RUNNING A COMPUTER SECURITY COURSE: CHALLENGES, TOOLS, AND PROJECTS*

Vladimir V. Riabov, Ph.D.**
Professor of Computer Science, Rivier College
and
Bryan J. Higgs, Ph.D.§
Milford, NH 03055

Abstract

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

1 Motivation

In this paper, authors share their experience in searching for new approaches in teaching computer system security courses. Their teaching methods are based on several techniques [1, 2] that challenge and motivate students to become passionate in their studies and be active in the classroom. Starting every class with small challenging exercises [1], the instructors encourage students to select and develop their own projects. They demonstrate to them the best achievements of professionals in the related fields of expertise, the best projects of students (available on the instructors' websites; e.g., http://www.rivier.edu/faculty/vriabov/) who took similar courses in the past, and the challenges of the discipline [3-6].

This paper demonstrates the advantages of using a project-based approach [1, 2] in course delivery that motivates students in studying and learning modern computer system security technologies. Discussions of recent research publications, lectures, overview of the security tools, and labs stimulate students in selecting topics for their technology overviews and research projects and provide them with knowledge, instruction, and hands-on experience. The students who accept the challenges of innovations in computer security area gain real-world experience by delivering their presentations at national and international conferences [7], publishing their first articles in professional journals [8-22], and promoting their findings among college peers and colleagues in companies and organizations [23, 24].

The paper is organized as follows: In section 2, the authors present an overview of some Web-enhanced classes in computer system security technologies that they have taught at Rivier College. Examples of lecture notes, and course assignments are discussed in section 3. The core of the paper consists of sections 4-7, in which the authors describe what makes the courses challenging and valuable for students. These sections also include students' responses to developing virtual labs by using the OPNET IT Guru™ Academic Version software [25-27], examples of their overviews of modern computer-system security technologies with demonstrations using OPNET and simulations [9], and examples of students' research studies [8-22]. The paper closes with a Conclusions section.

ISSN 1559-9388 (online version), ISSN 1559-9396 (CD-ROM version).

2 Web-Enhanced Computer-System Security Technology Classes at Rivier College

Rivier College offers computer science courses on computer security at both undergraduate and graduate levels, as elective courses in B.S. in Computer Science, B.S. in Information Technology, M.S. in Computer Science, and M.S. in Computer Information Systems programs. These courses are introductions to the methods, algorithms, and tools of computer system security. Course topics include both the theoretical and practical aspects of security including cryptography, protocols, and system design. Security standards and security implementation examples are also covered. An important part of the courses are surveys of actual techniques used by hackers to attack systems. The CS572 Computer Security graduate course has a prerequisite course, CS553 Introduction to Networking Technologies.

These courses have three interrelated major goals:

- Introduce students to fundamental concepts in computer system security and some of their relevant applications,
- Have students take an active role in their learning by experimenting with various computer-security networking techniques (e.g., emulating firewalls and virtual private networks with OPNET IT Guru™ software [25]) and tools, and
- Instruct students in writing overview papers on modern computer security technologies and in conducting their own first research studies.

Many students, who have taken these elective courses, continue their projects on similar topics in CS700 Reading & Research and CS699 Professional Seminar in Computer Science courses.

All the courses are Web-enhanced, and a student can remotely access any course material (a syllabus, class schedule, assignments, lecture notes, software tools, lab manuals, examples of project papers and research reports, Internet links, lists of recommended readings, etc.) from the instructors' Web sites and Blackboard™ sites. This "virtual" learning environment supports communication between students and the instructor, as well as among peers working together on a team project beyond the classroom. Also, it becomes a valuable resource for those students who have missed a class for some reason, or who continue working online.

3 Lecture Notes, Assignments, and Web Resources

3.1 Instructor's Web sites (Teaching, Research and Publications)

The authors' websites (e.g., see http://www.rivier.edu/faculty/vriabov/) are the gateway to the instructors' courses, their research agendas, publications, and numerous Web resources. Each course has a portal to various course-related materials, including syllabi, class policies, schedules, assignments, lecture slides and notes, tools, software installation instructions, tutorials, lab manuals, examples of project topics and papers, research reports, Internet links, lists of recommended readings, etc. The instructor designs assignments and tests, which require the students to use resources from the Web sites, digital libraries, and the Internet [through the World Wide Web, Secure Shell (SSH), and Secure FTP (SFTP)]. This skill can be directly transferred to others, when students begin their careers in companies.

The project-based teaching strategies (including lectures, homework-, computer-lab-, and project assignments, resources on the instructors' Websites for supporting the students' studies and learning, authors' publications, and presentations) are interdisciplinary. They combine research from Computing Education, Computer Science, Mathematics, Networking Technologies, Physics, and Ethics.

3.2 Lecture Notes

The introductory classes in computer security technologies (e.g., CS572) 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; network basics, TCP/IP protocol architecture, standards, and products [4, 5, 28]; Web security and privacy for users; tunneling, and virtual private networks (VPNs); and malware. Students are encouraged to establish a VPN connection between their office (home) computers and the College network system to remotely and securely access the computing resources for the entire campus.

The instructors' lecture materials, homework-, computer-lab-, and project assignments, presentations and publications combine research from various disciplines. For example, in the CS572 Computer Security classes, we study selected topics from the Mathematical Theory of Numbers, Theory of Graphs, Physics of Electromagnetic Fields, Optical Physics, Theory of Algorithms, Mathematical Statistics, Management, Encryption, and Psychology. 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 [29]. At the same time, it illustrates a strong bond between mathematics and computer science. A student (even if he/she is not familiar with the theory of numbers) can try to solve the problems by a simple experimentation with the Java Applets Tools especially designed for these courses.

The lecture notes for the courses (both Microsoft PowerPoint™ presentation slides and files of video conference recordings created by using LearnLink™ software [30]) are available online for students via the Blackboard™ sites. Both undergraduate and graduate students have access to materials for all the courses. This option helps students in reviewing current, past, and future topics, and helps them to prepare better for a test, lab, or homework, and in selecting the next course in the program.

3.3 Security Tools

A set of security tools (shown in Fig. 1 – the opening window for the Java applet) has been developed for these courses by using a Java applet.

The tools have been used by students to create and decipher simple shift substitution ciphertexts, MonoAlphabetic substitution cipher, the Playfair and Vigenère ciphers [3], as well as to explore modular arithmetic and message digests [4-6]. They also were used in reviewing the concepts of probabilities and combinatorics.

Figure 1: The Set of Security Tools

3.4 Course Assignments

The assignments for the CS572 course include three homework questionnaires, one lab, midterm and final exams, and a project paper that covers in depth one of the computer system security technologies. A student can gain extra points towards his/her final grade as a result of active participation in various class activities, such as project presentations, lab demonstrations of computer security modeling, team project leadership, and submission of papers (on the course-related topics) to conferences or journals.

3.4.1 Homework Assignments

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. Here are a few examples of the homework assignments:

Assignment 1: Cracking a Simple Cipher

Students are asked to solve two following ciphers (both are taken from the textbook for the course [3]) by using any method:

1. On the page immediately following the title page [3], there is the following ciphertext:
   Si spy net work, big fedjaw iog link kyxogy

2. Page 44 [1] contains the following ciphertext:
   Cf lqr'xs xsnyctm n eqxxqgsy iqul qf wdcp eqqh, erl lqrx qgt iqul!

These ciphers are simple substitution ciphers of the type that many people like to amuse themselves trying to solve, e.g., newspapers often publish a daily cryptopuzzle (along the lines of a daily crossword puzzle), which readers try to solve – often during their daily commutes. In preparation for this activity, students are encouraged to read Edgar Allan Poe's "*The Gold Bug"* [31], and Sir Arthur Conan Doyle's "*The Adventure of the Dancing Men"* [32]. These stories can help with the necessary mindset necessary for such a simple cipher solution.

It is interesting to note that students typically find the second cipher easier to solve, probably because there are more 'hints' in the text, and more repetition. Also, if students solve the first cipher and then move onto the second, their mindset is likely already to be set in such a way that the second seems easier to solve.

Assignment 2: Cracking Classic Ciphers

After cracking a couple of simple, but short, ciphers (see Homework-1 Assignment section), students are asked to explore how cryptographers might actually crack some 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 that maps individual plaintext letters to individual ciphertext letters, on a 1-to-1 unique basis. (For example, the oldest such cipher known is the Caesar cipher [3], where the mapping involved a simple circular shift within the alphabet). 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. For example, using this substitution table, we can take the message:

Once more unto the breach, dear friends

and encipher into the following:

Lkzb jlob rkql qeb yobxze, abxo cofbkap

Of course, to decipher the text, they simply reverse the process – or equivalently, use the negative of the original shift value. Both encryption and decryption can be done manually, or by using one of the Java Tools, available [33].

Finally, students examine the Letter Frequency Analysis approach. First, some assumptions about the plaintext should be made:

- That the plaintext consists of characters, not some kind of binary code.
- That it is written in some known natural language (e.g., English).
- That we know the frequency of letters in a typical piece of text in that language.
- That the plaintext is typical of English text, and so we expect the same frequencies of letters (approximately, within statistical fluctuations).

As long as we know that there is a 1-to-1, unique, mapping from plaintext to ciphertext (and therefore also from ciphertext to plaintext), we can employ our knowledge of those letter frequencies to help us crack a substitution cipher. It is important to note that we need a large enough piece of text to give us some expectation that we have a large enough statistical sample. The longer the message, the better statistical sample we are likely to have.

Known letter frequencies in typical English text may be found on the following web sites, among others:

http://www.simonsingh.net/The_Black_Chamber/frequencyanalysis.html
http://rinkworks.com/words/letterfreq.shtml
http://pages.central.edu/emp/LintonT/classes/spring01/cryptography/letterfreq.html
http://deafandblind.com/word_frequency.htm

A typical representation of the letter frequencies in traditional English is shown on the histogram/bar chart below (see Fig. 2, which shows a window from one of the Java Tools; it also allows the student to view the letter frequencies for the ciphertext being examined.). The left hand side is in order by the letter position within the alphabet, while the right hand side is in decreasing order by frequency.

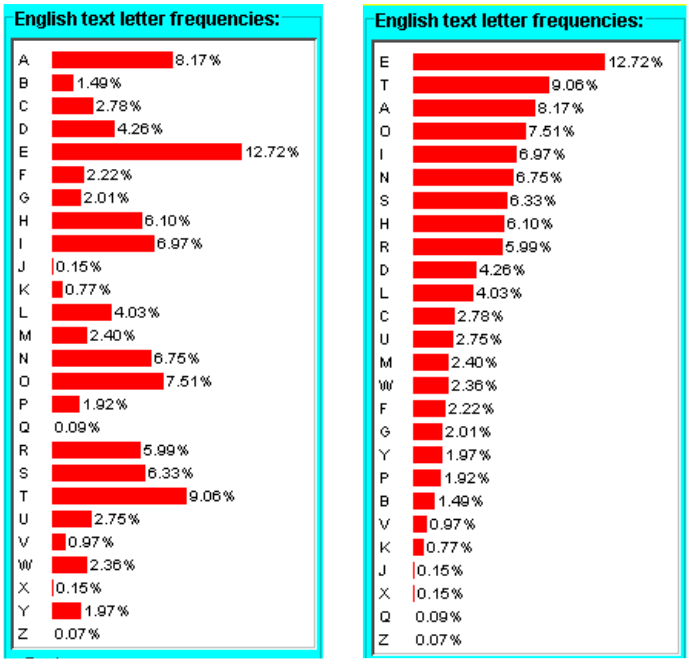

Figure 2: Letter Frequencies in Typical English, as shown by one of the Java Tools

Note that the twelve most common letters in English are famously (see http://www.worldwidewords.org/weirdwords/ww-eta1.htm):

ETAOIN SHRDLU

However, in the above histogram, the most common letters are:

ETAOIN SHRDLC

Notice that the last letter is C, not U.

This is a useful lesson in itself. Notice that the relative frequencies of U and C are 2.75% and 2.78%. That is, the frequencies of both are already quite low – certainly when compared with E at

12.72% – and also quite close. Different sets of English texts will produce slightly different frequencies, and the numbers are also subject to statistical fluctuations.

After the concept review and exploration with the Java Applets tool, students are asked to study the two ciphertexts: 1) Ciphertext-1 (3 pages, 620 words, 2,685 characters [no spaces], and 128 lines), where the original word spacing, punctuation, and style have been retained; and 2) Ciphertext-2 (46 pages, 25,955 words, 103,818 characters [no spaces], 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 (for example, one enterprising student wrote some custom Unix scripts and a standard Unix dictionary to help with the mechanics of the solution).

Assignment 3: Exploring Probabilities

This 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: 1) "CIA Hiring"; 2) "Brobdingnag Battles"; 3) "Delta Force"; and 4) "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".

4 Virtual OPNET™ Labs

Several classes were designed as hands-on computer labs [1, 9, 34, 35] that help students in understanding the network-related study cases and finding ways of solving them. Usually a small college has limited opportunity to offer a variety of physical networks (that accommodate computer security methods) to students and faculty to use them in the classrooms. As an option, they can use a unique application, the OPNET IT Guru™ Academic software package [25] that offers all the tools for virtual network model design, simulation, and analysis. OPNET software can simulate a wide variety of different networks, which are linked to each other through routers and switches [1]. Students can work from their PCs independently or under the instructor's supervision to simulate different networks (ATM, Frame Relay, X.25, Fiber Optics, etc.) and study visually the impact of various factors (e.g., traffic load, bandwidth, data rate, etc.) on the network [9, 17]. Providing means for analysis and modeling of network performance (including firewalls and virtual private networks) [28], OPNET IT Guru™ tool can also be used for studying data message flows, packet losses, link failures, bits errors, etc.

Following the methodology described by K. Brown and L. Christianson [27], L. Peterson and B. Davie [28], and R. Panko [34], a lab assignment was designed and offered to students for exploring firewalls and virtual private networks (VPNs). Using this knowledge and skills, students develop their own lab projects [9, 17] and include virtual lab techniques into their research projects related to various network security application protocols, such as the Diffie-Hellman asymmetric key agreement protocol [8] and RADIUS Protocol.

5 Examples of Students' Papers on Computer Security Methods Overview

In computer security classes, instructors encourage students to conduct research and write project papers on modern computer-security technologies. The assigned individual projects include the components of feasibility study, analysis, application, and evaluation of selected computer security methods. Students are motivated to select topics for projects that would be beneficial for their careers and valuable for

companies and the community. Usually, they 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 students' projects are implemented in local companies and the community:

- Senthil Balakrishnan, “Wireless Encryption Technology”
- Tom Borick, “Secure Wi-Fi Technologies for Enterprise LAN Network”
- Travis Bryant, “Steganography and Steganalysis”
- Soumya Busani, Anitha Karthikeyan, and Sunitha Malipeddi, “Intrusion Prevention System”
- Praveen Dandu and Vineeta Sharma, “Security and SQL Injections”
- Nigel D'Souza, Charles Heintzelman, and Suresh Kumar Sundaravadivelu, “Virtual Private Networks”
- Harika Samudrala, “Firewalls Overview”
- Tejinder Singh, Arti Sood, and Daniel Szilagyi, “RADIUS Protocol”
- Pratheeba Thangavel and Malathi Thiagarajan, “Secured Communication in Java.”

Seniors and all graduate students publicly delivered their presentations of individual and team projects in the classroom and in seminars [23, 24]. The instructor helps them in organizing the presentations and in developing professional skills for public speaking.

Working on the individual projects in the CS448 Introduction to Computer Security and CS572 Computer Security classes, students search information on modern computer security technologies from the prime sources, such as the Request-For-Comments organization (a repository of the standards in networking industry [36]), IETF Secretariat [37], WiFi Alliance (an association that promotes secure solutions for wireless networking technologies [38]), and others.

Many graduate students who are employed by local networking, computer and IT companies select topics for individual projects based on their experience with the company. The computer security systems tested by the students under the instructors’ supervision are offered for implementing in the company's environment and receive great support from their supervisors and managers. This fact helps the students in their job promotions and careers.

6 Examples of Research Studies

Students are encouraged to submit summaries of their research projects to professional journals and magazines. Eleven graduates, John Dion [10, 11], David Dwyer [12], Jay Grossman [22], Jhansi Jujjuru [13], Ajay Kumar [9, 15], Martin Milkovich [16], David Snogles [8], Arti Sood [17, 18], Bruce Trull [19], Vandana Wekhande [20], and Robert J. Zupko [21], have recently published their manuscripts in the *Rivier Academic Journal*. These activities develop a *strong bond* between students and faculty members that will last forever.

The individual capstone project on development of a new computer-system security concept is described in detail by David Snogles, a Rivier College graduate student, in his article, “Personal Encrypted Talk - Securing Instant Messaging with a Java Application” published recently in the Rivier Academic Journal [8]. The primary goal of the project was to secure Instant Messaging Communication between two parties on the Internet. The Personal Encrypted Talk (PET) system was designed to operate on Microsoft XP and Microsoft 2000 machines with an active connection to the Internet. Microsoft

Visio with UML Template and Jude UML Community Edition (Version 1.4.3) have been used as UML tools for object-oriented system analysis and design. The State Chart has provided details into the interaction of multiple users with the PET application. It illustrates the exchange of secret keys according to the Diffie-Hellman asymmetric key agreement protocol. The sequence diagram was used to solidify the interaction of the main components of the PET system and its end users. UML diagrams were developed for all eleven classes and integrated into a system-level UML class diagram.

7 Challenges

Certain challenges arise in the teaching of computer security courses, including:

- There is a widely-held assumption in the computer industry that security mainly consists of implementing an appropriate level of cryptography in the appropriate places in a software or hardware product. In addition, many computer software companies too often regard security as an expense that will not have any positive effect on the bottom line, and so are not motivated to implement the proper security solutions in their products. It is important to discuss these misconceptions with students and try to encourage them to seek solutions to them. As with other aspects of industry, politics can rear its ugly head, so such discussions must go beyond purely technical, logical arguments.
- Many security topics involve some familiarity with Math concepts that are not often taught, or inadequately covered, including:
    - Sets, Permutations, Combinations, and Probability
    - Number Theory (Divisibility, Prime Numbers, Groups, Rings, and Fields)
    - Modular Arithmetic
    - Computability Theory (in particular, the reasonableness of algorithms)

  These topics form the basis for many security areas, but most students will have limited exposure to them. The challenge here is how to introduce these topics to a generally Math-phobic audience, without eliciting a "deer in the headlights" response. Since this is not a pure Math course, we make no attempt to be mathematically rigorous, nor to expect students to come away with advanced skills in these areas; rather we try to motivate coverage based on simple, real-world applications of these topics.
- The techniques used by students to solve the various ciphertexts vary widely. In the past, some students have arrived at the same solution by using very different approaches and mixtures of techniques. Some students are more comfortable with some techniques, some with others. Some students have expressed real interest – fascination, even – in solving ciphertexts, while others have expressed frustration and a resulting dislike for them. This is really another aspect of the need for problem-solving skills, which are so necessary in all areas of computer science. We would like to encourage all students to try to strengthen their abilities in those techniques in which they are weak, because we believe that this will benefit them in the real world. The challenge is how best to do this, effectively, without alienating them.
- Computer Science is a fast-moving discipline – perhaps the one most subject to rapid change. Computer security is no exception to this, and indeed is currently one of the "hottest topics" in Computer Science. As a result, the material for such a computer security course is likely to change rapidly, from one iteration of a class to the next, on an on-going basis. Simply staying

up to date with the latest threats and techniques is a real challenge, and can consume large amounts of time and resources.

The solutions to these, and other, challenges are not cut and dried. They are likely to be dependent on the circumstances, on the students, on the instructors, and on other factors.

8 Conclusions

The authors have described the goals, demand, challenges, design, tools, implementation, and experience of running Web-enhanced computer security courses for seniors and graduate students. The experience has been in general a very positive one, while at the same time providing useful lessons learned. 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, and believe that the model can be extended to other engineering disciplines beyond the computing sciences.

9 References

[1] Riabov, V. Challenging Projects and Virtual Labs in Web-enhanced Networking Technology Classes. In Journal of Computing Sciences in Colleges 21(6) (June 2006), 88-99.

[2] Sabin, M., Higgs, B., Riabov, V., and Moreira, A. Designing and Running a Pre-College Computing Course. In Journal of Computing Sciences in Colleges 20(5) (May 2005).

[3] Kaufman, C., Perlman, R., and Speciner, M. Network Security: Private Communication in a Public World (2nd ed.). Pearson Prentice Hall (2002).

[4] Whitman, M., and Mattord, H. Principles of Information Security (2nd ed.). Thomson Course Technology (2005).

[5] Campbell, P., Calvert, B. and Boswell, S. Security+ Guide to Network Security Fundamentals. CISCO Learning Institute. Thomson Course Technology (2003).

[6] Conti, G. Googling Security. How Much Does Google Know About You? Addison-Wesley (2009).

[7] Milkovits, M. Digital Video Cluster Simulation. In M.E. Kuhl, N.M. Steiger, F. B. Armstrong and J. A. Joines (Eds.), Proceedings of the 2005 Winter Simulation Conference. Orlando, Florida (December 2005).

[8] Snogles, D. Personal Encrypted Talk - Securing Instant Messaging with a Java Application. In Rivier Academic Journal 1(1) (December 2005). Retrieved July 25, 2009, from http://www.rivier.edu/journal/

[9] Kumar, A. Development of Laboratory Exercises Based on OPNET IT Guru Academic Version. Rivier Academic Journal, 1(1) (November 2005). Retrieved July 25, 2009, from http://www.rivier.edu/journal/RCOAJ-Fall-2005_table.htm

[10] Dion, J. Automated Music Composition: An Expert Systems Approach. Rivier Academic Journal, 2(1) (April 2006). Retrieved July 25, 2009, from http://www.rivier.edu/journal/RCOAJ-Spring-2006_table.htm

[11] Dion, J. Musician Web-service Using Ruby-on-Rails, SOAP, FLEX, and AJAX. Rivier Academic Journal, 2(2) (November 2006). Retrieved July 25, 2009, from http://www.rivier.edu/journal/RCOAJ-Fall-2006_table.htm

[12] Dwyer, D. Software Reliability Estimations/Projections, Cumulative and Instantaneous. Rivier Academic Journal, 2(1) (April 2006). Retrieved July 25, 2009, from http://www.rivier.edu/journal/RCOAJ-Spring-2006_table.htm

[13] Jujjuru, J. An Overview of Internet Protocol Multimedia Subsystems (IMS) Architecture. Rivier Academic Journal, 4(1) (April 2008). Retrieved July 25, 2009, from http://www.rivier.edu/journal/RCOAJ_Spring_2008_table.htm

[14] Riabov, V. Simple Mail Transfer Protocol (SMTP). In The Handbook of Information Security: Key Concepts, Infrastructures, Standards and Protocols, Vol. 1, Chapter 60, Wiley & Sons (2005).

[15] Kumar, A. An Overview of Voice over IP. Rivier Academic Journal, 2(1) (April 2006). Retrieved July 25, 2009, from http://www.rivier.edu/journal/RCOAJ-Spring-2006_table.htm

[16] Milkovits, M. Using OMNeT++ to Simulate a Heterogeneous Digital Video Cluster Fabric. Rivier Academic Journal, 1(1) (November 2005). Retrieved July 25, 2009, from http://www.rivier.edu/journal/RCOAJ-Fall-2005_table.htm
[17] Sood, A. Network Design by Using OPNET™ IT Guru Academic Edition Software. Rivier Academic Journal, 3(1) (April 2007). Retrieved July 25, 2009, from http://www.rivier.edu/journal/RCOAJ-Spring-2007_table.htm
[18] Sood, A. Network Access Control. Rivier Academic Journal, 3(2) (November 2007). Retrieved July 25, 2009, from http://www.rivier.edu/journal/RCOAJ-Fall-2007_table.htm
[19] Trull, B. An Overview of Broadband over Power Line. Rivier Academic Journal, 2(1) (April 2006). Retrieved July 25, 2009, from http://www.rivier.edu/journal/RCOAJ-Spring-2006_table.htm
[20] Wekhande, V. Wi-Fi Technology: Security Issues. Rivier Academic Journal, 2(2) (November 2006). Retrieved July 25, 2009, from http://www.rivier.edu/journal/RCOAJ-Fall-2006_table.htm
[21] Zupko, R. Introduction to the IEEE 802.16 Standard: Wireless Broadband Access. Rivier Academic Journal, 3(1) (April 2007). Retrieved July 25, 2009, from http://www.rivier.edu/journal/RCOAJ-Spring-2007_table.htm
[22] Grossman, J. Coding Theory: Introduction to Linear Codes and Applications. Rivier Academic Journal, 4(2) (November 2008). Retrieved July 25, 2009, from http://www.rivier.edu/journal/RCOAJ-Fall-2008_table.htm
[23] Riabov, V. Mathematics and Computer Science Lecture Series (2002 – 2005). In Rivier Academic Journal 1(1) (December 2005). Retrieved July 25, 2009, from http://www.rivier.edu/journal/
[24] Riabov, V. Professional Seminar in Computer Science (Spring 2009). In Rivier Academic Journal 5(1) (April 2009). Retrieved July 25, 2009, from http://www.rivier.edu/journal/
[25] IT Guru Academic Edition. OPNET Technologies (2005). Retrieved January 20, 2006, from http://www.opnet.com/services/university/itguru_academic_edition.html
[26] Hnatyshin, V. Y., and Lobo, A. F. Undergraduate Data Communications and Networking Projects Using OPNET and Wireshark Software. ACM SIGCSE Bulletin, 40(1) (2008), 241-245.
[27] Brown, K. and Christianson, L., OPNET Lab Manual to Accompany Data and Computer Communications (7th ed.), Pearson Prentice Hall (2005).
[28] Peterson, L. L. and Davie, B. S., Computer Networks: A System Approach, 3rd ed., Morgan Kaufmann (2005).
[29] Rivest, R.; Shamir, A.; and Adleman, L. A Method for Obtaining Digital Signatures and Public Key Cryptosystems. In: Communications of the ACM (February 1978).
[30] LearnLinc Tool Panel Overview. iLinc Communications, Inc. (2009). Retrieved July 25, 2009, from http://www.ilinc.com/pdf/trc/ilinc-learnlinc-tool-panel.pdf
[31] Poe, E. The Gold Bug. Retrieved July 25, 2009, from http://www.online-literature.com/poe/32/ (For another copy of the text with an annotated vocabulary see here: http://poestories.com/text.php?file=goldbug); (Also see here: http://en.wikipedia.org/wiki/The_Gold_Bug)
[32] Conan Doyle, A. The Adventure of the Dancing Men (A Sherlock Holmes story), Retrieved July 25, 2009, from http://en.wikisource.org/wiki/The_Adventure_of_the_Dancing_Men
[33] Linton, T. Shift Substitution Cipher Tool: ShiftApplet.java. Retrieved July 25, 2009, from http://pages.central.edu/emp/LintonT/classes/spring01/cryptography/java/Shift.html
[34] Panko, R. Seven OPNET Labs (2005). Retrieved July 25, 2009, from http://www.opnet.com/services/university/itg_panko.html
[35] Wooley, B. Utilizing a Computing Lab to Improve Retention and Recruiting of Computer Science and Computer Information Science Students. In Proceedings of the 18th Annual CCSC Eastern Conference (Bloomsburg, PA, October 2002).
[36] The Request For Comments Editor (2009). Retrieved July 25, 2009, from http://www.rfc-editor.org/
[37] IETF Secretariat (2009). Retrieved July 25, 2009, from http://www.ietf.org/rfc.html
[38] WiFi Alliance (2009). Retrieved July 25, 2009, from http://www.wi-fi.org/OpenSection/index.asp

[*] The paper was presented at the 15th Annual Conference of the Northeast Region of the Consortium for Computing Sciences in Colleges (CCSCNE-2010), Hartford, CT, April 16-17, 2010.

[**] **Dr. VLADIMIR V. RIABOV** is a professor of Computer Science and director of Computer Science Programs at Rivier College. He teaches Networking Technologies, Software Engineering, and System Simulation and Modeling. His research interests include Computational Algorithms, Complexity Code Studies, Networking Software Test Strategies, and Object-Oriented System Design. He received a Ph.D. in Applied Mathematics and Physics from Moscow Institute of Physics and Technology and M.S. in Computer Information Systems from Southern New Hampshire University. Vladimir worked as a senior researcher and the Deputy Director at the Central Aero-Hydrodynamic Institute (TsAGI, Moscow, Russia), taught at Worcester Polytechnic Institute, Daniel Webster College, and the University of New Hampshire, and was a senior software engineer at Newbridge Networks Inc. and Nortel Networks Inc. He is a co-founder of the Russian Branch of the Open University of Great Britain, and a founder and the Editor-in-Chief of the Rivier Academic Journal. Vladimir is a member of ACM, AIAA, IEEE, and MAA.

[§] **Dr. BRYAN J. HIGGS** holds a B.Sc. in Physics from the University of Liverpool, UK, and M.Phil. and Ph.D. degrees in Physics from Yale University. In 1974, he moved into the computer industry and joined Digital Equipment Corporation where he worked for 20 years in a variety of positions. In 1994, Dr. Higgs transferred to Oracle, together with the rest of Digital's Database group, and worked in their Software Engineering group for 7 years. In 2002, Dr. Higgs joined the full-time Computer Science faculty at Rivier College, and retired in 2008. His major interests are database systems, programming languages (especially Java and C/C++), computer security, and Web development. Recently, he has become interested in scripting languages, including Perl, Python, JavaScript, PHP, and Ruby.