Project Title:

Wireless Security Course Materials, Labs and Teaching Aides

Applicant(s):

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

Proposal Brief Summary

The proposal seeks as its main goal, the development of a unique and effective learning environment within a course that combines security and wireless elements. 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.

Final Report

In preparing this report, I decided to address each one of the areas outlined in the proposal and use the same headings as those seen in the RFP. As the summary describes, at its’ most basic level, I was building a lab based course for wireless security. However, further examination will show that what I am really trying to do is create an environment that fosters teamwork, in-depth analysis, learning of advanced topics and iterative evaluation, all while leaving no student behind the group. All of this will occur in a sort of networking arena where teams are surrounded by attackers, and so must defend themselves, while launching their own attacks.

As of today, this course has been run twice, with modifications made at the midpoint and end of each section. Further modifications will be made for the third iteration of the course this spring. So far, the students have stated that they have been challenged, that they have enjoyed the course and have learned a great deal. The complaint that stands out as having to with the actual running of the course is that there was so much to do, that little time was left for the attack/defend exercises. I will be addressing this in the next class.

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. This is simply because this course is the third in a concentration. Most students outside of our department do not have room in their schedules for an entire concentration outside of their area. However, to date we have had students from four different program codes in the class.

Anticipated impact on teaching and/or learning.

In order to create the desired environment, I chose to combine hands on activities, tools, techniques, interactive team assignments, attack/defend, in-depth analysis, cause/effect and documentation.
experiences. The objective was to combine them in such a way as to maximize student learning while creating students that had precisely the skill level and understanding demanded by wireless security experts in today’s industry. To this end, I decided on a three phase approach. Each phase contained the following elements; lecture topics, building (adding on to) the network, faculty evaluation of student abilities, attack/defend and finally, debriefing.

Students would learn about security techniques and concepts before deploying them in the lab. The instructors would then evaluate the students to determine their level of understanding and completeness of the deployment. Students would then engage in war games between the teams. After approximately one week, the entire class would debrief the attack/defend period. During this time students would discuss strengths, weaknesses, techniques and how well the program is progressing. The entire process represents a significant departure from traditional lab based classes and certainly lecture based classes on security.

**Student success**

The teaching approach was really an attempt to maximize the benefits to the student. A high level of student interest is maintained because they are actively dealing with two of the hottest topics for the real world – wireless and security. In addition, they are given a chance to engage in the attack/defend activities which, for lack of a better term, are fun. The debriefing periods provide immediate feedback, opportunities to share your knowledge and learn from the success/failure of other teams. The number of companies aware of our methods is increasing. Primarily we have engaged in two methods for ensuring this; our annual industrial advisory board and direct communication with organizations during the school year regarding a particular course of study or class. Companies that we can include in this list over the last 18 months include Cisco, Avaya, Extreme, MacSource and MDS.

**Measurement and Reporting**

So, how have we determined our level of success? The most obvious is the evaluation of student work. This currently includes the security/network construction modules, final exam, midterm exam, site book documentation and lab activities. These grades provide one form of data but another is provided by the oral exams given during the lab activities. At this point the instructor discusses the activity or technique used in an attempt to determine the level of understanding for each member of the group.

The debriefing period provides additional feedback regarding the success of the class. Not only for sharing of information, students are free to discuss their views on course direction and methodology. It is the intent of this portion to ensure that no student is isolated. Everyone taking the course should understand what is going on, what has been done and why. This is vital to the success of a security deployment.

Written evaluations of their teammates are also part of the process. By design the students are given more than any single “superior” student could complete. So, it is a must that team members work together. If not, the team is at a disadvantage during the attack/defend phases and may become the accepted target for all teams. The peer evaluation is part of their grade calculation. Students also provide the final piece of information in the form of course evaluations done privately.

In the end, faculty members take all of this information and attempt to assess what changes should be made and the direction for the course. As security techniques change rapidly and new attacks are created quite often, this is a dynamic, ongoing process.

**Rationale**

What is the right approach? The question that regularly appears in this class is whether or not we should teach hacking. My response has always been – without knowledge of the tools and techniques used by the
bad guys; you cannot know how to defend yourself. I also believe that based on current results, with minor changes, this is absolutely the best technique to ensure learning by all students in the class, improved student skill levels and attractiveness to industry.

**Dissemination**

Over the next several weeks I will be offering a series of bootcamps on wireless security and home network security to the Golisano college departments. Initial interest is high with over two dozen faculty members expressing interest.

During the October 2005 SIGITE conference I presented my paper on Teaching Wireless Security for Results. The paper was peer reviewed and is published in the proceedings form that conference. The URLs for both the paper and the presentation follow.

http://www.it.rit.edu/~bhh/fp1054-hartpence.pdf

http://www.it.rit.edu/~bhh/TeachingWirelessSecurity.ppt