On the Development of Networking and Information Security Degree Programs in a Four Year University

Weidong Liao¹, Osman Guzide²

¹ Department of Computer Science, Mathematics and Engineering, School of Natural Sciences and Mathematics, Shepherd University, Shepherdstown, WV 25443, USA
² Department of Computer Science, Mathematics and Engineering, School of Natural Sciences and Mathematics, Shepherd University, Shepherdstown, WV 25443, USA

Abstract - In this paper, we describe our experience in developing and implementing our security and networking degree programs at a small four year institution setting. Motivation for developing these programs is discussed. We then introduce security courses as part of our security curriculum development. Also presented here are our laboratory settings as an essential component for successful networking and security degree program, and our ethical hacking student club.

Keywords: Networking, Information Security, Curriculum Development

1 Introduction

Computer and network security has gained increasing popularity in the past two decades. As more and more business practices and governmental services became accessible on the Internet and Web, the threat and concerns of security have also grown. The recent development of IT areas such as social networks, cloud and mobile computing and services, has created more demand in qualified IT personnel in the area of computer and networking security.

Shepherd University is located at the four state area in the northwest of Washington DC. With its easy access to federal agencies such as Coastal Guard, IRS, FBI and NSA, the demand of students and graduates with solid knowledge and skills in computer and network security grows year by year. Our students have been hired as student interns by local government agencies every semester. Our recent graduates have found jobs in FBI, CIA, NSA, Coastal Guard and IRS, etc. It has been an imperative choice for us to develop a degree program or programs in the area of computer, network and information security.

As a department offering computing degree programs, our department had a Networking and Data Communication (NDC) concentration in the B.S. of Computer and Information Sciences program. The NDC concentration had served its purpose very well in the era that computers started to be connected to local area networks and later to wide area networks such as the Internet. However, the coverage in the security topics became insufficient as the usage and popularity of the Internet/Web surged.

We have also interviewed with and consulted local employers in information technology area, which further strengthened our motivation to have degree programs in the area of computer and network security. The demand of IT security personnel was increasing and has been increasing ever since the Internet and Web became popular for everybody. The superficial coverage of security subjects might have help teach security literacy so that students became aware of importance of computer and information security, but it was far from sufficient to train students into well prepared employers who were able to develop security solutions for business and governmental organizations.

Moreover, community colleges in our area, especially Hagerstown Community College, had established 2-year Cyber Security programs with funding from National Security Agency. Each year we had inquiries from graduates from these two-year programs requesting smooth transfer into four year degree programs. As a result, the department became fully convinced to develop degree programs in the area of security.

The timing for developing our security-centric programs seemed excellent as our computing curricula were due for revisions. Since computing and information technology are ever changing, their curricula must be revised periodically to catch up the trend. For small four year colleges, it would make the revision of computing curricula easier by following the ACM/IEEE computing curricula recommendation (We adopted the 2005 ACM/IEEE recommendation as it was the latest version in that time). The ACM recommendation requires necessary coverages of security and privacy issues in all computer science, information science, information
technology degree programs. So to follow the ACM/IEEE recommendations, we would have to develop new courses in the area of security. Degree programs in computer and network security area that embrace these courses certainly made our curricula revision easier.

The rest of this paper is organized as follows. Section 2 describes the development of our degree programs in the security area. In section 3, we discuss the security courses that are essential components our security program curricula. Section 4 focuses on our networking and security laboratory settings that are used for both security related courses and student organizations. Section 5 presents lessons learned and our latest changes in these programs, and summarizes the paper.

2 Degree Programs in Security Areas

Our first security degree program, Networking and Security concentration in CIS degree program, was developed by revamping the Networking and Data Communication (NDC) concentration. The NDC concentration was very popular among our students. Its curriculum was mostly on how to set up and manage Ethernet based local area networks. Since system and network administration was very demanding in job market in that time, the program had served its purpose very well. However, as the Internet and Web caught widespread interest in both industry and government, it became evident that its curriculum needed to be revised. During the revision of the NDC program, feedback from our graduates and their employers had suggested that we should add more the security subjects in the curriculum. They stated that the difficult and challenging part for the daily routine job for system and network administrators was to make sure the computer and network system stays secure and reliable. Based on the survey, we decided to add several security focus courses to cover the subjects in cryptography, information security, computer and network security, and change the title of degree program to Networking and Security. After revision, our new Networking and Security concentration had more coverage on the Internet and TCP/IP protocols.

It didn’t take much time that we realized from students’ reaction that the curriculum for the Networking and Security concentration was overwhelming for many of our students, particularly due to its mathematical requirements. Our Networking and Security concentration curriculum includes a comprehensive cryptography course which demands through understanding of mathematical topics in number theory, abstract algebra, and probability. Unfortunately, many students don’t have such mathematical background, although they had shown great interest and even potential for a four year degree in security focused area.

The imbalance of great interest toward security degree programs and insufficient mathematical background from potential students became worse for transfer students, especially for those who transferred from Cyber Security programs in local community colleges. Some community colleges in the area are designated by National Security Agency and Department of Homeland Security as National Centers of Academic Excellence in Cyber Defense 2-Year Education (CAE-2Y). Students from CAE-2Y came with great interest and background in cyber and information security, but many of them may need to make up great number of mathematics courses before they could take our theoretical cryptography course. So another security program that focuses more on hands-on security practice and operations seems an obvious choice.

Consequently, we developed our second security program, Biometrics and Information Security (BIS). The biometrics component was added due to the growing demand for IT personnel equipped with biometrics knowledge and skills from local government agencies such as FBI branches. The new BIS program was developed as a concentration under our Computer and Information Technology (CIT) major. Our CIT major prepares students for existing and emerging jobs and careers in the applied computing area. Students in this program learn the most current knowledge, concepts, and tools in a variety of IT areas, and develop an appreciation of the connection between the real life and digital world. A practical and hands-on based security and biometrics concentration fits very well in CIT degree program.

Figure 1 shows the computing degree programs in our department, with two newly developed security-focused fields of study highlighted.
3 Developing Security Focused Courses

Five security centric courses are included in our security degree programs: one was an existing course and four others were newly developed courses. The existing course is CIS 486: Network Security. The four newly developed courses are CIT 310: Information Security, CIT 372: Introduction to Biometrics, CIS 395: Introduction to Cryptography and Computer Security, and CIT 486: Network Security. We intentionally to have the last course, CIT 486, shares the same course title as CIS 486 because we anticipate we may have to offer CIT 486 as a cross-listed courses of CIS 486 in the beginning when we don’t have great number of senior students in the Biometrics and Information Security degree program.

<table>
<thead>
<tr>
<th>Courses</th>
<th>Prerequisites</th>
<th>New Course or Existing</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIT 310: Information Security</td>
<td>CIT 234: Intro to Networking</td>
<td>New</td>
</tr>
<tr>
<td>CIT 372: Biometrics</td>
<td>CIT 361: Information Security</td>
<td>New</td>
</tr>
<tr>
<td>CIS 486: Network Security Advanced</td>
<td>CIS 395: Intro to Cryptography</td>
<td>Existing</td>
</tr>
</tbody>
</table>

Table 1: Security Centric Courses

As indicated in [1], it is important to cover ethical and cultural issues in a security degree program or a focus of student study, and revision of existing computing courses may be necessary to cover certain security subjects in a more efficient and effective way. For this purpose, some existing courses in our curriculum are revised or being revised to cover some aspects of networking and information security. For example, SQL-injection has been very common security breaches in recent years. However, to discuss SQL-injection, students must have thorough understanding in Structure Query Language and therefore it is better to discuss this subject in Database Management System class.

Another discussion we have in particular to our security degree program is Web application security. One may imagine it is reasonable to develop a specific course to discuss Web application security because Web application and mobile apps become more and more important daily, so is security concerns on Web applications and mobile apps. On the other hand, since we have a number of Web development courses, we have decided to utilize and revise our existing Web development courses to cover Web application security topics. In the future, as student enrollments increase to certain level, we would add another course dedicated to Web Application security.

Notable enhancements in our existing courses to cover security topics are summarized in Table 2.

<table>
<thead>
<tr>
<th>Courses</th>
<th>Enhancements</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIT 234: Intro to Networking</td>
<td>Basic network security, computer virus</td>
</tr>
<tr>
<td>CIS 361: E-Commerce</td>
<td>Web Security in Electronic Commerce Web sites, Social Engineering, Denial of Service attack, SQL-injection, HTTPS protocol</td>
</tr>
<tr>
<td>CIT 388: Database Management System</td>
<td>Database Security, SQL-injection</td>
</tr>
<tr>
<td>CIS 419: Data Communication and Computer Networks</td>
<td>Secure Communication, Firewalls, Port Scanning, Virtual Private Network, Cloud Security</td>
</tr>
</tbody>
</table>

Table 2: Enhancements in Existing Courses

3.1 Developing a Biometrics Course

CIT 372, Introduction to Biometrics, is a core course for students in the degree program of Biometrics and Information Security. Students in other degree programs can take it as an elective course. This course is developed as an introductory course to cover the basics of biometrics and the mainstream biometric technologies. Since it is a course in Information Technology area rather than in the areas of computer science and engineering, the underlying theoretical background in image processing, voice sampling and recognition, and signal processing in general are discussed as optional and advanced subjects. It does provide detailed coverage in ethics and privacy concepts, and the future of biometric technologies.
In short, the following topics will be covered in CIT 372 class.

- Taxonomies of Biometrics Devices and Applications
- Basic Probability and Statistical Testing Methods
- Biometrics devices: fingerprinting, voice recognition, facial recognition, and iris scanning
- Biometrics and information security
- Social, Legal, and Ethical Concerns

Upon completion of this course, students are expected to be exposed to basic concepts of biometrics such as the fundamentals of fingerprinting, iris scanning, speaker verification, and hand geometry. A weekly lab is also designated for the provision of hands-on experience to students.

In the weekly lab sessions, students will form teams to work on a semester long project to design and develop a full-featured biometrics system consisting of biometrics devices, computing hardware and software applications. Student teams will have flexibility to choose the team projects, ranging from blood vessel authentication system, biometrics enhanced distance learning community, to a human resource management system that requests employees to use hand geometry or fingerprint to sign on when they arrive to work and sign out when they are ready to go home. Many open-source biometrics packages are available for student teams to experience and integrate into their team projects.

3.2 Covering Information Security, Network Security and Cryptograph

The difference between terms of information security, computer security and network security has been unclear for many people. Some people think information security is an umbrella term that includes both computer security and network security (and possibly cyber security). Other people may disagree and think information security is just the newer term for computer security, and network security is a subdomain of information security. In our curriculum design, we follow the later viewpoint. Thus two courses are developed: in sequence: CIS 310 Information Security and CIT 486 Network Security.

As indicated in the course title, CIT 310, Information Security, discusses a full range of topics in information security, including confidentiality, integrity and availability of information. CIT 486, Network Security, describes how to create a secure and networked environment for your resources, including data, hardware and software resources. It utilizes a combination of network hardware, the topology and software to ensure security, and thus it is a more technical demanding course that is offered after networking, data communication and ideally server operating system courses.

The fourth new course, CIS 395, Introduction to Cryptography, is a more theoretical course. It covers intermediate and advanced cryptography topics: symmetric ciphers, asymmetric ciphers, analysis and comparison of symmetric and asymmetric ciphers, cryptographic protocols such as DES, 3DES, AES and application level protocols such as IPSec. CIS 395 provides students comprehensive understanding to the modern cryptography as foundation of information and network security. Students in the class typically are required to complete a term paper or programming projects. In the past, students have worked on developing cryptographic applications using Java cryptography extension (JCE). It also prepares our students to work as student interns in government agencies or industry, such as the NIST/SURF program as discussed later in this article.

4 Laboratory Settings

We have two computer laboratories reserved for networking and security based classes and activities. These two laboratories are equipped with all necessary security hardware devices and software for students to conduct hands-on lab activities in information and network security.

The following software and hardware devices have been made available in our laboratories.

- Security cameras.
- High-end Switches with firewall capabilities.
- MegaMatcher Software Development Kit, including 1 Cluster Server, 2 Cluster Nodes, 1 MegaMatcher Server and 2 Client licenses.
- MegaMatcher additional Client License.
- Futronic Fingerprint scanners.

The security laboratory topology is as shown in Figure 2. The network is separated into two sub-networks. The BLUE network is used for lecturing and programming based lab exercises. While it is not part of the university network, it is configured with high security measurement. The RED subnet is used for fairly risky lab experiments such as hacking and anti-hacking lab assignments; it is also used for Ethical Hacking Club to conduct extra-curriculum activities.

5 Student Involvement and Outcomes

As part of their learning process, our students have been heavily involved in managing these two laboratories. Lab
assistants are work-study students who are in our security degree programs. These student assistants help design, install and monitor our security labs with guidance from our faculty members. Over the time, they gain valuable hands-on experiences that benefit them greatly in seeking internship and/or their first job after graduation. The work-study students are also members of and among the leadership in our Ethical Hacking Club.

The Ethical Hacking club, also known as Whitehat Hacking Club, is a student organization with focus and goal in learning how hackers work and ultimately how to make computing systems more secure. Most members in the club are students in our security and networking degree programs, although the club is also open to any students who are interested in getting involved in an active student organization to socialize with peer students, and learning more about networking and information security.

The Ethical Hacking club also provides a change to engage and retain students. The club hosts weekly activities for students to get together to participate in team based attacking and defending games and projects. It is our observation that female students and minority students are fond of team based learning environment. Thus our ethical hacking club also helps increase diversity in our student population.

The outcomes of our recently created security centric degree programs have been positive. They have been very active and successful area of study, not only for students in these two programs, but also for students in their computing areas. All graduates from our computing majors became more security literate by taking our security focused classes or participating in Ethical Hacking club. Our security degree programs have generated about 10 graduates annually in recent years.

The job placement for graduates from our security programs has been extraordinary. Our alumni are now hired by government agencies such as CIA, FBI, Coastal Guard and industry companies such as IBM, HP, General Dynamics, First Data, Bank of America, and Citi Corp. etc. In recent two years, two of our students have been selected by NIST (National Institute of Standards and Technology) into their competitive Summer Undergraduate Research Fellowship (NIST/SURF) program to stay on NIST campus for 11 weeks to work on their security-oriented projects. Another student has been chosen by NASA Greenbelt to work on cryptographic projects during summer time.

6 Conclusions

This paper presented our experiences in developing four year degree programs in security areas. The structure of our degree programs has been described. We then discussed curriculum development as part of the implementation of these degree programs, which includes creating new courses and enhancing existing courses. As our case study, our lab settings and student involvement are also introduced. At last we present the current status of these programs.

Our security degree programs are flexible to suit needs for students with a variety of background and career plans. Our programs have accommodated students who transferred from a Cyber Security program in community colleges to complete their four year degree, and students who want to go to graduate schools or work in government agency as security engineers or researchers.

7 References


