Session Number: 2558

Building an Undergraduate Security Curriculum

Anne Marchant, Edgar H Sibley, Hugh Tazewell (Taz) Daughtrey Jr.

George Mason University/ James Madison University

Abstract

Faculty at George Mason University (GMU) and James Madison University (JMU) in Virginia are collaborating on a project to develop a model for an undergraduate Information Security curriculum to be implemented beginning in the fall of 2004 at both institutions. The curriculum will include coursework in programming, operating systems, and networking as a basis for the major courses in security. Security coursework will include topics such as security technologies, forensics and auditing, network security and intrusion detection, risk management, security policy, modeling and authentication. Throughout the curriculum, modules in ethics and social responsibility will be woven into the coursework. A capstone course including cyberdefense exercises, such as those performed at the US Military Academy at West Point and the George Washington University in DC will be employed to challenge and motivate students. The cyberdefense exercises will also serve as a tool to assess the effectiveness of the curriculum. GMU is currently developing the curriculum as part of its BS in IT degree and JMU is integrating it into their BS in CS program. The goal of these joint endeavors is to develop a set of courses that will produce students qualified to perform security engineering roles and to prepare them for graduate coursework in Information Security Assurance. By combining the assets of faculty and students at two state institutions in parallel efforts, resources can be used to best advantage. Not only is duplication of effort avoided, but also the final curriculum will benefit from the cross-pollination of ideas and best practices. By starting with graduate level prototypes for teaching Security and then implementing these prototypes into both traditional CS and interdisciplinary IT undergraduate streams, we abstract a curriculum that can be replicated to meet the needs of programs nationwide as one strategy to help improve our nation's overall information security defense.

A joint MS/PhD class was used during the fall 2003 semester at GMU to test possible exercises for the capstone course as well as provide a pool of teaching assistants and mentors for the undergraduate program. The curriculum was also expanded in the spring 2004 semester jointly by JMU and GMU. The capstone course, which will be taught in a closed laboratory setting, will be piloted by faculty from both institutions in the summer semester of 2004 at GMU.

1. Introduction

The US Government's response to the events of 9/11 in setting up the Department of Homeland Security has resulted in an increase in public awareness of the need for security in all walks of life. Increasingly frequent Web hacking incidents and the proliferation of "ready-to-use" malicious programs also serve as warnings that our increasing dependence on the Internet has resulted in exposure of public networks and institutions to cyber-attacks. The Commonwealth of Virginia and other government and national institutions have expressed their belief that the current state of cyberdefense requires a new infusion into the economy of specialists who understand the strategies and techniques required to protect governmental, private, and other systems in order to deal quickly with cyber-attacks. Developing undergraduate programs in information security is a grassroots strategy to improve these information security defenses. The academic community has responded with great energy and in a spirit of cooperation. Many institutions of higher education have started to develop both graduate and undergraduate courses in various forms of *Systems Security* in many curriculum streams, from public policy to engineering. The foundations for defining a "common body of knowledge" (CBK) and the domains within the CBK have been laid[1,2]. This paper addresses steps in two Virginia universities that begin applying the conceptual framework developed so far in the implementation of new curricula from a practical perspective.

In the 2002-2003 academic year, the School of Information Technology and Engineering at George Mason University (GMU) launched an undergraduate bachelor's degree in Information Technology (BSIT). This degree program, headed by an Assistant Dean, is already showing great promise, enrolling over 600 students. The challenge to produce security engineers in an undergraduate program further motivated GMU to incorporate a comprehensive security curriculum through new IT Security courses into its BS program especially in the Security and Networking concentration (80% of students in the BSIT have formally declared for this option as of fall 2003). Since the Virginia Community College System already had a Network Security certificate program in place for students seeking an Associate's degree, and GMU already had very successful MS and PhD programs in Information Security, the BSIT, with a concentration in Security and Networking, filled the gap at the baccalaureate level.

Subsequently, GMU and James Madison University (JMU) were funded jointly under a Critical Infrastructure Protection Project grant sponsored by NIST, to develop, deliver, and implement the curriculum of a cyberdefense BS program over a 15 months period through the fall Semester of 2004. The course material for the undergraduate option is now being incorporated into undergraduate programs: a BS in Computer Science at JMU and in the Information Technology undergraduate degree at GMU. This coordinated effort will help produce similar courses for students at both institutions.

2. The Cyberdefense Capstone Course

One novel aspect of this joint program is that it will end with a capstone course to be held in a special hands-on teaching laboratory. This course will teach the basics of cyberdefense with enough attack knowledge to allow the separate courses to coordinate a final week's exercise involving a war-game, i.e., cyber-attack and defense exercise, between JMU and GMU classes over a virtual private network (VPN). As a result of this exercise, several practical benefits will accrue: the architecture of the laboratories, the curricula, and a description of the problems and successes of the program will be reported widely in papers and talks at conferences. Our intent in subsequent years will be to expand such exercises to conforming state and local universities and state institutions of Virginia in a competition. Later we expect to expand this effort and join with others in developing security exercises with nation-wide institutions and organizations.

A *prototype* of the capstone course is currently under development at GMU. GMU has been analyzing and experimenting with the problems and curricula developed for courses in cyberdefense at West Point[3] and George Washington University (GWU)[4]. Close collaboration exists with these two organizations and materials are being shared freely with them.

- Students and staff from GMU visited the US Military Academy at West Point in the summer and fall of 2003 to obtain their virtual system (lap-top version) and to inspect their new labs. Col. Daniel J. Ragsdale visited GMU on July 2, 2003 to meet with faculty and staff to discuss and advise on the curriculum and laboratory space at West Point.
- GMU faculty and graduate student Research Assistants (RAs) have visited and are working with GWU by analyzing their graduate security curriculum and exercises. Two PhD candidate RAs enrolled in GWU's spring 2004 semester course to gather experience and critique their material. Discussions during the fall of 2003 with Professors Lance Hoffman and Tim Rosenberg on their portable laboratory (the Portable Educational Networks – PEN and PEN2) and curriculum material have been very effective in improving GMU course development and designing its laboratory changes.

A GMU joint MS/PhD Denial of Service security course in the fall 2003 semester used the GWU exercise set for PhD student participants as special homework to help assess the use of such exercises at GMU, to aid in deciding needs for the laboratory where it would be implemented, and as a vehicle for incorporating students and RAs into the prototyping process. Some of them will aid in teaching the capstone course and in developing new bridging courses, act as mentors, and help develop any required additional software. Some students are employed locally: of these, two are full time network administrators and another two have experience in teaching security curricula within the SANS Institute. They will add best current practice and practical experience to the curriculum as well as serve as a conduit through which lessons learned and new ideas can be implemented by government and local industry.

The capstone course will be piloted to a select group of top undergraduate students and special graduate students at GMU's Prince William Campus in the summer of 2004 (June and July) using, as additional reading, Chirillo's book[5], and probably some of his bundled software. The undergraduate students will be taking this as a normal, "for credit" course while some graduates will be acting as co-instructors and as mentors for undergraduate students having difficulty in any topic. Feedback will be used to improve the fall 2004 and subsequent semester's courses. The graduate students will also act as the attacker contingent in this first cyberdefense exercise at GMU. Because the security curriculum has been underway at GMU for several semesters and because of the way that it is being implemented into the computer science curriculum at JMU, we will be ready to start the final courses in the fall semester of 2004. Regular offerings of the capstone will start thereafter at both GMU and JMU. Thus the goals of the undergraduate curriculum will be to provide material that fully engages student interest and stimulates creativity with the capstone. This will double as an assessment tool that measures the success of overall course outcomes and prove their value in real-life situations. After successful testing, the model undergraduate cyberdefense curriculum will be made available to federal and state organizations as well as other universities in the United States. We hope to extend our efforts to other universities in Virginia and the DC metropolitan area and conclude the security curricula with cross-university attack and defense exercises. We therefore intend to graduate students capable of excelling in careers as *information security engineers* or as *computer science graduates* with a specialization in *computer and network security* and, by collaborating and integrating work from other institutions, reduce costs in duplication of curricula.

3. Security Lab Architecture

A considerable amount of energy has gone into the design of a security lab to support the capstone cyberdefense exercises. We are studying both the IWAR[6] (Information Warfare Analysis and Research) laboratory at the US Military Academy at West Point and the PEN[4] (Portable Educational Network) at George Washington University. While our plans continue to evolve, certain elements are clear:

- Since this equipment is expensive, it should be designed to be multi-purpose. This has been well illustrated by the work in IWAR at West Point. The network must be secure and have the ability to be isolated from the campus backbone and Internet. This point cannot be over-emphasized.
- Systems should be flexible to support a range of inter-collegiate exercises. Some degree of portability may be desirable to permit demonstrations (e.g. the new architecture being developed for the PEN2 at GWU).
- While students should get experience with actual switches, routers, firewalls, and sniffers, use of a virtual machine tool, such as **VMWare**, allows one to teach concepts faster and more effectively.
- Dual removable hard drives allow the student to experiment with different operating systems, configurations, save configurations, and to rebuild corrupted machines. The latter is a necessity in laboratories that may be expected to carry noxious software such as viruses.

4. Undergraduate Security Curriculum in the BSIT at GMU

In addition to foundation coursework in telecommunications theory, office applications and web pages, programming, and computer architecture, the BSIT at GMU includes a "core" that includes multimedia, database, telecommunications, law and ethics, networking, and security, as well as two business courses and IT resources management. In the fall of 2004, a Human-Computer Interaction course will be added to the core, in anticipation of accreditation requirements. Students take 12 credits of mathematics, including courses in Calculus and Discrete Mathematics. Students opting for the concentration in Security and Networking take an additional 5 courses including at least one from the sub-categories of Security, Networking and Operating Systems, and Telecommunications. Finally, all students participate in a year long, senior design projects class, working in teams on integrated IT projects. With the development of the Cyberdefense Capstone course, our plan is to create a separate Security track using the existing Security Concentration Courses as a base.

The track includes the following courses.

Required Preparation

Introduction to Information Security. Topics to include: overview of security technologies, cryptography and its applications, physical security and basics of database security and ecommerce security.

Operating Systems. Topics to include: file systems and I/O devices, memory management, system administration, network services and resources.

Students choose 4 of the following 5 Security Concentration Courses, depending on interest:

Security Policy and Management. Topics to include: computer crime, law, and law enforcement, developing a security policy, incident recovery, security auditing, forensics, and intrusion detection. Ethical issues may be addressed by having a guest speaker from law enforcement.

Network Security: Topics to include: protocols, VPNs and secure communications, authentication, firewalls, advanced intrusion detection and analysis. Ethical discussions will include the responsibilities and professionalism required of system administrators. A guest speaker from a Network Operations Center (NOC) would be an effective backdrop for such discussions.

Advanced Security Principles. Topics to include: access controls, privacy and information integrity, analyzing and detecting malicious code, automated countermeasures, risk analysis. Ethical issues might well be addressed by having a guest speaker from the security field (preferably a student employed doing security analysis) talk about his or her work.

Information Warfare and Defense. Topics to include: espionage, PsyOps, SIGINT, open sources, physical attacks, cyberterrorism and hacking. Ethical discussions will include defining the rules of engagement, how to restrict open sources in a free society, and examples from recent conflicts.

Capstone Cyberdefense Course. Topics to include: methods of attack and defense, honeypots and honeynets, statistical analysis of network logs. This course will include a number of cyberdefense related exercises, and culminate in a competitive event.

A Bridging Course

A bridging course will be added to provide a way for top undergraduate students to supplement their information security knowledge as an elective or as a rapid start for a Master's degree at GMU in Information Security Assurance. This presupposes approval of an accelerated BS/MS degree program in information security, similar to other accelerated BS/MS degree programs GMU already has in place. Topics for this bridging course are still being articulated but should include: Formal methods in assessing and implementing secure systems, distributed denial of service attacks and hacking, professional ethics for the Information Security specialist, security architecture and models.

5. Integrating Information Assurance (IA) into a Computer Science Curriculum (JMU)

James Madison University has a conventional CS curriculum for undergraduates, as well as Master's degrees offered in two programs: on campus and online. The online Master's program has, since its inception in 1997, been devoted to Information Assurance: the degree is formally designated a "Master of Science in Computer Science with a concentration in Information Security." The on-campus graduate program, beginning with the 2003-2004 academic year, includes a new concentration entitled "Secure Software Engineering."

In 2002, a special-topics survey course was offered to upper-level undergraduates as well as graduate students, with rotating presentations by a number of faculty members. This led to the development of a new undergraduate course, "Information Security," that debuted in the 2004 spring semester. This course is one pre-requisite to the capstone cyberdefense course. The Critical Infrastructure Protection Project grant supports integration of IA throughout the undergraduate CS curriculum, mostly built around the new capstone course, already discussed above, involving cyberdefense exercises.

The new undergraduate "Information Security" course covers the basic issues of information system security. The course has the following learning objectives:

- Understand the basic issues of information system security
- Describe the roles of planning, management, policies, procedures, and personnel in protecting the confidentiality, integrity, and availability of information
- Understand specific information security threats (malicious code, network attacks, and hostile content) and widely used countermeasures (access control mechanisms, firewalls, intrusion detection systems)

In November 2003, the Computer Science Department faculty approved an Information Assurance concentration within the CS major. Information Assurance is regarded as an essential part of the Computer Science education, and the certificate is designed to map to the NSTISSI No. 4011 Certification standard[7]. Hence, this certification is approved and honored by the NSA and the DoD. This makes JMU students more marketable because the NSA hires employees with this certificate at a grade higher than the ones who do not have the certificate.

Certificate requirements:

1) CS major
2) The Introductory Information Security course
3) Internetworking course
4) One of the following courses
    a. Network Applications Development
    b. Network Analysis and Design
    c. Selected Topics in Information Security

The capstone cyberdefense course will be first taught in the fall semester of 2004 under the "Selected Topics" heading and then transition into a permanent course. The capstone will draw upon student learning in lower-level courses, including programming and networking. It will also be an excellent opportunity for applying skills in critical thinking, problem solving, communication, and teamwork.

Undergraduates will need adequate preparation prior to this course. We are investigating the knowledge and skills required of students to benefit fully from this capstone experience. Based on the experience of the US Military Academy at West Point and GWU, students should have completed prerequisite courses including programming, networking, security and operating systems.

The existing JMU CS curriculum requires majors to have completed programming in Java through a second semester, as well as an additional semester of programming principles in which they explore a number of other languages. One semester each of operating systems and networking are also required. We will explore whether these global mappings to the military-academy prerequisites are adequate, and whether supplemental material needs to be injected into any of these or other courses.

The laboratory established for this course will be a multipurpose facility. We can envision the configuration – especially multiple virtual machines and monitoring tools – being used for more fundamental courses in networking and related topics. As a demonstration tool, various attack and defense capabilities could be shown for awareness to a wide range of student (and even non-student) audiences.

6. Conclusion

Just as the Information Security Assurance field involves the application of technology and aspects of psychology, such as human factors, and business, such as economies of the marketplace, etc., so too the development of security curriculum involves creating a community of educators at all levels. While the creation of syllabi, lecture slides, exams and exercises are all important first steps, the creation of successful courses in such a dynamic field also requires the training and coordination of human assets. These include not only faculty and administrators, teaching and research assistants, but also laboratory support staff and undergraduate teaching assistants. They must share a common, if not necessarily uniform, vision, which is molded in part by the ethical and policy components of the curriculum. Reciprocal linkages to industry and government will help drive innovation and collaboration.

Part of the challenge in creating a new undergraduate curriculum is to separate out the durable concepts from technology that is transitory and then to use this as the basis for defining quantifiable programmatic outcomes. We want to find a balance in defining course content that is flexible enough to meet the needs of different types of programs that serve differing regional needs, yet is sufficiently standardized to offer some degree of compatibility without stifling creativity. An independent assessment tool, such as the (ISC)2 CISSP and SSCP certifications may be one way to measure success[7].

As a final note, it is clear that a single course in ethics and professionalism is not sufficient. Rather, themes of social responsibility need to be integral to and thus threaded through the material of each course. Students need to understand that the skills needed to defend the security of our nation and enterprises are far greater than those needed to attack them; the graduate must also have an appreciation for the costs of defense as opposed to the loss due to compromised systems by our society and the economy.

References

1. Davis, J., M. Dark, *Defining a Curriculum Framework in Information Assurance and Security*. http://vulcan.ee.iastate.edu/~davis/papers/ASEE-6-2003.pdf (visited 1/2/04).

2. "Common Body of Knowledge," International Information Systems Security Certification Consortium, https://www.isc2.org/cgi-bin/content.cgi?category=8 (visited 1/2/04).

3. D. Welch, D. Ragsdale, W. Schepens, "Training for Information Assurance," IEEE Computer. April 2002, pp. 2-9.

4. The Portable Educational Network" by Tim Rosenberg, Lance Hoffman, and Steve Willmore; http://www.cs.seas.gwu.edu/seccert/pen.doc (visited 1/2/04).

5. J. Chirillo, "Hack Attacks Revealed: A Complete Reference for UNIX, Windows, and Linux with Custom Security Toolkit," John Wiley and Sons, 2002.

6. "The Information Warfare Analysis and Research Laboratory (IWAR) and the Virtual Information Assurance Network (VIAN)," http://www.itoc.usma.edu/iwar/ (visited 1/2/03)

7. "National Training Standards for Information Security Professionals, http://www.nstissc.gov/Assets/pdf/4011.pdf (visited 1/2/04).

8. "Certification," International Information Systems Security Certification Consortium, https://www.isc2.org/cgi/content.cgi?category=3 (visited 1/2/04).

Biosketches of the Authors

TAZ DAUGHTREY is Computer Science faculty at James Madison University. His career has included programming, quality assurance, and training responsibilities in the nuclear engineering industry, as well as serving as Director of Quality and Chief Security Officer for an Internet-based medical information provider. He is Founding Editor-in-Chief of SOFTWARE QUALITY PROFESSIONAL and Editor of FUNDAMENTAL CONCEPTS FOR THE SOFTWARE QUALITY ENGINEER (2001). He is a Fellow of the American Society for Quality (ASQ).

ANNE MARCHANT is Assistant Dean for IT Undergraduate Education at George Mason University. Her career has focused on teaching and undergraduate curriculum development for UC Berkeley and for GMU. She has developed and administered GMU's BS in IT since its inception in 2002. She has participated in the development of accreditation standards for IT by SIGITE and has been active in developing articulation of IT programs between GMU and the Virginia Community College System. Her research interests include Computer Ethics and the scholarship of teaching.

EDGAR SIBLEY is University Professor and Eminent Scholar in the Schools of Information Technology and Engineering and Public Policy at George Mason University. His early work included database management in large corporations and US governmental agencies. More recently he has received funding in the field of secure systems, especially reduction of DDoS attacks and intrusion detection. Dr. Sibley has been the Chairman of the Board of Editors of *Information and Management* since its inception in 1977. He has published over 120 articles and acted as an expert witness for 4 law firms.

Appendix A: Some Useful Textbooks and Educational Materials

R. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems. John Wiley and Sons, 2001.

Bishop, M. Computer Security, Art and Science. Addison Wesley, 2002.

J. Chirillo, "Hack Attacks Revealed: A Complete Reference for UNIX, Windows, and Linux with Custom Security Toolkit," John Wiley and Sons, 2002.

CERIAS, The Center for Education and Research in Information Assurance and Security, http://www.cerias.purdue.edu/education/post_secondary_education/ undergrad_and_grad/curriculum_development/ (visted 1/2004).

Holden, G. A Guide to Network Defense and Countermeasures. Course Technology, 2003.

International Information Systems Security Certification Consortium https://www.isc2.org/cgi-bin/content.cgi?category=89 (visited 1/2004).

Tjaden, Brett C. Fundamentals of Secure Computer Systems. Franklin Beedle & Assoc., 2003.

Appendix B: Curriculum Outline of the Introductory Security Course at JMU

Week 1: Introduction to information security
1. Threats, vulnerabilities, confidentiality, integrity, availability, countermeasures
2. Cryptography overview
3. Operations, physical, personnel, administrative, and computer security

Week 2: Information security basics
1. Threats to and vulnerabilities of systems
2. Countermeasures
3. National policy and guidance, legal elements

Week 3: Information security basics (cont)
1. Trust, risk management
2. System lifecycle management
3. Protection, monitoring, and reporting

Week 4: Planning and management
1. Roles of organizational personnel
2. Security planning
3. Recovery and response

Week 5: Policies and procedures
1. Physical security measures, TEMPEST, security evaluation
2. Personnel and administrative practices and procedures
3. Software security

Week 6: Cryptography
1. Symmetric-key cryptography
2. Symmetric-key cryptography
3. Symmetric-key cryptography

Week 7: Cryptography (cont)
1. Public-key cryptography
2. Public-key cryptography
3. Key management

Week 8: Computer security mechanisms
1. Identification mechanisms (dictionary attacks, salts, password checking)
2. Access control policies (access control matrix, Bell-LaPadula, Biba)
3. Access control mechanisms (access lists, capabilities, multi-level security)

Week 9: Computer security threats
1. Coding faults, operational faults, environmental faults
2. Malicious code - Trojan horses, viruses
3. Malicious code - worms

Week 10: Network security mechanisms
1. Kerberos
2. CORBA
3. Firewalls

Week 11: Network security threats
1. Probes and scans
2. Teardrop, fraggle, land, ping of death
3. Distributed denial of service attacks – trinoo and tribe flood network

Week 12: E-mail and WWW security mechanisms and threats
1. Vulnerability of e-mail to interception and modification, PGP
2. Vulnerability of web traffic to interception, SSL
3. Mobile code, Java, and hostile content

Week 13: Intrusion detection and response
1. Intrusion detection
2. Intrusion detection
3. Audit and response

Week 14: Electronic commerce
1. Intellectual property
2. Online privacy
3. Electronic payment schemes]