Academic Papers

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

Keith Rand, Shamik Sengupta, David Feil-Seifer

🕓 2:00 PM to 2:35 PM 📍 La Salle A

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.

Cyber Security Education for Liberal Arts Institutions

Xenia Mountrouidou, Xiangyang Li

🕓 2:35 PM to 3:05 PM 📍 La Salle A

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.

Modules for Teaching Secure in Android Application Development

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

🕓 3:05 PM to 3:35 PM 📍 La Salle A

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.

Cybersecurity Education with POGIL: Experiences with Access Control Instruction

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

🕓 3:35 PM to 4:05 PM 📍 La Salle A

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

🕓 4:05 PM to 4:35 PM 📍 La Salle A

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.

Presentations

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

Blair Taylor, Siddharth Kaza, Melissa Dark, Steven LaFountain

2:00 PM to 2:30 PM La Salle B

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'?

Power and Responsibility in CS

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

2:30 PM to 3:00 PM La Salle B

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.

A Bluetooth LE Security Investigation

Gabriel Bello, Yesem Kurt Peker

3:00 PM to 3:30 PM La Salle B

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.

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

Marc Dupuis

🕓 3:30 PM to 4:00 PM 📍 La Salle B

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.

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

Seth Martin, Lt. Col. Mark Reith

🕓 4:00 PM to 4:30 PM 📍 La Salle B

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.

Implementing Lightweight Intrusion Detection Systems Based on Network Function Virtualization

Young Park, Nikhil Vijayakumar Kengalahalli, Suhas Janardhan

🕓 4:30 PM to 5:00 PM 📍 La Salle B

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.

The Evolution of Cybersecurity Education in Four-Year Undergraduate Programs

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

🕔 5:00 PM to 5:30 PM 📍 La Salle B

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

Anatomy of Attack

Mangaya Sivagnanam

🕒 2:00 PM to 2:20 PM 📍 La Salle C

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.

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

Ravi Rao

🕒 2:25 PM to 2:40 PM 📍 La Salle C

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.

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

Steven Fulton

🕒 2:45 PM to 3:00 PM 📍 La Salle C

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.

Challenge-Based Education: Bringing Cybersecurity to K-12

Joe Chase, Premchand Uppuluri

🕒 3:05 PM to 3:20 PM 📍 La Salle C

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.

Identity Theft Education: Engaging Students in the Age of Cybercrime

Susan Helser

🕒 3:25 PM to 3:40 PM 📍 La Salle C

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.

Guiding Healthcare Adoption Implementation via the Consolidated Framework Approach

Subrata Acharya

🕒 3:45 PM to 4:00 PM 📍 La Salle C

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.

The Security Risk and Protection on Social Media

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

4:05 PM to 4:20 PM La Salle C

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.

Big Data Technology for Cybersecurity Lab Design

Alex Rudniy

4:25 PM to 4:40 PM La Salle C

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.

Augmented Reality Mobile Forensic Laboratory (AMFL)

Nikitha Reddy, Faisal Kaleem

4:45 PM to 5:00 PM La Salle C

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.

Programming Projects for Undergraduate Information Security Education

Mohamed Said Aboutabl

🕓 5:05 PM to 5:20 PM 📍 La Salle C

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.

Cloud-based Environments for Cybersecurity Education

David Raymond, Sandra Schiavo

🕓 5:25 PM to 5:40 PM 📍 La Salle C

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.