2021 ASEE ANNUAL CONFERENCE
Virtual Meeting | July 26–29, 2021 | Pacific Daylight Time
Paper ID #35029

Computer Science Technology-Cyber Security Option

Dr. Asad Yousuf, Savannah State University

Asad Yousuf is the Coordinator and Professor of Electronics Engineering Technology at Savannah State University

Mr. Alberto G. De La Cruz, Savannah State University

Instructor and Program Coordinator of Computer Science Technology at Savannah State University

Prof. Frederick T. Sheldon, University of Idaho

Prof. Sheldon has 35+ years of experience from academia, industry and government in various roles working a diverse set of computer science problems within the scope of software engineering, formal methods and information assurance and security in domains such as embedded real time avionics/vehicular, energy delivery systems, supply chain, cryptographic key mgmt. He received the Sigma Xi research and UT-Battelle key contributor and significant event awards and is an IEEE/ACM Sr. Member. He has degrees from the University of Minnesota and Texas at Arlington.

Computer Science Technology – Cybersecurity Option

With the growing interest in cybersecurity and lack of institutions with a degree program in the discipline in our region; designing, promoting and implementing a degree program in an institution that traditionally attracts students from the minority population will represent a viable pathway to increasing the participation of underrepresented minorities in this emerging industry. After an extensive search we could not identify any Minority Serving Institution (MSI) that offers a degree program in Cybersecurity in our region. This paper will describe how the Cybersecurity program can contribute to the production of these vitally needed scientists, by increasing the number of underrepresented minorities and women with a degree in Cybersecurity. The department of Engineering Technology currently offers an undergraduate degree inComputer Science Technology (CST). The CST curriculum is a hybrid of software and hardwarecourses designed to prepare graduates with a strong background in computer and information systems. This unique program would provide a good base for an academic program that addresses the Cybersecurity problem. This paper will present a project, which will design and implement a cybersecurity degree option in its CST program for students who wish to concentrateand develop strong skills in cybercrime detection, disruption and defenses. This paper will discuss the Curriculum grid showing the educational goals and the requirements for a baccalaureate (BS) degree in Cybersecurity designed and published in the University catalogue. This curriculum will include both currently existing courses (including hardware courses) and the newly developed courses. The development of Cybersecurity program is funded by the Department of Education.

Introduction

The need to have computer security has been in place for decades, going to back the mainframe and mid-level computers, but then the protection was limited to securing files on a single system. The landscape of computing is changed by the rise of computer networking and the Internet. Computers are now connected by using a wide range of topologies such as the Wide Area Network (WAN), Local Area Network, and Metropolitan Area Network (MAN). The demand for cybersecurity professionals across the United States is accelerating, according to the new data published on CyberSeek [1]. Furthermore, the study conducted by Cybersecurity Ventures [2] shows that around 3.5 million cybersecurity worldwide will be unfilled by 2021. The interest in Cybersecurity education is growing at an astronomical rate. The reason for this growth is the information system, databases, Internet based distributed systems and network communication is now coordinated with security related attacks. This demands the need for trained professionals who can protect systems against the cyber-attacks [3].

It is important that the curriculum at the undergraduate level should address the issues related to the protection of the system at both the hardware and software level. Analyzing the security of a system requires training in both hardware and software aspects of Cybersecurity. The Cybersecurity certificate education program is designed to increase the Cybersecurity awareness regardless of their major. The four-year Cybersecurity option in Computer Science Technology will focus on the vulnerabilities in computer hardware, software, cyber-space infrastructure, and communication protocol to attack private and government organizations. These attacks undermine the integrity and availability of the affected system and compromise the

confidentiality of data and information. Recent news and periodicals are replete with reports/examples of cyber espionage and its catastrophic impacts on US businesses and institutions [4,5,6].

Cybercrime continues to escalate since the growing of society's dependence on computers and the Internet. A continuous emergence of an army of exploits and malware through vectors ranging from social networks to mobile devices should be expected as the ranks of cybercriminals have been expanded from common criminals to dangerous terrorists, including even foreign government agencies.

News of foreign government attempts to influence the last national election by feeding WikiLeaks with information it obtained from hacked U S political institutions' computer systems is another example of the threats cyber criminals pose on our society. Cybercriminals are getting more and more sophisticated in their hacking skills. Every effort to improve Cybersecurity has been challenged by modern hacking techniques. A recent report by Morgan [2] on Cybersecurity labor market shows a projected shortage of manpower for Cybersecurity workforce. Therefore, there is an urgent demand for a continuous production of scientists with diverse expertise in enhancing Cybersecurity.

In this paper, we provide the details of the four-year Cybersecurity option in Computer Science Technology program. A minimum of six technical courses in Cybersecurity were designed. These courses are designed to provide advanced technical electives for Computer Science Technology students to pursue a concentration in Cybersecurity. Security courses will include topics such as security fundamentals, Embedded Systems with focus on security issues, intrusion detection, forensics, and network security. The following paragraphs will describe the newly designed Cybersecurity option in Computer Science Technology. The Computer Science Technology is a hybrid of software and hardware courses designed to prepare graduates with a strong background in computer and information systems. The Cybersecurity option in Computer Science Technology will provide a good base for an academic program that addressesthe Cybersecurity problems. The curriculum also includes Cybersecurity courses for non- STEM majors who wish to learn about the cybercrimes. Homeland Security students, Forensic Science and other STEM majors will also have the opportunity to obtain a certificate, or minor in Cybersecurity.

The Cybersecurity option will enable students to explore the trends and impact of current and past actions within the cyber world. Students will become adept at making rationalized digital decisions, evaluating threats, and managing risks in today's cyber infrastructure. Students in this option will learn how to apply the tools required to solve problems and mitigate new risks. Students pursuing the Cybersecurity option will be marketable and prepared for future-proof employment in the areas such as below:

- **Information security analyst:** responsible to design and implement security systems to protect an organization's computer infrastructure from cyber-threats.
- **Data security analyst:** responsible to safeguard an organization's computer systems and networks by developing strategies and maintaining security to ensure that an organization's networks has no security breach.

- **Penetration tester:** is an ethical hacker responsible for testing Information Technology / Operations Technology (IT/OT) systems to identify vulnerabilities using a wide variety of penetration software tools methods and tactics to simulate cyber-attacks.
- **Forensic computer analyst:** responsible to investigate computer-related crimes by using forensic tools to recover electronic data/information that serves as legal evidence.
- **Cybersecurity analyst:** responsible to assess, plan and enact security measures to safeguard the privacy, integrity and availability of an organization's cyber and information assets by preventing compromise (e.g., outside/inside security breaches).
- **Security Software Developer:** responsible to implement and develop security software and systems to ensure an organization's network continuity of operations (i.e., maintains confidentiality, integrity and availability).

Below is the program of study for the Bachelor in Computer Science Technology with Cybersecurity option. This paper will discuss the six newly developed courses with focus on Cybersecurity.

Program of Study –
Bachelor of Science in Computer Science Technology
Areas A, B, C, D, E, and additional requirements 43 hrs.

MATH 1113 Required in Core Area A

COST 1103	**First Year Experience**	**2 hrs**
***Area F**		**17 hrs**
CSCI 1301	Computer Science I	3 hrs
CSCI 1302	Computer Science II	3 hrs
MATH 2101	Calculus I	4 hrs
MATH 2301	Discrete Mathematics	3 hrs
CSCI 2231K	Introduction to UNIX	3 hrs
***Major Requirements**		**62 hrs**
CSCI Core Courses		*15 hrs*
CSCI 3000	Data Structures & Algorithm	3 hrs
CSCI 3385K/ CISM 3325	Computer Network and Design/ Data Comm & Comp Network	3 hrs
CSCI 4110	Operating Systems	3 hrs
CSCI 4210	Database Management	3 hrs
CSCI 4310	Compiler Construction	3 hrs
Engineering Technology Core Courses		*15 hrs*
ENGT 2101K	Computer Graphics	3 hrs
ELET 3101K	Electrical Circuit I	4 hrs
ELET 3301K	Digital Systems I	4 hrs
ELET 3411K	Microcontrollers	4 hrs
Math Core Course		*7 hrs*
MATH 2111	Calculus II	4 hrs

Mathematics Elective (Upper level 3000-4000 course		3 hrs
Cybersecurity/Engineering Technology Option		*23 hrs*
CSCI 2601K	Info. Security Fundamental	3 hrs
ELET 3412K	Cyber Sec. & Embed Sys.	4 hrs
CSCI 4010K	Ethical Hacking & Penn. Test	4 hrs
CSCI 4020K	Mobile Computing	4 hrs
ELET 4402K	Net. Def. & Counter Measures	4 hrs
CSCI 4622K	Cyber Forensics	4 hrs
Or any approved CSCI, ELET, ENGT or ENGR course by the advisor		
TOTAL 122 hours		

***A grade of "C" or better is required**

Design of Cybersecurity courses: Six technical courses were developed in Cybersecurity to provide basic and advance technical elective courses for Computer Science Technology students who wish to concentrate in the Cybersecurity for their baccalaureate degree. Following paragraphs will discuss the six newly developed courses:

CSCI 2601K Information Security Fundamentals: This course will introduce students the fundamental concepts and practices of information security. Topics included in this course are: introduction to Information Security, introduction to Program Security, Operating System Security, Database Security, Network Security, Administrating Security, the Need for Security, Legal issues, Ethical issues, Risk Management, planning for security, firewalls, VPNs, intrusion detection and prevention systems, cryptography, code Injection, and information security maintenance [8]. The prerequisite for this course is Computer Science I. Upon successful culmination of this course, students should be able to do the following:

1. An ability to design and maintain Information Security strategy
2. Understanding of the Need for Information Security, including Program Security, Operating System Security, Database Security, Network Security, Administrating Security.
3. An ability to plan for Security Technology: Firewalls, VPNs, and Wireless
4. An ability to design and implement Security Technology: Intrusion Detection and Prevention Systems.
5. Understanding of Cryptography, Code Injection, Physical Security.

ELET 3412K Cybersecurity and Embedded Systems: This course prepares students to understand the security of embedded systems. The course covers the critical system software and hardware issues that must be considered when designing secure embedded systems [9]. Prerequisite for this course is Microcontroller. Upon successful culmination of this course, student should be able to do the following:

1. Learn and understand embedded hardware and firmware analysis.
2. Learn fundamentals of secure embedded software development and practices
3. Learn and understand embedded cryptography
4. Learn the fundamentals data protection protocols for embedded systems and emerging applications of embedded network.

CSCI 4010K Ethical Hacking and Penetration Testing: This course is an introduction to a wide range of topics related to ethical hacking and penetration testing. It provides an understanding of the importance of how to effectively defend computer networks [10]. The course provides introduction knowledge in OS vulnerability, port scanning, reconnaissance, spoofing, exploitation, web application attacks, Trojan horse, social engineering and enumeration. The course provides an introduction to hands-on to ethical hacking and penetration testing tools and testing methodologies used by ethical hackers to protect and safeguard individuals, corporate and government data from cyber-attacks. Prerequisite for this course is Information Security Fundamentals.

As an indication of successful culmination of this course, students will:

1. Learn and understand the importance of the principles of ethical hacking
2. Learn and become skilled in using different penetration testing tools to perform port scanning, sniffing, reconnaissance, TCP/IP and OS vulnerabilities.
3. Learn, understand and practice the fundamental principles of encryption and decryption to protect information.
4. Recognize the different types of malicious software and attacks and be able to the proper defense to protect the integrity of the information

CSCI 4020K Mobile Computing Fundamentals: This course will introduce students the fundamental concepts and practices of mobile application development for the Android platform [11]. Topics included in this course are: introduction to the Android Studio SDK and tools, activity lifecycle, intent, fragment, geolocation tools, working with audio and video files and device built-in camera. Students upon successfully completion of this course will be able to design, develop, simulate/emulate, debug, test and deploy Android applications. Prerequisite for this course is Data Structures. As an indication of successful culmination of this course, students will:

1. Understand and explain data types, variables, control statements, methods, arrays, inheritance, interfaces and classes.
2. Understand and explain Android application lifecycle, intents, fragment, and user interface of objects such as fields, buttons, containers and menus.
3. Ability to work with video and audio files, built in SQL database, device's built-incamera and geolocation services.
4. Use Android Studio SDK and API tools to design effective and attractive applications for the Android platform by using fundamental concepts and object oriented programming.

ELET 4402K Network Defense and Counter Measures: This course prepares students to protect networks against attacks by implementing hands-on protection measures and by responding to active and potential threats. The course covers multiple techniques for network defense, including firewalls, intrusion-detection systems, VPNs, encryption, and process of

securing system configuration and settings to reduce surface of vulnerability [7]. Prerequisite for this course is Computer Network and Design. As an indication of successful culmination of this course, students will:

1. Learn and understand how to defend network against attacks.
2. Learn fundamentals of Firewalls and implement firewall for network protection
3. Learn and implement the concepts of intrusion detection, encryption, and Virtual Private Networks (VPN).
4. Learn the fundamental of hardening.

CSCI 4622K Cyber Forensics: This course will introduce students to the fundamental concepts andpractices of Cyber Forensics. Topics included in this course are: Principles of Digital Forensics, intellectual property, privacy issues, legal codes, risks-vulnerabilities-countermeasures, methods and standards for extraction-preservation-deposition of legal evidence. Students will learn different aspects of digital evidence: ways to uncover illegal or illicit activities left on disk and recovering files from intentionally damaged media with computer forensic tools and techniques [12]. Prerequisite for this course is Operating Systems. Upon successful culmination of this course,students should be able to do the following:

1. An ability to implement data recovery, identifying hidden data, Encryption/Decryption, Steganography, and recovering deleted files.
2. Understanding of the need for computer forensics, computer hacking, evidence, extraction, and preservation.
3. An ability to plan for Digital evidence controls, uncovering attacks that evade detection by event viewer, task manager, and other windows GUI tools, data acquisition, disk imaging, recovering swap files, temporary and cache files.
4. An ability to design and implement network forensic, collecting and analyzing network based evidence, reconstructing web browsing, email activity, windows registry changes, intrusion detection, and optioning offenders.
5. Understand software reverse engineering, defend against software targets for viruses, worms and malware, improving third party software library, identifying hostile coded buffer overflow, and provision of unexpected inputs.

The Computer Science Technology-Security option is approved by the New Program Curriculum Committee (NPCC). The program is scheduled to be launched in Fall 2021. We plan to offer Information Security Fundamentals, Mobile Computing and Network Defense and Counter measures. All courses offered in the area of Cybersecurity have a strong laboratory component to provide hands-on experience to the students. The following paragraphs will discuss some of the lab components of Network Defense and Counter Measures course [7].

Network Defense and Counter Measures Lab Structure: The instructor took a course in the basics of Cybersecurity and has done extensive research to learn the labs offered by SEED for security education. The development of SEED labs was funded by three grants from the US National Science Foundation; Awards No. 0231122 and 0618680 from TUES/CCLI and Award No. 1017771 from Trustworthy computing. Following labs are planned for Fall 2021:

- Buffer Overflow
- Linux Access Control Lists
- Metasploit
- Snort –Intrusion detection
- Virtual Private Network (VPN)
- Encryption
- Message Authentication Code (MAC) and Hash functions
- TCP/IP

Below is the brief description of each lab to give reader an idea of the labs that will be conducted in the Network Defense and Counter Measure course.

Buffer Overflow Lab: The learning objective of this lab is for students to gain experience with buffer-overflow vulnerability. The students will be given a program with a buffer overflow vulnerability and their task is to develop a scheme to exploit the vulnerability and finally gain the root privilege. In addition to attacks, students will also learn about several protection schemes that have been implemented in the operating system to counter against the buffer-overflow attacks.

Link Access Control Lists: This lab was developed for the Labtainer framework by the Naval Postgraduate School, Center for Cybersecurity and Cyber Operations under National Science Foundation Award No 1438893. The lab explores the use of Linux Access Control Lists to provide access control over files, with more flexibility than the access control offered by the traditional UNIX file permission.

Metasploit: This lab was also developed for the Labtainer framework by the Naval Postgraduate School, Center for Cybersecurity and Cyber Operations. The explores the use of metasploit tool which is installed on a Kali Linux system (attacker) and is meant to learn simple penetration skills on purposely vulnerable metasplotable host (victim).

Snort Intrusion Detection: This lab was also developed for the Labtainer framework by the Naval Postgraduate School, Center for Cybersecurity and Cyber Operations. This lab introduces the use of snort system to provide intrusion detection within a Linux environment. Students will configure simple snort rules and experiment with a network intrusion detection system.

Virtual Private Network: In this lab the students will explore the VPN protocol to connect two networks securely to each other over another unsecure network. All data is transmitted securely over an encrypted tunnel.

Encryption: In this lab the process of encoding a message in such a way that only authorized parties can access. Students will work with the plain text (Message to be encrypted), ciphertext (Encrypted message), and cipher encryption algorithm. The concept of symmetric and public key will be learned.

Message Authentication Code (MAC) and Hash functions: In this lab Message Authentication code will used to check the data integrity and authenticity of message. The

Message Authentication code will be generated by using a cryptographic hash function (ex: MDSSUM, SHA, and etc.)

TCP/IP: In this lab the students will work with the TCP/IP vulnerabilities. SYN flood attack will be examined which is the denial of service attack that looks to prevent connection from succeeding by overflowing specific data structure on the target operating system. TCT RST attack which terminate connection between two host by making them think that the end points have asked to stop the connection. TCP session hijacking attack is about being man in the middle. The lab setup will use the simple network topology in which the attacker is in the same Local Area Network.

Conclusion

The cybersecurity curriculum design results from the funding by the grant provided by the Department of Education. The creation of the option was challenging, and courses' development isthe first important step to successfully implementing the curriculum in the dynamic field of cybersecurity. We look forward to making collaborations with the industry to explore internship opportunities for the students. Recently, we have received an initial offer from one of the companies to establish a partnership to explore internships, employment opportunities, and support for the curriculum and laboratory design. We are excited to launch the program in Fall 2021.

References

[1] CyberSeek Data Confirms the Ever-Present Need to Expand Cybersecurity Talent Pipeline. NIST.gov https://www.nist.gov/news-events/news/2020/07/cyberseektm- data-confirms-ever-present-need-expand-cybersecurity-talent (retrieved February 1, 2021).

[2] Morgan, Steve. Cybersecurity Talent Crunch To Create 3.5 MillionUnfilled Jobs Globally By 2021. https://cybersecurityventures.com/jobs/ (retrieved February 1, 2021).

[3] How to Protect Your Business from Cyber Attacks. NIST.gov https://www.nist.gov/blogs/manufacturing-innovation-blog/how-protect-your-business-cyber-attacks (retrieved February 1, 2021).

[4] Significant Cyber Incidents. CSIS.org

https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents (retrieved February 1, 2021).

[5] Types of Cybersecurity threat & how they will impact your business. MIND-CORE.com

https://mind-core.com/blogs/cybersecurity/types-of-cyber-security-threats-and-how-they-will-impact-your-business/ (retrieve February 1, 2021)

[6] Nation State Cyber Espionage and its Impacts. CSE.WUSTL.edu

https://www.cse.wustl.edu/~jain/cse571-14/ftp/cyber_espionage/index.html (retrieved February 1, 2021)

[7] S. Williams; L. Brown, Computer Security, Pearson, 2018

[8] M. Whitman, Principles of Information Security, Cengage Learning, 2014

[9] T. Stapko, Practical Embedded Security: Building Secure Resource-Constrained System (Embedded Technology), Newnes, 2011

[10] M. Simpson; N. Antill, Hands-On Ethical Hacking and NetworkDefense, Cengage Learning, 2016

[11] B. Phillips, Android Programming: The Big Nerd Ranch Guide, Big Nerd RanchGuides, 2017

[12] B. Nelson; A. Phillips; C. Steuart, Guide to Computer Forensics andInvestigations, Cengage Learning, 2018