td>The class project was a valuable component of the course.</td>
<td>1</td>
<td>5</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The class project provided me with practical experience in creating and executing a security awareness program.</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>The planning process was adequate to implement the project.</td>
<td>5</td>
<td>2</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The advertising was effective / adequate in encouraging students to attend.</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>The project provided a benefit to the students of AASU</td>
<td>2</td>
<td>6</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>I perceive that the students who participated in the session really needed the assistance we provided.</td>
<td>7</td>
<td></td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>This project should be performed again in future cohorts of ITEC 3100</td>
<td>5</td>
<td>2</td>
<td>1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Despite the poor attendance, the responses detailed above and comments of the project team members indicated that they felt that the project was worthwhile. They felt that it benefited the project team members and the student participants, and that it should be continued as an integral part of the course in the future.
CONCLUSIONS

Each team member wrote recommendations for improving the project in future Information Security classes. Most frequently mentioned were the need to hold the scan sessions on multiple days and the need to improve the promotion of them. Rather than use print advertising posted on university bulletin boards, team members felt that online advertising could be more effective. Some of the more original suggestions were to use the university portal Pirates Cove, a social networking site such as Facebook, or to use a survey site such as SurveyMonkey;com to advertise the scan sessions. Surveys and e-mail blasts could be sent to all AASU students via the Pirates Cove. One particularly innovative recommendation was to use SurveyMonkey.com to survey the general student population before the scheduled scan sessions, and then invite those students who respond to the survey to attend. In this way, we would be able to know in advance the number of students the class would be servicing.

There were significant improvements in this exercise from 2006 to 2007. The most important factor in achieving success was including the entire class in the project. This not only made it easier to run the scan session, but improved the organization and preparation of the assignment. With each student assigned different tasks and a group leader working to ensure that they were completed on time, the project was executed without difficulty. Students do not often care for group projects, but those in this class overwhelmingly felt that the planning process was instrumental in achieving its success. In addition, this assignment exposed them to some of the components of a SETA, and the tasks necessary to implement one.

Pedagogically, this project had value to these Information Security students. Coupled with their recommendations, this security awareness program will become a fundamental component of this course in the future.

REFERENCES