Proceedings of the 12th Colloquium for Information Systems Security Education
University of Texas, Dallas
Dallas, TX June 2 - 4, 2008

Engaging Millenials with Information Technology: A Case Study Using High School Cyber Defense Competitions

Doug Jacobson and Julie A. Rursch, *Iowa State University*

Abstract – Those of us in the fields of computer engineering and computer science find ourselves in the middle of an oxymoron. We are at the intersection where enrollments in our disciplines are dropping while at the same time the need for creative minds to solve pressing security problems is on the rise. Our institution, a well-known land grant with robust programs in computer security and information assurance at the undergraduate and graduate levels, recognized the need to encourage more Millenials to study in an information technology-related area and has started a program to try to entice students to enter our chosen professions.

Aimed at high school students, our program was started as an after-school, extra-curricular activity which allows students to explore information technology (IT) in a non-threatening, non-graded environment. At the time of this writing, the program was in the middle of its third year of implementation. In addition to educational materials such as video-taped lectures and lab experiments for students to watch and try on their own, the high school IT club gets equipment to setup their own cyber security lab and a local IT professional to serve as their mentor to guide them in their exploration. The students' end goal in their experimentation is to compete in a state-wide cyber defense competition. This goal is what guides their progression throughout the months of IT club meetings and experimentation prior to the event.

Although the primary goal of the program was to help students explore information technology, a secondary, an ultimately as worthy goal, was to make the whole experience fun. The program is not about structured learning or examinations, but exploring networking and security concepts. It also is about participating in an event where students can simultaneously compete on a team and make friends from other schools at the same time. The resulting atmosphere is a cross between competitive sporting environment and IT celebratory party with just a hint of an all night pajama party rolled into it.

Doug Jacobson is a professor in the Department of Electrical and Computer Engineering at Iowa State University.
Julie Rursch is a Ph.D. candidate in the Department of Electrical and Computer Engineering at Iowa State University.

I. INTRODUCTION

It is a well-documented fact that enrollments in computer science and computer engineering are on a decline[1] at the exact time when more and more technology is being used in the work place and in research. Current high school students are being counseled away from careers in information technology (IT) in some part due to the media campaigns about information technology jobs, especially technical support jobs, moving off-shore. Coupled with these reports are parents' and high school guidance counselors' recent recollections of the harm from the dot-com bubble burst. It isn't hard to remember back six to eight years when technology-related company stocks that had soared skyward based upon artificially inflated hopes plummeted to rock bottom prices. Companies contracted. Some folded. Many had huge reductions in information technology work force which sent ripples through the nation's economy.

However, there has been a national report[2] demonstrating that just in a time when we need knowledge workers the most, students are not being encouraged to enter these areas. Additionally, parents are not counseling students to take advanced math and science in high school -- a choice which heavily influences and effects their selection of college career and employment paths. Additionally, high school curriculum is relatively rigid and legislated by states. There is very little room for creativity in curriculum development at a high school level when there are standards and standardized tests to be taught to and which students must pass. This minimal knowledge approach is meant to improve our society, but in fact reduces the opportunities for students to explore and interact with exciting new areas such as information technology.

Many high schools do not have even one class in computer programming or networking, let alone a whole track where the logic and creativity found in information technology can be explored. In a rural-oriented state such as the one in which we are located, high schools are relatively small in enrollment numbers and geographically disperse. Many high schools provide the basics to students with not many additional course selections. In

more urban centers in our state, there are larger high schools that offer courses such as Cisco networking or Visual Basic programming. However, these courses do not tend to engage any other than those students who have already self-selected into a technology-oriented program. Many times this self-selection comes from contact with family members or other influences who demonstrate the exciting opportunities that are available through information technology areas.

So, at a time when information security threats and issues are on a rise our nation finds it has fewer people entering the computer science and computer engineering fields and challenging themselves with our most pressing problems. Our institution, a well-known land grant with robust programs in computer security and information assurance at the undergraduate and graduate levels, recognized the need to encourage more Millennials to study in an information technology-related area and opted to start a high school program to encourage more students to at least explore, and hopefully select, information technology areas as possible career options .

Our high school program was created as an after-school, extra-curricular activity structured so that students can explore information technology in a non-threatening, non-graded environment. In addition to educational materials such as video-taped lectures and lab experiments for students to watch and try on their own, the high school IT club gets equipment to setup their own cyber security lab and a local IT professional to serve as their mentor to guide them in their exploration. The students' end goal in their experimentation is to compete in a state-wide cyber defense competition. This goal is what guides their progression through out the months prior to the event.

This paper discusses the objectives for the program; the implementation of the IT clubs; the execution of the cyber defense competition; the results we have had in two completed years of the project; and the future areas in which we are growing the successful program, including the expanded third year venues.

II. OBJECTIVES

The concept of hacking, being attacked and fighting off attackers is an enticing, romantic notion for many Millennials who may not be excited about math or science as pure subjects but can get excited about learning about something that is but a stone's throw from crossing the line between right and wrong. This attraction is very apparent to anyone who has taught an information warfare class which includes attack and defend labs as components. University students generally cannot contain their enthusiasm for their assigned projects. The large break-in labs are much anticipated and are generally thoroughly discussed well-after the lab and/or course ends.

It behooved us to leverage the seducing aspects of attack/defend exercises that are so clearly demonstrated in our undergraduate and graduate students' education and couple it with the unbridled enthusiasm that can be found when students are given equipment, a little knowledge and allowed to explore at their own pace, using their own constructs.

The primary goal of the high school cyber defense program was to pique the interest of students in information technology and through that increased interest, raise the number of students who opt to study information technology as their college career and their employment path.

A secondary, and ultimately as worthy goal, was to make the whole experience fun. The program is not about structured learning or examinations, but exploring networking and security concepts using our provided educational materials and personal contact with a local IT professional who serves as a mentor. It also is about participating in a team event where you are competing with other schools, but also making friends with them in a real celebration of IT which, at times, has the ambience of an all night pajama party.

The program has been successful in allowing high school students who may not self-select into studying information technology areas for a grade or exploring them on their own time to join in club activities that are completely creative and not evaluated in the usual academic sense. Through this exposure we are trying for more high school students to become aware of the opportunities to study in information technology areas and choose to follow one of these paths which may include computer science, electrical engineering, computer engineering and/or management information science.

III. PROGRAM IMPLEMENTATION

Our project is designed as an after-school, extra-curricular program that is based upon inquiry-based learning and not strict curricular content, although educational materials are provided for students as a starting point. In 2006, our first year of work with the project, the program was run strictly as a cyber defense competition for high schools in the state. In the second year, 2007, the concept of each high school forming an IT club that meets for several months preceding the competition and covers many different security topics, not just the anticipated competition, was added.

The basic construct of creating a student club to study information technology was very loosely modeled after our successful collegiate information assurance student group, albeit with major additions to compensate for the age of the participants, level of knowledge and skill, as well as geographic dispersion.

Like the collegiate group, our high school IT club provides the arena for students to meet and discuss security issues, as well as participate in hands-on labs which provided them real world experience and an opportunity to partake in a cyber defense competition. The major differences stem from the need to provide educational materials as a framework for network concepts, the need to dispense equipment across the state to each high school and the necessity for an IT professional to be available to help answer questions about IT for the students.

The requirements for the high schools to participate in the program were few and came with very little monetary cost. A high school had to allow an IT club to be formed with an advisor, to setup a cyber security lab by either accepting the equipment we provided or providing their own, to allow students to meet and experiment with the equipment in the high school and to provide transportation to the university so the IT club could participate in a state-wide cyber defense competition.

A. IT Club Structure

While we do not have bylaws or other formal structures for our IT clubs, there is a need for the local high school to have an advisor, an adult who is responsible for those students meeting in the school. Some of the advisors to the IT clubs are IT instructors at the high school because there is an IT or computer-based curriculum available. However, more of our advising teachers are just someone who really cares about students and student learning. Some example employment roles our advisors have in the school system are the talented and gifted coordinator, IT support specialist, science/biology teacher, industrial arts teacher and librarian. Many of them are not content specialists in information technology or are not certified teachers in the case of the support specialist. They only recognized an opportunity for sparking interest in students.

This, of course, presents challenges in instructing the advisors. This is why we modeled the IT clubs to have not only an advisor, but also a mentor. In the cases where the advisor is an IT instructor, the need for a mentor may not be as great. However, for those advisors with little to no information technology background, the mentor fills in the missing gaps. The IT mentor is an individual who can help the club members when they experience technical problems in their labs and experiments. The local IT professional can also provide real world insight into careers, technical problems and solutions in IT arena which will also stimulate interest in those career paths. Generally, the IT mentor is a working IT professional from the local area, however, in some cases, students from our collegiate information assurance student group have provided mentorship for high schools that are close to the university.

B. Educational Materials

Although we provided an IT mentor, many of those folks were volunteers with limited time and could not cover all the basics to bring the students up to a level to begin experimentation. Therefore, there was a need to provide basic networking and system operating system concepts that are prerequisite to competing in a cyber defense competition. This includes the knowledge of IP schemes, routing, firewall, services and protocols.

In 2006 undergraduate and graduate students from the electrical and computer engineering program created five demonstrations on operating system installation and networking which were video-taped and delivered to each team via DVD. In the second year, 2007, a graduate student took on the responsibility for creating the lectures and generated ten lectures that included step-by-step installation instructions for operating systems and services that would need to be run for the cyber defense competition, as well as basic networking concepts. Each lecture included a printed document and any visual aids used in the presentation so that students or advisors could use them to review and practice with. As in the first year, the lectures were delivered by graduate students in our program and video-taped for electronic delivery.

The lectures, which were developed in year two, are also being used for the third year of the program (2007-2008) which is discussed in the results section of this document. The lecture topics covered included FreeBSD installation, basic unix commands, basic network concepts, an explanation of ports and protocols, implementation of sendmail, POP/IMAP and DNS, securing a remote programming environment, installation and securing of an Apache web server and PHP, installation and setup of a firewall, as well as securing Windows and unix-based systems through limiting of services and watching of log files. These additional lecture materials and more step-by-step instructions were created to help the students master network setups and solidify their understanding of what they were doing.

As anyone who studies information assurance and cyber security knows, ten lectures could not possibility cover the complete scope of topics that need to be attended to. However, these educational materials were intended to

point the students in a direction where further, in depth, inquiry-based approach can be undertaken. The overarching goal of competing in the state-wide cyber defense competition narrows the spectrum of topics for the students while allowing them freedom to explore different options to install and secure their systems.

C. Cyber Security Lab

As part of the program, we provided computers and networking equipment to each high school. Each school was shipped equipment several months before the competition. The equipment allowed students to setup their own cyber security lab and replicate the lecture steps that were demonstrated. As the students work through the lab materials, they can explore and combine the techniques presented in the video, as well as experiment with other options they discover or create on their own. This experimental environment with no wrong or right answers provides a route for IT naïve students to explore in a non-threatening way. It also provides an avenue for IT aware students to take leadership roles in the club, teaching and helping other students while honing their own skill sets.

This cyber security lab was to be their test environment which allowed them to choose and experiment with different operating systems and services so that they would have some experience before they made their final decisions about the operating systems and services they were to run in their competition network.

In years one and two the equipment supplied was modest. Two to three computers, a four or eight-port hub, keyboards, mice and a KVM were supplied. In year two a wireless access point and two wireless cards were also supplied for the students to experiment with. The only operating system supplied on cd was FreeBSD since it was covered in the installation lecture, however, students were encouraged to download other operating systems such as Ubuntu and Fedora which may seem more intuitive for them since they come with a GUI interface by default.

D. Cyber Defense Competition

Cyber defense competitions have various incarnations from capture the flag competitions where students try to earn entrance into systems and gain access to specific files to competitions where students defend sets of systems that either they configure or have been preconfigured for them. [3] [4] Our competition is a hybrid one which falls under the realm of competitions in which students configure their own networks, but ours includes a set of additional challenges – supporting end users throughout the event who test usability and request additional services.

Students in our competitions are required to configure their networks as described by a scenario published one month before the competition. The scenario details the services that they have to implement in a short story format, as well as their network address space. They are told they are the IT support staff for a company or school and have to implement services such as email, web mail, remote programming, file sharing and web hosting. They are also told they are responsible for their own DNS and would be wise to implement a firewall to help protect their networks. They are also given some service that is a legacy installation which must be supported in a present state which provides some inherent security vulnerabilities that they have to protect against. In our competitions, these student teams are known as the Blue Team and are given t-shirts of that color when they arrive to designate their role in the competition.

Our twist on the cyber defense competition is that in the scenario they are told that they will need to support end users which will be people at the competition who use their network and request changes to be made to it throughout the 18-hour competition. These end users are called the Green Team. The addition of the Green Team is what helps keep the students focused on providing a useable network, as well as a secure one. As with the Blue Team, the Green Team members are given color-coded shirts so it is immediately apparent what team a specific individual is on as we work throughout the 18-hour event.

The group who tests each Blue Team network for vulnerabilities and play the role of attackers in the competition are IT professionals and graduate students who are dubbed the Red Team. The White Team oversees the event, as well as records scores from the Green and Red Teams.

Our competition is organized and run by our collegiate information assurance student group. Club members serve as the overall director, Green Team leader and general coordinators with help from our faculty members.

Unlike our collegiate cyber defense competitions where most teams come to the facility to configure their network, the high school students could not be physically present for setup. Therefore, for the high school cyber defense competition, the Internet-Scale Event and Attack Generation Environment (ISEAGE – pronounced ice-age) research facility was opened for remote setup of the competition network one month before the actual competition date. In addition to a printed document about how to access remote setup, a video-taped lecture was also provided to help illustrate the remote access

procedures to our facility for the high school students and their advisors.

The ISEAGE research facility is a first of its kind facility in a public university dedicated to creating a virtual Internet for researching, designing and testing cyber defense mechanisms, as well as the analysis of cyber attacks. Unlike computer-based simulations, real attacks are played out on real equipment against real equipment. It is a controlled environment that allows us to play real attacks against the students' networks and demonstrate to them real world security concepts.

As a competition network each school was assigned a rack of eight computers that they could remotely load with any legal operating system and configure in any manner they chose. Operating systems were primarily installed through a PXE-boot environment with operating system images from which to choose. However, there was also some demand by the high school students for other, lesser known open source operating systems which required cds to be made and inserted into drives for them. This was accomplished through the use of a chat room was manned approximately 20-30 hours per week, mainly in the evening, by members of our collegiate information assurance student group for the month leading up to the competition.

Assistance provided to the high students through chat included answering setup questions, physically assisting them with their racks of computers which they were configuring, installation of additional memory or network card, rewiring their "network" so that their firewall could be implemented. This was a beneficial exercise for both the high school students and our college students in terminology, network design and implementation.

After the month-long remote setup, the IT clubs arrive at the ISEAGE research facility and the real work began. They had to finalize their setups, defend their network and test what they had learned in the preceding months over an 18-hour period. The facility opened at noon and the teams are given approximately five hours to complete their setups before the first network scans by the attackers (or Red Team) were made. The 18-hour competition ends with a debriefing by the Red Team of what teams did right, what teams did wrong and how they could go home and practice for next year's competition, as well as an award ceremony.

IV. RESULTS

In May of 2006, we had 12 high schools and 75 high school students who participated in the event. With a few exceptions these schools were either geographically close to the center of our state where our university is located or near more densely populated, urban areas.

In 2007 we doubled the number of students with more than 150 coming to play who represented 19 high schools from across the state. We were able to not only expand the number of schools and students, but to reach farther outside our circle of influence to gather up participants. Granted that our reach had grown in our second year, it still had a disproportionately higher number of entrants from urban centers in our rural state.

Both years, all teams in the cyber defense competition are "owned" by the Red Team. There are enough Red Team members attacking and exploiting the high school teams' networks that all of them are eventually compromised. However, the level of ownership and the actions taken during the attack clearly demonstrated different levels of understanding and skill of the Blue Teams.

As stated in the implementation portion of this paper, the second year (2007) was the first time the IT club concept was included in our program. The IT clubs were formed in the high schools in the month between the end January and the end of February. This only gave the clubs 1 ½ months of experimentation on their own networks before they began setting up their competition networks. This small lead time was not uncomfortable for some teams, but others needed a longer lead time.

So, for the third iteration of the program, we began recruitment of high schools to participate in June of 2007. Recruitment continued into the fall 2007 term with the goal of running the IT club as an academic year-long club. So, our third season is considered the 2007-2008 year.

In the third year, through the generous donation of used equipment from a large grocery chain based in our state, we were able to increase the number of desktop machines shipped to ten. In addition to more computers, in year three we provided three Microsoft XP licenses through the Microsoft Authorized Refurbishing program for the students to install, as well as additional open source cds to give them more exposure to other operating system. We chose to include two GUI and two command line interfaces: Fedora Core 8, Ubuntu Desktop 7.10, Ubuntu Server 7.10 and FreeBSD 6.3.

Additionally, the year three format has expanded into new areas of experimentation to include robotics based upon the Lego Mindstorms NXT platform and game design based upon the virtual world programming environment of Alice. However, cyber defense is still the most wildly popular venue with nearly 35 high schools signed up at this point in time to learn about the topic.

We also have rented our athletic coliseum in which to hold the competition because to date we have recruited 40 high schools to participate in our program with approximately 400 high school students signed up to explore information technology. We expect approximately 300 of those students to travel to the university in April to compete in the two-day competitive event we are calling the IT-Olympics. To support this move in location from our research facility, we have to call into service our portable version of ISEAGE, named ISECUBE, on which to run the cyber defense competition. The change in location from our research facility to the athletic complex means the we will have the high school students remotely setting up one month ahead of time in our research facility and then logistically moving all the competition networks to the coliseum the night prior to the event.

With an expanded format of three venues instead of one and an addition of 300 students competing, the event will be two full days instead of the 18-hour event. It will include other activities such as track for participant siblings to play with Lego robots and a track for IT club advisors to earn graduate credit. Further, there will be an industry leader summit for students to talk to IT professionals, as well as vendor booths where students can interact with companies who hire IT staff. Finally, there will be admissions counselors from our three state institutions and some of the 15 community colleges in attendance to answer any questions the students, parents or teachers may have about IT educational options.

One final addition for the third year is the requirement that the IT club must complete an IT-related community service project and exhibit a poster about the project at the competition. This poster and the project will be judged and the scores will be calculated into their overall competition scores.

Although we have only begun tracking former participants in our high school cyber defense program, we have five students who participated in the 2007 event who entered our university as freshman with a declared major of computer engineering. We will track these students through their collegiate career to see if they stay in an IT-related area which we broadly define to include computer science, management information systems, electrical engineering or computer engineering

We are having a hard time tracking those students who entered in other departments, but we will work with our admissions office to see if we can correct this problem. Also, we have no real way to track those students who participated in our program, but entered other colleges and universities.

To date we have some anecdotal evidence about students' work in other subjects while participating in our program. One of our high school IT club advisors reported to us that other teachers in the high school remarked to him that the students who are actively participating in the IT club have improved their grades and their attention to course work that is not directly related to information technology. While we cannot extrapolate any significant meaning from these general remarks, it was encouraging to hear those remarks.

We have found that there is an absolute need for an IT mentor, especially for smaller schools. However, this poses a problem because IT companies are not abundant in rural areas. We have tried to look to the local Internet Service Providers (ISPs) and telephone companies to help us fill these positions. An additional solution has been proposed which is discussed in the future plans section.

V. FUTURE PLANS

As noted above a community service project has been included in the competition. This was added to see if we could change the gender imbalance in the makeup of the high school students participating in our program. In the past two years less than 1 percent of the participants were female. In working with our women in engineering program coordinators it was suggested to include community service as part of the overall track to attract girls who may not be excited by the hacking aspects. Additionally, the venues of robotics and game design seem likely to attract additional female participants, although we do not have solid numbers on that.

To address the lack of IT mentors for the program, especially in rural areas, we are working with our university extension branch to find IT mentors through the local extension offices. We also are exploring ways that we could implement the use of virtual meetings and conference calls to provide virtual mentors when a physical mentor cannot be located. We also have solicited the help of the local chamber of commerce to find smaller, local companies who are interested in taking on the role of mentor.

We see this program only expanding. We hope that while the project currently culminates in one overall competitive event, we could expand into multiple competitive opportunities for students. We are working to expand the high school enrollment to the point where we enlist the help of our 15 community college districts to host regional competitions that will feed into our statewide competitions. When scaled to full operation, the regional events hosted by the community colleges

would act as feeders into the statewide event that we continue to host.

Additionally, other competitions with specializations such web design could be added as the project matures.

Finally, there is a desperate need to determine a way to not ship equipment to all the high schools, but to find local companies to donate the equipment so that shipping costs, labor to recondition the machines and valuable time can be reduced.

---

[1] http://logos.cs.uic.edu/recruit/CSStatistics.htm

[2](2005) "Rising Above The Gathering Storm: Energizing and Employing America for a Brighter Economic Future Committee on Prospering in the Global Economy of the 21st Century:An Agenda for American Science and Technology", National Academy of Sciences, National Academy of Engineering, Institute of Medicine.

[3] Conklin, A. (2006). "Cyber Defense Competitions and Information Security Education: An Active Learning Solution for a Capstone Course", International Conference on System Sciences, p.200b. Hawaii.

[4] Hoffman, Lance J., Tim Rosenberg, Ronald Dodge, Daniel Ragsdale (2005). "Exploring a National Cybersecurity Exercise for Universities", IEEE Security & Privacy, Vol. 3, No. 5, p. 27-33.