A Multi-Tier Approach to Cyber Security Education, Training, and Awareness in the Undergraduate Curriculum (CSETA)

Dr. Nikunja Swain P.E., South Carolina State University

Dr. Swain is currently a Professor at the South Carolina State University. Dr. Swain has 25+ years of experience as an engineer and educator. He has more than 50 publications in journals and conference proceedings, has procured research and development grants from the NSF, NASA, DOT, DOD, and DOE and reviewed number of books on computer related areas. He is also a reviewer for ACM Computing Reviews, IJAMT, CIT, ASEE, and other conferences and journals. He is a registered Professional Engineer (PE) in South Carolina and ETAC of ABET reviewer for Electrical Engineering Technology and Computer Engineering Technology.
A Multi-Tier Approach to Cyber Security Education, Training, and Awareness in the Undergraduate Curriculum (CSETA)

Abstract

The demand for cyber security experts in both the public and private sectors is far outpacing the development of the talent pool, making for a hyper-competitive labor market. Against ever evolving cyber-threats the need to graduate students skilled in the concepts and technologies of cyber security is becoming a critical responsibility of academic institutions in order to help preserve the sovereignty of the US and her allies. It is crucial that more undergraduate majors receive education and training that deepens their conceptual and practical understanding of issues in cyber security. In addition to educating computer professionals, undergraduate students of all disciplines should have the opportunity to be exposed to issues regarding computer security. As a result, we should all recognize the importance of cyber security in the undergraduate curriculum. Our graduates must have security skills in addition to communication, critical thinking and analytical skills. This additional skill will offer our majors the opportunity to extend the security focus beyond the department, to raise awareness outside of the computer science community, and provide a path for further studies and employment in cyber security. The objective of this paper is to discuss these activities.

Introduction

Information and Communication Technologies (ICT) have become increasingly important for US citizens, who are becoming dependent on the use of information networks and services in their daily lives. Yet, while uptake of new technology among citizens is high, a large portion of the population remains unaware of their exposure to risks from security breaches and “cyber-abuse” in the form of network disruptions, malicious code, criminality and hackings, as well as hardware and software failures. There is an urgent need for the development and implementation of awareness-raising campaigns targeted at safe and responsible use of ICT.

As software systems become increasingly complex, there is an urgent need to address defects and security attacks. The 2005 U.S. President's Information Technology Advisory Committee (PITAC) report Cyber Security: A Crisis of Prioritization included statistics on attacks and vulnerabilities. It concludes with:

Today, the threat clearly is growing. Most indicators and studies of the frequency, impact, scope, and cost of cyber security incidents – among both organizations and individuals – point to continuously increasing levels and varieties of attacks. The data show that the total number of attacks – including viruses, worms, cyber fraud, and insider attacks in corporations – is rising by over 20 percent annually, with many types of attacks doubling in number. For example, according to Deloitte’s “2004 Global Security Survey,” 83 percent of financial service organizations experienced compromised systems in 2003, more than double the percentage in 2001. Moreover, the reported level of security incidents almost certainly understates the actual
level. There are few incentives – but strong disincentives – for large organizations to report incidents in a public forum. Targets of cyber attacks typically are concerned that widespread disclosure of their victimization could shake public confidence in their operations, not to mention attract other attackers.

While the economy may be slowly nursing itself back to health and remains marred by an elevated unemployment rate, the job market for cyber security experts is booming. The relatively young field of Cyber Security is flourishing as threats to critical infrastructure proliferate, and there is an increasing reliance on the Internet for financial transactions, medical records and other sensitive information. The demand for cyber security experts in both the public and private sectors is far outpacing the development of the talent pool, making for a hyper-competitive labor market. Against ever evolving cyber-threats the need to graduate students skilled in the concepts and technologies of cyber security is becoming a critical responsibility of academic institutions in order to help preserve the sovereignty of the US and her allies. Universities are only beginning to catch up.

Security programs, security tracks and certificates in information security exist, but often these courses are available only for computer science majors or majors in computer related disciplines. Breaches in cyber infrastructure impact everyone, not just computing professionals. It is crucial that more undergraduate majors receive education and training that deepens their conceptual and practical understanding of issues in Cyber Security. In addition to educating computer professionals, undergraduate students of all disciplines should have the opportunity to be exposed to issues regarding computer security. Improving user responsibility is a desirable and achievable goal. Security awareness training is also critical for the future workforce. Roughly two-thirds of security practitioners indicate that their organization does not invest enough in security awareness training. Professionals in the field consider it imperative for academic institutions to increase course development in computer security to make students both knowledgeable and technologically prepared for future challenges in this field.

As a result, we should all recognize the importance of Cyber Security in the undergraduate curriculum. Our graduates must have security skills in addition to communication, critical thinking and analytical skills. This additional skill will offer our majors the opportunity to extend the security focus beyond the department, to raise awareness outside of the computer science community, and provide a path for further studies and employment in Cyber Security.

To address the problem of the lack of awareness and participation in Cyber Security, we propose a Multi-Tier Approach to Cyber Security Education, Training, and Awareness in the Undergraduate Curriculum (CSETA). This proposed CSETA will use a multi-tier approach to increase capacity in Cyber Security education, training, and awareness in the undergraduate curriculum by (1) Assembling a diverse team of leaders from academia, business, industry, and professional organizations with experience and expertise in various aspects of Cyber Security education, (2) Developing collaborative relationships with academia, government and industry, (3) Introducing course modules and/or a minor in Cyber Security for engineering technology (ET) majors, (4) Enhancing faculty expertise through summer workshops and graduate school opportunities, (5) increasing awareness in Cyber Security career opportunities in the K-12 grade levels through outreach activities, and (5) creating an external committee and an internal committee for assessment and continuous improvement.
CSETA Activities

The proposed activities for CSETA are shown in Figure 1 below. The activities are discussed in detail following the figure.

Figure 1 – Proposed activities for CSETA
Education

Course Modules

Trying to integrate security into an existing curriculum gives rise to various concerns including the inability to provide special degree programs, tracks, and/or even one specialized course in security. We realize that we cannot develop security specialists with our current computer science undergraduate program. We do, however, feel that students should have an awareness of the issues and be able to evaluate, make decisions, and take responsible actions in the context of computer security. The best and most effective way to accomplish this is to provide an early introduction with continued discussion throughout the curriculum. Almost every career path open to a bachelors degree student encompasses some aspect of security. System administrators must be able to properly configure and maintain a system; programmers must know how to build secure software from the bottom up; web development personnel must understand the risks involved and how to best reduce the potential impact of these risks; and project managers must understand the cost/benefit tradeoffs involved with implementing secure systems. The field of security is large and rapidly changing, and one could easily offer multiple courses on computer security. However, we propose to integrate basic concepts into the undergraduate curriculum. These are the topics we feel should be addressed:

1. Security Literacy: a basic understanding of security terms
2. Security risks: a basic understanding of what is at risk (confidentiality, integrity, availability) and threat sources (such as connectivity, physical threats, etc.)
3. Spoofing: email and IP address spoofing
4. Reconnaissance software: packet sniffers and port scanners
5. Encryption: types, limitations, and uses
6. Operating system vulnerabilities: buffer overflow conditions, supplied daemons, flaws/patches
7. Denial of service: email and network attacks
8. Viruses and worms: construction and protection
9. Remote monitoring programs: basic configuration and purpose
10. Trojan horses: mechanisms and common attacks
11. Secure email: filters and hoaxes
12. Firewalls: tasks and implementation
13. Mobile code: usefulness and potential for malicious code

These topics may be addressed either as embedded modules with a duration of 1 to 2 weeks in selected existing courses or as separate standalone courses or as a mixture of both a and b.

Laboratory Modules

Laboratory modules will be used for teaching, research and outreach, and the design of laboratory modules must reflect these uses. Since designing and developing a Cyber Security laboratory is expensive and time consuming and many institutions do not have the required resources, the institutions may consider using “Deterlab” a free online Cyber Security laboratory. Here is a brief description of the Deterlab:
DeterLab Support for Cyber Security Educators (www.deterlab.net)

DETER’s support for education includes the basic use of the DeterLab, and use of exercises within it, as well as development of new exercises and incorporation of changes to exercises. The most important support for education in DeterLab consists of the capabilities for re-using packaged experiments that comprise a lab exercise. In addition, the DETER team has developed several DeterLab features for supporting instructors in common teaching or class management tasks, so that the exercises are turnkey, usable without prior training of DeterLab usage.

- Introduction to Linux and DeterLab
- Buffer overflows
- Pathname attacks
- SQL injections
- OS hardening
- Permissions and firewalls
- Computer forensics
- Network intrusion detection
- ARP spoofing
- Man-in-the-middle attack
- DNS man-in-the-middle attack
- TCP SYN flood
- Worm modeling
- Worm detection
- P2P botnet

Security Lab Exercises Available in DeterLab

Educators’ use of DeterLab shares the basic capabilities of research usage, with over 400 physical machines, configurable network elements, and a base of network emulation management capabilities. This hardware and software enables DeterLab users to construct test networks with a wide variety of topologies, and with nodes and virtual machines that run OS and application software of the user’s choice. Interaction with DeterLab occurs via a Web interface, with graphical tools for managing
experiments conducted in a dedicated experimental network.

DeterLab further provides two modes of working on an exercise. An instructor may choose an individual mode, where each student’s work is protected from the others, or they may choose a group mode where students collaborate within a group and expose their work to each other. Simple, well-defined lab exercises are well-suited for individual work while more complex, research exercises often demand engagement by a group of students to complete within a semester.

Over 30 educational institutions in 6 countries have made educational use of DeterLab, some with a single course using a single exercise, some with several courses using many of the available exercises, or developing a new exercise. In Fall 2010 there were ten courses that used DeterLab, from a set of schools diverse in size, ranking, location, and course size, and number of exercises performed.

List of institutions using Deterlab

<table>
<thead>
<tr>
<th>Institution</th>
<th>Students</th>
<th>Exercises</th>
</tr>
</thead>
<tbody>
<tr>
<td>USC</td>
<td>100</td>
<td>5</td>
</tr>
<tr>
<td>UCLA</td>
<td>50</td>
<td>5</td>
</tr>
<tr>
<td>Youngstown State Univ.</td>
<td>50</td>
<td>1</td>
</tr>
<tr>
<td>San Jose State Univ.</td>
<td>45</td>
<td>3</td>
</tr>
<tr>
<td>Santa Monica College</td>
<td>45</td>
<td>4</td>
</tr>
<tr>
<td>Colorado State Univ.</td>
<td>40</td>
<td>6</td>
</tr>
<tr>
<td>University of Portland</td>
<td>30</td>
<td>3</td>
</tr>
<tr>
<td>Vanderbilt Univ.</td>
<td>15</td>
<td>2</td>
</tr>
<tr>
<td>John Hopkins Univ.</td>
<td>13</td>
<td>1</td>
</tr>
<tr>
<td>Stevens Inst. of Tech.</td>
<td>10</td>
<td>14</td>
</tr>
</tbody>
</table>

Professional Development

Workshops in Cyber Security will be provided for selected faculty and staff members from SC State and local K-12 schools. The workshops will be conducted during each summer of the project. Approximately twenty faculty and staff members will participate in the workshops and preference will be given to faculty teaching the courses and laboratory mentioned earlier. Seminars and presentations will also be provided for faculty, staff and students. There will be three to four seminars during each
Outreach activities

Three faculty and ten students of the Department of Mathematics and Computer Science are currently involved in a project dealing with K-12 outreach activities in local schools (Marshall Elementary School and Felton Laboratory School in Orangeburg, SC). The department is also working on arrangements to extend these activities to other local schools. The central theme of this K-12 outreach is “Computational Thinking Using Hands-On Activities” such as introduction to Excel, PowerPoint, Robotics, and Visual Programming. These K-12 outreach activities are supported through a project titled - STARS (Students & Technology in Academia, Research & Service) Alliance. The primary objective of the STARS project is the **broadening of participation in computing through best practices and community building.**

**Provisions will be made for visits to these and other K-12 schools to advertise the program and make presentations on Cyber Security.** We plan to make few of the Cyber Security courses and modules online to K-12 schools teachers, local two year and four year college teachers and others interested in Cyber Security education and awareness.

Assessment and Evaluation

We will formulate an external advisory team for evaluating our progress and suggesting changes as needed. The team members will be selected from academia, industry, business, and community. The external and internal evaluation and assessment team will be also a part of this advisory team. The short-term assessment and evaluation report will include:

- (a) students’ grades and progress towards their degrees;
- (b) students’ progress in their learning of computer technology; and
- (c) students’ attendance and participation in the project’s academic enhancement activities.

Students will evaluate all program activities regarding the relevance and presentation of information, pointing out the program’s strengths and weaknesses. Of course, they will also have the opportunity to write or discuss additional comments or concerns. Lastly, each scholar will have one hour exit interview with the external evaluator. This interview will be a useful tool to learn the positive and negative aspects of CSETA in an effort to go beyond the written evaluations from the Scholars. The external evaluator will prepare a report, plan for next year, and discuss the findings at the annual Project Advisory Board Meeting in order to improve the program. The long-term assessment and evaluation report will include:

- (a) the percentage of students entering graduate programs related to Cyber Security;
- (b) the number of students entering the workforce related to Cyber Security; and
- (e) the percentage of students who participated in outreach and professional development activities.

Summary and Conclusions

Few of the SCETA activities are currently being implemented in our institution and others are in the planning phase. We are currently offering an elective course titled “Introduction to Cyber Security”. Nine computer science majors are enrolled in this course and preliminary data indicates that students are
satisfied with course. We have added Cybersecurity component to our K-12 outreach program and it is progressing well. Few of our computer science majors are actively involved in introducing this component to the 6th, 7th and 8th graders (approximately 50 students) in one of our local middle schools. Preliminary data indicates that student and faculty satisfaction with this activity is very high. We plan to analyze the data after the end of this semester and present the findings during the conference presentation. The Faculty attended workshops and seminars on Cyber Security offered by IBM and DOE. We are currently working on the laboratory component and assessment component of CSETA. We are also collaborating with other local colleges and universities to establish a Cyber Security consortium with DOE. We strongly believe that various activities of CSETA will help us to increase capacity in Cyber Security education, training, and awareness in the undergraduate curriculum.

References