Computer Security in Undergraduate Curriculum

M. Nazrul Islam, Joseph Abel and Qinghai Gao
Security Systems & Law Enforcement Technology
Farmingdale State College, State University of New York
Email: islamn@farmingdale.edu

ABSTRACT

Digital information and infrastructure are crucial components in every aspect of today's world. There is a huge need for security professionals with expertise to analyze the security threats, design and develop security tools, and manage and update security architecture. A computer security technology program is developed for undergraduate curriculum following the industry needs and standards. Students will be trained on the latest technologies in the field with applied learning objectives so that they can address real-life security challenges.

Keywords: computer security, computer vision, digital image processing, forensics, pattern recognition.

INTRODUCTION

As digital technology is growing at an exponential rate with unbelievable features at an affordable cost, the whole world is moving in to digital environment for data processing and storage purpose. The data now includes all kinds of information in personal, social, professional and national levels. Digital processors, storage systems and networks are seriously vulnerable to malicious activities, which imposes not only financial loss but also severe threats to social harmony as well as national sovereignty. Another study from Juniper Research in 2018 demonstrates that around 33 billion records will be compromised by 2023 [1]. Therefore, protection of digital information and infrastructure has become an increasingly challenging task for the society and the industry.

There is a huge demand of skilled and trained professionals to design, develop, monitor, analyze and update security systems. As per the U.S. Department of Labor, the number of jobs in the computer and information security field in 2016 was 100,000 with a median salary of $95,510 per year. It is also estimated that there will be a growth of 56% over the next 10 years [2]. The computer and information systems manager position has a demand of 367,600 with an annual salary of $153,120, where the growth over next 10 years is expected to be 12% [3].

However, there has been no undergraduate program to train the professionals for the growing field of information security. There are a couple of graduate programs in the field, which are not as efficient because very few professionals pursue any graduate studies. Typically the Computer Science and related programs have been producing graduates who are working in the field. But the feedback from the industry shows that these graduates don't present sufficient skills in computer security. Based on industry needs and standards, we have developed an undergraduate curriculum

in computer security technology that will train the students with necessary skills in hardware and software tools for securing critical digital information and infrastructure.

OBJECTIVES OF COMPUTER SECURITY CURRICULUM

The Computer Security Technology program is designed with the educational objectives listed below.

1. To provide students with the fundamental knowledge in computer security.
2. To train the students with hands-on experience on technologies and tools on how to protect information and related resources.
3. To prepare graduates that can design, analyze and manage computer security systems.

Students will be introduced to a wide range of topics, including electrical principles, digital electronics, computer programming, biometrics, data security, network communications and security, and smart grid security. They will then be trained on the hardware tools and software algorithms for cryptography, identification of user, authentication of user and data, monitoring of critical digital activities, and prevention from intrusion. Students will also be engaged in real-life problem solving process through design projects. Graduates of the program will be equipped with skill in state-of-the-art technology in the field and hence be competent to serve the public and private sectors to ensure security and privacy in the digital world and to help development and growth of the community.

AREAS OF EXPERTISE

The curriculum will incorporate the following areas of expertise.

1. Computer Programming
2. Digital Logic and Systems
3. Cryptography
4. Computer Network
5. Data Security
6. Operating Systems
7. Digital Signal Processing
8. Biometrics
9. Infrastructure Security

Table 1 lists the major courses in the curriculum along with the relevant learning outcomes.

Table 1: Courses and learning outcomes

Course Title	**Student Learning Outcomes**
Digital Systems and Security	• Students will learn how to analyze different security threats and attack vectors within a given system • Students will learn different Firewall's which are used in enterprise settings and how they differ from Intrusion Detection based systems

	• Students will learn the basic Mathematics & programming behind cryptography
Data Security and Privacy	• Students will learn the basic concepts of stenography and other digital forensic tools, which can be used over networks. • Students will design how data pipelines and learn how they can be secured this will be done using the python programming language. • Students will learn how to comply different data techniques with the GDPR guidelines
Digital Signal and Image Processing	• Students will learn different image processing techniques which will enable them to alter pictures around using the Matlab programming language • Students will learn how to restore images after they are blurred or distorted. • Students will design Computer Vision programs and see how it can be applied to facial recognition mechanisms and eye recognition mechanisms.
Biometric Recognition	• Students will learn how to design biometric systems through programming & design. • Students will learn the privacy issues related biometrics and how they can be avoided. • Students will learn about biometric sensor technology and how it integrates into cyber and physical systems
Operating System and Security	• Students will understand how operating systems function on a low level • Students will learn about the design process of an operating system and where the most common vulnerabilities are of one • Students will learn how to parse through data log files within operating systems and learn how to secure them with best practices.
Foundations of Cryptography	• Students will be able to apply different linear algebra theories in order to learn different cryptography algorithms. • Students will learn about different bases and how they can be used in cryptography • Students will learn about Public Key, Private Key cryptosystems and how it can be applied into a production environment.
Applied Cryptography	• Students will design different public-key cryptosystems which include AES, DES, MD5, SHA, RSA and blowfish. • Students will compare cryptographic weaknesses in the different code design structures and protocols • Students will learn about one-way hash functions and how they play a role in enterprise settings
Network Security	• Students will identify security weakness of a computer network in a real-world scenario • Students will detect any intrusion/detection with in the given system and monitor traffic

	• Students will learn through a real world Firewall application how to secure production grade environments.
Penetration Testing	• Students will learn how to develop ongoing security strategies in order to mitigate and protect a given infrastructure against computer-security attacks. • Students will perform penetration testing on a secure network for a given evaluation purpose • Students will analyze code with malicious attempt and audit the given code in order to understand how it will impact a given system.
Smart Grid Security	• Students will design a security architecture to a smart grid in order to learn how to protect its vulnerabilities • Students will define a security policy in order for dealing a smart grid. • Students will understand how networking plays a vital role in smart grid security development.
Distributed Systems and Security	• Students will design distributed systems architectures and how to implement it in a real world setting. • Students will have to analyze a real-world scenarios and how they are able to secure a given infrastructure using distributed systems architectures • Students will design a security assessment plan for a given distributed systems environment.
Senior Project	• Students will learn how to develop a project requirements document for their design • Students will develop a solution to a real-world challenge • Students will create a report summary/ paper on their solution and how it was designed and how it impacts our society.

SKILLS FOR APPLIED LEARNING

The curriculum will incorporate applied learning where the students will not only learn the theories and principles of computer security technologies but also be able to apply them to real world challenges and systems. It will be conducted through individual course projects and the Senior Project course.

Students will develop skills in different topics of computer security, some of which are listed below.

1. **Security Attacks**: Students acquire a thorough understanding of the most common web application security risks and other common security attacks through the student learning about the Open Web Application Security Project (OWASP) and its features. They are trained on how different security attacks can happen, how they can be mitigated, and how to prevent an attack.
2. **Firewall Design**: Students will learn what a firewall is, how it fits into production grade network, how they can be used to secure data, and which production grade firewalls exist

currently. They will be able to design firewalls for the company environment and assess the environment in which the company runs their production grade network.

3. **Python Programming**: Students will develop expertise in python programming so that they can design and develop tools for computer forensics, automated networking, port scans on a given network, and cryptography schemas.
4. **Computer Vision**: Students will use Matlab programming language to apply computer vision in computer security. They will be trained on techniques, including image filtering, edge detection and pattern recognition.
5. **Biometrics Analysis**: Students will learn the fundamental principles and applications of biometrics, including fingerprints, face, iris, palm geometry, voice and DNA. They will be able to incorporate biometrics in the security tool design.
6. **Operating Systems**: Students will learn about different parts of an operating system (OS), semaphores, schedulers, and vulnerabilities with an OS. They will be able to secure a custom-made OS and develop security protocols for it.
7. **Cryptography and Cryptanalysis**: Student will be trained on the principles of cryptography and how to design cryptographic infrastructures in python. They will also be able to investigate the robustness of a cryptographic tool.
8. **Network Security**: Students will learn about the basic principles of computer networks. Then they will be able to analyze different security threats to computer networks, identify areas of weakness in a network infrastructure, monitor data traffic and activities on a computer network, detect an intrusion or malicious code and implement intrusion detection principles. It will incorporate real world Palo Alto Network First Generation Architecture.
9. **Penetration Testing**: Students will learn about different computer security techniques, which range from packet sniffing tools, foot printing, enumeration and even an exploit database (Google Hacking).
10. **Smart Grid Security:** Students will learn how to build and secure a smart grid applying cryptography tools, how to maintain the network of a smart grid, and how to create a security plan for the smart grid.
11. **Distributed Systems**: Students will learn about different cloud virtualization platforms, security threats arising from cloud platforms, fault tolerance with in a cloud platform and application level threats arising in a cloud platform.

INDUSTRY APPLICATIONS AND STANDARDS

In the realm of computer security there are a set of standards designed from the International Organization Standardization (ISO) and International Electrotechnical Commission (IEC), more formerly quantified as the ISO/IEC 27000. The ISO/IEC 27000 is the de-facto security standard for providing requirements for an Information Security Management System (ISMS) or a systematic approach for managing sensitive company information so that it remains secure. The standards are used throughout almost every organization, and hence will be incorporated in the computer security technology curriculum.

Another standard for computer security is the National Institute of Standards and Technology (NIST), which allows companies to understand threats, vulnerabilities and impacts on a larger scale and how they can reduce their risks with customized measures [4]. The framework has five

core aspects to it, which are recover, identify, protect, detect and respond. The first aspect, recover, allows companies to understand how to plan for recovery in case of a data breach or a malware attack. These procedures are executed and maintained to ensure timely restoration of system assets which are affected by cybersecurity incidents. The second part to the framework is identify, which allows individuals to assist in developing an organizational understanding to manage cybersecurity risks to systems, people, assets and data. Once a security professional understands the identify function, the individual can help identify related risks in an organization and focus and prioritize its effort with the risk management of the system. The third part to the framework is the protect function, which allows safeguards to be put in place in order to ensure delivery of critical infrastructure services. It also assists threats to be contained within impact to an organization. The fourth function is the detect function, which defines the appropriate activities to identify the occurrence of a cybersecurity event. It enables discovery of cybersecurity events, which means that there is continuous monitoring on a system in order to detect different security threats. The fifth framework is respond, which enables appropriate actions to take place regarding a cybersecurity incident. It also enables the ability to contain an impact of an incident within a company.

The third sets of standards are designed by the Institute of Electrical and Electronics Engineers, Inc. (IEEE), for security professionals [5]. The first standard is the IEEE C37.240-2014, which enables protection of the power systems from cybersecurity attacks. This is based on the engineering principle of securing voltage meters and other electrical components so that the power grids do not get overloaded. The second measure is the IEEE P1711, which is the standard for a cryptographic protocol for cybersecurity of substation serial links. This allows protection of integrity and confidentiality of communication over phone lines, radio waves and fiber optics.

The fourth standard is the General Data Protection Regulation (GDPR), which is the European Union (EU) law on data protection and privacy for individuals [6]. The GDPR standard is composed of six key principles, which include lawfulness of data, purpose limitations, data minimization, and accuracy of data, storage limitation, and integrity and confidentiality of data. The lawfulness of data relates to processing of personal data in a fair and lawful manner, which means that any organization needs to notify individuals how it will handle their data and how any security incidence will be handled. The second action is purpose limitations, which show how personal data can be collected and used. This means that the data can only be used for what is specified but nothing else. The third fact is data minimization, which means only to collect personal information that is necessary for the purpose of the business. The fourth role is accuracy, which means that personal data must be kept accurate and current and no errors should be presented to individuals using a platform. The fifth principle of the GDPR standard is limit storage of the data and do not retain data for an extended period of time for processing. This step is important because it involves removing the data when it is no longer necessary. The sixth principle to the GDPR standard is being able to maintain the integrity and confidentiality of the data [7].

The most salient feature of the curriculum is that it is aligned with industry needs and standards. It will have collaborations with outside agencies and experts in the field to provide the students with better learning outcomes. Several agencies and standards are already being considered, including, Palo Alto, Red Hat Academy, and Amazon Web Services.

CONCLUSION

As cybersecurity is on the rise in today's world, we need a lot number of professionals with expertise in security tool design and development. The computer security curriculum is developed with the state-of-the-art technology and concepts in the field. Graduates of this program will be able to immediately address the challenging security threats and protect the digital information and infrastructures.

REFERENCES

[1] "10 cyber security facts and statistics for 2018," Norton, https://us.norton.com/internetsecurity-emerging-threats-10-facts-about-todays-cybersecurity-landscape-that-you-should-know.html

[2] "Occupational outlook handbook: Information security analyst," US Department of Labor, https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

[3] "Occupational outlook handbook: Computer and information systems managers," US Department of Labor, https://www.bls.gov/ooh/management/computer-and-information-systems-managers.htm#tab-1

[4] "Cybersecurity framework," NIST, https://www.nist.gov/cyberframework/online-learning/five-functions

[5] "IEEE standards on cybersecurity, IEEE, http://theinstitute.ieee.org/technology-topics/cybersecurity/ieee-standards-on-cybersecurity

[6] "The principles," Information Commissioner's Office, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/

[7] "Data Protection Act 2018," UK Legislation, http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted