PANEL: TEACHING UNDERGRADUATE INFORMATION ASSURANCE

Matt Bishop
Department of Computer Science, University of California, Davic, bishop@cs.ucdavis.edu

As the importance of information assurance and computer security has become recognized, the number of institutions teaching these subjects in their undergraduate curriculum has grown. But methods of integrating this material into the undergraduate program are varied, as are the methods used to teach the material itself. Two key issues highlight the differences in instructional methods and techniques.

There is no commonly accepted body of knowledge in information assurance that an undergraduate should know. The first question is whether an undergraduate should be taught about information assurance, and if so, in what courses. Specifically, should undergraduates take a course in information assurance, or should the contents of such a course be distributed over existing courses such as networks, operating systems, software engineering, and theory? The importance of this question lies in the structure of the undergraduate programs. Many, particularly those in engineering, require a large number of courses. In some cases, there is enough room for electives that a student can take a course in information security (possibly at the loss of taking another course). In other cases, there is little room for electives, and adding a course in information security may not be feasible. If a course on information assurance provides a better education in that subject than integrating the material into other courses, then the undergraduate program will need to be revised to allow such a course. Otherwise, the material in each course must be revised to include information assurance aspects of the subject.

When teaching information assurance (either in its own course or as part of other courses), many instructors assign projects. Often, these projects take the form of penetration testing (or "ethical hacking") projects. The second question is whether these penetration testing projects are effective and

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

appropriate vehicles to supplement classroom education? The importance of this question lies in the way a project relates to the material being taught. Survey papers and projects cover lots of material, but rarely in depth. More focused projects provide the depth but not the breadth. Some projects present unique problems. Penetration testing in particular is a popular project, but is it useful pedagogically? If so, why, and how should the exercise be conducted and evaluated? How can the exercise be contained to minimize the effects of errors? If not, what other types of projects would be useful?

PANELISTS

Mr. Colin Armstrong is the Overseas Program Manager for the School of Information Systems in the Curtin Business School, Western Australia. He administers off shore undergraduate and postgraduate courses for the School. He also established a Center for Information Warfare. He currently teaches classes in computer and Internet security, and computer forensics.

Dr. Natalia Miloslavskaia is an associate professor of Information Security of Banking Systems at Moscow Engineering Physics Institute (State University). She has taught undergraduate and graduate classes in network security and has supervised post-graduate students in computer security. Her Information Security Faculty is a Head educational and scientific center on information security of the Russian Ministry of Education.

Dr. Daniel Ragsdale is a lieutenant colonel in the US Army, and a professor in the Department of Electrical Engineering and Computer Science at the United States Military Academy, West Point. He teaches undergraduate computer security and information warfare courses, and has supervised information warfare exercises involving both students and other military personnel. His program has been designated a Center for Academic Excellence in Information Assurance Education.

Dr. Rayford Vaughn is currently a professor of computer science at Mississippi State University where he teaches and conducts research in the areas of Software Engineering and Information Security. He established the MSU Center of Computer Security Research and led the effort at MSU to obtain a National Security Agency designation of Center of Academic Excellence in Information Assurance Education – one of only thirty-six in the United States.

MODERATOR

Dr. Matt Bishop is an associate professor in the Department of Computer Science (a Center of Academic Excellence in Information Assurance Education) at the University of California at Davis. He has taught undergraduate and graduate courses in computer security there and at Dartmouth College. He has been active in information assurance education for many years, and gave the academic keynote addresses to the first and fourth Colloquia on Information System Security Education. His textbook, *Computer Security: Art and Science*, was published by Addison-Wesley-Longman in December 2002.