RUNNING A COMPUTER SECURITY COURSE:

CHALLENGES, TOOLS, AND PROJECTS*

POSTER SESSION

Vladimir V. Riabov and Bryan J. Higgs
Department of Mathematics and Computer Science
Rivier College
Nashua, NH, 03060
603 897-8613
vriabov@rivier.edu and bryanhiggs@gmail.com

Challenges and effective ways of instruction in computer security classes (security tools, technology overviews, research projects, virtual labs, and Web resources) are discussed with examples of lecture notes, OPNET™ lab assignments, homework study cases, and projects available on the instructors' Websites. The project-based approach motivates students in exploring computer-security techniques, writing technology overviews, and conducting research, and provides them with knowledge, instructions, and hands-on experience.

Rivier College offers courses on computer security at both undergraduate and graduate levels in Computer Science programs. These courses are introductions to the methods, algorithms, and tools of computer system security. Topics cover both the theoretical and practical aspects of security including cryptography, protocols, standards, and security implementation. An important part of the courses are surveys of actual techniques used by hackers to attack systems.

The authors' websites are the gateway to courses, publications, and numerous resources on the Internet (through the World Wide Web, Secure Shell, and Secure FTP). Each course has a portal to syllabi, assignments, lecture slides and notes, tools, software installation instructions, tutorials, lab manuals, examples of project papers, research reports, Internet links, lists of recommended readings, etc.

The classes cover security concepts; history of cryptography; theory of sets, permutations, combinations, and probability; number theory and modular arithmetic; classical cryptosystems; symmetric block ciphers; public key cryptography; an overview of message authentication codes, hashes, and message digests; principles of authentication; Web security and privacy for users; tunneling and virtual private networks (VPNs); and malware. The instructors discuss with students secure ways of sharing the

---

network resources, issues of confidentiality, medical and personal information security on the Internet, and protection from electronic spam. This overview helps in introducing encryption algorithms such as the RSA Public-Key encryption algorithm.

A student can try to solve the problems by a simple experimentation with the Java Applets Tools especially designed for these courses. Students use these tools to create and decipher simple shift substitution ciphertexts, MonoAlphabetic substitution cipher, the Playfair and Vigenère ciphers, as well as to explore modular arithmetic and message digests. The tools also are used in reviewing the concepts of probabilities and combinatorics.

The course assignments include three homeworks, one lab, midterm and final exams, and a project paper that covers in depth one of the computer security technologies. Every class starts with a brief discussion of a topic that is related to the homework exercises. After this "warm-up" introduction, the instructor offers a discussion on the main topic and asks students for a feedback on lecture materials and their arguments on selecting a competitive strategy for the problem analysis and development. These discussions help students to focus on the main point of the class session and stay active in class. After cracking a couple of simple short ciphers, students are asked to explore how cryptographers might actually crack classic ciphers. The students are encouraged to use various components of the Java applet while working on this assignment. They start by exploring a MonoAlphabetic Substitution Cipher (e.g., the oldest Caesar cipher) that maps individual plaintext letters to individual ciphertext letters, on a 1-to-1 unique basis. To encipher a message, students simply take each letter in the plaintext, find that letter in the Plaintext row, and substitute the corresponding letter immediately below it, in the Ciphertext row.

Finally, students examine the Letter Frequency Analysis approach based on assumptions that the plaintext consists of characters written in some known natural language (e.g., English), and the frequency of letters in a typical piece of text in that language is known. After the concept review and exploration with the Java Applets tool, students are asked to study the two ciphertexts: Ciphertext-1 (3 pages, 620 words, 2,685 characters, and 128 lines), where the original word spacing, punctuation, and style have been retained; and Ciphertext-2 (46 pages, 25,955 words, 103,818 characters, and 2,596 lines), where word spacing and punctuation have removed, and the text has been organized in groups of four letters. This makes it more difficult to decipher the ciphertext using the context that those clues (word spacing and punctuation) provide. Usually it takes more than 6 hours for a student to decipher these ciphertexts, using a variety of techniques and tools (e.g., one student wrote some custom UNIX scripts and a standard UNIX dictionary to help with the mechanics of the solution).

The last assignment gives students an opportunity to review the theory of probabilities that plays an important part in many areas of security. It covers four topics: “CIA Hiring”; “Brobdingnag Battles”; “Delta Force”; and “Ethnic Dispute”. In an attempt to overcome the all too common “Math-phobia” of students, some standard statistical/probability problems were re-cast using scenarios that were more “security-related”.

Several classes were designed as computer labs that help students in exploring the network-security study cases and finding ways of solving them. The OPNET IT Guru™

Academic software package was used for studying firewalls and virtual private networks. Using this knowledge and skills, students develop their own lab projects and include virtual lab techniques into their research projects related to various network security protocols, such as the Diffie-Hellman asymmetric key agreement protocol and RADIUS protocol.

Students are encouraged to conduct research and write project papers on modern computer-security technologies. They select projects that would be beneficial for their careers and valuable for companies and the community. Usually, students demonstrate their project portfolios during job interviews. Such demonstration of their actual professional skills in computer security helps students in finding a job immediately after the graduation. Many projects are implemented in local companies and the community, e.g., “Secure Wi-Fi Technologies for Enterprise LAN Network”, “Steganography and Steganalysis”, “Intrusion Prevention System”, “Security and SQL Injections”, “Virtual Private Networks”, “Firewalls Overview”, “RADIUS Protocol”, and “Secured Communication in Java”. Students are encouraged to submit summaries of their research projects to professional journals and magazines.

The authors believe that this project-based, tool-exploration, and virtual-lab approach can be effectively applied to future courses of a similar nature in academia.