Cybersecurity Education

The Obstacle and Challenges

Panel Discussion
Summer Workshop on Cyber Security Education for Community College Faculty in West Texas

Texas Tech University
August 13, 2013
COMPUTER SECURITY EDUCATION

Past, Present and Future

A Paper by
Carol Taylor, Rose Shumba, and James Walden
University of Idaho, Indiana University of Pennsylvania, and Northern Kentucky University
Computer Security

• Computer security became a tangible Computer Science sub discipline in the 1970’s as the need to protect information became important with growing computer use in government and industry.

• At that time computer security research was funded by the military and primarily aimed at the protection of sensitive information.

• Computer security researchers and practitioners were few in number, worked primarily in the defense industry, and were mostly self taught.

• Today, computer security is well established as an area of research and study within Computer Science.
But!!

• Popular press reports describe daily the number of vulnerabilities found and the latest abuse of our systems by individuals in search of easy profit.

• Several well-respected Computer Security researchers and educators also question the state of our knowledge and practice as a discipline.
As security researchers, it is discouraging to see the low level of practice in the *real world* with the constant stream of new system vulnerabilities and the increasing number of malicious programs in search of one of the many un-patched systems.

But, as educators, we are hopeful that in time, through education, we can improve the current state of computer security by producing students trained in secure coding, with knowledge of secure system design and operation.
COMPUTER SECURITY EDUCATION IN THE PAST
Academic Programs

• Early academic programs in INFOSEC education were primarily for graduate students. Consequently, undergraduates wanting to learn about computer security had to take graduate courses or do so through independent study.

• Graduate level security courses typically concentrated on Multi-level Security (MLS) concepts or simply covered cryptography without a lot of practical system analysis.
Government Support for Academic Programs

• The first NCISSE conference was held in 1997 and was established as a forum for dialog between government, industry and academia to define requirements for information security education and encourage development and expansion of information security curriculum at the graduate and undergraduate levels.

• Around the same time 1996-1999, President Clinton established the President’s Council on Critical Infrastructure Protection (PCCIP) and subsequent President Decision Directive 63 (PDD63).

• In establishing the PCCIP, the president recognized the vulnerability of the US infrastructure and acknowledged its importance to national security.

• PDD63 simply expanded the definition of critical infrastructure to include cyber security.
• Soon after PDD63 appeared, in 1999, NSA established the Centers for Academic Excellence in Information Assurance (CAEIA).

• These centers were academic institutions with expertise in cyber security as demonstrated by a number of security oriented faculty and curriculum that met federal security training standards.

• The purpose of this program was to increase the number of “security professionals of different disciplines”.
In February of 2000, President Clinton released the National Plan for Information System Protection [9] which established the Scholarship for Service (SFS) (Thanks to this program, we have this workshop) program managed by the National Science Foundation (NSF).

This program provided scholarships for undergraduate and graduate students for up to two years in exchange for an equal amount of Federal Job service upon graduation.

In order for a school to obtain a scholarship program, they must first qualify as a Center for Academic Excellence.

During the first two years of the program, 150 students were enrolled.
In 2003, the President’s National Strategy to Secure Cyberspace was passed by President Bush. It identified four major actions and initiatives for awareness, education and training which include:

1. Promote awareness nationally to empower all Americans to secure their own systems.
2. Foster training and education programs to support national and cyber security needs.
3. Promote private sector to support widely recognized cyber security certification and training programs.
4. Increase efficiency of existing federal cyber security training programs.

From 1997 to 2003, the US government created many initiatives for cyber security which appeared to recognize its importance for national security and the continued well-being of our nation. However, the only money allocated to academic security education was from the NSF SFS program (we are one of those who received the fund).
COMPUTER SECURITY EDUCATION IN THE PRESENT
Academic Programs

• Recently, a number of colleges have reported on their experiences adding computer security to their programs.

• Most schools appear to take one of two approaches:
  - integrate security within individual CS courses or
  - create a special computer security degree or track.

• A few schools have opted for a combined approach where they have both specialized and integrated courses.
• Schools that choose to create a computer security track or special degree appear to have faculty that have experience in computer security or are strongly interested in pursuing security training.

• There also appears to be department or institutional support for a Security track and at least enough funding for course development.

• Integrating security into existing CS courses without offering specialized Security courses is one way that schools with limited resources in terms of faculty or funding can still offer security to students within their programs.

• Faculty in these programs do not need not be retrained or develop completely new courses
The effectiveness of each approach relates back to the goals for the CS graduates of a particular program in terms of computer security expertise.

Programs that want to produce graduates with strong computer security skills capable of obtaining a computer security position have created specialized programs in computer security.

CS programs that want their students to have exposure to computer security but not necessarily produce computer security professionals can achieve this through an integration of security principles into existing CS classes.

There is no clear evidence that specialized courses in computer security are superior to standard CS courses with integrated security components.
• However, schools that have chosen to integrate security within their existing curriculum point out several advantages over the specialized course path:
  □ Provide a security foundation to all their CS students as opposed to only those with a security interest
  □ Security concepts are learned within the broader CS topics such as system design, network administration, and programming
  □ The approach is available to all schools even those with limited resources and only requires faculty creativity and motivation
Government Support of Academic Programs

• The government has several programs that currently support academic computer security education. Many of these programs were begun as the result of government initiatives related to national security. Here, we view the current status of these programs.

  NSA-DHS Centers of Academic Excellence in Information Assurance
  Current: Has 67 Centers in 27 states
  Started: 7 schools
  Funding: Provides no monetary support for the Centers

  NSF Scholarship for Service Program
  Current and Future: 350 graduates by 2005
  Started: 150 enrolled
  Funding: An annual budget of $30.5 million

• The programs directly support Computer Security education within academic institutions. These programs appear to be thriving with an increasing number of Centers and students enrolled in scholarship programs.
Research Funding

- In order to provide incentives for faculty and attract students into a field, the field of computer security needs a certain level of support in research dollars.

- Several long-time researchers and educators have noted that Computer Security needs a continued long-term commitment of basic research funding if it is to sustain itself as a viable area of study.
However,

• It has been claimed that a lack of government investment in security research discourages PhD students from entering the field. This in turn creates shortages of faculty trained in security at academic institutions that produce the students entering the work force as programmers.
Another recent funding trend that affects computer security programs is the significant cuts from DARPA spending for university research.

DARPA has been a long-term source of basic Computer Science research funding for many years. This past year DARPA has cut the portion that goes to universities from $214 million to $123 million.

They have shifted away from general research projects to more concrete deliverables produced in shorter time frames.

This shift has resulted in a huge increase of proposals being directed towards NSF as one of the last Computer Science funding sources.
COMPUTER SECURITY EDUCATION IN THE FUTURE
Computer Security Education
Objectives

• In trying to visualize the future of computer security education, it is useful to set goals and define specific objectives for reaching those goals.

• No one in the security field would argue with the general belief that providing a security background is beneficial to all students graduating from CS departments.

• One overall goal would be to increase the number of CS graduates with an understanding of computer security principles. Consequently, one objective that would help in reaching this goal is to increase the number of CS programs that teach computer security.

• Analyzing the specific steps needed to realize the objective of expanding the security education programs leads to a discussion of barriers to success for computer security education, the topic of the next section.
Barriers to Success for Computer Security

- Achieving the objectives of promoting or increasing security concepts in CS programs requires some investment on the part of both institutions and the faculty member(s). These respective responsibilities for faculty and institutions are outlines in Table.

<table>
<thead>
<tr>
<th>Institution</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reduced Teaching Load</td>
<td>Faculty Learn Computer Security</td>
</tr>
<tr>
<td>Travel and/or Training Support Grants</td>
<td>Collaborate with Computer Sec. Research Inst.</td>
</tr>
<tr>
<td>Tenure Support</td>
<td>Travel to Conferences</td>
</tr>
</tbody>
</table>
Barriers to Success for Computer Security

• In addition to the specific activities of faculty and institutions that wish to add computer security to the curriculum, there are other possible barriers to establishing a computer security emphasis. These are outside the control of faculty and their colleges and include:

  - No standard for CS curriculum development
  - Lack of government funding in basic research
  - Limited industry involvement
There is currently no accepted standard for college level computer security curriculum development.

The lack of government funding was addressed in a previous section and noted as a disincentive for promotion of security education. If there is little or no research funding available in a given field of study, then there is no way to support graduate students who are to become future faculty and eventually promote their own research programs.
• The software industry is concerned with the perceived lack of security awareness in students graduating from CS programs.
• We would like to hear your voice and learn about the problems you are facing when it comes to:

**cybersecurity education**