Women in Cybersecurity Conference

March 27 & 28
Atlanta, GA

2015
27-MAR-15

10:00 - 2:30pm
GRAND Foyer

Registration
Registration will open at 10:00 am

10:30 - 12:30pm
AUGUSTA

Workshops

Discovering Cybersecurity: Jackson State Community College
This workshop is intended to introduce participants to the field of cybersecurity and opportunities within. It will focus on engaging participants in hands on activities so that participants catch a glimpse of typical responsibilities held by a security.

ATLANTA

Introduction to Digital Forensics in the IoT (Internet of Things): TRUST Center, University of California, Berkeley
Digital Forensics has grown in the new millennium to keep pace with technology. Deleted files, deleted emails, instant messaging, encrypted files? How does one deal with this? This introductory hands-on workshop in digital forensics sponsored by the TRUST Center. Participants will learn what can and cannot be retrieved, where to look and be introduced to a popular forensics tool.

BRUNSWICK

Network Packet Analysis: Women’s Society of Cyberjutsu
Wireshark is a very powerful and popular network analyzer for Windows, Mac and Linux. It’s a tool often used by Network/security engineers to troubleshoot network/security problems. In this workshop, we will introduce the tool and the interface, basic usage and file carving. We will conclude with performing forensic analysis of output files from a Wireshark capture. Participants will leave this workshop with a foundation of how to use Wireshark and build upon this skill.

12:30 - 2:00pm
SALONS A-E

Lunch
Welcome: Vahid Motevalli, Associate Dean, College of Engineering, Tennessee Tech University

Keynote: Jenn Lesser Henley, Facebook
What is a Security Engineer? Debunking the Myths: Security of the Internet is paramount. Studies have shown there are 6 reasons why people don’t see cyber security as an appealing job field. Let’s talk about those, address those head on and start taking actions to dispel them.

2:00 - 3:15pm
SALONS A-E

Student Sessions
Student Poster Session

RESUME CLINIC

2:00 - 4:00pm
HARTSFIELD/SOUTHSIDE

Coffee/Drink at Southside

3:15 - 4:00pm
FLORIDA/TENNESSEE

Session I: Distinguished Speakers

Track A
Carrie Gates, Dell

The Detection and Prevention of Insider Threat: This talk will discuss the interesting challenges around insider threat detection, while weaving throughout the talk practical advice about the development of a research program.

Track B
Lorrie Faith Cranor, Carnegie Mellon

Security, Privacy, and Human Behavior: Human factors play an important role in development of secure systems and privacy tools. Speaker will present her research in this area and discuss approaches to educating security and privacy students and professionals about how to make security and privacy tools more usable.
Track C
Roxane Divol, Symantec

Career Path for Women in Cyber Security: Speaker will share her own journey and talk about the critical need for talent that is opening up tremendous opportunity for women in Cyber Security field.

Fairs & Workshop
Career and Graduate School Fair

Faculty Workshop

Using RAVE to Encourage GenCyber Outreach: University of Alaska, Fairbanks and National Security Agency

This workshop will provide participants with hands-on experience using the Remotely Accessible Virtualized Environment (RAVE) for cybersecurity exercises. The RAVE environment is available for faculty around the US to use in their courses at no cost to provide the valuable hands-on experiences associated with cybersecurity without the challenge of building scenarios and support platforms. RAVE has partnered with the federally funded GenCyber Program to provide funding for summer camps for high school students through the GenCyber Program with an emphasis on cybersecurity.

Session II: Technical Presentations by Attendees

Track A
Sakshi Jain, Mobin Javed, Vern Paxson, LinkedIn, UC Berkeley

Automated Discovery of User Trackers: Web tracking is highly prevalent on the web today. Conventional trackers like browser cookies and Flash cookies are widely known to the community, however there is potentially more tracking information being sent to servers around the world unbeknownst to the users and security community at large. This work is motivated by the possibility of discovering previously unrecognized forms of trackers, either potential or actual in an “automated” fashion from raw network traffic. In this work, we built a tool that processes users’ network traces and outputs tracker strings such as usernames, cookies, IMEI numbers and the like, that uniquely identify a machine/device/browser.

Track B
Cheryl Calhoun, Santa Fe College

Developing a Comprehensive Cybersecurity Curriculum in a Collaborative Learning Environment: This talk will present a project whose primary goal is to develop a comprehensive cybersecurity curriculum that would be more inclusive of women and other underrepresented groups. As part of this process we looked at both learning theories and environmental factors that research shows has been effective in providing a learning environment that is more appealing to a diverse group of students. In this presentation we will share how we remodeled our classrooms to create collaborative learning spaces. We will look at how we updated both our online curriculum and our face to face courses to include inquiry based collaborative learning. We will discuss the challenges and success of incorporating a collaborative weekly threaded case study assignment in an online Fundamentals of Information Security course.

Track C
Chris Carlson, IBM

Web Application Security: Getting and Staying Ahead of Hackers: This talk will cover the current state of web application security in the wild and demonstrates some of the most common web hacks that exploit security vulnerabilities. It then presents various security testing options and their advantages and drawbacks - and the reasons why you can’t depend on only last-minute automated security testing to be sure your application is secure. Topics covered include: the taxonomy of hackers, what does site security mean?, an overview of hacker tools, a demonstration of several hacker
techniques, “input validation” is not a magical phrase, security testing approaches, secure development, threat modeling, and more.

6:00 - 7:15pm
SALONS A-E

Dinner
Welcome: Iulia Ion, Google

Keynote: Sherri Ramsay, CyberPoint

Cyber Security—It’s All about the Numbers: From her days as a mathematics teacher, to her technical and leadership roles defending the nation against increasing numbers of cyber threats, to being one of only a few women entering the newly emerging field of cybersecurity. The speaker’s career has been one about numbers. Speaker will be sharing her insights on the challenges facing those embarking on a career in cyber security and her thoughts on the industry’s future.

7:15 - 8:00pm
FLORIDA/TENNESSEE

Session III: Panel Session

Track A
(Moderator) Kathryn Roberson: US Office of Personnel Management (Panelists) Melissa Dark: Purdue University; Danielle Santos: Department of Homeland Security; Michelle Monsees: George Washington University; Gabby Buchanan: Hampton University

Opportunities in Cybersecurity Education – CyberCorps® Scholarship for Service (SFS)
Program: This panel will discuss the CyberCorps® Scholarship for Service program, which provides an opportunity for selected students to excel within the profession by providing tuition funding and stipend at participating SFS institutions in return for government service post-graduation. SFS Scholars, administrators and educators will share their experience.

Track B
(Moderator) William Newhouse: National Institute of Standards & Technology (Panelists) Victor Piotrowski: National Science Foundation; Steven LaFountain: Department of Defense; Claire Vishik: Intel

Opportunities in Funding Cybersecurity Programs: This panel will discuss different funding sources and opportunities in security education and research.

Track C
(Moderator) Micaela Hoskins: Cisco Systems (Panelists) Tolu Onreti, Jay Koehler, Jennie Kam: Cisco Systems

Roles in Cybersecurity Careers: This panel will discuss different roles in security: Breakers, Builders, Defenders, Leaders, and Influencers. Where do you belong? What are the skills required for each role? Can you move between roles?

8:00 - 9:00pm
SALONS A-E

Speed Networking/Mentoring Session
Cold treats

End of Day 1
Breakfast
Welcome: Victor Piotrowski, National Science Foundation
Keynote: Phyllis Schneck, Department of Homeland Security
DHS Cyber Vision: Industry, Technology and Trust: This talk will address the future of DHS cybersecurity in today’s fast-paced and A1:E32 threat environment. Through a combination of vision and the Department’s continuing work with public and private partners, DHS is building a national capacity to support a more secure and resilient cyberspace.

Session IV: 5 Minute Lightning Talks
Karla Burnett, Stripe
Capture the Flag to be a Better Defender: Knowing how an attacker thinks is vital to being a good defender - you need to know what to defend, and how. This talk is about how CTF competitions are an underutilized resource to learn and develop these skills, and why they’re worth doing with practical tips.

Tamara Shoemaker, The Colloquium for Information System Security Education
CISSE Community and Conference: CISSE Colloquium provides a central clearinghouse where ideas about how to develop and communicate the fundamental concepts of Cybersecurity education can take place. Find out how you can be a member of the CISSE community and take part in annual CISSE conference.

Apoorva Phadke, Meera Subbarao, Cigital
The Girl with the Hacker Crew: Ethical hacking for a living is totally cool. Coming up with remediation solutions is even cooler! Find out just how fun it is to be an application security consultant.

Meagan Krumen, Facebook
Cyber Security and Geo-Politics: There are non-technical roles available in the cyber-security field that have great impact. This talk will provide a brief overview of the work tracking geopolitical events and threats.

Kathy Peters, KeyBank
Debrief Grief: Helping Development Teams through the 5 Stages of Coping with Application Security Findings: Find out about the 5 stages of grief that leave developers to feel blind-sided, embarrassed, attacked, or picked on after application testing. Understanding them can put the team on positive track towards remediation of the findings.

Priya Jain, Georgia Institute of Technology
Securing a Cybersecurity Internship: A freshman’s perspective on attaining the elusive Cybersecurity internship. Advice and tips will be offered, geared towards fellow freshmen or those with similar experience levels.

Desiree Reagan, University of Maryland University College
Experimenting with OWASP’s Most Wanted: Based in SQL Injection, an ethical hacking class project experience shared by a graduate student.

Deanne Wesley, Forsyth Technical Community College
Engaging Students in a Computer Forensic Course Utilizing a Mock Crime Scene: Experience of teaching computer forensics to students with mock crime scene to expand their knowledge in investigation techniques.

Kelley Goldblatt, Michigan State Police
Cyber Security and the Law Enforcement Arena: Different components of the law enforcement cyber arena. Areas covered will include the current landscape, training opportunities, skills needed, and
Group Picture Session

Grab and Go Refreshment Break

Session V: With Distinguished Speakers

Track A
Karyn Higa-Smith, Homeland Security Advanced Research Projects Agency

Role of STEM in Cybersecurity and My Journey Within: Science, technology, engineering, and math (STEM) fields play an essential role in advancing cybersecurity: This talk will present the path of an aspiring young women in STEM and her current role and responsibilities as a cybersecurity professional leading research to secure information sharing and protect identities in cyberspace.

Track B
Tracy Camp, Colorado School of Mines

What I know now ... that I wish I knew then: The speaker was utterly shocked she became an ACM Fellow. How was that possible, when one considers all the mistakes she made in her career! In this presentation, she will present what she knows now ... that she wish she knew then.

Track C
Joyce Brocaglia, Alta Associates

Lead Like a Woman: Explore your personal Leadership Journey to becoming a more conscious, confident and authentic leader. Learn how to establish your leadership vision, develop your personal style and the important roles that fear, confidence, optimism and taking action play in your success.

Session VI: Technical Presentations

Track A
Elizabeth Philips, Oxford University

Applying Social Network Analysis to Security: This project explores the many ways in which Social Network Analysis (SNA) can be applied to the field of security, and especially, investigating what interactions could someone (e.g., an attacker) infer if they were able to gather data on a persons friend groups or technology devices (e.g., email interactions) and whether this could be used to predict the hierarchical importance of the individual. In this talk, we report results of our initial investigation on the Enron email dataset and investigated the effectiveness of existing SNA metrics on establishing hierarchy from the social network created from the email communications.

Track B
Tony Coulson, Cal State San Bernardino/Cyberwatch West; Michelle Cantone, Houston Community College

Mentorship: There is immense value in mentorship. Finding a mentor is highly encouraged for all people, regardless of their stage in education or profession. However, finding and establishing a fulfilling and meaningful relationship can seem daunting. This presentation will talk about challenges and suggestions to discovering and nurturing a beneficial partnership. It will also describe and demo the Faculty Mentor program available for free from Cyberwatch West.

Track C
Meera Subbarao, Cigital

Know Your Enemy, and Yourself: Demystifying Threat Modeling: Security professionals have been presenting and publishing on threat modeling for decades. Yet, many managers avoid discussing threat
modeling because they believe it’s expensive, time consuming, and difficult to maintain. During this talk, we’ll attempt to bust these myths and show how organizations can incrementally obtain better results over time while making threat modeling “seem easy.” Threat modeling is in many ways one of the foundational practices of information security. We will demonstrate the process of determining which threats and attacks are relevant for a given application and environment, allowing security professionals to make real risk-based decisions about where to focus on defenses.

**Session VII: BoFs (Birds of a Feather Sessions)**

**Track A**
Amelia Phillips, Debra Mcneil, Jennifer Jovanovich, Kylee Mcdonald, and Katrina Schliebe: Highline College; Laura Wilkinson and Whitney Maxwell: Brigham Young University

**Using Network Penetration Tools Ethically:** This discussion will focus on usage of penetration testing tools for educational purposes: types of tools, their advantages, applicable environment, ethical issues, challenges, and personal stories.

**Track B**
Yesem Kurt-Peker, Aurelia Smith, Columbus State University

**Resources for Teaching Practical Cybersecurity:** This discussion is about freely available resources for teaching cybersecurity related topics to undergraduates with various backgrounds in security. Topics such as how to access these resources, what topics they cover, and what kind of background they require will be covered. We will also share ongoing challenges and experiences with teaching practical security.

**Track C**
Debbie Taylor Moore, Cyber Zephyr

**Bringing a Successful Cyber Product to Market:** This discussion will explore the world of Cybersecurity start-ups and their associated product development and go-to-market strategies. Attendees will share and gain perspective on how and why some cybersecurity solutions fail in the marketplace while others are wildly successful and widely adopted.

**Lunch**
WiCyS Poster Awards

**Closing Keynote:** Angela Kay, Microsoft

**The Adaptive Individual:** The time for cybersecurity is now. The cyber risks facing our globally interconnected society, including individuals, enterprises, and governments around the world, are real, and a diversity of perspectives and experiences are needed to drive cybersecurity innovations to counter these risks. Angela will discuss how women can and will make a difference at this pivotal juncture, and in the future. Through example, she will highlight how recognizing individuality - in yourself and in others - and being adaptable - demonstrating versatility and agility in changing circumstances - are essential for advancing not only professional, but also personal, goals.

**Workshops**

**A Walkthrough of Capture the Flag (CTF): Facebook Inc.**

A Capture the Flag (CTF) is a computer security competition that encourages players to solve security puzzles in a safe and controlled environment. This workshop will provide guidance on how to play a CTF. CTFs typically consist of challenge “levels” that represent real security issues found in networks and systems. The players will compete with each other, often in teams, to see who can solve these levels first and thereby win valuable points to progress up a leader-board. Our goal is to expose players to the most common methods hackers use to break into systems, and then to think about how they would defend against these attacks.
The workshop will use real-world case studies from our experiences at Adobe as the foundation for learning how to manage security throughout the whole product lifecycle. The first half will discuss the best practices, processes, and tools used to help integrate security into the software development and deployment process. The second half will cover how to properly respond to and manage incidents that occur once the product is in customers' hands and how to make sure that knowledge is funneled back into the development lifecycle.

The ACM CS2013 curriculum includes Information Assurance and Security as a pervasive knowledge area. However, introducing security in computing curriculum is challenging because of lack of appropriate teaching resources and training. If you are a faculty member who is interested in incorporating security related lab assignments in your security or CS courses (C++, Java, Python programming and/or software engineering and/or networking and/or database and/or operating systems), this is the workshop for you! As part of the CReST project (CyberWorkshops: Resources and Strategies for Teaching Cybersecurity in Computer Science, NSF Award# 1438861), this workshop will introduce attendees to add-on security modules.

End of Day 2
Data Spillage in a Hadoop Virtual Environment: Data spillage occurs when sensitive information is moved to an unauthorized or non-designated compute node or memory media (e.g. disk). The ability to control the privacy and security of sensitive information is a critical component in protecting national infrastructure and security. Currently, little research exists that is focused on understanding and determining incident response techniques for data spillage incidents within Hadoop’s distributed file system (HDFS). In addition, military and other government entities perceive data spillage as a security threat when sensitive information is introduced onto one or more unauthorized locations. As the use of Hadoop clusters to manage large amounts of data both inside and outside of government grows, the ability to locate and remove data effectively and efficiently in Hadoop clusters will become increasingly important. In this project we demonstrate the manner in which traditional tools used in digital forensic investigation tools can be repurposed as information recovery tools in achieving data sanitization within a Hadoop virtual cluster.

Gamified Permission Model for Facebook’s Third Party Applications: Facebook's existing application permission model lacks in communication of related privacy and security issues to users. This is an important issue because, 1) Many applications request more permissions than required by the application's functionality. 2) Social interaction driving application use is leading to a lack of awareness of data sharing, its risks, and its implications. 3) The end user gets used to viewing install-time dialogs, and grants all permissions without paying attention. We propose a scheme to engage a social network user during application installation by leveraging a gamified model of the requested permissions. Our main goal is to increase the user understanding of 1) the difference between the type of permissions 2) dangerous permissions that risk user privacy and security 3) the entities involved in accessing and storing their data. In our model, each permission is represented by a box, whose size, color, and icon depict its dangerousness, type and description respectively. To install an application that leverages gamified permission model, the user plays a game to allow and deny permissions to the application.

Using Unrestricted Mobile Sensors to Infer Tapped and Traced User Inputs: As of January 2014, 58% of Americans over the age of 18 own a smart phone. Of these smart phones, Android devices provide some security by requiring that third-party application developers declare to users which components and features their applications will access. However, the real-time environmental sensors on devices that are supported by the Android API are exempt from this requirement. We evaluate the possibility of exploiting the freedom to discretely use these sensors and expand on previous work by developing an application that can use the gyroscope and accelerometer to interpret what the user has written, even if trace input is used. Trace input is a feature available on Samsung’s default keyboard as well as in many popular third-party keyboard applications. The inclusion of trace input in a key logger application increases the amount of personal information that can be captured since users may choose to use the time-saving trace-based input as opposed to the traditional tap-based input. In this work, we demonstrate that it is indeed possible to recover both tap and trace inputted text using only motion sensor data.

Privacy Implications of the Facebook API: With more than 1 billion users, Facebook is pervasive in modern life. This large number of people sharing their information on such an expansive network raises concerns for privacy and security online. The purpose of this project was to explore how invasive Facebook’s API (Application Programming Interface) can be when developers create applications used by Facebook users. This research goal was accomplished by developing an application that retrieves music pages that the user likes and suggests new music artists for them to listen to. Skills utilized to complete this project included learning the Facebook API, mastering regular expression parsing, and construction of a SQL database. Preliminary results indicate that users are unaware of the privacy issues related to the public sharing of their musical likes.
Victoria Kisekka and Bich Vu  
*University at Buffalo*

**Investigating the Factors Influencing Health Information Sharing on Online Social Networks:** Development in online social networks have supported the creation of communities of practice where people who share similar interests come to seek and/or share knowledge through collaboration. Several scholars have determined that health information sharing is beneficial to patients in several ways; as an example, the sharing of medication information, disease management information, and other experiential knowledge benefits patients that are in the early stages of ailments who may be in search of informational and emotional support. Because of the benefit of health information sharing to patients, it is of critical importance to encourage patients to contribute by participating in online health social networks. The purpose of this research is to investigate the factors that may encourage or deter health information sharing on Online Social Networks (OSNs). The factors we investigate are: information privacy concerns, information trust, access to personal health records, mobile device usage, health status, quality of physician-to-patient interaction, and online health information utilization.

Julie Smicinski and Emily Leiby  
*Mercyhurst University*

**Peculiar Practices of Penetration and Protection:** How can a piece of paper be used to penetrate a secure network? Can that same piece of paper also prevent intrusions? This project examines how everyday objects can impact cybersecurity. Two perspectives are examined for each object: a red team perspective, which aims to use the object to penetrate a network, and a blue team perspective, which aims to use the object to defend a network. Using i2, the students created a graphic to illustrate the task at hand.

Gabrielle Buchanan  
*Hampton University*

**HTTPS: Is Your Website Truly Secure?:** Hypertext Transfer Protocol (HTTPS) was created to secure many. It is considered by many to be one of the best ways of ensuring browser security. However there are some security flaws can be found in HTTPS. What this project will be doing is gathering data on how secure various sites are using packet sniffing software including Wireshark and Cryptool 2. This paper will be comparing the amount of information that can be discovered on different sites with the help of these tools. During the course of the project, the traffic of HTTP-only sites and supposed HTTPS sites will be observed. Then based on the results it will be determined if the site is truly secure or not. There is little expectation for the HTTP-only sites to be secure but what this project is really hoping to figure out is if HTTPS-sites are impenetrable and if it is not the reason why and how could it be fixed.

Karolina Alvarez, Karen Lamb, Kenneth Jabon, Wesley Brooks  
*University of Illinois Urbana Champaign*

**Securing Embedded Systems with Spintronics:** Spintronics are an increasingly attractive alternative to CMOS technologies because of their size and speed. They provide new quantum physical features to computing that allow us to reimagine processes like random number generation. In this poster, we leverage two recent developments in secure computing that utilize spintronics: a true random number generator and a physically unclonable function. We couple these designs with our own components to present a unique cryptographic embedded system module. The true random number generator extracts entropy from electron spin, producing highly secure encryption, and the authentication routine of the physically unclonable function is strengthened by its application of spintronics.

Lindsay Simpkins  
*North Carolina A&T State University*

**Teaching Logic Flaws using a Case Study on Cashier-as-a-Service Attack:** Define bugs are implementation problems in software, such as buffer overflows, and flaws as code and design issues, like fail-open errors. Bugs can be found with automated tools, but not flaws. Therefore, it is important that students learn how to reduce logic flaws when developing software, and for them manually. A course module on logic flaws was created. A document covers where flaws come from, reducing flaws during development, and manual testing methods. A short reading quiz ensures this was read and understood. A case illustrates how a logic flaw could cause security vulnerabilities, based on the article How to Shop for Free Online. When Interspire used PayPalExpress as a 3rd party payment, a flaw let attackers place an expensive order using payment from a cheaper order. An animation shows HTTP interactions and back-end code for the steps of this exploit. A set of questions on finding and fixing logic flaws were designed for the students to discuss and answer. This poster introduces the topic of logic flaws and demonstrates the exploit from the case. It presents the discussion questions designed for the case study. Our teaching experience will also be discussed.
**Poster ID: 10**

Blaize Strothers  
*Hampton University*

**Health Care Laws and Cyberspace: Examining Cyber Threats to HIPAA:** Recent years’ rapid progression of technology and the subsequent encroachment of the digital world upon the physical has been a source of concern for many in fields where privacy is of the utmost importance. Despite the stringent regulations on health care privacy created by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the increasing sophistication of cyberattacks poses a significant threat to medical information security, with many doubting the ability of health care privacy policies to withstand innovative cybercriminal activity. Increased attention to cybersecurity with respect to recent threats, in addition to laws on the privacy of medical data, would allow HIPAA to remain current and truly address the security of health care information. By examining threats to HIPAA posed by medical cyberattack, the theft and sale of medical records, and the hacking of medical devices and equipment, we can identify opportunities for the modernization of HIPAA health information regulation to meet the needs of the technological age.

---

**Poster ID: 11**

Sarah Kern  
*University of Pittsburgh*

**A Call for Simpler Router Updating and Manageability:** For the majority of non-technical individuals, a router is best recognized for its use in connecting home computers and devices to the Internet via an Internet Service Provider (ISP). While many users are familiar with utilizing the provided security patches for their computers and mobile devices, router security and updates are generally overlooked. This phenomenon is not surprising given the intimidating architecture provided for router configuration. This is not acceptable for modern technology. Vendors must start designing for the average user in mind by providing a usable interface, additional explanation of technical terms and settings, and an increase in awareness and accessibility of firmware updates. ISPs need to become involved as well, by alerting customers of vulnerabilities and updates. Customers and users must participate too by utilizing the knowledge and services provided, and altogether we can gain more intuitive and secure routers.

---

**Poster ID: 12**

Elizabeth Phillips  
*Oxford University*

**Applying Social Network Analysis to Security Poster:** In this project we set out to explore the many ways in which Social Network Analysis (SNA) can be applied to the field of security, and especially, investigating what interactions could someone (e.g., an attacker) infer if they were able to gather data on a person’s friend groups or technology devices (e.g., email interactions) and whether this could be used to predict the hierarchical importance” of the individual. For this experiment we conducted our initial investigation on the Enron email dataset and investigated the effectiveness of existing SNA metrics on establishing hierarchy from the social network created from the email communications. We were able to identify 5 metrics that proved effective in predicting hierarchy, namely weighted_cliques, HITS authority (and by its nature HITS hub as well), degree and average distance. After performing supervised machine learning with the available ground truth data available for Enron dataset, our MultiLayer Perceptron classifier was able to identify the “Boss” category with an ROC area of 0.939. We then collected a secondary dataset with which to verify the effectiveness of the results discovered from the Enron dataset.

---

**Poster ID: 13**

Saradha Kannan  
*Lewis University*

**Securing the Medical Devices:** By using a cyber physical system, we are securing medical devices.

**Poster ID: 14**

Laura Wilkinson, Emily Atwood, Whitney Winders, Whitney Maxwell, Cara Cornell, Cj Cornell, Allie Larson, Sarah Cunha, Dale Rowe: *Brigham Young University*

**The Customer Knows Best - (aka. We Made a Malware Course...):** This year, we have begun teaching a new senior/graduate level course in malware analysis. Last year, a mixed student body was invited to participate in course design. Eight women accepted this invitation and designed a semester-long malware analysis course with a faculty mentor. This poster aims to increase awareness of using students in course design and show some of the process that went into this new course. As added impact, it shows what a team of eight committed women, ranging from freshmen to graduate, can achieve!

---

**Poster ID: 15**

Anahita Davoudi  
*University of Central Florida*

**Trust Based Product Recommendation in Social Networks:** In this project, we utilize different centrality measurements to model
time evolution of each node’s opinion about a product based on it neighbors’ opinion which involve trust score of each corresponding neighbor. For doing so, we incorporate trust matrix, which is how much a user trust other user, a value between in range of [0,1] into centrality definitions. The centrality is used to determine importance of a node in network. Although degree centrality is the simplest indication of centrality of a node, it might not give valuable meaning, since it just rely on the number of neighbors and ignores the importance of the neighbors. Taking to account that not all neighbors of a node are of equal importance, which usually increase if that node has neighbors that are themselves important, we use EigenVector centrality to analyze each neighbor option after different time stamp being marked by the timer.

Poster ID: 16
Sayonnha Mandal, Robin Gandhi, Harvey Siy
University of Nebraska, Omaha

A Framework for Analyzing Federal Regulations for Information Security: This research examines regulatory compliance in information systems from a software assurance perspective. Today information systems are software intensive. They are thus prone to software weaknesses, which are exploited by various attacks on the systems. However, when stakeholders are incorporating new systems, they usually tailor security controls based on system needs, thereby, software security concerns receive very less attention than it deserves. In our research, we extend NOMOS, a framework for modeling roles, norms and situations, and evaluate its applicability to information security regulations. We present a case study with the Federal Information Security Management Act (FISMA) of 2002. FISMA statements with high variability space for categorizing information and information systems across multiple documents are examined to explore the utility and limits of the NOMOS framework. Finally, we introduce mechanisms to determine applicability of FISMA and related standards to tailored constraints on software components in a larger information system.

Poster ID: 17
Nirmala Rai and Rakesh Verma
University of Houston

Phish-IDetector for Email Header Based Phishing Detection: Phishing is a very popular and widely used technique for stealing sensitive information like account login credentials, credit card numbers etc. The most common attack means are carefully designed phishing emails that mislead individuals into divulging such private and sensitive information. Huge monetary losses are incurred every year due to such attacks. I would present the poster as a consolidated account of a novel approach to solving the well-known nuisance of phishing emails. Together with my academic advisor, I research in the field of phishing email detection. Our study revealed that email body is completely under the control of sender unlike the header which follows a relatively stricter format. So we focused on detection based on email headers. Our approach centers on the useful properties of email header and exploits it by using machine learning. It is simple yet effective producing detection rate of over 99%. The robustness of our technique is proven by getting consistent results for several datasets with a variety of emails in each. Also an independent experiment with ten volunteers supports the relevance of our technique in the present era of electronic communication.

Poster ID: 18
Hilary Hayes and Maria Yacaman
Brigham Young University

CyberIQ: CyberIQ is a project that is aimed toward enabling teens everywhere to establish safe, lifelong online habits. Technology usage is increasing daily and will continue to increase as teens begin to take over our world. It is crucial that they learn now how to be safe online and protect themselves from the many dangers. As part of our effort to keep teens safe online, CyberIQ mentors have gone to high schools around the state to teach these concepts in classrooms. Mentors have selected students to promote the “Teens Teaching Teens” program through CyberIQ. With this program, teens will be teaching their peers how to stay safe online via various resources. CyberIQ will continue to expand on topics, videos and current content to keep teens up-to-date with current events occurring in the technology world. Visit CyberIQ at www.cyberiq.org

Poster ID: 19
Nicole Hands, Harish Kumaravel, Prajwel Hegde
Purdue University

Malware Defense with Access Control Policy and Integrity Levels: With the persistent threat of cyber attacks of many, ever-changing forms, the need for computer systems to have a comprehensive protection schema that can provide security against unknown, known, and polymorphic threats becomes apparent. Working under the premise that compromise is inevitable, the system should be able to detect that it has been compromised and respond in such a way that functionality degrades incrementally. This study represents a synthesis of multiple fields of research from integrity levels of operation to malware detection methods to access control policy. The system function of FTP will be used as a model and broken down into discrete computational units which will each be assigned attributes from which access control policy can be created. Upon change in the state of the attribute based on the premise that this change was caused by malware infection, the system would respond by lowering its integrity level, with processes
Poster ID: 20
Jarilyn Hernandez and Desiree Reagan
West Virginia University

Ancient Foundations and Modern Uses: the Evolution of Steganography: Steganography, the art and science of hiding information, has been used in our civilization for centuries. The SANS Institute reports that a new age of terrorism is among us and that terrorist organizations such as Hamas, Hezbollah, and Al-Qaeda are now employing advanced steganography techniques to pass sensitive communications across the Internet undetected. Specifically, steganography has been used by these terrorist organizations to hide maps and photographs of terrorist targets as well as posting instructions for terrorist activities on various web sites. This behavior can affect the critical infrastructure of our country, since we are completely blind against these threats. In better understanding these threats we are more able to protect ourselves against them. The objective of our research is to educate the scientific community about what steganography is and what the existing techniques are for sharing undetected information. Specifically, we present a brief history of steganography and the science behind modern steganography. Finally, we demonstrate how modern technologies allow us to use steganography techniques from the convenience of our very own mobile devices.

Poster ID: 21
Jing Chen, Christopher Gates, Zach Jorgensen, Weining Yang, Aiping Xiong, Ninghui Li, Ting Yu, Robert Proctor
Purdue University

Effective Risk Communication for End Users: A Multi-granularity Approach: We proposed a multi-granularity approach to present risk information of mobile apps to the end users. Within this approach the highest level is a summary risk index, which allows quick and easy comparison among multiple apps that provide similar functionality. We have developed several types of risk index, such as text saying “High Risk” or number of filled circles (Gates, Chen, Li, & Proctor, 2014). Through both online and in-lab studies, we found that when presented the interface with the summary risk index, participants made more secure app-selection decisions.

Poster ID: 22
Bianca Colon-Rosado and Humberto Ortiz-Zuazaga
University of Puerto Rico

Techniques for Anomaly Detection in Network Flows: A general method for detecting anomalies in network traffic is an important unresolved problem. Using Network Flows it should be possible to observe most anomaly types by inspecting traffic flows. However, to date, researchers are still struggling to find an effective and lightweight method.

Poster ID: 23
Mohamed Shehab and Abeer Aljarrah
UNCC

Reducing Attack Surface on Cordova-based Hybrid Mobile Apps: Hybrid mobile application development is increasingly being adopted by the mobile development community since it provides the answer to the challenge of having the right mix of accessibility to mobile native features at an affordable development cost. Apache Cordova library is an example of a middle-ware that enables developers of different mobile operating systems to access mobile native features through web frameworks, such as HTML and JavaScript, which at the same time introduces several security challenges. In this paper, we highlight current security setting limitations of hybrid mobile frameworks and propose a policy based approach to provide limited access to the different pages/states of the app to mitigate the effect of possible attacks. In addition, we downloaded and analyzed 622 real hybrid apps, and presented settings and security statistics.

Poster ID: 24
Christa Cody
Tennessee Technological University

Decision Trees for Energy Fraud Detection in Smart Meters: The electrical grid is transitioning to new smart grid technology requiring accurate energy fraud detection techniques. The use of machine learning techniques by researchers has been a very common approach to energy fraud detection by detecting patterns within the data. Patterns in energy consumption can be utilized to detect anomalous behavior. This research explores the use of decision trees to classify energy consumption data to allow the detection of potentially fraudulent activity.

Poster ID: 25
Kelley Misata, Raymond Hansen, Baijan Yang
Purdue University
A Taxonomy of Privacy-protecting Tools to Browse the World Wide Web: There is a growing public concern regarding big data and intelligence surveillance on unsuspecting Internet users, and an increase in public conversation around what does privacy really mean in the digital realm. Although technologies have been developed to help generate public protect their privacy, average users found the tools complex and difficult to decipher. This research aims to weed through some of these complexities by reviewing 6 publicly recognized technologies promoted to help users protect their privacy while browsing the web. The scope will be broad in order to touch on the important aspects each technology including promises, privacy realities, technical construct, ease of use and drawbacks average users should be aware of before using.

Poster ID: 26
Alicia Pope
Davenport University

Technical Approach to A Case Investigation: I reviewed the hard drive and e-mails of a Michigan man sentenced to 30 months in prison, who conspired to conduct highly destructive computer attacks on competitors of his online sportswear business, including a web-based New Jersey company. Mr. Arabo, the defendant, admitted that in online “instant messages” conversations, that he met a New Jersey resident, Jasmine Singh, who communicated using the online name “Pherk”. Mr. Arabo learned that Singh or Pherk, covertly infected some two-thousand personal computers with programs that enabled him to remotely control them. Singh demonstrated to Mr. Arabo online that he could command these computers to conduct attacks, known as distributed denial of service, or “DDOS attacks, on computer servers and disable websites supported by those servers. Arabo admitted that he asked Singh to take down the websites and online sales operations of certain of his competitors. Arabo promised to compensate Singh for the attacks with merchandise, including designer sneakers.

Poster ID: 27
Tia Pope
Georgia Institute of Technology

Most Americans Don’t Secure Their Smartphones?: Keeping our mobile devices secure can be the least of our worries when it comes to working long hours, meeting with friends, engaging with our families and the like. How many people do you think consider the security of their mobile phones when going through the fast pace of life? CNBC tells us that “Most Americans don’t secure their smartphones.” This is a survey of a random spread of Atlanta Residents to test this claim and to explore the possible causes.

Poster ID: 28
Mnar Alnaghes and Fayez Gebali
University of Victoria, Canada

An Approach to Defend Against Blackhole Attack in Ad Hoc Networks: The elasticity of Ad hoc networks (MANET) infrastructure and its characteristics introduce new security risks apparently. One of their possible attacks is the Black Hole attack which has received a great deal of recent attention. In the Black Hole attack, a malicious node uses the routing protocol to declare itself as having the shortest path to the node whose packets it wants to intercept. It is needed to understand this risk with a view to extract preventive and corrective protections against it seeking for security and safety. We introduced an approach that could stop this attack from happening in such a network by using an algorithm which controls the communications between nodes and let each node becomes identified and authorized in a group of nodes. In this algorithm, stable nodes which called leaders are responsible for routing and forwarding packets from source to destination nodes. This poster declares brief details about the black hole attack, and, explains the algorithm that helps throughput to be increased as a consequence.
Women in Cybersecurity

Workshop Organizers
Aimee Tabor, TRUST Center, Berkeley
Betsy Bevilacqua and Eleni Gessiou, Facebook
Kara Nance, University of Alaska Fairbanks and Steve LaFountain, NSA
Marcelle Lee, Mari Galloway, Lisa Foreman-Jiggetts, Women’s Society of Cyberjutsu
Siddharth Kaza, Blair Taylor, Towson University and Sheikh Ghafoor, Tennessee Tech University
Tom Pigg and Lisa Matlock, Jackson State Community College
Wendy Poland and Julia Knecht, Adobe

Resume Clinic Experts
Anna Wilbanks, MIT Lincoln Laboratory
Betsy Bevilacqua, Facebook
Bianca McNair, DoD
Christina Martinez, Moraine Valley Community College
Dane Dungee, Harris Corporation
Kathleen Smith, ClearedJobs.Net
Kira Gantt, Virginia Tech
Linda Avers, Lockheed Martin

Student Poster Session Judges
Aparna Mahadev, Worcester State University
Christa Anderson, Microsoft
Debra Chapman, University of South Alabama
Idongesit Mkpong-Ruffin, Faulkner University
Janell Straach, UT Dallas
Joanne Sexton, Georgia Regents University
Julia Bell, Walters State Community College
Julia Taylor, Purdue University
Kim Rogers, Adobe Systems
Mari Galloway, Women’s Society of Cyberjutsu
Maria McClelland, Oak Ridge National Laboratory
Marc R Conner, Henry Ford College

Mike Doyle, Cigital
Molly Ukwutije-Uzoh, Learning Right Technologies
Monica Ipong, Symantec
Morgan Zantua, University of Washington
Patrick Skelly, IBM
Pete Bugnatto, Lockheed Martin
Rosie Hall, Cisco

Mona Sana, ViaSat
Na Li, Northwest Missouri State University
Patricia Okorie, Prince George’s Community College
Paula Mitchell, Microsoft
Rekik Tilahun, Ausgar Technologies
Sheila Mifsud, Facebook
Sumita Mishra, Rochester Institute of Technology
Susan Warshaw, Santa Fe College
Xenia Mountroudiou, Jacksonville University
Yin Pan, Rochester Institute of Technology
Women in Cybersecurity

Session Chairs

Akila Srinivasan, Microsoft
April Tanner, Jackson State University
Barbara Hewitt, Texas A&M University--San Antonio
Chutima Boonthum-Denecke, Hampton University
Cindy L. Bethel, Mississippi State University
Deborah Shands, National Science Foundation
Diane Williams, Lockheed Martin
Dianne Fodell, IBM
Elizabeth Bautista, Lawrence Berkeley National Laboratory
Heather McCalley, Malcovery Security
Jim Caristi, Valparaiso University
Julia Knecht, Adobe Systems
Laura Pullum, Oak Ridge National Laboratory
Lila Rajabion, Penn State University
Natalie Tran, Facebook
Noni M. Bkohonak, University of South Carolina Lancaster
Ronda Henning, Harris Corporation
Susanne Wetzel, Stevens Institute of Technology
Sy Goodman, Georgia Institute of Technology

Speed Mentoring Session Mentors

Aimee Tabor, TRUST Center, University of California, Berkeley
Areej Albatainehe, Our Lady of the Lake University
Ashley Podhradsky, Dakota State University
Cathy Coon, ViaSat
Claire Jefferson-Glipa, Girl Scouts of San Gorgonio Council
Claire Vishik, Intel
Corrinne Sande, Whatcom Community College
Dawn Carroll, Cigital
Eleni Gessiou, Facebook
Evan Snyder, Facebook
Jana Duffy, Facebook
Jennie Kam, Cisco Systems, Inc.
Karyn Higa-Smith, DHS Science and Technology
Lesley Piper, The MITRE Corporation
Limin Jia, Carnegie Mellon University
Lora McIntosh, Regions Financial Corporation
Iulia Ion, Google
Meagan Krumian, Facebook
Micaela Hoskins, Cisco Systems
Sherri Ramsay, CyberPoint International
Soledad Antelada Toledano, Lawrence Berkeley National Laboratory

For more information, visit us at: www.WiCyS.net
We're proud to support the 2015 Women in Cybersecurity Conference!

Come say hi! Our own Sherri Ramsay will be giving the Keynote address Friday night, and we'll be at the career fair!

Learn more about our Women in Cyber Security event taking place in Baltimore this fall.

cyberpoint.com/wcs

DREAM BIG

Come join us facebook.com/careers
A message from the Women of Facebook Security.
Thank You to Our Sponsors!

Diamond Sponsors

Platinum Sponsors

Gold Sponsors

Silver Sponsors

Bronze Sponsors