PANEL: TEACHING UNDERGRADUATE INFORMATION ASSURANCE

Rayford Vaughn
Mississippi State University, vaughn@cs.msstate.edu

It is rare to find computer security course offerings at most academic institutions today. There are exceptions, of course, and some institutions are offering concentrations in this area of study. Such courses are found at NSA Centers of Academic Excellence and in some cases, degree programs in IA topics are being implemented or proposed. While NSA certifies COE/IAE's based on published criteria – there is no established program of study and each institution approaches the topic in their own way. At Mississippi State University, we believe that IA is properly placed within our Software Engineering research area and that it is best taught by integrating it into existing courses in our Software Engineering degree and our Computer Science degree programs. We also believe that by doing so, it better prepares the student for a dedicated IA course during their senior year of study.

The practice of security engineering requires a foundation of study in operating systems, database systems, networks, architectures, and, to some extent, artificial intelligence. It would appear that including computer security course offerings toward the end of a computer science or software engineering undergraduate program as a required course is an effective way of providing graduates with an emphasis in security engineering. One would expect that a comprehensive pedagogical approach would suggest that current CS or SE course content be modified to include course specific discussion related to security in networks, database, operating systems, architectures, and software engineering followed by a capstone course toward the end of the program that is specific to information security issues. The prerequisites for the capstone course should likely include, as a minimum, operating systems, database, and software engineering.

When teaching the senior level capstone course in IA, it seems critical to have a series of lab exercises that some might consider the "teaching of

C. Irvine et al. (eds.), *Security Education and Critical Infrastructures*

hacking". This panel member has sixteen labs over a sixteen week period that involve the cracking of passwords, spoofing of web sites, sniffing of networks, and other such activities that acquaint the student with risk and vulnerabilities in a way that lecture cannot. Having taught the IA course with and without a lab, this panel member believes strongly that the lab exercises are a necessary part of learning in this area.