Academic Papers

Paper of the Year: *Industry Priorities for Cybersecurity Competencies*

Michael Whittman

With the projected global shortfall of almost 2 million Cybersecurity professionals, it become increasingly critical to promote the development of new Cybersecurity degree programs across the U.S. This raises the question of exactly what should these degree programs prepare students to do? In order to examine this question, this study seeks to identify industry priorities for Cybersecurity competencies based on the Department of Labor's Cybersecurity Industry Model, which creates a tiered set of competencies focusing on the NIST NICE Cybersecurity Workforce Framework categories. The study also seeks to determine if these priorities vary by organizational size or industry.

Student Paper of the Year: *Predicting Cyber-Attacks Using Publicy Available Data*

George Onoh

Cyber-attacks are often detected too late. According to reports on reported cyber-attack incidents, most victim organizations do not know that their systems have been breached until they are informed by organizations or individuals external to the victim organization's physical or logical network. This is a significant problem for cyber security professionals and organizations. To further understand this problem, I investigated the following questions in this study: How are external organizations able to detect cyber-attack incidents using only publicly available information? How can cyber-attacks be predicted based on only publicly available data? I collected data on indices representing mentions of a certain type of attack (brute-force / password guessing attack) from public data repositories as well as ground truth data for a target organization. I extracted and stored the data daily. I used the collected data as training data in a machine learning algorithm. After limited training, the system was able to predict future attacks. The results suggest that it is possible to predict cyber-attacks based on publicly available data.

A Study of the Evolution of Secure Software Development Architectures

Leah Winkfield, Yen-Hung Hu, Mary Ann Hoppa

Emerging technologies such as containers, microservices, DevOps, Agile software development life cycle (SDLC), and cloud-native applications have gained popularity and traction in the industry and among enterprises. These modern application technologies and architectures are being adopted because they enable greater flexibility, scalability, portability and more rapid development. Consequently, how to build and maintain secure applications and systems is being reevaluated. Since the total responsibility is now larger and more complex, the application developer role is expanding to include greater security obligations and concerns. This paper explores the evolution of software development architectures and consequent implications on security, to better understand the technology landscape driving this change and its impacts on application development. To remain competitive, organization must be prepared to invest in ongoing training of their developers in the latest best practices. To remain relevant, higher education must adapt curriculums to prepare future professionals in the appropriate cybersecurity and secure coding practices to match the development shifts observed in industry.

All About SQL Injection Attacks

Vinitha Subburaj, Daniel Thomas Loughran, Mayar Kefah Salih

With advancements in Internet technologies, there is an increasing growth of applications that are web based. With smaller software development cycles and faster delivery, security has become an important issue. There are many types of security attacks that are made on Web applications and SQL injection attack is one type of an attack. Recently, studies have shown that more and more web applications are getting attacked by different types of SQL injection attacks. To effectively detect and prevent these attacks, a deeper understanding on the different types of SQL injection attacks, the nature of the attacker, and the mechanism used is very important. This paper discusses details that one would need to understand all about SQL injection attacks. This paper presents a detailed study of most recent SQL injection attacks on web applications, SQL injection prevention and detection mechanisms. The classification of different types of SQL injection attacks, prevention and detection mechanisms discussed in this paper highlights the need for future improvements in the detection and prevention mechanisms to secure web applications from SQL injection attacks.

Cyber Security Education for Liberal Arts Institutions

Xenia Mountrouidou, Xiangyang Li

Cybersecurity is a broad, dynamic, and ever-changing field that is difficult to integrate into undergraduate Computer Science (CS) curriculum. The absence of sanitized labs coupled with the requirement of specialized faculty to teach the subject pose obstacles many primarily undergraduate colleges face in adopting cybersecurity education. In this paper we describe a set of labs that have been implemented using the Global Environment for Network Innovations (GENI) cloud infrastructure as a solution to teaching experientially with low overhead. These labs are developed for different levels of experience, based on Capture The Flag (CTF) competitions that include short questions and answers, scenario-based exercises, and upper level research skills. Curriculum for Liberal Arts Institutions is presented starting from the core general education as a vehicle to bring cyber security to a diverse population of non-CS majors and moving to introductory and upper level CS courses. These labs and curriculum are part of the project CyberLIA (Cyber security and LIberal Arts) with goal to broaden the path tocyber security profession for a diverse population of Liberal Arts students.

Cybersecurity Education with POGIL: Experiences with Access Control Instruction

Li Yang, Xiaohong Yuan, Wu He, Jennifer Ellis, Jonathan Land

Given the ever-increasing realization as to how cybersecurity integrates into all aspects of daily life, cybersecurity education becomes increasingly important. While cybersecurity skillset certainly includes being equipped to safeguard businesses / organizations from cyberattacks, it also includes "professional skills" as also called "soft skills", such as teamwork, critical thinking, communications, etc. In this regard, it is important for colleges and universities to promote pedagogical frameworks that approach education in a way that does not dichotomize theory and praxis but encourages their interrelationship in terms of educating students towards these ends. In this paper, we introduced cybersecurity education materials we developed with Process-Oriented Guided Inquiry Learning (POGIL) which provides a promising educational framework for re-envisioning a holistic methodology for technical studies, specifically for the discipline of cybersecurity. The POGIL materials for teaching access control are described, and our experiences with using these materials in classroom are discussed. Through assessing the developed POGIL

materials and teaching pedagogy, we found that cybersecurity POGIL helps students to solve problems and gain both cybersecurity content knowledge and soft skills.

Engaging Airmen with Cyber Education and Training: Designing a Platform Using Gamification

Landon Tomcho, Lt. Col. Mark Reith

Several issues have impeded the effectiveness of United States Air Force cyber education and training in terms of ensuring that Airmen at many different levels of cyber are sufficiently up to speed with cyber. The framework proposed in 'Rethinking USAF Cyber Education and Training' [1] is a response to these issues. The framework suggests a well-designed platform built around the idea of crowd-sourced content and community engagement and feedback. This paper proposes several ideas of implementing gamification and human-focused design concepts on the platform and includes an analysis of how this can affect Airmen at different tiers of cyber development. Ideas relating to community involvement, introducing non-cyber-experts to the platform, and a navigable cyber topic map are proposed. These ideas represent only some of the foundational concepts that can be applied to the platform; data from the platform should be used to continuously tailor the platform to maximize user engagement and consequently their cyber knowledge and training.

Examining the Level of Education Factors on Reducing Data Security Breaches

Steven Brown, Oscar Ukpere

The purpose of this quantitative correlational research study was to examine the relationship between the levels of educational factors possessed by information security managers (ISMs) and the number data security breaches in their organizations. Previous research reported that levels of educational factors have an increasing impact on the reduction of organizations' data breaches, leading researchers to conclude that various levels of educational factors are effective in implementing appropriate controls to address data breaches. A quantitative correlational study was used to determine the relationship between data security breaches and ISMs' levels of educational factors (level of completed formal education, number of professional certifications, number of training programs, and years of work experience) to provide quantifiable data on data security breaches. Data analysis revealed a significant, positive correlational relationship between the reduction of organizations' data breaches (dependent variable) and each of the four independent variables (levels of formal education, completed data security certifications, on-the-job training, and hands-on experience).

Example Security Injections for Hardware Courses

Chenyang (Nick) Li, Sohum Sohoni, John Acken

This paper gives examples of security injections in computer engineering courses, including courses on hardware design. More broadly, the paper aims to show how knowledge of hardware and software implementations relate to security exploits is important for students who design computer hardware, and how knowledge of the hardware and architectural features is important for those who focus on computer security. The paper provides examples to illustrate the impact of the knowledge of underlying architectural optimizations and hardware limitations on security features and exploits. Examples of educational tools and methods for integrating security education in context in the computer engineering curriculum are also described.

Faculty and Staff Information Security Awareness and Behaviors

Johnathan M. Yerby, Kevin S. Floyd

The purpose of this study was to determine the information security awareness and behaviors that faculty and staff report. A sample of 321 participants consisting of 164 faculty and 157 staff members from a public, state university located in the Southeastern United. The results indicate that overall, faculty and staff have high to moderate levels of information security awareness and behaviors. An independent samples t-test found that there was no significant difference in security awareness, but there were four behaviors differences between faculty and staff. Participants that reported higher levels of security policy awareness demonstrated significantly more secure behaviors in ten of the 18 items measured. Given these findings, comprehensive security awareness training will be essential for institutions of higher education as a means of minimizing threats to information technology resources.

IoTCP: A Novel Trusted Computing Protocol for IoT

Paul Wang, Amjad Ali, Ujjwal Guin, Anthony Skjellum

The ability to understand, predict, secure and exploit the vast array of heterogeneous network of things is phenomenal. With the ever-increasing threats to cyber physical systems and Internet of Things, security on those networks of data-gathering sensors and systems has become a unique challenge to industries as well as to military in the battlefield. To address those problems, we propose a trusted computing protocol that employs discrete Trusted Platform Modules and Hardware Security Modules for key management, a blockchain-based package verification algorithm for over-the-air security, and a secure authentication mechanism for data communication. The IoT-based Trusted Computing Protocol implements integrated hardware security, strong cryptographic hash functions, and peer-based blockchain trust management. We have tested the protocol under various circumstances where devices have built-in securities while others do not. We apply the new protocol to a SCADA system that contains more than 3,000 edge devices. The preliminary results show that proposed protocol establishes trust, improves security, integrity, and privacy.

Modules for Teaching Secure in Android Application Development

Christopher C. Doss, Xiaohong Yuan, Varshar Chennakeshva, Aakiel Abernath, Kenneth Ford

The rise of mobile computing devices has resulted in an increased emphasis on mobile application development courses within computing curricula. While there are many available teaching modules for app development, there is a dearth of materials that incorporate secure software development for mobile devices. The goal of this project is to develop teaching modules that highlight the need for security in app development. These modules are based on CERT Java secure coding rules applicable to developing Android applications published by the Software Engineering Institute at Carnegie Melon University. This paper describes the modules we developed / are developing. These modules are further development and extension of a set of hands-on labs developed and assessed in two courses in the Spring 2017 semester. The assessment results is also discussed. These modules can be adopted by instructors of Android application development.

NICERC's Cyber Interstate: The Next Generation of Cyber Worker can be Found at the Intersection for Classroom Content and Teacher Support

Chuck Gardner

Since 2012, the National Integrated Cyber Education Research Center has existed with the express goal of supporting local workforce development in the areas of STEM, cyber, and computer science. In that time, a variety of subject matter experts have contributed to writing content that is now in use by more than 8,000 teachers across the country. In addition to providing that content to United States public school teachers at no cost, the organization and subject matter experts also provide free professional development to ensure that teachers are as prepared as possible when they present this content in their classrooms. Lastly, the organization also provides opportunities for extracurricular engagement by students outside of the traditional classroom model. Content for events such as robotics competitions, science fairs, and maker spaces are also provided by the organization. This paper will investigate a variety of research studies that support the organization's mission as well as particular studies that identify the organization's offerings as a critical need to education in the 21st century.

Quantum Key Exchange Simulator

Michael McGregor

Quantum cryptography and key exchange is an important and challenging topic for cybersecurity and information assurance students, and one that is difficult to teach without an appropriate demonstration platform. In this paper, we describe the background of quantum key exchange (QKE) theory, modern implementations of QKE, and the role it plays in classical, symmetric key cryptography. We present a QKE simulator that can be used by educators to aid in the teaching of quantum key exchange concepts and processes. The simulator provides a hands-on learning mechanism with which the participants interact. It is designed to be engaging and practical for students to use by supporting the ability to walk through phases of quantum key exchange, pausing at each step, to facilitate discussion and comprehension of this complex security topic.

QUSAIM: A Multi-dimensional Quantum Cryptography Game for Cyber Security

Abhishek Parakh

Discovering and predicting a gamer's behavior and adapting the game environment to improve the learning is a challenging task in any game-based learning environment. QuaSim is a gamified intelligent tutoring system (ITS) developed to teach quantum cryptography. In QuaSim, students solve problems related to quantum cryptography through different lessons/game plans. In this paper, we provide an overview of QuaSim, and our approach to analyzing students' performance and gameplay behavior based on activity sequence modelling and clustering. We present the results of our analysis and identify different student groups having distinct gaming patterns and problem-solving behaviors. Finally, we discuss the pre- and post-game survey results.

Unplugged Robotics as a Platform for Cybersecurity Education in the Elementary Classroom

Keith Rand, Shamik Sengupta, David Feil-Seifer

Robotics may be an ideal way to teach cybersecurity concepts to young students in the elementary classroom. Research shows robots can be an engaging experience and benefit learning in ways useful in other areas of education. Programming robots provides an ideal context for compelling demonstrations of cybersecurity concepts.

Unplugged robotics activities benefit from the engaging aspect of robots but have the added advantage of bypassing hardware and making some concepts more transparent. Señor Robot is a gamified unplugged robotics activity modeled after some activities used before but specifically designed for cybersecurity education in the context of mathematics. The design and implementation of Señor Robot in a third-grade classroom is discussed along with observations and results of student assessments. Strengths and weaknesses of Señor Robot are examined and guide a proposed revision of the game called Frogbotics. An expanded instruction set and applicability to English language arts are considered along with ways to use Frogbotics to teach specific topics in cybersecurity. A website is provided as a dissemination point for materials developed in the study.

Presentations

A Bluetooth LE Security Investigation

Gabriel Bello, Yesem Kurt Peker

Bluetooth LE (Low Energy), otherwise known as Bluetooth Smart, has seen widespread adoption in various technological fields since its release in 2010. From smart watches to heart rate sensors, Bluetooth LE serves as a communication vector with a low energy consumption cost. With millions of devices implementing this particular brand of Bluetooth technology transmitting various types of data, questions of its security arise. In this paper, we analyze the architecture and security features available to Bluetooth LE developers and observe the network traffic of LE devices to analyze their security features. Upon investigation, we find drastically differing results, as one manufacturer provides security mechanisms and other developers provide none. The severe lack of security has implications for users; device tracking is trivial without proper address security and data interception is elementary, making user privacy nonexistent. These security features, or lack thereof, are present in widely available commercial devices that transmit personal information, such as heart rate, geolocation, or even keyboard strokes. We discuss the impact on users that a security-absent manufacturing practice has. As the technology stands, Bluetooth Low Energy (LE) severely falters with regards to security in commercial implementations, and private user data is at risk.

A GenCyber Camp Case-Study: Teaching Defensive Programming at the Pre-University Level Using A Novel Data-Tampering Theme

Ankur Chattopadhyay, Elizabeth Quigley, Sallie Petty

The current IEEE/ACM curricular recommendations and the latest CSEC2017 cybersecurity curriculum guidelines advocate for the inclusion of software security related topics within the present computing disciplinary knowledge-areas. Recent statistics estimate that 90% of reported security incidents result from exploits against defects in the code-design of commonly used software. With the rising demand for cybersecurity workforce, as we look to prepare our youth in cybersecurity, a lack of basic-awareness and understanding of software security may expose our young generation to cyber attacks. For this matter, it is important to teach software security related topics to pre-university learners at an early age. However, even though there are several software security based curriculum development initiatives at the university level, there are limited pre-university focused initiatives in this context, and none of them focus on the theme of data tampering in parameter passing. Therefore, in order to bolster the ongoing efforts in K-12 towards building hands-on software security learning modules and to introduce the topic of parameter-passing based data-tampering, we have designed a unique lesson-plan on defensive-programming for educating pre-university students about relevant secure-coding topics, like parameter passing, function vulnerabilities, buffer-misbehavior, integer error and buffer overflow. This paper describes our creative pre-university educational module on software security, which has been successfully used to conduct several hands-on workshop sessions with middle school students (grades 6-9) as part of our NSA/NSF GenCyber camp-program. Our paper also presents the survey-data collected from the workshop-participants for gauging their interests in the covered topics as well as the overall impact of the lesson-plan leading to new knowledge insights and improved awareness levels, in an effort to evaluate our nifty experiential learning module as a potential outreach vehicle for engaging pre-university students.

Cybersecurity is like Medicine, Users are Patients, Let's Communicate That Way

Seth Martin, Lt. Col. Mark Reith

The fields of cybersecurity and medicine share a common challenge of experts guiding laymen into making good risk management decisions as they daily operate a system that they cannot possibly understand the full complexity of. Since the late 1960s, medicine has thoroughly researched the best methods for communicating with patients such that they are more likely to comply with the advice of medical experts. Compliance comes from trust, which is built on a foundation of competence and caring. Cybersecurity experts can utilize the same formula to engender the trust of their users, leading to superior outcomes in compliance with network policies to achieve the goal of robust cybersecurity defense.

Discovering Patterns and Sentiments about Hacking from Tweets

Azene Zenebe, Jessica C. Alcindor

As different events occur, people use social media to express their opinions about events, products and issues. It is useful to gage awareness and watchfulness of users on cyber security. This paper used analytics using twitter data as the main source and IBM's Watson Analytics software – an advanced cognitive and analytic solution, to identify different insights including trends and sentiments on the hacking subject. The tweets in English with the timeframe from May 2015 to June 2017 were selected. Twenty-five thousands (25,000) tweets that have #hacking were retrieved, relevant data were extracted and analyzed. We identified an increasing trend on the public interest on Hacking as well as more positive than negative sentiments about hacking. The results of this study encourage cyber security professionals and others to utilize big data that exist in social media such as Twitter and Facebook, and advanced analytics software to understand user awareness and discover actionable information for decision-making. Future research will focus on both topic modeling, and correlation and regression analysis among the discovered insights, actual threats and hacking incidents.

Evaluating Prevalence, Perceptions, and Effectiveness of Cyber Security and Privacy Education, Training and Awareness Programs

Marc Dupuis

Cyber security and privacy issues continue to mount, particularly for non-experts. Many different attempts have been made to address the lack of knowledge, skills, and abilities in this arena. This has largely been the catalyst for several different types of cyber security and privacy education, training, and awareness programs. We discuss these various programs, followed by a discussion on a large-scale survey that was conducted to learn more about the perceived effectiveness of these programs and how enjoyable they were to participants. We also compare the type of programs one has engaged in with their score on a cyber security and privacy knowledge quiz. Most of the programs examined in the survey did show a correlation with the results obtained on the knowledge quiz. A discussion with some recommendations follows.

Implementing Lightweight Intrusion Detection Systems Based on Network Function Virtualization

Young Park, Nikhil Vijayakumar Kengalahalli, Suhas Janardhan

The advent of Network Function Virtualization (NFV) has provided high scalability and flexibility in developing intrusion detection systems while replacing the deployment of hardware middleboxes with software-

based network appliances. This paper introduces a method of implementing intrusion detection systems (IDS) based on the concept of NFV by using ClickOS, an open source NFV project. According to, NFV enables students to develop intrusion detection systems to detect various network attack types utilizing very few computing resources. The survey results showed that students can easily understand the specific attacks and implement their own small IDS based on ClickOS.

Inter-Disciplinary Capacity Building in Cybersecurity

Shamik Sengupta, William Doherty

Recent literature recognizes that cybersecurity education should include skills outside of the traditional computing space to best prepare the workforce for current and future challenges. To address this need, a team from the University of Nevada, Reno and Truckee Meadows Community College created and pilot tested libraries of interdisciplinary modules that integrate cybersecurity concepts from Information System, Justice, Political Science and Computer Science. The modules are designed to be integrated into existing courses in any related discipline. Quantitative and qualitative data was gathered from each participating course to evaluate the effect of the module on student awareness and knowledge of the related cybersecurity topic.

LVA: A Network Monitoring and Visualization System for Cyber Defense Competitions

Claude Turner, Rolston Jeremiah, Dwight Richards, Jie Yan

This work presents the network monitoring and visualization application, LUCID Network Monitoring and Visualization Application (LVA); a Node.js app that uses D3 for dynamic generation of graphical units. The system is targeted to intermediary or expert spectators at cyber defense competitions. It leverages several open source components for collecting and processing network data. Results are then sent to a visualization component for interpretation by a scoring algorithm and presentation methods. The LVA consists of several sub-systems, including its core visualization component and the following external components: Node.js, Linux Auditd kernel facility, Redis server, MySQL server, Syslog-ng, Nagios network monitor and Snort intrusion detection system. Blue teams in the competition network are monitored by Auditd, Snort, and Nagios (monitors). Syslog-ng clients on the blue team machines or on machines in the administrative domain watch log files generated by the respective monitors for events of interest. These events of interest are then sent to a centralized syslog-ng server. The syslog-ng server in turn sends the data to a Redis server, also running in the administrative domain. Redis is an in-memory database utilized by LVA to listen for messages submitted to channels marked by keys. Received messages are then transmitted to clients over a web-socket connection. Specifically, they are sent to the core LVA visualization app, which processes each message, scores it, and displays it appropriately in a browser in format that depends on its source or data type.

Power and Responsibility in CS

Jane Heather Blanken-Webb, Nicholas C. Burbules, R. H. Campbell, Imani Palmer, Masooda N. Bashir

Cybersecurity education cultivates powerful capabilities in students. Prepared with knowledge of networking, cryptography, reverse engineering, penetration testing, and, most importantly of all - a security mindset, cybersecurity education equips students with the ability to take profound action in the world. Along with technological expertise, cybersecurity education needs to cultivate and develop wide-ranging capacities, skills, and dispositions that will prepare students to address ethical and technological conundrums that stand to shape the

future of society. We maintain that the immense reach of cyber, cyber-physical, and cyber-social systems now requires cybersecurity education to develop its own distinct focus on ethics.

Preserving Cell Phone Privacy

William Butler

Operators of international mobile subscriber identity (IMSI) catcher technology are compromising consumer cellphone privacy within the United States. These compromises of consumer cellphone privacy are illegal intercepts and man-in-the-middle attacks. Despite efforts by organizations concerned with privacy, such as the American Civil Liberties Union, to inform the U.S. Congress and the public of the threat, no significant legislation has resulted to protect consumers from direct network interceptions and attacks. Scientists and software and hardware vendors are developing countermeasures; however, these measures have not been categorized within an accepted framework such as the National Institute of Standards and Technology Risk Management Framework for consumers to evaluate these countermeasures against the three pillars of cybersecurity, namely, confidentiality, integrity, and availability. Five themes emerged from the results of this study identifying issues focused on consumers, hardware and software providers, network providers and standards making bodies. Based on these themes recommendations are presented for adoption to begin to address IMSI catcher issue.

RESCUE: A Cloud-based System for Cybersecurity Ed & Training

Anyi Liu, Dong Han, Huirong Fu

With the proliferation of the technology of virtualization, Software-Defined Network (SDN) and Network Function Virtualization (NFV), cloud computing has become a vital building block of the high-performance and low-cost computing paradigm serving for various educational purposes. In this paper, we first describe a free framework, namely ReScuE (Range for Security Education), which is a cloud-based networked virtual environment dedicated for cybersecurity education. We leverage the state-of-the-art technologies of SDN and NFV and elaborate the solutions to tackle the technical challenges of deploying ReScuE upon the underlying cloud infrastructure. Then, we present a set of hands-on labs that teach the students how to perform offensive, defensive, and forensic analysis tasks with the techniques and tools on the top of ReScuE. Finally, we tested both ReScuE and the hands-on labs with two groups of undergraduate students. Through the post-lab assessment and feedbacks, we gain some insights of how to effectively promote the wide adoption of the cybersecurity-related hands-on labs to the undergraduate and graduate-level courses at different educational institutions (e.g., community colleges, 4-years universities, and post-graduate schools).

Teaching Cyber Security Concept though IOT application based on Raspberry Pi

Ravi Rao

Currently, we are witnessing a massive increase in internet-of-things applications, which involves low-cost devices connected to the internet. This has been accompanied by an increase in cybersecurity breaches. Consequently, it has become important to teach students both about the internet-of-things applications, and their accompanying cybersecurity risks. This poses a dual challenge of creating the necessary course materials in each area, and teaching them concurrently in a single course.

In the current paper, we discuss the introduction of cybersecurity concepts in an embedded systems course. We present our experience with the students who were taught this material during the Fall 2017 semester at Fairleigh Dickinson University. Though some of the basic

concepts can be taught in one course, the learning curve is quite steep. The students were taught Python programming, the Linux environment, embedded systems programming and computer networking concepts within a single course. They were able to successfully complete a lab devoted to filtering internet traffic through the use of firewalls.

The course material we are developing could serve as a model for other institutions at the graduate and undergraduate levels. Other instructors and course developers could likely benefit from our experience.

The Cyber Cube: A Multifaceted Approach for a Living Cybersecurity Curriculum Library

Blair Taylor, Siddharth Kaza, Melissa Dark, Steven LaFountain

The global cybersecurity crisis has forced academic institutions to build and grow cybersecurity programs. Regardless of the discipline, in order to build an academic program, institutions need trained faculty / teachers, curriculum, infrastructure and administrative support. The current state of cybersecurity education is faced with three intersectional challenges: 1) a dire shortage of faculty / teachers, 2) a rapidly evolving field, and 3) the lack of quality curricular materials and infrastructure to rapidly deploy up-to-date cybersecurity programs. Given the interconnected nature of these challenges, this paper focuses on the need for a living digital library, surveys current cybersecurity repositories, and discusses factors that determine the success of a digital library. We introduce the "The Cyber Cube", a multifaceted solution that includes various lenses for accessing a living library of cybersecurity curriculum. The Cyber Cube requires an engaged community of educators, and we focus the discussion on a few questions – What are the challenges in developing a digital library? If we build it, will they come? How can we leverage existing cybersecurity resources, ranges, and libraries? How can the cyber community help to sustain and maintain at the 'speed of relevance'?

The Evolution of Cybersecurity Education in Four-Year Undergraduate Programs

Allen Parrish, Rajendra Raj, Edward Sobiesk, Andrew Hall, J.J. Ekstrom, Shannon Gorman

To meet enormous workforce demand, cybersecurity is being rapidly integrated into undergraduate computing curricula in baccalaureate programs across the world. Two central methods are currently being employed to accomplish this in computing-based programs. Many institutions are integrating significant cybersecurity concepts and principles into existing programs in the traditional computing disciplines ("integration method"). Other institutions are creating standalone programs in cybersecurity ("standalone method"). These two primary methods are simultaneously both converging and, in some respects, diverging, based both on program choices and on the needs of the various constituents the programs support. Both the "integration method" and the "standalone method" are supported by ACM/IEEE-CS curriculum recommendations, institutional designations such as NSA/DHS's National Centers of Academic Excellence, and ABET accreditation of cybersecurity degree programs. This paper discusses the existing and potential impacts of such curriculum recommendations, designations and accreditations on baccalaureate cybersecurity education.

Lightning Talks

A Gaming Platform for Cyber Security Education

Dipankar Dasgupta, Thomas L. Pigg

Traditional method of cyber-security education and training are not adequate for preparing students to defend against advanced cyber threats, spear phishing, targeted malware and zero day attacks. Education methods need to prepare a person to apprehend his / her knowledge, build analytical skills and thinking ability to defend the sophisticated attacks. This paper highlights an interactive game to teach cryptography concepts and approaches through a gaming platform. In particular, a multi-level game is developed using Unreal Engine for teaching cryptography (encryption / decryption exercises). This NSF-ATE funded project, called puzzle-based learning (PBL) is able to effectively integrate with instructional content and become highly successful for basic cyber-security education.

A Proposed Model to Unify Cybersecurity Frameworks and Certification Programs using NICE Framework Structure

Justin Smith, Kevin Kim, Dan Kim

Currently, the cybersecurity industry is seeing a boom workforce participation due to the growing popularity of its services in both commercial and government organizations. Therefore, there is a desire by industry clients and participants alike. This paper will outline the relationships between existing workforce frameworks and propose a single comprehensive and unified model for career progression using the NICE KSA structure.

Anatomy of Attack

Mangaya Sivagnanam

Today the cyber attacks are not only frequent but also innovative and creative. This presentation provides an overview of frequent and straightforward Level 1 and 2 IoT attack vectors that challenge most organizations, equipped with Building Internet of Things (BIoT). The Anatomy helps businesses to defend against all IoT attacks proactively. It provides a detailed anatomy of each attack and analysis of the attack approaches used by adversaries. It then discusses the required security controls needed to defend against each type of attack.

Augmented Reality Mobile Forensic Laboratory (AMFL)

Nikitha Reddy, Faisal Kaleem

In this paper, we describe ongoing research which explores the potential of augmented reality technology-based teaching and learning approach to enhance cybersecurity and forensics education. Augmented Reality (AR) superimposes digital information directly in front of a user's field of vision to supplement real world experiences with enriching content. We have developed an interactive windows Augmented Reality application for Microsoft which is aimed to enhance students' learning and understanding of cybersecurity concepts. Our work focuses on the capacity of the unique features of augmented reality via smart glasses to provide meaningful hands-on learning experiences. The application augments the step-by-step process of performing the lab along with some 2D images and videos to assist students in completing their lab successfully with minimal or no help from the instructor. Augmented reality techniques allow students to experience sensations and explore learning experiences that, in some cases, may exceed those offered by traditional laboratory classes.

Big Data Technology for Cybersecurity Lab Design

Alex Rudniy

Designed to address persistent cyberthreats, the Cybersecurity National Action Plan called for innovative learning experiences among other measures. Current work extends the ongoing trend of designing courses in cybersecurity and big data by bridging these two domains and utilizing Apache Metron, a recent community-developed open-source project.

This work illustrates application of big data software systems for distributed scalable computing in several settings pursuing design and subsequent distribution of lab exercises aim in the development of data analysis skills for tracing attacks and forensics. The discussion begins with an overview of the background, introduces several established objectives, reports on used methods and technologies, and achieved results, and discusses solved problems and relevant matters as well as the directions for future work.

Challenge-Based Education: Bringing Cybersecurity to K-12

Joe Chase, Premchand Uppuluri

Given the pressing demand for a cybersecurity workforce, the goal is to increase the pipeline of high school students who plan to pursue Computer Science / IT as a major with cybersecurity as their focus. We identified a variety of challenges to the introduction of cybersecurity topics in high school including lack of qualified teachers, limited number of students motivated to study IT topics, large number of prerequisite topics and scarcity of computing resources required for such topics. In response to these challenges, with support from four NSA grants, we developed a strategy that is exciting, rigorous and easy to adapt for high school students. This strategy employs active learning in the form of capture-the-flag (CTF) contests to drive learning within a short time span. Teams of three to five students work on security challenges while competing with teams from around the state and region. Foundational knowledge is introduced on a just-in-time basis. The contest is designed to be a bridge between basic cyber-awareness and the rigorous multi-semester courses. This paper describes these contests and their effectiveness.

Chief Information Security Officers (CISOs) as Endangered Species: Is the CISO high turnover problem a Mirage?

Frank Lin, Conrad Shayo

CISOs average job tenure is about 18 months in the USA. Although we know that such high turnover is a problem, it keeps happening. The impact of such turnovers has not been ascertained. The purpose of this panel is to explore the cost of CISO turnovers and strategies that may be used to increase their tenure. Many studies have found that retention of IT employees is important because when they leave their jobs, they leave with priceless and difficult to replace organizational knowledge, skills, and abilities (Wang & Kaarst-Brown 2014; Tnay, Othman, Siong, & Lim, 2013). Besides, it takes money and time to train a replacement CISO, who is most likely going to leave in a few months. The exploration of the CISO turnover problem will focus on the following: What is the organizational cost of replacing a CISO? Why are fired CISOs getting hired immediately? Why do some CISOs decide to run to the hills after a short tenure? What strategies can organization leaders use to retain their CISOs? Which strategies are working and which are not, and why? (Lee, C. Lee, C.C. & Kimb, S. 2016; Waldman, Carter & Hom, 2015). We hope this discussion panel will contribute to our understanding of the forces and determinants of CISO turnover and retention. Moreover, we intend to gather some survey data to continue with this line of research.

Cloud-based Environments for Cybersecurity Education

David Raymond, Sandra Schiavo

The supply of qualified cybersecurity professionals has not kept pace with increased demand in government and industry. To address this shortfall, Virginia and other states have worked to increase educational opportunities in cybersecurity, requiring a corresponding increase in infrastructure for hands-on student experiences. The Virginia Cyber Range was established to meet this demand. It is a scalable, public-cloud based cyber range environment that makes resources available to students in high schools and colleges across the state through a web portal without the need for special software or changes to their schools' network configurations. Students and faculty log in to the Virginia Cyber Range and are exposed to features based on their roles; teachers are presented with tools to enroll students in their courses and provision virtual environments for cybersecurity labs and exercises, while students log in to access environments provisioned by their instructors. We believe that we are the first to create a general-purpose cyber range platform based on public cloud technologies.

Creating an Anchor Hands-on Cyber Sec Course using Raspberry Pi

Ravi Rao

Given the increasing rate and sophistication of cyberattacks, there is an urgent need to train and expand the workforce in the area of cybersecurity. It is important to consider and create innovative approaches to increase the recruitment and retention of students that pursue cybersecurity concentrations. Our approach not only addresses cybersecurity needs but also the needs of other STEM disciplines such as different fields of engineering where it is challenging to recruit and engage students. We propose the creation of an anchor course, called the Core Hands-on Raspberry Pi Based Lab that is designed to satisfy multiple objectives including cybersecurity needs as well as basic engineering needs such as understanding sensing and control. By introducing this hands-on lab in the first semester of a multi-year program, we expect significant improvement in student interest, engagement and retention. We illustrate the flexibility of our approach by mapping proposed lab exercises to existing CAE knowledge units. We highlight our solution through a lab exercise dedicated to creating, displaying and interpreting the role of random numbers in both cybersecurity applications and general applications in multiple branches of engineering.

Cyber Criminology, Criminology and Cyber-crime Towards an Academic Discipline

Greg Laidlaw, Charles Wilson

Cybercrime is a growing global phenomenon that has created a significant paradigm shift in critical areas of the personal life of citizens, and in both the public and private sectors. The negative impact of cybercrime is felt in many diverse areas, such as politics, economics, national security, public safety, and in many critical societal activities related to quality of life. Today, essential online functions are constantly under attack by a growing cadre of sophisticated cybercriminals, organized crime organizations, and nation-state actors. The purpose of this paper is to synthesize current research literature on cybercrime to highlight the scope of the problem; and to suggest a notional concept of criminological theories that can be applied to enhance cybercrime investigation and enforcement efforts. Additionally, the paper proposes the establishment of an academic minor "Cyber criminology" based on an interdisciplinary approach.

Cyber Education Outside the Cyberspace

Ngatchu Damen, Leonnel Kwedeu, Divine Anye

The purpose of this paper is to extend the growing body of research on cyber education, by reporting the experiences of a cyber security department cut-off from Internet access. The value of Cyber education is expressed even beyond the cyberspace.

Designing and Delivering a Cybersecurity Curriculum for Middle Schools

Yesem Kurt Peker, Hillary Fleenor

The need for highly trained computing professionals continues to grow in our nation and throughout the world. Research has shown that more and more of these technology positions require a level of skill that cannot be accomplished in a university program without prior computing experience. This is also true for cybersecurity, one of the most in-demand fields today. Primary and secondary schools are essential for exposing students to computing and security topics at earlier ages in order to achieve levels of expertise needed by industry, government, and other organizations. It is also essential to attract a more diverse student body into the field. In this work, the authors develop a middle school cybersecurity curriculum to achieve two goals: 1) increase student knowledge in cybersecurity topics and 2) increase student interest in cybersecurity in general as well as a possible career path. The team consists of a tenure track assistant professor in computer science with a background in cybersecurity and an expertise in cryptography; a lecturer/outreach coordinator with a master's in computer science, a master's in education, and previous experience teaching middle school; and a current middle school teacher certified in business education. In the current (2017-2018) school year the team members have been collaborating to deliver the cybersecurity curriculum in two grade 8 classes, a total of 60 students, in a Title I middle school in the U.S. Almost all students in the two classes are African American and more than 50% are female. The curriculum includes standards, objectives, and lessons for implementation within a year-long business and computer science course. The project also includes a pre and post-test to assess the first goal of increasing student knowledge in cybersecurity topics and a pre-and post-survey to assess the second goal of gauging students' interest in cybersecurity in general and as a discipline. In this presentation we share our curriculum and resources as well as challenges we have encountered as we deliver the curriculum. Due to some scheduling constraints we have already administered the post-test for assessing the knowledge gain. We are happy to share that, despite the challenges, a preliminary analysis of students' pre- and post-test scores indicate a significant increase in their knowledge of cybersecurity.

Diffusion Metrics of the AES Symmetric Cryptosystem

Abdinur Ali, Yen-Hung Hu, Cheryl Hinds, Jonathan Graham

Compared to other selected block modes with other padding methods. In this paper we study the diffusion of the AES block modes. When the plaintext is encrypted, the diffusion obscures the redundant arrangements. Therefore, those repeated configurations can be hidden in the cipher text. In this paper we have compared four AES block modes with three key sizes and with five padding modes. First, the original plaintext was modified by changing a random letter in the plain text. Then, in order to study the diffusion metrics of the modification, the percentage of the match between the plain text and the cipher text was calculated. Based on these simulation metrics, the results indicate that CBC block mode with padding ANIS X.923 mode has more diffusion.

Guiding Healthcare Adoption Implementation via the Consolidated Framework Approach

Subrata Acharya

Implementation science continues to emerge as a valuable tool for providing benchmarks and metrics for the successful deployment of healthcare technology adoption. The following paper presents the results of a tool-based evaluation administered to key stakeholders of a large-scale hospital information system. The survey utilized constructs from the standard Consolidated Framework for Implementation Research to assess potential barriers to implementation of a technology adoption in a large clinical health care setting and provide feedback to stakeholders on areas of intervention to mitigate potential barriers and support successful health information system implementation. The designed survey instrument and research method presented in this study could be easily administered in any given distributed information system.

Identity Theft Education: Engaging Students in the Age of Cybercrime

Susan Helser

The tidal wave of financial losses due to identity theft is staggering. The fraud impacts individuals and businesses. Critical resources are lost. Higher costs result across all sectors of industry and are passed on, in turn, to the consumer. Hardware and software strategies to combat identity theft have experienced some success. In spite of technical attempts to mitigate the crime, hundreds of millions of people's identities have been stolen. Equifax and Facebook represent two recent examples where individuals' personal identity information (PII) was compromised. The problem is particularly severe in the United States. In addition to technical advances, behavioral changes are needed to address identity theft. Heightened awareness and informed choices can make a difference. The focus of this paper is to discuss methods to integrate identity theft education into the curriculum at the post-secondary level across disciplines. Current statistics provide cause for alarm. Multi-modal techniques to engage students' investigation, comprehension and discussion of identity theft and related cybercrime topics are considered. For example, several minutes of in-class discussion at the beginning of the period of "cyber current events" sets the tone and reinforces the importance of the work at hand. In addition, weekly blog posts that examine cyber activity that require reading and analysis of peer-reviewed articles as well as the assessment of classmates' posts generate dialogue and significant consideration.

New Approaches to Cyber Security Education (NACE)

Debasis Bhattacharya

Cybersecurity has become a prevalent topic in many colleges, but how it should fit into the overall educational process is still not fully understood. A cybersecurity project at the University of Hawaii Maui College (UHMC), funded by the NSF SFS and ATE program, spans multiple disciplines and targets women and minorities.

Professionalization of Cyber Security Education Experience: Creating a Dynamic Highly Nimble Cyber Workforce

Steven Fulton

In order to provide our students needed experience and knowledge in cyber security, the educational curriculum must be updated. Graduates must come into the workforce prepared to defend computer systems and networks in business and government. The support of the colleges and universities is required if they wish to produce graduates that can enter the workforce well trained. Incorporating lab exercises and competitions into

the computer science curriculum alone are not enough. Academic institutions must be willing to provide real world experience to their graduates.

The authors are proposing that cyber based degrees at the Masters level and potentially an aggressive undergraduate program should incorporate a program similar in nature in what doctors and lawyers complete prior to their beginning their practices. The real world experience and mentoring gained by each student will help pave the way for preparing graduates to provide immediate assistance to the businesses or organization that hires them.

Programming Projects for Undergraduate Information Security Education

Mohamed Said Aboutabl

Incorporating security mechanisms at the foundation of contemporary software systems has become mandatory for many applications. Universities must empower graduating software engineers with the necessary system / network security education and programming skills that various software developing houses expect. In this paper, I discuss the design and implementation of a set of pedagogical programming projects that supplement an undergraduate semester-long introductory course on information security, which I helped design at my institution. These projects introduce the students to the use of security software libraries in order to implement a diverse array of security mechanisms such as encryption, key exchange, and message authentication / integrity checking. These projects gradually increase in complexity as the semester progresses, and provide an opportunity for follow-up capstone projects suitable for honor classes and/or independent studies.

Security Lessons From Building A Back-end Service for Real-Time Data Collection

Halmon Lui

According to the 2018 Symantec Internet Security Threat Report, malware implants grew by 200% and Internet of Things (IoT) attacks grew by 600%. The Edgescan 2018 report found that 20% of all vulnerabilities discovered were either high or critical risk. Enforcing proper preventatives and security assessments can help mitigate those risks. In this paper, we present our security experiences of designing a back-end service for a web application, which was motivated and designed to support real-time data collection for a statistics class in higher education. Our findings are organized into three categories: system software, connection forwarding, and data storage. These categories are main components of the web application and most likely to be targeted by an attacker. These are the main components of the web application and the most likely to be targeted by an attacker. There are three contributions in this paper: (1) The demonstration of building a secure and light-weight back-end service with Node.js, Nginx, and MongoDB, (2) The discussion on the vulnerabilities of a web application from a back-end service perspective, and (3) An explanation of our security measurement to mitigate or prevent attacks on those vulnerabilities. The current findings are promising and we believe they are worth further exploration to help back-end developers create an efficient and secure web service.

The REACH Model: Reinforcing Student Learning Through Abstraction and Distraction

Henry Collier

Some educators believe it was easier to teach students before the Internet because today, students cannot pay attention to anything longer than a 140-character Tweet. In some respects, this is possibly true, but in others, this belief is certainly false. A student's failure to learn has more to do with how they were taught to learn, than their capacity to learn or how distracted they are.

The No Child Left Behind Act tied federal funding to Adequate Yearly Progress in test scores [1]. The result on the surface was that K-12 teachers were put in a position where they needed their students to do well on the tests, otherwise they risked losing funding for their school and in many cases their own jobs. The pressure applied by the No Child Left Behind Act has led to teachers teaching for the tests, rather than teaching for the student's ability to learn / ability to teach themselves and discover their own learning methods.

The Security Risk and Protection on Social Media

Abidemi Lawal, Vinitha Subburaj, Daniel Thomas Loughran, Mayar Kefah Salih

Over the last two decades, there has been a great evolvement and growth in technology. With this emergence comes the knowledge of Social Media. Social media is the new "weapon" in this age. It has been a very helpful and profitable resource as it has brought a lot of advancement in both the IT and business world. Every institution has had an add-on benefits in their productivity since the emergence of social media. Relationships have been built and developed across the world due to social media. Everyone, both young and old, rich or poor, has an interest in social networking. It has improved the way of life of the people. However, despite the merits that the social media has brought to this age, there are a few threats that comes with it. It will be illogical to neglect the risk associated with it. Hence, this research is going to focus on the security risk of social media. The author will focus on the different security threats of the social media and how these threats can be curbed or reduced.

We Are Fighting A Cyber War Right Now

Humayun Zafar

There is no denying it, we are fighting a cyber war right now. The responsibility undoubtedly lies with humans. Cybersecurity experts, such as the FBI and others have confirmed that the biggest weakness in in cybersecurity is human error. IBM in a study revealed that 95% of all security incidents involved some form of human error (e.g. phishing scams, falling victim to advanced persistent threats etc.). Is the issue lack of investment in this arena? Not at all. Firms continue to spend millions on security technologies. The only issue is that all it does is to make an executive feel safe as opposed to being safe. For years people have also been talking about training as the best way of ensuring that human errors are reduced. That's somewhat true. The only issue is that instead of looking at training at a macro level, we have to consider training at a group level. That is essentially why even with an industry that focuses exclusively on cybersecurity training programs, we continue to have higher rates of security breaches due to human error.

We investigated this issue in the healthcare and financial services arenas.