Project Title:

Wireless Security Course Materials, Labs and Teaching Aides

 Applicant(s):

<table>
<thead>
<tr>
<th>Name</th>
<th>Bruce Hartpence</th>
<th>Telephone</th>
<th>X57938</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dept.</td>
<td>Information Technology</td>
<td>College</td>
<td>GCCIS</td>
</tr>
</tbody>
</table>

Summary

Within the field of networking, there are no topics more important or prevalent than wireless and security. The proposal seeks as its main goal, the development of a unique and effective learning environment within a course that combines these two elements. The course will follow the lecture/lab model where students will learn basic and advanced security techniques as they apply to wireless networks. This course will be the third in a wireless concentration.

In order to provide the best possible learning experiences, the lab activities will be modified to create a team environment in which the students will learn to build secure wireless networks and then defend their networks against actual attacks created by opposing teams. In this fashion the students will gain greater depth of understanding for the threats and proficiency in security these types of networks. While this idea previously inspired visions students learning hacking from their professors, it is now believed that in order to be effective at prevention, students must have an intimate understanding of the tools used by the enemy [1,2,3,4]. I feel that the time and energy to create this environment will be well spent. The following is an outline of the course topics and the lab activities planned. The course has already been approved by the department. The budget for this project is for faculty time over the summer 2004 to research and create this setting.

Course Outline:

1. Security Outline: A layered approach
2. First Generation Wireless Security
3. Additions to first generation wireless security
5. Traditional Security Measures Overview
6. Protection implementation and scope
7. Virtual Private Networking
8. Encryption
9. Radius, Kerberos, user authentication
10. EAP
11. 802.1x
Lab Experiences

1. Basic Wireless Security: ESSID and WEP
2. Enhanced First Generation Security
3. Antenna and radiation based security
4. MAC based filtering
5. Virtual Private Networking
6. User Authentication
7. Encryption
8. Next Generation Security: 802.1x

Targeted learners or population

The primary audience for this course will be students matriculated in the Bachelors of Science in Information Technology and the Bachelors of Science in Applied Networking and Systems Administration degrees. Students from other departments also take the networking courses offered by the IT department. These departments include software engineering, computer engineering and computer science. It is anticipated that these students will also be interested in the wireless concentration.

During the first year the department will offer one section of each course during the fall, winter and spring quarters with a total capacity of 36 students per quarter. During the second year, initial indications are that the interest will be high enough to offer at least two sections per year with two different start dates for the beginning of the sequence. This will result in approximately 70 students per quarter and another 5-10 students from other departments per year. There is also good potential for growth beyond that.

The sequence requires that the students have had some of the basic networking courses offered within IT department or their equivalents. Thus, it is expected that the students in these courses will be entering their junior year. This targeted course is at the 500 level and is populated with students reaching their senior year. These students will be well known by this time and it is expected that they will exhibit a certain level of maturity and an understanding of the ethics involved.

Anticipated impact on teaching and/or learning.

I believe that when students are given topics to learn, particularly those topics that have a practical component to them, certain tools and techniques provide the best possible chance of learning and retaining information. These include hands on activities in support of the lecture theory and analysis of these activities. This proposal seeks to push this concept further through interactive team assignments, defense against real attacks, performing attacks and in-depth analysis. Teams will be built early and maintained through the course of the quarter. In-depth analysis will involve packet decoding, tracking of statistics for the network, site surveys and final documentation. Faculty involved will be developing and implementing the advanced techniques and must have a complete understanding of the security measures to be put in place, the attacks and their effect, and the particulars of wireless communication.

Student success

Wireless communication and security are topics that have the attention of everyone in our industry and the press. Our wireless coursework has been very successful with students filling all of the sections offered including the summer quarter. Tying these two ideas together will increase student interest and make this concentration even more valuable to RIT.

Students involved in the coursework will receive constant feedback as they advance towards educational goals and will be able to see their abilities grow and develop as they advance through their
classes. I believe that students that are successful and have measurable abilities are more confident and so are more likely to succeed. These students will also be valuable commodities to industry and so should enjoy an advantage in the marketplace.

I have established relationships with various companies including Cisco and Microwave Data Systems. These relationships provide several things to RIT including increased awareness of the programs offered by the department, feedback into the educational process by real world companies and coop opportunities for our students. The companies also benefit in that they receive qualified students with the needed skills. These companies have also donated equipment to our program.

All of these things result in improved scholastics, student success and confidence and finally, increased opportunity.

Measurement and Reporting

Because of this different approach, I will be increasing the evaluation of the course by the students. In addition to the standard “end of the quarter” evaluation we will be performing a midterm evaluation. This evaluation will include discussion time to help increase student involvement and feedback. We will also be ensuring that no student is left behind because he/she got stuck on a particular topic or experience.

Upon completion of the first quarter and a review of the evaluation materials we will present the results to the networking faculty and make recommended changes to the course prior to the spring quarter. The presentation to the faculty will typically be in a small group forum or faculty meeting. It is also possible that in tracking the results, we may find that the results exceed our own expectations of success and this will be presented in teaching conferences.

Students will be evaluated in a group as part of their team activities both by the faculty and by their peers. In addition, they will be evaluated on individual performance in the form of a practical exam. This will allow them to demonstrate personal skills and knowledge of the course material.

Rationale

As a teacher in the networking area, I am constantly seeking to improve our course offerings, update materials or fill in gaps where they exist and create the best possible experience for our students. As part of this process, we interface with industry professionals to help us determine strengths and weaknesses. In this case, we have identified these areas as important gaps to fill and have had confirmation from industry. In my view, this project is vital to the continued success of our program because it represents the combination of two of the foremost concepts facing network professionals today – wireless communication and security.

Until recently, security was viewed as an advanced topic and wireless communication was limited to a single course. We have now begun to integrate security into each of our networking courses and have dedicated lab space for wireless networking. We have yet to combine these growing concerns. Very few people understand wireless networking to the extent that is demanded by the threats facing deployed wireless infrastructures. Wireless presents difficulties not faced by traditional networks simply because you cannot trace signals back to their source visually or control existing nodes. This innovative teaching approach will fill in a very important component of a networking education and ensure that our students remain the top in the industry.

The number of faculty interested in wireless communication and security is increasing as is the number of students interested in pursuing advanced study in these areas. While I am the principle architect of the wireless curriculum, we have faculty who have come to the IT department with significant experience in wireless communication. Two such examples are Bo Yuan and Larry Hill, both of whom are involved in the concentration. Within the networking and systems administration cluster of IT, we have also written several grant proposals both for the curriculum and research projects. Currently Nirmala Shenoy and I are involved in a research project that is being funded by Cisco Systems to investigate
mobility and Quality of Service in wireless networks. As a result of the experience of the faculty, I believe that it would take only one or two quarters to adjust to the additional material and methodology I will be using in this new course.

I have had a good deal of success creating new and innovative teaching tools and approaches. I was one of the first in the department to teach a course in a studio model and I regularly create teaching tools to help students understand difficult concepts or gain significant real world experience. Examples of these include wave division multiplexers built with flashlights, cardboard boxes and tin foil, having students work on ITS projects for wireless network mapping, using water tanks to demonstrate wave motion, having students build their own antennas and the creation of wireless research carts. These carts are equipped with several different types of equipment and can remain in the field for several hours for advanced testing. It is my belief that approaches like these lead to improved increases in learning and interesting experiences that improve student confidence and their enjoyment of the class. Both of which may assist in student retention.

As I have mentioned, we will taking a team approach with attack and defend methodologies for the course. The idea is that the students will be building complex wireless networks with a wired core. They will deploy traditional and advanced wireless security mechanisms to protect their networks. They will then use well-known and emerging security exploits and attacks to subvert the security employed by opposing teams. These attacks will be analyzed and patches made on the systems. Students will be tested on their ability to build/secure networks, respond to attacks and finally analyze/document the experiences.

The department has every intention to develop a wireless security course. This grant will be for support during the extra time and effort dedicated to creating the unique learning environment outlined in this document. More than building labs or writing course material, the creation of this combat environment, control of the tools, design of the activities/analysis and the evaluation will require energy and research to ensure that all students benefit. This work will be well above that for normal course development.

To conclude; this idea is innovative because nowhere are the ideas of wireless communication and security combined where the students will be employing an attack/defend/analyze approach on real networks here at RIT.

**Timetable**

- **Summer 2004 (20034)** - Attack/defend methodology scenarios designed and tested.
- **Environment secured.**
- **Additional wireless and security topics developed and implemented on new lab equipment.**

- **Fall 2004 (20041)** - First section offered

- **Winter 2004 (20042)** - Evaluation of course results from previous quarter.
- **Necessary modifications made.**
- **Possible addition of new scenarios and techniques.**

- **Spring 2005 (20043)** - Second section of course offered.

**References**

2. [http://www.silicon.com/management/careers/0,39024671,39118900,00.htm](http://www.silicon.com/management/careers/0,39024671,39118900,00.htm)
3. [http://www.infosecinstitute.com/courses/ethical_hacking_training.html](http://www.infosecinstitute.com/courses/ethical_hacking_training.html)