CyberSecurity as General Education

Rajendra K. Raj, Sumita Mishra, Carol J. Romanowski and Trudy M. Howles, *Rochester Institute of Technology*

Abstract – The modern world of computing familiar to most college students is one based on mobile devices that rely increasingly on cloud storage. In this world, all students need to have a conceptual and practical understanding of the inherent computing, data, and privacy/security issues involved, but most institutions treat CyberSecurity education only as part of the institution's computing or information security curricula. At best, most students are introduced to this modern world through superficial courses on using mobile devices. The authors propose to make computer security and information assurance part of the general education for all undergraduates. They plan to develop a set of modules and courses meant to provide an introduction to, and deeper coverage of, the concepts underlying CyberSecurity. The proposed approach has several benefits: it will help to increase the size and diversity of the security-aware workforce, and also help to develop broad faculty expertise in CyberSecurity holistically across STEM and non-STEM disciplines via cross-disciplinary collaborations. This paper discusses the motivation underlying this change, initial plans, and the current status of this effort.

Index terms – Cyber Security, Information Assurance, General Education, Multidisciplinary Education

I. Introduction

The unprecedented expansion of the Internet accompanied by rapid advances in hardware and software development, have led to a wide-scale adoption of computing devices and technologies. The recent growth of mobile computing devices such as smartphones and tablets, as well as the availability of cloud computing resources (such as Google Apps, Flickr/Picasa, and Carbonite), has led to the reliance on a well-functioning cyber infrastructure directly critical to a significant portion of society. As breaches in the cyber infrastructure impact not only computing professionals but also everyone [1], it is crucial that all undergraduate majors receive general education that deepens their conceptual and practical understanding of issues in CyberSecurity.

At the same time, the success of general education at the university level has received more than its share of criticism; for example, a recent book [2] claims, with quantitative data to back it, that significant numbers of college students do not show gains in critical thinking, analytic reasoning, and other "higher level" college skills. This result has been disappointing to the universities that had revamped their approach to general education in the last decade but welcome news to others, including the authors' institution, that are about to begin significant restructuring of their general education curriculum. At our institution, general education traditionally was considered the purview of faculty in liberal arts and the natural sciences, but now all faculty members across the institution will be able to propose and deliver general education courses that meet outcomes defined by the institution's General Education Committee and New York State's requirements for undergraduate degrees [3], and any regional accreditation requirements for the university.

The new integrative approach to general education provides an ideal opportunity to educate all our students, not just computing majors, in CyberSecurity. That is, both new course modules and new courses in CyberSecurity will be created to target non-computing majors who can take the courses to satisfy their general education requirements. Some universities have developed targeted approaches for teaching security to non-computing majors, e.g., Information Policy (IPOL) specialization at University of Michigan [4]. However, our modular approach is designed for a much wider audience across several non-computing disciplines. As the number of women and minorities in these non-computing majors tends to be higher than in computing majors, this approach will allow us to reach a broader student audience. We therefore anticipate this project will result in a general population that is knowledgeable in CyberSecurity. In addition, we speculate that some of these students might be convinced that further education in CyberSecurity is worthwhile, thus increasing the number of students in CyberSecurity related majors.

This paper is organized as follows. Section II expands on the necessary background and motivation for this project. Section III presents course modules in CyberSecurity that we plan to integrate into existing non-computing courses.

R. Raj is with the Rochester Institute of Technology, Department of Computer Science, Rochester, NY 14623. rkr@cs.rit.edu.
S. Mishra is with the Rochester Institute of Technology, Department of Networking, Security and Systems Administration, Rochester, NY 14623. sumita.mishra@rit.edu.
C. Romanowski is with the Rochester Institute of Technology, Center of Multidisciplinary Studies, Rochester, NY 14623. cjrcms@rit.edu).
T. Howles is with the Rochester Institute of Technology, Department of Computer Science, Rochester, NY 14623. tmh@cs.rit.edu).

ISBN 1-933510-96-X/$15.00

Section IV describes a sequence of new CyberSecurity courses that have been proposed for general education, and Section V drills down to provide additional detail about one of the proposed new courses. Section VI provides a summary of the current status and discusses future directions of this project.

II. Motivation

In most undergraduate institutions across the country, general education is regarded as the foundation for preparing students for lifelong learning, for success in their chosen fields, and for their eventual role as well-educated and knowledgeable citizens in society [5]. Over the past three years, our institution, Rochester Institute of Technology, has thought deeply about revamping general education, created various strawman proposals, and finally selected a new framework for general education, developed with input from the faculty in liberal arts and sciences, and then reworked with input from the entire campus. The proposed General Education framework [5] has been designed as a three-phase structure: (a) a common *foundation* of two first year courses for all students, (b) a series of *perspectives* to introduce students to diverse but important areas of inquiry, and then (c) an *immersion* that provides the opportunity for deeper study and integrative learning experiences via a series of related courses that provide trans- and interdisciplinary experiences. Students also have the opportunity to take additional general education elective courses.

As stated earlier, to function as citizens in modern society, students must have a deep understanding of the cyber infrastructure in which they live, including issues of security and privacy involving personal devices, online behaviors, social networking and gaming sites, and downloading. It is simply not possible to develop this understanding with a superficial introduction such as a CyberSecurity 101 course. As a recent panel [6] commented, all computer users need to have some security knowledge, and addressing these concepts holistically, rather than focusing on stand-alone classes, is most effective. To provide the needed broad and deep understanding of CyberSecurity for all undergraduate majors, we propose a two-pronged strategy for developing CyberSecurity knowledge and skills:

1) Develop course modules that can be embedded into existing general education courses. Modules are a common pedagogical tool for computing and CyberSecurity topics, but are typically used in a single course or set of courses within computing disciplines [7-10]. Modules have also been used to embed security topics rapidly into an existing information assurance curriculum [11]. To our knowledge, however, no work has been done that includes delivery to non-computing disciplines. We expand on the modules concept in Section III.
2) Develop new courses in CyberSecurity that are targeted for all majors on campus. These are not superficial introductory courses, but courses that provide deep coverage in CyberSecurity topics so students gain both a conceptual and practical understanding of issues in this area. We expand on new courses in Section IV and describe one specific course in further detail in Section V.

III. Course Modules in CyberSecurity in Existing Courses

Fig. 1 shows example security module categories and possible topics in each category, and depicts the long-term vision for how modules and courses can impact a wide cross-disciplinary audience.

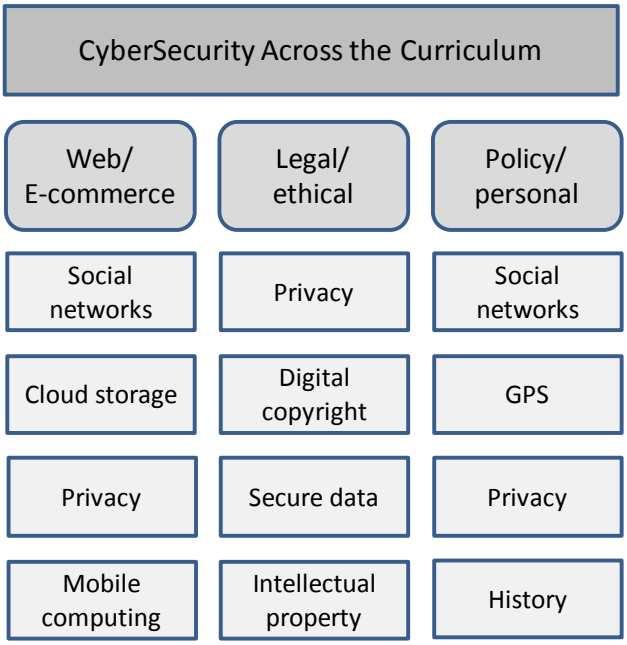

Fig. 1: Module categories and possible topics

To fulfill our goal of embedding CyberSecurity across the curriculum, the following modules are planned for non-computing courses. These modules represent the initial testbed for this effort and support current research agendas and teaching responsibilities of the authors and their colleagues. Additional modules for non-computing disciplines will be designed as the project progresses. Each of these proposed modules fits specific classes in three academic units in our university, and can be applied to other courses across different units in our institution.

A. Module: Critical Infrastructure Management

Critical infrastructure/key resources [12] encompass those physical entities and processes that make our communities function effectively. While computing is named as one key entity, the reality is that computing is *the* governing characteristic for the rest of them. The critical resources of energy supply, water/wastewater, transportation, telecom, emergency services/medical, facilities and finance depend upon computing, and our national icons are protected by security networks. Simply, computing supports the delivery of these products or processes to the public or provides the tools of protection for our communities.

This module will support the understanding of how computational security provides the backbone to our society and supports its function. The module will be inserted into the Risk Assessment, Management, and Communication course that examines this topic. The module will also be made available to other engineering technology educational programs to build expertise in improving a community's infrastructure systems, and ensuring that systems interact safely and securely.

B. Module: Security in SCADA systems

Supervisory Control and Data Acquisition (SCADA) systems are common in many industrial environments such as power plants, chemical plants, waste and water systems, and oil/gas pipelines. These systems are increasingly the targets of malicious attacks. This module will introduce students to the vulnerabilities of SCADA networks, the types of attacks likely to occur, and ways to harden the systems. This module will be used in quality management courses such as Statistical Quality Techniques, Management for Quality, Introduction to Asset Management, and mechanical engineering technology classes in operations management and new product and process design.

C. Module: Museum Studies

This module will address the critical lack of knowledge regarding CyberSecurity and ethical issues within the museum field. As museums add digital content and become more dependent on software and networks to carry out collection management, fund raising and publication, they must begin to address issues of security and privacy. This course module will identify and address vulnerable areas of the museum profession with regards to software, digital copyrights, privacy and social networks.

The focus of the module will be to raise awareness and build a working knowledge of these issues for those who will work in the museum profession. Museum Studies students have limited programming experience, thus this module will focus on developing vocabulary and raising awareness of issues that will be encountered in the field. This module could be incorporated into these existing courses for the Museum Studies major: Legal and Ethical Issues, The Forensic Investigation of Art, and Art Conservation.

D. Module: The 21st Century Siege

Throughout history, sieges have been a common form of warfare. The basic strategies of physical siege warfare have not changed over the centuries, although defensive and offensive weaponry advanced considerably. In the last two centuries, however, a new type of siege emerged—the cyber-siege. This module will explore the history of cyber attacks, discuss the attackers and their targets, and show how, as in the past, offensive tactics drive defensive advancements and vice versa. This module will be incorporated into a History and Manufacture of Siege Weapons course, and possibly other history/technology classes.

IV. New General Education Courses in CyberSecurity

Course modules in CyberSecurity embedded into existing general education courses, as discussed in the previous section, are arguably the best vehicles to reach the broadest possible student audience for several reasons. First, students already know these courses as serving the requirements of general education. Second, the modules are relatively the least intrusive way to add material. At the same time, course modules do not provide students with the depth needed to understand several concepts in CyberSecurity.

We therefore propose a set of general education courses in mobile computing security that forms an *immersion* sequence (as defined in our proposed general education framework) for non-majors. The computing faculty at our institution will offer these immersion courses. We define the modern world of computing as one based on mobile devices (e.g., smartphones, netbooks, tablets, and similar) as the fundamental computing units that rely on cloud storage (e.g., Google Apps, Flickr/Picasa, Facebook, file backup systems such as Carbonite, and similar). This is the world of computing familiar to our students, who need to have a conceptual and practical understanding of the inherent computing, data, and privacy/security issues involved. These courses are aimed at the non-major to reach the broadest audience possible with concepts and topics that are important and timely for all students at our university.

The sequence begins with an introductory course in mobile devices. Students with one General Education approved programming course will meet the prerequisite

for this course. Many non-computing disciplines, whether in the sciences or in engineering, already require such a course, and several such courses are offered on campus. Students in majors that do not currently require a programming course are likely to take such a course under the proposed general education framework because the course will count toward their general education requirements. To keep the prerequisite chain short, the other three classes in the sequence require only the Introduction to Mobile Computing course.

Preliminary course descriptions and some possible topics for these classes are given below.

A. Course 1: Introduction to Mobile Computing

Course Description: New, small and lightweight, intelligent mobile devices and embedded systems, such as smartphones, tablet devices, and other mobile Internet devices, have become popular in recent years. These devices present some challenges in programming, security, and data management. This course will introduce the student to basic concepts and issues in programming mobile devices; mobile device architecture; infrastructures needed to support such devices; power management issues; data management; information security; and legal, ethical, and privacy issues. The student will explore these topics through hands-on programming experiences with the devices. The course consists of lectures and laboratory exercises using two or more of the common mobile platforms such as Google's Android (several smartphones and now tablets), Apple's iOS (iPhone, iPod Touch, and iPad), Microsoft's Windows Phone 7 (smartphones) and Research in Motion's Blackberry OS (smartphones and tablets).
Pre-requisite: one General Education course that introduces students to computer programming. Note: several introductory courses in programming that will meet this prerequisite are offered by various departments in several colleges within the university.

B. Course 2: Programming the Mobile Device

Course Description: Expanding on Introduction to Mobile Computing, this course explores the computing aspects of mobile devices more deeply. The architectures of mobile devices are different from traditional desktop computers, laptops, or more powerful servers or workstations: they have limited processing power, storage, and battery power. Students will further their understanding of these non-traditional characteristics through hands-on experiences designing applications and systems for mobile devices. Other topics include networking issues, distributed systems, impact of partially available distributed systems, energy-efficiency, parallel computing, and storage in cloud computing. The course consists of lectures and laboratory exercises using common mobile platforms such as Android, Apple's iOS, Windows Phone 7, and Blackberry OS.
Pre-requisite: Introduction to Mobile Computing

C. Course 3: Data Security and Management in the Mobile Web

Course Description: Mobile web-enabled devices such as smartphones have increasingly become common personal productivity tools. Calendars, contacts, and even banking information are stored on these devices. Data is backed up to cloud storage, often without considering the privacy implications of doing so. In this course, students learn to identify security vulnerabilities, protect their vital personal information, and manage data stored and shared over wireless networks. Other topics include current state of privacy laws; privacy on the Web; how to keep personal data secure; GPS and locator issues; and data mining and its impact on privacy. The course consists of lectures and laboratory exercises using common mobile platforms such as Android, Apple's iOS, Windows Phone 7, and Blackberry OS.
Pre-requisite: Introduction to Mobile Computing.

D. Course 4: Security in Computer Games Platforms

Course Description: As mobile web-enabled devices become the major platform used for computer games, it is necessary for students to be knowledgeable about security issues related to games platforms. This course introduces students to the fundamental concepts of security on games platforms, starting with personal computers, dedicated games platforms such as the Xbox, Wii and Playstation 3, and then into games apps on mobile devices. The course consists of lectures and laboratory exercises using common mobile platforms such as Android, Apple's iOS, Windows Phone 7, and Blackberry OS. Pre-requisite: Introduction to Mobile Computing or permission of instructor.
Pre-requisite: Introduction to Mobile Computing

V. Details of a Sample Course

In this section, we describe the details of the course, Introduction to Mobile Computing, to illustrate some of the details of the course. The other courses will also be developed using a similar approach and emphasis.

A. Goals and Outcomes

The goal of this course is to provide students with theoretical and practical experience, stimulate students' creative thinking and develop their problem-solving strategies in the area of mobile computing. This course will support the general education goals of providing a relevant and innovative curriculum for a wider audience.

Specific general education outcomes supported by the course include:

1) Describe the potential and the limitations of technology.
2) Use appropriate technology to achieve desired outcomes.
3) Apply methods of scientific inquiry and problem solving to contemporary issues.
4) Identify contemporary ethical questions and relevant stakeholder positions.

B. Course Learning Outcomes

Upon completion of these courses, students will:

1) Explain the architectures of mobile devices and the infrastructure and platforms needed for their support. *Assessed through lab reports and exams.*
2) Describe security challenges in mobile computing and assess risks associated with a variety of approaches. *Assessed through lab reports and exams.*
3) Design and develop secure mobile computing applications. *Assessed through lab reports, programming assignments, and exams.*
4) Describe legal and ethical issues involved in mobile computing. *Assessed through presentations and exams.*

C. Lecture Material

This introductory course is designed to give students a broad overview of mobile computing area so that they gain conceptual and practical understanding of the inherent computing, data, and privacy/security issues involved.

Topics outline:

1) Introduction to mobile computing
2) Mobile device architectures
3) Programming mobile devices
4) Security and privacy issues
5) Data management in mobile computing
6) Power management
7) Legal and ethical issues in mobile computing

The lectures will be developed carefully to cover the material while keeping the students engaged. The hands-on lab exercises will help in reinforcing the learned concepts and provide practical knowledge along with the theoretical knowledge gained in the classroom. The lectures will be imparted with slides as well as interactive modules.

D. Lab Development

Smartphones with several different operating systems will be used as the basic platform for this course, providing a stimulating environment with hands-on experience, and generating student interest with timely subjects. The students who take this course will become more knowledgeable about mobile devices and will develop mobile applications over wireless networks; security will be a major theme in these lab assignments. The lab experience and knowledge will thus be invaluable not only in students' daily lives, but also when they join the workforce or pursue graduate study.

Most of the equipment needed for course development will be obtained from donations from companies in the mobile computing area. Additional funding will be obtained from the department of computer science to purchase needed equipment not available via corporate donations.

E. Course Assessment

We will supplement our course-outcome-level assessment and evaluation using overall project assessment and evaluation. We will constitute an advisory board of reviewers selected from other institutional faculty (but not the authors) and members of departmental Industrial Advisory Boards (each department at the institution typically has a board that typically consists of leaders from the industrial and government sectors who help each department to ensure that "real-world" concerns are incorporated into its programs). The project advisory board will also evaluate the feasibility, effectiveness, usefulness and students' learning experiences based on the course materials, student evaluations, and project outcomes. This review will help enhance the design, structure, and management of these courses.

We will also evaluate the effects of these courses based on the feedback received from external peer reviews of our scholarly works submitted to conferences or journals.

VI. Current Status and Future Directions

Module developers are working with instructional designers to create modules that are self-contained, consistent and can be linked together to form larger blocks of instruction. The modules will be created with a common style that is coordinated across module categories (for example, technical, social, or legal). This coordination will extend to the format of exercises, assessments, and other instructional elements. Each module will contain a short introductory section presenting the broad picture of CyberSecurity and where each module fits within that overview.

Currently, ten faculty representing five academic units in our university are committed to this approach. Our plan is to develop modules for each class taught by the ten faculty members on the team. As we progress in this effort, we will recruit other interested faculty to help expand the catalog of modules to the courses they regularly teach. Ideally, students should encounter at least one of these modules each year of their academic career. Incidentally, the course modules approach is likely to be transferable to other institutions where general education does not have the same degree of flexibility as provided by our new General Education Framework. These modules can be adapted and integrated into courses offered by 2-year institutions as well.

Targeted approaches to attract students towards the proposed general education courses need to be designed. Some ideas include but are not limited to inclusion of brochures in the institution's student recruitment mailing, advertisement on undergraduate admissions and academic units' website, and dissemination of information through student groups. We acknowledge that some "selling" of the courses may be needed to convince students to take these courses instead of other, perhaps less academically rigorous traditional general education courses that are perceived to be "easier." Since mobile devices and computing have become a part and parcel of their day-to-day lives, we do not anticipate this to be a hard sell, especially at a technical institution such as ours.

Despite the two approaches (the course modules and the immersion sequence) to CyberSecurity discussed in this paper, some students may be able to avoid any course with CyberSecurity content. We are therefore exploring a proposal to request our General Education Committee to add a new general education outcome that explicitly lists an outcome relating to CyberSecurity. With such an outcome, we can ensure all students learn CyberSecurity concepts in depth; of course, getting this outcome approved will not be easy and will require a concerted effort to educate out colleagues about its necessity.

The work described in this paper is part of a larger CyberSecurity education project whose goals are to:

1) Increase size and diversity of the CyberSecurity-aware workforce by pushing security concepts and courses to non-computing disciplines.
2) Develop faculty expertise in CyberSecurity holistically across STEM and non-STEM disciplines via cross-disciplinary collaborations.

We plan to develop such expertise in students who are traditionally underrepresented in CyberSecurity. Faculty collaborations across disciplines resulting from the project have already begun to pay dividends in terms of faculty scholarship, including papers and grants, as well as multi-disciplinary student projects.

VII. REFERENCES

[1] B.T. Delp, S. Nuristani, and B. Mitchell, "CyberSecurity: Congressional Action, Public-Private Partnerships, and Education are Key to Mitigating Vulnerabilities," *The CIP Report*, 9(7), January 2011.

[2] R. Arum and J. Roksa, "Academically Adrift Limited Learning on College Campuses," University of Chicago Press, 2011.

[3] New York State Education Department, "Definition of liberal arts and sciences," Accessed April 7, 2011. http://www.highered.nysed.gov/ocue/aipr/liberalarts.htm

[4] University of Michigan School of Information, "Information Policy (IPOL) specialization," Accessed April 7, 2011. http://www.si.umich.edu/msi/ipol.htm

[5] RIT General Education Committee, "General Education Framework," Rochester Institute of Technology, November 2010. Accessed April 7, 2011. http://www.rit.edu/conversion/media/documents/packet/General%20Education%20Framework_v12.pdf

[6] P. Mullins, J. Wolfe, M. Fry, E. Wynters, W. Calhoun, and R. Montante, "Panel on Integrating Security Concepts into Existing Computer Courses," *SIGCSE '02*, Covington, Kentucky, pp. 356-366, 2002.

[7] P. Denning and A. McGettrick, "Recentering Computer Science," *CACM*, vol. 48, no. 11, 2005.

[8] N. Herrmann, J. Popyack, B. Char, P. Zoski, C. Cera, R. Lass, and A. Nanjappa, "Redesigning Introductory Computer Programming Using Multi-Level Online Modules for a Mixed Audience," *SIGCSE '03*, Reno, Nevada, pp. 196-200, 2003.

[9] S. Sharma and J. Sefchek, "Teaching information security courses: A hands-on approach," *Computers & Security*, vol. 26, pp. 290-299, 2007.

[10] J. Walden and C. Frank, "Secure Software Engineering Teaching Modules," *InfoSecCD '06*, Kennesaw, Georgia, 19-23.

[11] B. Endicott-Popovsky and D. Frincke, "A Case Study in Rapid Introduction of an Information Assurance Track into a Software Engineering Curriculum," *Conference on Software Engineering Education and Training*, pp. 118-123, 2004.

[12] DHS: Department of Homeland Security, "National Infrastructure Protection Plan," Accessed April 7, 2011. http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf