Abstract

It has become imperative for companies, governments, and organizations to understand how to guard against hackers, outsiders, and even disgruntled employees who threaten their information security, integrity and daily business operations. To address national needs for computer security education, many universities have incorporated computer and security courses into their undergraduate and graduate curricula. At Miller College of Business, Ball State University, we have introduced a information systems security as a track for students majoring in information systems. This paper describes our experiences and lessons learnt of teaching security courses using hands-on approach.

Key Words: Computer security, education, hands-on, information systems security

Introduction

Information security is the key issue in today’s information technology world. Information security is required at all levels – personal level, corporate level, state and country level. There is a steady rise in the occurrence of cyber attacks. Cyber-security is a broad issue which is becoming increasingly important as computer networks become more widespread. It encompasses computer- and network-related crime, privacy issues, trust and confidence, and dependability of critical infrastructures. The evidence of the cyber threat is growing. New vulnerabilities are found each day. Those interested in exploiting these vulnerabilities are becoming a well-organized underground. Cyber threats can take a variety of forms, including espionage, hacking, identity theft, crime, and terrorism.

The first widespread worm attack through networked computers occurred in 1988 when Robert Morris, Jr., a Cornell University student and the son of a prominent NSA scientist, developed a program that crippled approximately 6,200 computers and caused over $98 million in damage in approximately 48 hours. Also in 1988, a hacker group called “Legion of Doom” demonstrated the vulnerability of the critical infrastructures by penetrating sensitive administrative computers. Even Hollywood contributed to the cyber security mystique. In 1983, the film War Games helped frame the view that cyber crime is mostly about smart teenagers testing their intellect and knowledge of computers.

Since the early 1990’s, it has been recognized that computer security needs to be a high priority in the modern world. The recommendations from the 1991 National Research
Council systems security study include the observation that "Computer system security and trustworthiness must become higher priorities for ... educators ..." In 1992, Richard Spillman noted several reasons that sensitivity to security issues was low and stated that "one source of this problem is the woeful lack of computer security education in computer science departments". In 1997, Matt Bishop noted that very few computer science students are required to develop robust, thoroughly tested, code and that until this problem is addressed "security problems will continue to plague computer systems". This vulnerability prompted the Clinton administration to examine ways to protect the critical infrastructure. Executive Order 13010 established the President's Commission on Critical Infrastructure Protection (PCCIP). This order identified "cyber threats" as "electronic, radio-frequency, or computer-based attacks on the information or communications components that control critical infrastructures." The commission was tasked to address these cyber threats as one of the two primary threats to critical infrastructures (the other was physical threats). One of the critical requirements identified by the commission was the need for more information security education.

To address these needs, many universities have incorporated computer and information security courses into their undergraduate and graduate level curriculum. The courses are designed teach students how to secure an information system from the design stage through the implementation and maintenance stages. Research has shown that students’ learning is enhanced if they can engage in a significant amount of hands-on exercises. It is therefore critical the students are provided with opportunity to practice the theories of systems security in an environment where laboratory exercises can be performed efficiently.

Security laboratories designs are still in the developing stages of their life. There exist many different approaches to the design of the security laboratory. The three of the most frequently used designs are as follows: the free-style approach, build-it-from-scratch approach, the dedicated computing environment. The free-style approach places the students in the lab where they are free to research security-related issues. The built-from-scratch approach has the students construct a secure system from the ground up. The dedicated computing environment is a contained environment where the students conduct analysis and implementation of security systems.

At Ball State University, we are currently using this network security lab to teach three courses; ISOM410, ISOM421 and ISOM424. The assignments and laboratory exercises developed for these courses are a combination of our own original exercises and some from books and other sources. The laboratory we have developed is a hybrid of all three of these designs. The laboratory was developed 1) to provide students with an environment to run structured security exercises 2) to provide an environment where students would be require to develop parts of a secure system and 3) to provide researchers with an environment where research on security related topics could be tested and pursued. During the process of creating the lab and teaching security courses, we experienced many challenges and unseen issues. This paper describes our experiences and lessons learnt of teaching security courses using hands-on approach. The paper also describe the challenges we faced and how we were able to deal with them.