Women in CyberSecurity Conference

2018

MARCH 23 & 24
CHICAGO, IL

WELCOME

All Hands on Deck! Yours, Mine and Ours!

You made it! You are here today with us and others like you, who share the same passion and aspiration for CyberSecurity as you do! I hope by being here, you realize, if you have not already, how rewarding and vital it is to contribute to this field for the betterment of today's technological society. We need more investments in broadening participation in cybersecurity with WiCyS being one such initiative. Every program, regardless of size and origin, which addresses the pipeline and diversity problems in this field, makes a difference. As individuals, as organizations, as a society - we can and will continue to have an impact!

This conference has only been possible because of the generous support from our community, industrial and academic sponsoring partners and the federal government. I am thankful for the support of the WiCyS 2018 planning committee. I want to express my sincerest gratitude to Drs. Janell Straach and Ray Trygstad, Co-chairs from The University of Texas at Dallas and Illinois Institute of Technology, respectively. The team of Illinois Institute of Technology led by Ms. Angela Jarka and Ms. Amber Chatellier has been a wonderful local host for WiCyS this year in Chicago. Both Tennessee Tech and IIT teams have worked very hard to ensure your time here at WiCyS 2018 is worthwhile.

WiCyS will continue to be a great example of a successful partnership between academia, government and industry, where we have join hands with a mission to increase pipeline and diversity in the cybersecurity workforce.

Dr. Ambareen Siraj (Founder and Conference Chair)
Professor, Computer Science, Director, CyberSecurity Education, Research & Outreach Center,
Tennessee Tech University

I'd like to personally welcome each of you to WiCyS 2018. It's an exciting time for us as we continue to expand by connecting inspired people like yourself. The program committee has created a packed agenda with a variety of sessions. I urge you to take full advantage of all the opportunities for learning, networking, and sharing. Be bold and introduce yourself to someone new in every session. Thank you for attending WiCyS 2018 and I look forward to meeting many of you over the next two days.

Dr. Janell Straach (Co-Chair)
Director of Center for Engaging Women in CyberSecurity, Computer Science, University of Texas at Dallas

---

We are so excited to have you here in Chicago with us for WiCyS 2018. Since our founding in 1890 with the goal of educating the sons and daughters of the working people of Chicago, Illinois Institute of Technology has had a strong commitment to the education of women. That commitment continues today, and we are delighted to have the opportunity to host this conference. We bring that same commitment to cyber security education--after five years of offering graduate education in the field, we are proud to introduce our Bachelor of Science in Applied Cybersecurity and Information Technology starting in fall 2018. Our students, our faculty, and most of all our amazing staff, Angela Jarka and Amber Chatellier, have worked tirelessly to ensure that you have this opportunity to interact with cybersecurity professionals, mentors, peers, and employers, with the goal of energizing your participation as a current or future cybersecurity professional. We hope that your stay in Chicago is exciting and productive.

Ray Trygstad (2018 Co-Chair)
Associate Chair, Department of Information Technology and Management, Illinois Institute of Technology

COMMITTEES

WICYS CONFERENCE ORGANIZERS

Dr. Ambareen Siraj (Founder and Conference Chair)
Professor, Computer Science, Director, CyberSecurity Education, Research & Outreach Center, Tennessee Tech University

Dr. Janell Straach (Co-Chair)
Director of Center for Engaging Women in CyberSecurity, Computer Science, University of Texas at Dallas

Ray Trygstad (2018 Co-Chair)
Associate Chair, Department of Information Technology and Management, Illinois Institute of Technology

PROGRAM COMMITTEE

Dr. Ashley Podhradsky (PC Chair)
Beacom College of Computer and Cyber Sciences, Dakota State University

Chris Carlson
Cyber Security - Engineering Director, Target

Keshanna Cooley
Sr. Cybersecurity Strategist, Office of the Assistant Secretary, Cybersecurity & Communications, DHS

Dr. Di Ma
Associate Professor, Computer & Information Science, University of Michigan – Dearborn

Dr. Patricia A. McQuaid
Professor of Information Systems,
California Polytechnic State University

Dr. Sumita Mishra
Professor, Rochester Institute of Technology

Lori Pfannenstein
CAE in Cyber Defense Program Manager, NSA

Heather Ricciuto
Academic Outreach Leader, IBM Security

Rinki Sethi
Senior Director, Information Security,
Palo Alto Networks

Michael Tu
Associate Professor, Purdue University Northwest

Lily Yang
Director, NSF CPS Center on Security, Intel Labs

WORKSHOP COMMITTEE

Kim Milford
Executive Director, REN-ISAC, Indiana University

Andreina Reyes
OPM Federal Investigative Services, CSRA Inc

SCHOLARSHIP COMMITTEE

Dr. Jing Chen
Assistant Professor, Old Dominion University

Anahita Davoudi
University of Central Florida

Dr. Amelia Estwick
Program Director, National Cybersecurity Institute at Excelsior College

Ann-Marie Horcher
Lecturer, Central Michigan University

Dr. Pushpa Kumar
Senior Lecturer, University of Texas at Dallas

Chris Lannin
GenCyber Evaluator, Dark Enterprises &
Media Specialist, Kasson-Mantorville High School

COMMITTEES

Dr. Leslie C. Leonard
Computer Scientist, U.S. Army Engineer Research and Development Center (ERDC)

Dr. Kelley Misata
Sightline Security

Diah Nasution
Cybersecurity Software Developer, Fidelity Investment

Tolu Onireti
Cybersecurity Manager, EY

Dr. Alicia Pearlman
Adjunct Faculty, Schoolcraft College

POSTER SESSION COMMITTEE

Dr. Chutima Boonthum-Denecke
Associate Professor, Hampton University

Joan Soo Li Lim
Researcher, University of Toronto

Dr. Debra A. Nakama
Vice Chancellor of Student Affairs, University of Hawaii Maui College

Bridget Pelletier-Ross
Cyber Security Engineer, Facebook

OUTREACH

Jennifer Eiben
Director of Community Outreach and Social Media Editor, CyberWire

CAREER FAIR COMMITTEE

Kathleen Smith
Kathleen Smith, CMO, ClearedJobs.Net/CyberSecJobs.com

SPEED MENTORING SESSION COMMITTEE

Kaitlyn Bestenheider
Cyber Technologies Teacher, Rockland BOCES & Graduate Student, Pace University

Andrea Frost
Engineer, ActionSprout

LOGISTICS COMMITTEE

Amber Chatellier
Program Manager, Department of IT and Management, Illinois Institute of Technology

Suzanne Henry
Contract Compliance Assistant, Tennessee Tech

Angela Jarka
Assistant Program Manager, Department of IT and Management, Illinois Institute of Technology

Lana Richardson
Financial Analyst, Tennessee Tech

SOCIAL MEDIA TEAM

Candace Fukuda
Information Security Event Manager, Facebook

Jennie Kam
Security Researcher, Cisco

Mansi Thakar
Information Security Analyst, Playstation

WICYS AT A GLANCE

THURSDAY, MARCH 22, 2018		
8:30am - 4:00pm	GenCyber at WiCyS	Waldorf
2:00pm - 4:00pm	Workshop Series 1	C1-2, C3-4, C5-6, C7-8
4:30pm - 6:30pm	Workshop Series 2	C1-2, C5-6, C7-8, Continental A
7:00pm - 9:00pm	Mentoring Socials (Strategic/Diamond Partners)	4th & 5th Floor
7:00pm - 9:00pm	General Mentoring Social	Marquette
7:00pm - 9:00pm	Scholorship For Service (SFS) Meet & Greet	4th Floor
8:00pm - 9:00pm	1:1 Meet-up For Educators w/ Funding Agencies	4th Floor

FRIDAY, MARCH 23, 2018			CAREER FAIR
8:30am - 10:45am	Breakfast, Keynote & Lightning Talks	Continental Ballroom	
10:45am - 12:00pm	Student Poster Session	Salon C Foyer	SET-UP AT 11:00AM
10:45am - 12:00pm	Resume Clinic	Buckingham	
12:00pm - 12:45pm	Distinquished Speakers	C1-2, C3-4, C5-6	
12:45pm - 2:15pm	Lunch & Keynote	Continental Ballroom	
2:15pm - 3:00pm	Technical Presentations	C1-2, C3-4, C5-6	
3:00pm - 6:30pm	*CAREER FAIR DAY 1*	Salon D	OPEN
3:45pm - 5:45pm	Workshop Series 3	C1-2, C3-4, C5-6	
5:45pm - 6:30pm	Panels	C1-2, C3-4, C5-6	
6:30pm - 7:00pm	Group Picture in Lobby	Lobby	CLOSED AT 6:30PM
7:00pm - 8:30pm	Dinner & Keynotes	Grand Ballroom	

SATURDAY, MARCH 24, 2018			
8:30am - 10:15 am	Breakfast, Keynote & Lightning Talks	Continental Ballroom	CLOSED
10:15am - 12:15pm	*CAREER FAIR DAY 2*	Salon D	OPEN
10:15am - 10:30am	*BREAK*		
10:30am - 11:15am	Distinquished Speakers	C1-2, C3-4, C5-6	
11:15am - 11:30am	*COFFEE BREAK*	Salon C Foyer	
11:30am - 12:15pm	Technical Presentations	C1-2, C3-4, C5-6	
12:15pm - 1:00pm	Birds of a Feather	C1-2, C3-4, C5-6	TEAR DOWN
1:00pm - 2:30pm	Lunch, Keynote, Poster Awards & Closing Remarks	International Ballroom South	
2:30pm - 4:30pm	Workshop Series 4	C1-2, C3-4, C5-6, C7-8	

THURSDAY AGENDA

8:30am - 4:00pm WALDORF	GENCYBER AT WICYS
12:00pm - 7:30pm	REGISTRATION *(8TH ST. SOUTH LOBBY DESK)*
2:00pm - 4:00pm SALON C1-2	WORKSHOPS SERIES 1 **Recruiting Cybersecurity Talent: A workshop for hiring managers and external recruiters.** *Deidre Diamond and Veronica Mollica, **CyberSN***
SALON C3-4	**N00bSec to Cyber-Champion: Hacking the National Cyber League for Success** *Kaitlyn Bestenheider, Elizabeth Molloy, Vincente Gomez and Andreea Cotoranu, **Pace University**; Michael Lavacca, **Bloomberg***
SALON C5-6	**Introduction to iOS Application Security Testing** *Dawn Isabel and Jessica Sexton, **IOActive***
SALON C7-8	**Threat Intelligence: Beyond the Basics.** *Rachel Giacobozzi and Breanna Laconic, **Target Inc.***
4:30pm - 6:30pm SALON C1-2	WORKSHOPS SERIES 2 **Conducting Meaningful Research and Presenting Effectively** *Anna Trikalinou, Lily Yang, Reshma Lal, Tania Skinner, **Intel**; Dr. Melissa Dark, **Purdue University**; Dr. Ann Cox, **DHS**; Dr. Celeste Matarazzo, **Lawrence Livermore National Lab***
CONTINENTAL A	**Cyber Competition to Engage and Inspire** *Oxana Pelc and Tiffany Benjamin, **Facebook***
SALON C5-6	**Practical Network Forensics** *Marcelle Lee, **LookingGlass Cyber Solutions**; Jennie Kam and Ellie Daw, **Cisco***
SALON C7-8	**Building a Home Lab for Malware Analysis** *Sarah Kern and Susie Heilman, **The MITRE Corporation***
7:00pm - 9:00pm 4TH & 5TH FLOOR	MENTORING SOCIALS FOR STRATEGIC & DIAMOND PARTNERS
MARQUETTE	GENERAL MENTORING SOCIAL
4TH FLOOR	SCHOLARSHIP FOR SERVICE (SFS) MEET & GREET
8:00pm - 9:00pm 4TH FLOOR	1:1 MEET-UP FOR EDUCATORS WITH FUNDING AGENCIES

FRIDAY AGENDA

7:30am - 6:30pm	**REGISTRATION *(CONTINENTAL FOYER)***
8:30am - 10:45am CONTINENTAL	**BREAKFAST, CONFERENCE OPENING, KEYNOTE & LIGHTNING TALKS** **Welcome by:** • **Ray Trygstad**, WiCyS Conference Co-Chair • **Dr. Ambareen Siraj**, WiCyS Founder and Chair • **Dr. Gerald Gannod**, Chair, Computer Science, Tennessee Tech **Opening Remarks: Dr. Nirmala Kannankutty**, Deputy Division Director, Division of Graduate Education, National Science Foundation **Keynote: A Career in Cyber Security in the Intelligence Sector** *Sherrill Nicely, **Chief Information Security Officer, Central Intelligence Agency*** **Lightning Talks:** • **Cyber Political Engineering - Mother of ALL Cyber Attacks,** *Kavya Pearlman, **Linden Lab*** • **NSA Day of Cyber Program Partnership with WiCyS,** *Kim Paradise, **Life Journey*** • **What are Apprenticeships?,** *Carolyn Reinick, **Department of Labor*** • **Hacking the Law: The Legal Terms of Bug Bounties Explored,** *Amit Elazari, **UC Berkeley*** • **Watson for Cybersecurity and IBM's Cyber Range,** *Alison Ritter, **IBM*** • **Investing in Your Professional Network,** *Tolu Onireti and Nana Ahwoi Larson, **Ernst and Young*** • **Malice in Wonderland,** *Preethi Josephina Mudialba, **Carnegie Mellon University***
10:45am - 12:00pm SALON C FOYER	**STUDENT POSTER SESSION *(WITH COFFEE BREAK)***
10:45am - 12:00pm BUCKINGHAM	**RESUME CLINIC**
12:00pm - 12:45pm SALON C1-2	**DISTINGUISHED SPEAKERS** **Bridging Cybersecurity Research and Education** *Dr. Susanne Wetzel, **National Science Foundation***
SALON C3-4	**Cyber Security Research: A Data Scientist's Perspective** *Dr. Celeste Matarazzo, **Lawrence Livermore National Laboratory***
SALON C5-6	**Leadership in Cybersecurity: Pathways and Strategies for Success** *Dr. Deanne Cranford-Wesley, **Forsyth Technical Community College**; Dr. Margaret Layton, **Symantec**; Yabing Wang, **Alight Solutions**; Marian Merritt, **National Institute of Standards and Technology***
12:45pm - 2:15pm CONTINENTAL	**LUNCH & KEYNOTE** **Keynote: The Cybersecurity Threats are Real, the Opportunity is Yours: Tips on Navigating the CyberSecurity Career Field** *Mona Bates, **CIO & VP of Information Technology, Raytheon***

FRIDAY AGENDA

2:15pm - 3:00pm SALON C1-2	**TECHNICAL PRESENTATIONS** **Cyber-Arcade: An Innovative Approach to Promote Cybersecurity and Engage Women to Pursue STEM Careers** *Pauline Mosley, Dawn Tucker, Li-Chiou Chen and Andreea Cotoranu, **Pace University***
SALON C3-4	**Data Spillage Remediation Techniques in Hadoop** *Sunanda Mani and Srinivas Jantali, **Northeastern University***
SALON C5-6	**Twitter Spam Detection based on Self-taught Learning and Sparse Auto-encoder** *Lijie Zhou and Hao Yue, **San Francisco State University***
3:00pm - 6:30pm	**CAREER FAIR OPENING *(WITH REFRESHMENTS IN SALON D)***
3:45pm - 5:45pm SALON C1-2	**WORKSHOP SERIES 3** **Teaching Cyber Ethics and Societal Impacts in Introduction Computing Courses** *Dr. Yesem Kurt Peker, **Columbus State University**; Dr. Florence Appel, **St. Xavier University***
SALON C3-4	**Adventures in Cyberspace: Cyber Security Literacy for K-12 and Beyond** *Julie Rursch and Tracy LaVan, **Iowa State University***
SALON C5-6	**Hacking Discourses - Exploring Feminist and Critical Theory through Cybersecurity** *Nathan Fisk, **Florida Center for Cybersecurity**; Felice Flake, **ScySec LLC***
SALON C7-8	**Skills and Inspiration for Career Journeys in Cybersecurity** **Facilitator:** *Felicia Jackson, **Raytheon**;* **Panelists:** *Cheryl Whitis, Kathy Frain, Kathy O'Donnell, Mary Ann Waddick, and Jordan Miller, **Raytheon***
5:45pm - 6:30pm SALON C1-2	**PANELS** **Securing the Nation: How NSA is Working to Improve Cybersecurity Education** *Blair Taylor, **Towson University/NSA (CON)**; Steve LaFountain, Tina Ladabouche and Karen Leuschner, **National Security Agency***
SALON C3-4	**Oopsie: The Saga of Accidental Awesomeness** *Prajakta Jagdale, Muoi Landivar, and Jen Miller-Osborn, **Palo Alto Networks**; Joy Forsythe, **Mango Health**; Morgan Bjerke, **Booz Allen Hamilton***
SALON C5-6	**Diversity in Cybersecurity: An International Perspective** *Keenan Skelly, (**USA**), Monica Zhu (**Australia**), Laura Payne (**Canada**), Isabelle Landreau (**France**), and Susana Mejido (**Spain**)*
6:30pm - 7:00pm	**GROUP PICTURE IN LOBBY *(NEAR CLOCK TOWER)***
7:00pm - 8:30pm GRAND	**DINNER & KEYNOTE** **Panel Keynote: Men as Allies: Partnering to Advance Women in Cybersecurity** *Michele Guel & Tony Jeffs, **Cisco**; Ben Hagen, **Facebook**; Douglas Maughan, **DHS**; Dan Shnowske, **FMR**; Allan Paller, **SANS**; Dr. Greg Shannon, **Carnegie Mellon University**; Tony Baylis, **Lawrence Livermore National Laboratory***

SATURDAY AGENDA

8:00am - 1:00pm	**REGISTRATION**
8:30am - 10:15am CONTINENTAL	**BREAKFAST, KEYNOTE & LIGHTNING TALKS** **Welcome by:** • **Janell Straach**, Director of Center for Engaging Women in CyberSecurity, UT Dallas • **Dr. Vahid Motevalli**, Associate Dean, College of Engineering, Tennessee Tech **Opening Remarks: Rodney Petersen**, Director of the National Initiative for Cybersecurity Education, NIST **Keynote: Be the Energy in Cybersecurity** *Diane M. Janosek, **Deputy Commandant for the National Cryptologic School, NSA*** **Lightning Talks:** • **Bananapeelbot: The Gamification of Corporate Security,** *Carla Sun, **SurveyMonkey*** • **From Pre-Nursing to Pen Testing,** *Shea Mchugh, **Intrinium Inc.*** • **Turning "I'm not qualified" into "I'm a great fit for this job",** *Roselle Safran, **Rosint Labs*** • **When a Picture is Worth a Thousand Alerts,** *Aditi Chaudhry, **Capital One*** • **"Build me a world class security program in three months",** *Christie Terill, **Bishop Fox*** • **Between you, me, and the Board of Directors (BOD): How to gain BOD support for your cybersecurity program and live to tell the tale,** *Lena Singer, **Independent*** • **WiCyS Student Chapters: How to Create and Sustain a Chapter,** *Dr. Vitaly Ford, **Arcadia Unversity,** Dr. Masooda Bashir, **University of Illinois at Urbana-Champaign***
10:15am - 12:15pm	**CAREER FAIR RE-OPENING - SALON D**
10:15am - 10:30am	**BREAK *(NO REFRESHMENTS)***
10:30am - 11:15am SALON C1-2 SALON C3-4 SALON C5-6	**DISTINQUISHED SPEAKERS** **Building a Culture of Cybersecurity** *Dr. Eman El-Sheikh, **University of West Florida*** **Securing the Digital City: Cyber Threats and Responses** *Quiessence Phillips, **New York City Cyber Command*** **Security Must Reflect Those We Protect** *Aanchal Gupta, **Facebook***
11:15am - 11:30am	**COFFEE BREAK IN SALON C FOYER**
11:30am- 12:15pm SALON C1-2	**TECHNICAL PRESENTATIONS** **Ethical Thinking in Cyber Space Curriculum Development** *Jane Blanken-Webb, Imani Palmer, Masooda Bashir,* ***University of Illinois at Urbana-Champaign***

SATURDAY AGENDA

SALON C3-4	**The Gapless Air Gap** *Rachel Schmierer-Davis,* ***Johns Hopkins University Applied Physics Laboratory***
SALON C5-6	**The Missing Link between Blockchain and Privacy** *Parisa Kianmajd,* ***Intel***
12:15pm - 1:00pm SALON C3-4	**BIRDS OF A FEATHER** **Joining the Game: A Discussion on Approaches to Recruite Women into Cybersecurity** *Yesem Kurt Peker,* ***Columbus State****; Rae-Kelly Hamilton,* ***United States Naval Academy****; Paula Fetterman,* ***Financial Services Information Sharing and Analysis Center****; Marla Lamont,* ***Tractor Supply***
SALON C1-2	**Staying in the Game: Challenges and Solutions to Retain Women in CyberSecurity** *Caryn Truitt,* ***Highline College****; Ernest Wong,* ***Army Cyber Institute***
SALON C5-6	**Thriving in the Game: A Disucssion on How to Advance Women in Cybersecurity** *Lisa Lafleur,* ***Raytheon****; Limor Elbaz,* ***Peerlyst***
12:15pm	**CAREER FAIR CLOSES**
1:00pm - 2:30pm INTERNATIONAL SOUTH	**LUNCH, KEYNOTE, POSTER AWARDS & CLOSING REMARKS** **Poster Awards: Cheryl Whitis**,Vice President/Chief Information Officer, Information Technology, Raytheon Missile Systems **Keynote: Listening In: Cybersecurity in an Insecure Age** *Dr. Susan Landau,* ***Professor, Tufts University***
2:30pm - 4:30pm SALON C1-2	**WORKSHOP SERIES 4** **Hunting for Anomalies** *Fatima Rivera and Natalie Roe,* ***Google***
SALON C3-4	**Thinking Out of The Box: Using a Cyber Security Mindset to Escape the Room** *Suzanne Mello-Stark, Emily Hao and Maryann Vanvalkenburg,* ***Worcester Polytechnic Institute***
SALON C5-6	**Ethical Hacking Challenge** *Amanda Bondoc,* ***EC-Council***
SALON C7-8	**Profiling Cyber Adversaries (Hackers): Introduction to Cyber Intelligence** *Edna Reid,* ***James Madison University****; A.J. Nash and Ali Alison,* ***Symantec***

KEYNOTE DESCRIPTIONS

Keynote 1:
“A Career in Cyber Security in the Intelligence Sector”
Sherrill Nicely, ***Chief Information Security Officer, Central Intelligence Agency***

This talk will provide some background on how Ms. Nicely became a Cyber Security professional and Senior Leader within a very crucial public service sector of the Government. The talk will also focus on the rewarding and interesting work that CIA cyber security officers perform to protect sensitive government intelligence missions.

Keynote 2:
“The Cybersecurity Threats are Real, the Opportunity is Yours: Tips on Navigating the CyberSecurity Career Field”
Mona Bates, ***Chief Information Officer & Vice President of Information Technology, Raytheon***

Join the speaker to explore the Cyber Security landscape and how the growing threats present opportunities for aspiring professionals in the field. Mona will share tips on exploring and advancing careers in Cyber Security in the digital era.

Keynote 3:
“Men as Allies: Partnering to Advance Women in Cybersecurity”
Michele Guel and Tony Jeffs, ***Cisco****; Ben Hagen,* ***Facebook****; Douglas Maughan,* ***DHS****; Dan Shnowske,* ***FMR****; Lucas Moody,* ***Palo Alto Networks****; Allan Paller,* ***SANS****; Dr. Greg Shannon,* ***CMU****; Tony Baylis,* ***Lawrence Livermore National Laboratory***

As one of the handful of women in your organization or at a conference, you may feel like an empowered warrior or a token item. We want all represented groups to feel they are part of a community and equally respected. In our dinner keynote panel, we will hear from supporting male allies where they will share their personal stories and perspectives on the challenges faced by women who are trying to get into, or stay in a cybersecurity profession. Join us as we work with our allies to own the solution addressing diversity and inclusion in the cybersecurity industry.

Keynote 4:
“Be the Energy in Cybersecurity”
Diane M. Janosek, ***Deputy Commandant for the National Cryptologic School, National Security Agency***

During this engaging talk, Ms. Janosek will discuss her thoughts on what enables success in cybersecurity with a focus on energy and connections. She’ll highlight the women who have impacted, are impacting, and will impact cybersecurity, with an emphasis on national security.

Keynote 5:
“Listening In: Cybersecurity in an Insecure Age”
Dr. Susan Landau, ***Professor, Tufts University***

What makes us most secure? Is it enabling the police and intelligence agencies to unlock digital devices and listen to communications? Or is it securely protecting devices and communications against intrusions? In this talk, our most serious threats and what’s needed to protect against them will be discussed.

SESSION DESCRIPTIONS

WORKSHOP SERIES 1 - THURSDAY, 2:00PM - 4:00PM

“Recruiting Cybersecurity Talent: A workshop for hiring managers and external recruiters.”
*Deidre Diamond and Veronica Mollica, **CyberSN***

Cybersecurity professionals know that recruiters don’t speak the language of cybersecurity. There are 35 job categories in cybersecurity and our community posts the same five descriptions for all of our job postings. In order to attract talented candidates in a market that has several hundred thousand unfilled openings, one must understand how to market to cybersecurity professionals. This workshop will discuss ways to market your organizations career openings to recruit the best cybersecurity experts, and will conclude by drafting effective job descriptions.

“N00bSec to Cyber-Champion: Hacking the National Cyber League for Success”
*Kaitlyn Bestenheider, Elizabeth Molloy, Vincente Gomez and Andreea Cotoranu, **Pace University**; Michael Lavacca, **Bloomberg***

This workshop will focus on analyzing internal phishing and network indicators of compromise (IOCs) to find patterns for detection and blocking. The phishing portion starts with the types of IOCs that can be tracked from phishing emails, how to create a template that can be used for tracking over time, and the internal and external uses for the information. The network portion focuses on how to track network IOCs, IOC pivoting, and how use your results for detection and blocking.

“Introduction to iOS Application Security Testing”
*Dawn Isabel and Jessica Sexton, **IOActive***

This workshop will introduce fundamentals of iOS application security testing. Topics include understanding the structure of iOS application packages, App Store encryption, examining the application binary, and collecting information about the application’s attack surface, application data, location of sensitive data, and clues that indicate an application may not be handling data securely. Hands-on exercises will be conducted on sample files with provided tools.Participants will work through exercises focused on straightforward static analysis and review of application artifacts. Participants need to bring a laptop capable of running VirtualBox. No prior mobile or iOS experience is required, but attendees should be comfortable working with tools at the Linux command line.

“Threat Intelligence: Beyond the Basics”
*Rachel Giacobozzi and Breanna Laconic, **Target Inc.***

This workshop is an introduction to collegiate cybersecurity competitions through the National Cyber League (NCL). Participants will be guided through a Capture-the-Flag style Hack-a-thon using an extensive list of tips and tools that ensure success. By working through hands-on challenges, ranging from Open Source Intel to Cryptography to Network Traffic Analysis and more, participants will gain exposure to the skill sets needed to succeed in NCL. Participants will be able to keep the resources provided in workshop.

WORKSHOP SERIES 2 - THURSDAY, 4:30PM - 6:30PM

“Conducting Meaningful Research and Presenting Effectively”
*Anna Trikalinou, Lily Yang, Reshma Lal, Tania Skinner, **Intel**; Dr. Melissa Dark, **Purdue University**; Dr. Ann Cox, **DHS**; Dr. Celeste Matarazzo, **Lawrence Livermore National Labratory***

SESSION DESCRIPTIONS

This two-hour workshop will consist of a one-hour panel discussion followed by one-hour small group discussions. In the panel, notable professionals and faculty will provide their insights into the most important cybersecurity topics for research and analysis. They will also offer advice on how to conduct and present your research to different audiences, address career challenges (common or specific to a research career), highlight different career paths and the qualities that can make you stand out to advance your career. Following the panel, you will have the opportunity to personally meet and interact with the panel members, our Intel professionals and the other workshop participants in one-hour smaller group discussions. You will also be given special attention during this part of the workshop to practice your poster presentation interactively in a very supportive environment. You will receive feedback to help you prepare the right pitch for the specific audience.

"Cyber Competition to Engage and Inspire"
*Oxana Pelc and Tiffany Benjamin, **Facebook***

Cyber competitions draw people in and engage them towards cybersecurity. Want to interact with a new inclusive platform? Come play, engage, inspire and learn how to use for yourself or host your own. Did we also mention there is gonna be awesome Facebook swag and special prizes for the top players?

"Practical Network Forensics"
*Marcelle Lee, **LookingGlass Cyber Solutions**; Jennie Kam and Ellie Daw, **Cisco***

Analysis of network traffic can provide a wealth of forensic data and is an essential aspect of many fields of cybersecurity work, including incident response, security operations, and malware analysis. Artifacts obtained through network traffic analysis can reveal hacker techniques and methodology, such as use of malware, network traversal, privilege escalation, establishment of persistence, and data exfiltration.

In this hands-on workshop, the participants will use Wireshark to examine custom packet captures showing both "normal" and malicious network activity. Participants will be provided with the captures and solutions that they can apply in their own environments.

"Building a Home Lab for Malware Analysis"
*Sarah Kern and Susie Heilman, **The MITRE Corporation***

This workshop will provide a walk-through of how to set up an a home-based malware analysis lab with emphasis on best practices for constraining malware to a controlled, isolated environment. Attendees will receive an overview of popular free tools (Procmon, Process Explorer, Regshot, and more) and instruction on how to customize and maintain the environment after initial configuration. There will be opportunity for hands-on experience with behavior monitoring tools and examples of the fundamental artifacts that shed light on malware functionality. All experience levels welcome! Laptop with VirtualBox installed is required. A Windows 7/10 ISO or similar is recommended, though not required.

WORKSHOP SERIES 3 - FRIDAY, 3:45PM - 5:45PM

"Teaching Cyber Ethics and Societal Impacts in Introduction Computing Courses"
*Dr. Yesem Kurt Peker, **Columbus State University**; Dr. Florence Appel, **St. Xavier University***

This workshop is a hands-on faculty development session introducing the Catalyzing Computing and Cybersecurity in Community Colleges (C5) project. The workshop will present modularized content, lecture materials, active learning exercises, and assessment questions that can be integrated into existing computing courses. Workshop participants will need a WiFi-enabled laptop to download the instructional module and gain access to VirtualBox and an Ubuntu image. All seven instructional modules carry a creative commons license for adoption and adaption, and are available for free download from https://c5colleges.org/index.php/cs-course/module-downloads.

“Adventures in Cyberspace: Cyber Security Literacy for K-12 and Beyond”
*Julie Rursch and Tracy LaVan, **Iowa state University***

At Iowa State University, we are embarking on an adventure that few have attempted. We want to share cyber security with all ages and in a way in which they can apply it in their daily lives. In this hands-on workshop, we will share materials from our college course, high school curriculum, video modules and CyberToons, professional development, and our upcoming online lab. All materials are available to instructors free of charge and the participant will leave with access to web sites, printed materials, open-ended and discussion questions, and curricular ideas that can be modified for all ages. Materials are based on information presented in Computer Security Literacy: Staying Safe in a Digital World by Douglas Jacobson and Joseph Idziorek. Resources can be found here: http://www.security-literacy.org/

“Hacking Discourses - Exploring Feminist and Critical Theory through Cybersecurity”
*Nathan Fisk, **Florida Center for Cybersecurity**; Felice Flake, **ScySec LLC***

Finding yourself all too frequently charged with “convincing” resistant students or colleagues that diversity in cybersecurity matters? Stereotypically privileged cybersecurity dudes got you down? Just want to know a little more about feminist social theory? This workshop will explore the intersections between cybersecurity and feminist theory, from hacker history and critical pedagogy to penetration testing and standpoint epistemology. The workshop will provide participants with tools and concepts for deconstructing and resisting the more oppressive elements of cybersecurity culture. As such, this workshop will be broadly applicable for multiple roles and positions within the field of cybersecurity, although will likely be most useful for educators and professionals in training or communications roles.

Skills and Inspiration for Career Journeys in Cybersecurity
Panelists: *Cheryl Whitis, Kathy Frain, Kathy O’Donnell, Mary Ann Waddick, and Jordan Miller, **Raytheon**;*
Facilitator: *Felicia Jackson, **Raytheon***

Thinking of a career in cybersecurity? This workshop will share with you 6 (six) multi-generational testimonials from people just starting in a cyber career through senior cyber leadership. This workshop will also discuss the skills required for your transition into the cybersecurity world. We hope this may inspire you to your own pathway. This workshop will be a very interactive workshop that includes a speed-networking portion to allow for Q&A and personal networking opportunities!

WORKSHOP SERIES 4 - SATURDAY, 2:30PM - 4:30PM

”Hunting for Anomalies”
*Fatima Rivera and Natalie Roe, **Google***

Security leaders need to understand their network and have the ability to identify anomalies in traffic that could indicate an active, persistent or past threat. This workshop will introduce the concept of threat hunting. Various hunting techniques and tools will be discussed and the workshop will culminate with a hands-on exercise. Attendees will get first-hand lessons-learned from Google security leaders and understand how to apply the practices at their own organization

SESSION DESCRIPTIONS

"Thinking Out of The Box: Using a Cyber Security Mindset to Escape the Room"
Suzanne Mello-Stark, Emily Hao and Maryann Vanvalkenburg, ***Worcester Polytechnic Institute***

Cyber attacks succeed when resources are exploited and used in a manner contrary to their intended purpose. A cyber security specialist needs to think like an attacker to apply effective defensive strategies. Escape rooms challenge participants to interact with their surroundings to uncover clues. Additionally, puzzles are designed in such a way that participants must work together to find the solution. This workshop introduces an escape room focusing on teaching fundamental principles of cyber security. Participants will learn how an escape room is designed and will be given materials to create their own escape rooms. Participants will also have the opportunity to demo a real escape room. No formal knowledge of cyber security is required.

"Ethical Hacking Challenge"
Amanda Bondoc, ***EC-Council***

This hands-on workshop will demo modules in the Certified Ethical Hacker certificate program, including sniffing and hacking wireless networks. Each participant will need a laptop with internet connection and the participants will be presented with a competition challenge. The participant who completes the challenge first will receive a choice of certification package. The package will include eBook, video lectures, iLabs, and testing voucher. The package is valued at $1899.00. All participants will receive access to iLabs for each session participant (30 Day Access).

"Profiling Cyber Adversaries (Hackers): Introduction to Cyber Intelligence"
Edna Reid, ***James Madison University****; A.J. Nash and Ali Alison,* ***Symantec***

Cyber intelligence (CYI) is an emerging specialization focusing on the analysis of cyber threats and cyber adversaries to support decision making about cyber security defense and risk management. Profiling and analyzing cyber adversaries are skills that cyber analysts and/or cyber intelligence professionals develop. This workshop introduces strategies and tools that organizations use to conduct cyber threat intelligence as well as how to profile cyber adversaries to identify their motivations, cyber attack patterns, geopolitical situations, and other activities that can be used to help in anticipating their actions. We will conclude with team-based activities such as profiling cyber adversaries and participating in a Symantec cyber analytical challenge.

LIGHTNING TALKS - FRIDAY, 8:30AM - 10:45AM

"Cyber Political Engineering - Mother of ALL Cyber Attacks"
Kavya Pearlman, ***Linden Lab***

Many people struggle to make sense out of what happened in the 2016 US Elections. The social media events of 2016 were so unique that we needed a new term to define and identify the impact, Cyber Political Engineering. The impact of Cyber Political Engineering will be discussed as well as solutions to address it.

"NSA Day of Cyber Program Partnership with WiCyS"
Kim Paradise, ***Life Journey***

Learn about the partnership between WiCyS and the NSA Day of Cyber Online Cyber Career Exploration Platform to bring the NSA platform to WiCyS student chapters and other educational institutions across the country in an effort to inspire more young women to pursue a career in cybersecurity. You will learn more about the NSA Day of Cyber experience, how to use it and how you can set up a customized Day of Cyber challenge in your school, camp, or WiCyS student chapter.

SESSION DESCRIPTIONS

"What are Apprenticeships?"
*Carolyn Reinick, **Department of Labor***

Apprenticeship programs have the ability to have a powerful impact on the field of cybersecurity. This talk will discuss how apprenticeships have been extended into this field and the benefits for employees and employers.

"Hacking the Law: The Legal Terms of Bug Bounties Explored"
*Amit Elazari, **UC Berkeley School of Law***

Bug Bounty programs allow security researchers to legally trade newly discovered vulnerabilities for monetary and reputational rewards. This practice of organizations inviting individual hackers to perform penetration testing is becoming a popular in cybersecurity and is expanding across industries and governemnt agencies. But who dictates the rules of this emerging "bug bounty" economy? Ultimately, the terms of the programs are prescribed by the rewarding companies and intermediary "hackers'" platforms, using unilaterally drafted "take-it-or-leave-it" terms. This talk will discuss the pitfalls security researchers should beware of in light of recent developments in anti-hacking laws, but also which terms they should demand to see to ensure "authorized access" and minimize their legal risks.

"Watson for Cybersecurity and IBM's Cyber Range"
*Alison Ritter, **IBM***

Companies have runbooks prepared for incident response but when the runbooks are put to test in a live event like cyber-attack, the results can be startling. IBM introduced the world to the industry's first commercial cyber range, the IBM X-Force Command Center in Cambridge, Massachusetts. This presentation focuses on how teams from across the organization are immersed in a real-life cyberattack and not only help to identify an attack but also how to effectively respond."

"Investing in Your Professional Network"
*Tolu Onireti and Nana Ahwoi Larson, **Ernst and Young***

Exposure to a reliable professional network is key to career advancement. As noted by Nora Denzel "It's not who you know or what you know, it's about who knows what you know". With the vast array of tools and media available to create and maintain a network, cybersecurity professionals as well as other professionals are under investing in their professional network. During this session, Nana and Tolu will have a candid interactive discussion with the audience on networking challenges, myths about networking and practical approach to developing and maintaining a strong professional network.

"Malice in Wonderland"
*Preethi Josephina Mudialba, **Carnegie Mellon University***

The game titled "Malice in wonderland" is an educational tool meant to help user learn about the following types malicious software: computer viruses, worms, trojans, adware, keyloggers, backdoor attack and Rootkit and the security measure that can be taken to protect devices from malicious software. We will discuss how this tool helps users understand that viruses are just one type of malicious software. More importantly, we will discuss how the tool also highlights the fact that different security measures need to be taken to protect against different types of malicious software.

SESSION DESCRIPTIONS

LIGHTNING TALKS - SATURDAY, 8:30AM - 10:15AM

"Bananapeelbot: The Gamification of Corporate Security"
*Carla Sun, **SurveyMonkey***

How do you balance keeping people on their toes about security, while still positively contributing to the culture and expectations of your growing company? What happens when they slack on security? This talk will discuss using gamification to empower hawk-eyed co-workers to spot security vulnerabilities such as unlocked computers. This talk will discuss the feedback loop that ultimately helped improve the security habits of my coworkers.

"From Pre-Nursing to Pen Testing"
*Shea Mchugh, **Intrinium Inc.***

Breaking into cybersecurity can be a difficult process, especially when you start college as a Pre-Nursing major. Shea McHugh will outline the process that brought her into the cybersecurity world, focusing on her time in the SANS Women's Academy and the challenges and triumphs she faced along the way. As an inaugural graduate of the SANS Women's Academy, she completed 3 GIAC certifications in 8 months and landed a Security Analyst job before the end of the program. Now she works full time in cyber security and helps mentor women who are going through the same program that gave her the tools she needed to get started in this wildly fascinating and constantly changing career field. If you are interested in breaking into cyber security, or would like to learn how more women can get into cyber security, this is the talk for you.

"Turning "I'm not qualified into "I'm a great fit for this job"
*Roselle Safran, **Rosint Labs***

It is not uncommon for an aspiring cybersecurity professional to read a job description and feel underqualified or unprepared for the work. But there are plenty of opportunities that are suitable for individuals who are new to the field. This presentation will discuss some of the tricks of the trade when it comes to cybersecurity job applications. Topics covered will include what hiring managers look for in new hires, what types of junior and senior jobs are available, how to build the skill set needed for your first cybersecurity job, how to create a standout resume, and how to identify potential opportunities that will move your cybersecurity career in the right direction.

"When a Picture is Worth a Thousand Alerts"
*Aditi Chaudhry, **Capital One***

There have been over 200 attacks on major industrial control systems since 2013. At a time when cyber risk is at an all time high, how can a company protect itself? Visualizing cyber threat data can help characterize, prioritize and communicate cyber risks for an enterprise. By creating a cyber risk dashboard, a company can see their current cybersecurity posture, describe their target state for cybersecurity, identify and prioritize opportunities for improvement, assess progress towards the target state and communicate risk among stakeholders. This talk provides an overview on how data-visualization of cyber risk can help drive action to mitigate enterprise risk.

"Build Me a World Class Security Program in Three Months"
*Christie Terill, **Bishop Fox***

Building a security program (staffing, processes, vendors, metrics) is a tough challenge many of us unfortunately inherit. Using my own personal experience as a case study, I will share the lessons learned during a 9-mouth joint client-consulting effort to transform and grow a security program at a healthcare provider. This presentation will give you actionable tips on how to navigate the expectations of executives, of the existing team, and of the new team members who join your organization.

"Between you, me, and the Board of Directors (BOD): How to gain BOD support for your cybersecurity program and live to tell the tale"
Lena Singer, ***Independent***

Board of directors are concerned about potential lawsuits from shareholders and fines from regulators in regard to cybersecurity incidents. Many regulatory agencies, such as the Federal Trade Commission (FTC) and Securities and Exchange Commission (SEC), have made strong public statements to that effect and followed up with enforcements against entities that failed to take appropriate steps to safeguard data. Directors need actionable advice. They need senior-level executives to understand and frame cybersecurity issues appropriately in order to inform boardroom discussions about cybersecurity. Chief Information Security Officer (CISO) or a cybersecurity lead plays an important role in enabling a strategic approach to cyber risk oversight by the board by providing answers and supplying just the right amount of data.

"WiCyS Student Chapters: How to Create and Sustain a Chapter"
Dr. Vitaly Ford, ***Arcadia Unversity;*** *Dr. Masooda Bashir,* ***University of Illinois at Urbana-Champaign***

Learn about how Women in Cybersecurity (WiCyS) student chapters can be established at 4 year Universities with support and guidance from the WiCyS organization. With your help, WiCyS student chapters can empower more students to pursue cybersecurity careers by providing support, mentorship, training and network opportunities, and access to industry leaders.

DISTINGUSED SPEAKER PRESENTATIONS - FRIDAY, 12:00PM - 12:45PM

"Bridging Cybersecurity Research and Education"
Dr. Susanne Wetzel, ***National Science Foundation***

Given the interdisciplinary nature of and ever changing challenges in Cybersecurity, continuously "building bridges" in some fashion is a must. In this talk I will highlight some of the activities I have engaged in: bridging mathematics and computer science, bridging theory and practice in research, bridging education and research, or bridging industry, academia, and government service.

"Cyber Security Research: A Data Scientist's Perspective"
Dr. Celeste Matarazzo, ***Lawrence Livermore National Laboratory***

As all aspects of our lives become increasingly dependent on computing networks and the Internet, cyber security has grown from a localized economic problem to a major national imperative. Situational awareness of computer networks presents many challenges including but not limited to the volume of the data and the dynamic and evolving nature of the problem space. For example, at the perimeter of a corporate enterprise computer network, it is common to see terabytes of network traffic each day, containing millions of unique IP addresses and connection records that number in the hundreds of millions. Celeste will provide an overview and discuss recent trends facing computer security researchers and practitioners. She will describe recent work at Lawrence Livermore National Laboratory to enable analysis of computer networks. Characterizing network-wide activity depends critically on understanding time-varying patterns of system behaviors, such as the actions and connections between components. This approach makes use of state of the art data collection, building and accessing largescale graph representations, and new capabilities and advances in data science and machine learning.

SESSION DESCRIPTIONS

“Leadership in Cybersecurity: Pathways and Strategies for Success”
*Dr. Deanne Cranford-Wesley, **Forsyth Technical Community College**; Dr. Margaret Layton, **Symantec**; Yabing Wang, **Alight Solutions**; Marian Merritt, **National Institute of Standards and Technology***

This panel discussion will bring together industry, government and academic cybersecurity leaders who will share their career pathways toward leadership and strategies for success. Panelists representing diverse perspectives across academia, government and industry will discuss challenges and opportunities for leading cybersecurity initiatives, and their roles in advancing cybersecurity education and practice. The session will highlight leadership pathways and future initiatives in cybersecurity.

DISTINGUSED SPEAKER PRESENTATIONS - SATURDAY, 10:30AM - 11:15AM

“Building a Culture of Cybersecurity: Innovative Strategies, Leadership Pathways and Future Directions”
*Dr. Eman El-Sheikh, **University of West Florida***

As cyber threats continue to increase in complexity and intensity, the cybersecurity workforce continues to lag behind. The number of unfilled jobs is projected to reach 3.5 million and cyber crime damage will cost $6 trillion annually by 2021. Now more than ever, we need to build a cyber-secure and aware culture. Dr. El-Sheikh will discuss challenges, current initiatives and opportunities for advancing cybersecurity education and practice and building a culture of cybersecurity. The session will highlight innovative strategies, leadership pathways and future directions in cybersecurity.

“Securing the Digital City: Cyber Threats and Responses”
*Quiessence Phillips, **New York City Cyber Command***

Speaker will discuss securing one of the largest digital cities and its latest work in pioneering a data-driven approach to cybersecurity for the City’s information assets -- building on New York City’s reputation as a technology leader and therefore as a cybersecurity leader. As information technology evolved and proliferated throughout NYC government agencies, the City of New York understood the need to establish a centralized entity responsible for managing Citywide cyber risk. At the same time, the cyber threat landscape has evolved rapidly and now includes destructive malware that can spread worldwide in a matter of hours, potentially disrupting government and business service delivery in the world’s largest cities. The only way to counter attacks that spread at machine speed is to build defenses that can move just as quickly, emanating from a strong, centralized, authoritative body. New York City Cyber Command (NYC3) is a new cybersecurity organization for the City of New York that works across more than 100 agencies and offices to prevent, detect, respond, and recover from cyber threats.

“Security Must Reflect Those We Protect”
*Aanchal Gupta, **Facebook***

The cybersecurity industry needs to be more reflective of the people we aim to protect. As a director of security at Facebook, I’m in a position to help more than 2 billion people feel safe while using our service. I have learned that hiring a team of people proficient in the same exact skill is not as good as building a team with different genders, ethnicities and capabilities. Learn how Facebook is inspiring younger generations, and how you can too.

SESSION DESCRIPTIONS

TECHNICAL PRESENTATIONS - FRIDAY, 2:15PM - 3:00PM

”Cyber-Arcade: An Innovative Approach to Promote Cybersecurity and Engage Women to Pursue STEM Careers”

Pauline Mosley, Dawn Tucker, Li-Chiou Chen and Andreea Cotoranu, ***Pace University***

Recognizing the urgent need to expand the cybersecurity workforce, particularly underrepresented groups, Cyber-Arcade was created to engage women and minorities in cybersecurity. Cyber-Arcade is designed to engage and recruit high school students to explore the concepts of cybersecurity through a set of five challenges: cyber jeopardy, raspberry pi puzzle, cryptography with cipher wheel, mini-drones, and password strength and promote STEM awareness and cybersecurity interest while developing problem solving, critical thinking, and communication skills. Cyber-Arcade is a one-day workshop specifically for high school students with an emphasis on young women and minorities. Information on recruitment and joining the program will be presented.

“Data Spillage Remediation Techniques in Hadoop”

Sunanda Mani and Srinivas Jantali, ***Northeastern University***

Hadoop is java-based open source programming framework that aids in the processing and storage of big data sets in distributed computing environments. Data Spillage is a common problem that plagues Hadoop. Data Spillage is a condition where a data set of higher classification is accidentally stored on a system of lower classification. When deleted, the spilled data remains forensically recoverable. This presentation proposes three approaches to eliminate such risk. In the first approach, the spilled data is securely overwritten with zero and random fills multiple times at the OS level, to render it forensically irretrievable. In the second approach, the Hadoop inbuilt delete function is enhanced to implement a secure deletion mechanism. In the third approach, the hard drives of the data nodes which have spilled data is replaced with new ones after destroying the old drives. The evaluation of each approach will be discussed.

“Twitter Spam Detection based on Self-taught Learning and Sparse Auto-encoder”

Lijie Zhou and Hao Yue, ***San Francisco State University***

Twitter spam is a critical problem that is a challenging to solve. Prior reserach has focused on machine learning to solve this problem, however we propose deep learning. In this technical presentation, a deep learning approach to solving twitter spam and feature selection for social media will be discussed. We compared our strategy with the traditional machine learning feature selection method results will be presented.

TECHNICAL PRESENTATIONS - SATURDAY, 11:30AM - 12:15PM

”Ethical Thinking in Cyber Space Curriculum Development”

Jane Blanken-Webb, Imani Palmer, Masooda Bashir, ***University of Illinois at Urbana-Champaign***

Innovative approaches to cybersecurity education are needed to equip these next generation professionals who are technologically savvy, ethically minded, and capable of meeting the heavy burden of responsibility that comes with increased technological skills and access to sensitive data. This presentation will introduce core ideas driving a curriculum development project funded by the NSA entitled: Ethical Thinking in Cyber Space. This case study based curriculum immerses students in real-life ethical dilemmas inherent to cybersecurity and engage them in open dialogue and debate within a community of ethical practice.

SESSION DESCRIPTIONS

"The Gapless Air Gap"
*Rachel Schmierer-Davis, **Johns Hopkins University Applied Physics Laboratory***

Air gapped systems are desiged to physically isolate networks from other unsecured networks, such as the Internet. In theory, an isolated network would be unreachable by a cyber attack. Often, these networks lack a management team to protect against known threats. The little known secret is that air gapped systems are not air gapped, and are therefore, not protected. For starters, data transfers and software updates are intentional breaches of the gap. In other cases, systems that are otherwise considered air gapped might receive RF input, or utilize Bluetooth or RFID capabilities. This talk will highlight known issues with air gapped systems and discuss ways to counteract them.

"The Missing Link between Blockchain and Privacy"
*Parisa Kianmajd, **Intel***

Blockchain is an emerging technology for decentralized data sharing in a network of untrusted parties. Blockchain is synonymous with Bitcoin but it's applications go far beyond cryptocurrency to smart contracts, supply chain management, and to the Internet of Things (IoT). Blockchain enables trust to be more transparent by making the transactions' provenance public but this comes at the expense of users' privacy. During this presentation, the fundamentals of blockchain privacy will be discussed, along with a solution of applying a cryptographic layer over the blockchain to mitigate the privacy risks which allows users to control their data. Preliminary results on using blockchain for coordinating actions in a smart community in a privacy-preserving manner will be discussed.

PANEL PRESENTATIONS - FRIDAY, 5:45PM - 6:30PM

"Securing the Nation: How NSA is Working to Improve Cybersecurity Education"
*Blair Taylor, **Towson University/NSA**; Steve LaFountain, Tina Ladabouche and Karen Leuschner, **NSA***

A critical piece of addressing the global cybersecurity challenges is building a diverse cyber-skilled workforce. Towards that goal, the College of Cyber at the National Security Agency (NSA) is leading several important initiatives to improve national cybersecurity education. In this session, representatives for the College of Cyber will discuss the following programs: GenCyber, the National Centers of Academic Excellence, and the National Cybersecurity Curriculum Program.

"Oopsie: The Saga of Accidental Awesomeness"
*Prajakta Jagdale, Muoi Landivar, and Jen Miller-Osborn, **Palo Alto Networks**; Joy Forsythe, **Mango Health**; Morgan Bjerke, **Booz Allen Hamilton***

Dont't be afraid of making mistakes. Hear from successful women about their encounters with mistakes, big and small. The panelists will discuss how mistakes can actually lead amazing solutions or technological breakthroughs. They will talk about blunders they have made and how they managed to transform some of them into success stories. The audience will walk away knowing that it's ok to stumble every once in a while.

"Diversity in Cybersecurity: An International Perspective"
*Keenan Skelly, **(USA),** Monica Zhu (**Australia**), Laura Payne (**Canada**), Isabelle Landreau (**France**), and Susana Mejido (**Spain**)*

The panel will discuss the state of cybersecurity affairs overseas. France, Spain, Australia and Canada will be represented in the panel and diversity initiatives will be discussed.

SESSION DESCRIPTIONS

BIRDS OF A FEATHER - SATURDAY, 12:15PM - 1:00PM

Joining the Game: A Discussion on Approaches to Recruite Women into Cybersecurity
*Yesem Kurt Peker, **Columbus State**; Rae-Kelly Hamilton, **United States Naval Academy**; Paula Fetterman, **Financial Services Information Sharing and Analysis Center**; Marla Lamont, **Tractor Supply***

Building a strong cybersecurity workforce for our increasingly digital world requires cultivating students at all levels and skill-sets. How are we empowering minds for the future? This BoaF session will spark a discussion about current efforts to introduce and refine cyber and computing skills within the body of tomorrow's security leaders through providing experience, exposure, mentorship, and the vast network integral to success in our collaborative field. Representatives from non-profits, educational institutions, and industry will discuss their outreach efforts to build tomorrow's cybersecurity workforce. We strive to inspire attendees to either implement similar programs in their environment or participate in one of the existing efforts.

Staying in the Game: Challenges and Solutions to Retain Women in CyberSecurity
*Caryn Truitt, **Highline College**; Ernest Wong, **Army Cyber Institute***

Once women get into tech, how do we retain them in the cyber security workforce? Studies have shown that the there is a "quit rate twice as high for women as men" (Catherine Ashcraft, 2016). There are many challenges women face in the workplace. How do we remedy this? Through the ideas, thoughts, and opinions of all who attend this session, our hope is that we can collectively come up with even better ways to change the future. To start with how we can improve women's retention rates in cyber security, Caryn Truitt, Cyber Security student, former Operations Manager and business owner, will supply resources for women including information about a new non-profit called Project Include that has a mission to give everyone a fair chance to succeed. Ernest Wong, a Military Intelligence Officer in the US Army and a research scientist at the Army Cyber Institute, will share how the US Army is working to attract and retain women to help improve our nation's cyber security posture and win in 21st Century warfare. We are all ears to hear your thoughts on the issue!

Thriving in the Game: A Disucssion on How to Advance Women in Cybersecurity
*Lisa Lafleur, **Raytheon**; Limor Elbaz, **Peerlyst***

In this BoaF session, you will learn tips to thrive in cybersecurity, advance in your career and develop a great work-life balance. You will learn about available resources to advance your career, gain new skills and network like a pro. Every new person you meet is an opportunity to open a new door, learn about ways to build your network to thrive in cybersecurity. https://www.peerlyst.com/

POSTER DESCRIPTIONS

#1 - A Two-Phase Think-aloud Exploration on Usability and Acceptability of FIDO U2F Security Key

*Sanchari Das, Gianpaolo Russo, Andrew C. Dingman and L. Jean Camp, **Indiana University Bloomington***

What are the limitations when it comes to acceptability of Two-Factor Authentication (2FA) and why do individuals choose to use weaker and possibly more difficult passwords? We sought to answer this by implementing a two-phase think-aloud exploration on the usability and acceptability of the Yubico Security Keys. Despite them being among the best in class for usability, participants still encountered several difficulties. Based on the halt and confusion points identified in the experiment, we proposed design changes, some of which Yubico adopted. After a year we repeated the experiment and found increased ease of use but cannot confirm any corresponding increase in acceptability. Since the primary halt points were attenuated to a considerable extent, we could identify the principal remaining reasons for rejecting 2FA which lied anywhere from personal preferences to poor perception of risks. Participants believed that their passwords were strong enough and that their accounts were sufficiently secured by their own acumen. We further suggested future recommendations to enhance usage of Yubico Security Keys and to provide improve user security and remove incorrect risk perception.

#2 - Exploring Child Data Risks With Smart Toys

*Olivia Kenny, Sanchari Das and Jean Camp, **Indiana University***

In the internet era, in addition to the physical safety of a child one should also be aware of the safety of their data, what is being recorded, and who is monitoring them. IoT devices, like the Fisher Price Smart Toys which are designed to play with children of ages 3-8 and entertain them with various activities, have expanded into children's toys. Parents or guardians may choose to connect to the parent app of the bear; which would then give the parent ultimate control over the toy through Bluetooth or Wi-Fi as the application picks. This possesses various threats if a malicious actor is controlling the toy and can lead to devastating results. The Bear not only has the ability to listen to a child's speech but also has the ability to recognize the images of its associated cards. We examined the potential of the toy's camera and noted that it has the ability to read a very blurred bright image but was unable to comprehend a blurred dark image even if kept within a range of 4 inches. To analyze further, Bluetooth scanning was performed and we noted the bear is communicating through Bluetooth. We wish to explore further to understand the extent of such communication since a previously observed vulnerability showed uploading of unencrypted child data in the cloud; this was patched by the company later. However, we still expect The Smart Toy to be vulnerable to attacks such as- the Man in the Middle attack since these devices have the potential to be recording information and can constantly transmit information to the cloud.

#3 - Privacy preserving Cloud-based Quadratic Optimization

*Andreea Alexandru, Konstantinos Gatsis and George Pappas, **University of Pennsylvania***

This work proposes a protocol for privately solving constrained quadratic optimization problems with sensitive data. The problem encompasses the private data of multiple agents and is outsourced to an untrusted server. We first consider the case when only a part of the data in the problem belongs to the agents and the rest is public and work towards the case when all the data in the problem is private data of the agents. Firstly, we describe the desired security goals and investigate the information leakage from duality theory. Then, we present an interactive protocol that achieves the solution of a strictly quadratic convex optimization problem with private cost and private linear inequality constraints, by making use of partially homomorphic cryptosystems to securely effectuate computations. Furthermore, we provide extensions to the protocol in order to also consider equality constraints and to obtain a speedup of the performance.

POSTER DESCRIPTIONS

#4 - Multilevel Data Concealing Techniques Using Steganography and Visual Cryptography

Chaitra Rangaswamaiah, ***California State University-Fullerton***

Steganography is a data hiding technique which uses images, audio or video as a cover medium. Now cryptography has become an essential part of security. Image Steganography is one such way to hide secret messages in an image to reduce vulnerability to cryptanalysis. We are overcoming the drawbacks of using only textual steganography as it is easier to intercept and decipher. We are encrypting the plaintext with a randomly generated key using XOR and One Time Pad(OTP) Algorithm and in turn embedding it into the Least Significant Bit(LSB) of the cover image. To enhance and ensure security we use visual cryptography along with image scrambling. Image scrambling is a technique in which the location of pixels is scrambled to provide extra protection to the stego image. Visual cryptography is a method used to encrypt the visual information by breaking it into shares. We embed the ciphertext in LSB of the pixels of the cover image to form stego image. This stego image is further broken into shares using visual cryptography. Using both image scrambling and visual cryptography makes the system not only more secure but also difficult to decrypt. A decryption algorithm for the same is also constructed in this paper. The proposed system checks the performance of the system by analyzing the Mean square error and Peak Signal Noise Ratio parameters.

#5 - Wearable Internet of Medical Things Security: Stakeholder’s Perspective

Swapnika Reddy Putta and Abdullah Abuhussein, ***St. Cloud State University***

Internet of medical things(IoMT) is a fast-emerging technology in healthcare with a lot of scope for security vulnerabilities. Like any other internet connected device, IoMT is not immune to breaches. These breaches can not only affect the functionality of the device but also impact the security and privacy(S&P) of the data, which can be devastating as well as life-threatening. According to a survey by HIMSS (www.himss.org), two-thirds of healthcare organizations experienced a significant security incident in recent past. Many researchers, manufactures, and regulatory authorities have recognized the importance of this problem and started serious steps towards ensuring (1)the protection of patient health information and (2)compliance of medical devices. Stakeholders of IoMT(i.e., Healthcare practitioners and patients) focus more on the functionality and performance of the device but often overlook the S&P issues associated with these devices. In most cases, the reason to overlook these security issues is due to lack of proper awareness. The proposed methodology uses a stakeholder-centric approach to improve security of wearable IoMT devices. The novelty of this work lies in that it defines security according to every stakeholder’s interaction with the wearable IoMT device. This approach assists stakeholders with different requirements, goals, and tolerance to risk manage issues that arise from stakeholders’ conflicts of interests broadly and thoroughly.

#6 - A Comparative Social Media Pilot Study: Are applications with self deleting features the new preference?

Vibha Iyengar, Audasia Ho, Gabe Hobeika, Yuankun Li and Eileen Jiang, ***Carnegie Mellon University***

Applications designed for Social Media that use Self-deleting features allow users to post content that automatically gets deleted after a certain amount of time, as opposed to more traditional applications that keep content online by default. This study focused on how applications that have Self-deleting features affect users’ decisions to post certain content. We narrowed down our study to compare Snapchat, a popular social media application with a default Self-deleting feature for all its content, and Facebook, another widely used application that permanently keeps content online. In this two-part study, the first part looks at user decisions to post content given various scenarios, and the second part tests their ability to control their privacy settings. Our results suggest that most users feel more secure about content posted to applications with Self-deleting features, leading them to trust them more and share more compromising content.

POSTER DESCRIPTIONS

#7 - World building in vSphere to create a mockup for Investigations and Trial

Vanessa Primer, ***Highline College***

This was a multi-quarter, multi-class project to purpose build a world and networks that could be investigated as preparation for a mock trial run in conjunction with legal students. Then also being one of the participants in the Investigations and Trial stage. Our Data Recovery and Forensics Specialist program has a series of computer forensics classes that culminate in taking a 3rd Computer Forensics class concurrently with a Legal class on Computer Search and Seizure. This is a partnership class set where we work with paralegal and legal students to run a full quarter long mock trial scenario including the investigation leading up to the trial. To make this a better experience for those students (who will eventually be us); we had a multi quarter team Honors Project where we set up a network, the scenario, and played out the evidence creation organically over nearly 6 months. We set up the case to eventually be investigated and tried. Then I was able to also participate in the computer forensic evidence gathering and investigation, as well as the “trial”.

#8 - Security Implications of Connected Vehicles

Grace Mcpherson and Li Yang, ***University of Tennessee Chattanooga***

By 2020 there will be ten million user-operated autonomous vehicles on the road. Since these cars have a human driver we tend to forget the vulnerabilities about the new attack surfaces created by these autonomous features. These semi-autonomous vehicles, along with emerging fully self-driving cars, have many weaknesses when it comes to cybersecurity. Gray hats and black hats are already demonstrating that vehicles with one or two autonomous features are vulnerable and can be manipulated, attacked, or stolen. Research and development departments are working to prevent theft of parked vehicles, but little research has been done on protecting vehicle-to-vehicle communication of active cars. In my research, I am looking into the vulnerabilities of connected vehicles particularly remote attack surfaces such as Bluetooth, radio, telematics, GPS, and other vehicular sensors. Attacks including spoofing, tampering, and denial of service are major threats to the Vehicular Ad-Hoc Network (VANET) and the connected vehicles that communicate in such a system. Investigation of connected vehicles and their cybersecurity implications is paramount if autonomous vehicles are going to be accepted.

#9 - Authentication At Hogwarts: Lessons in Security Usability From the Wizarding World of Harry Potter

Ann-Marie Horcher and Michele Bartosek, ***Central Michigan University***

The Harry Potter book series by J.K. Rowling has been both a literary and cultural phenomena, changing the rules of book marketing and reaching an unprecedented audience of readers worldwide. Beyond the obvious use of the series to instruct on literature, Harry Potter has been successfully used to teach mathematics, politics, psychology, and even foreign languages. An examination of the seven Harry Potter books reveals a wealth of examples of usable security best practices and failures that could be used in security awareness education. Non-expert computer users do not typically receive formal security education. Updates through the media don’t translate to informed decisions because the users lack a theoretical grounding to absorb the complex topic. Research on the use of folk models to communicate security information has revealed stories are a powerful source of security information. The sources of the informal information exchange are trusted and the concepts are expressed in an entertaining fashion which makes the information easy to recall and understand. Security advice dispensed by relatable characters in television shows was shown to be an effective teaching tool. Folk models and fairy tales are also used to communicate complicated usable security technology concepts. The research study tracked the impact of the Harry Potter examples to teach cybersecurity.

POSTER DESCRIPTIONS

#10 - Exploiting Hardware Return Policies to Implant Malware on Consumer Devices

Raissa Engelhard and Jo Needleman, ***Cal Poly Pomona***

The purpose of this poster is to test return policies of major retailers and manufacturers to determine whether devices are properly reset and validated before being resold to consumers. Unlike computers, consumer electronics (routers, cameras, and similar products) are considered appliances and have different policies for returns. If retailers that fail to follow the proper procedures when refurbishing electronic devices, consumers may be put at risk. Devices could be infected with R.A.Ts (remote access Trojans) or implanted with code to capture information and send it back to hackers. To determine the risk attempt would be made to test this theory by purchasing routers, returning, tracking the device via DNS updates. If successful, it could identify potential flaws within store Return policies that could put the consumer at risk. In addition to evaluating policies, we evaluate devices purchased from several consumer-to-consumer stores to see if data is stored on the devices.

#11 - Perceptions of Geo-Privacy Among Smartphone Users

Carrie O'Connell, Kristina Sawyer, Maitrai Kansal, Manaswi Karra and Unaiza Faiz, ***University of Illinois Chicago***

This study explores the relationship between user perceptions of risk and actual behavior regarding geolocation privacy. The primary focus is to understand how location-aware scenarios impact user attitudes towards and engagement with LBS-supported applications. Recent research involving location-aware scenarios indicates that user attitudes towards location services are negatively impacted by awareness, yet whether behavior changes once awareness is attained is less clear. This paper builds upon existing research concerning location-aware scenarios and expectations for privacy in order to understand the gap between user perceptions and actual behavior. Lastly, this work seeks to provide theory-informed best practices for alerting users to location-aware scenarios that provide the user more control.

#12 - SPAAS - A tool to mitigating cross-site scripting vulnerabilities by implementing security patterns

Priya Anand, ***Penn State***

Security patterns are solutions for a recurring security issues that can be applied to mitigate security weaknesses in a software system. When an appropriate pattern is identified as a potential solution by a software professional, applying that pattern and its level of integration is purely dependent on the software experts' skill and knowledge. Also, adopting the security pattern at an architectural level may be a time consuming and cumbersome task for software developers. To help the software developers' community by making this pattern implementation to be a relatively easy task, we developed a tool - SPAAS – Security Patterns As Architectural Solution, that would automate the process of implementing the selected security pattern in the software system at an architectural level. Our tool was developed to assess potential vulnerabilities at an architectural level and possible fixes by adopting security patterns. We demonstrate the use of our tool by conducting a case study on an open-source medical software, OpenEMR, to point out the vulnerable source codes in the system that have been missed by some generic vulnerability assessment tools. Using our tool, we implemented the input validation pattern as a solution to mitigate cross-site scripting attacks. We analyzed OpenEMR software that has 12318 lines of codes. Our experiment on OpenEMR software to identify codes that are vulnerable to XSS attacks took 2.08 seconds, and reported the presence of 341 lines of vulnerable codes. We used our tool to implement input validation pattern on those 341 lines, and we could successfully implement the patterns in 2.28 seconds at an architectural level. Without a deep understanding of security patterns, any software professional can implement the security pattern at an architectural level using our proposed tool, SPAAS.

POSTER DESCRIPTIONS

#13 - Cybercrime Economics

Rachel Porter, ***University of Tulsa***

Cybercrime is one of the costliest threats companies are currently facing. I have examined previous cyber incidents and their costs, as well as looked at statistics of cybercrime between industries. My goal is to spread awareness to organizations about the cyber threats they face and the most cost-efficient way to lessen the impact if they become victim to an attack. It is vital companies are aware of the attack vectors used to commit a cyber-attack, such as phishing, malware, session hijacking, and weak security in third party vendors. Data loss is the most expensive attack, and has cost companies such as Target, Home Depot, and Anthem hundreds of millions of dollars. The attacks on these companies could have easily been prevented if they would have investigated the security of their third-party vendors and had required employee training to raise awareness on the signs of a phishing email. I have looked into the effects of recent ransomware attacks as well as what companies should be doing to prevent this attack. To prevent ransomware, organizations need to be quick to patch and update their systems. Cyber criminals prey on companies that have not updated or patched their systems, and made attacks such as WannaCry and NotPetya devastating events for this reason. Organizations need to implement preventative measures for cyber-attacks and prepare for an attack to ensure that their business does not fail because of a single cyber incident.

#14 - The Benefits of Sharing Cybersecurity Data

Hannah Robbins, ***University of Tulsa***

A common question researchers might ask upon completion of research is what do I do with the data I collected? Most researchers keep their data to themselves or only share it upon request. However, some make it publicly available, either on websites or online in databases such as the DHS's IMPACT database. In this work, I use citation statistics collected from Google Scholar to quantify the benefits of sharing cybersecurity data publicly. Using research papers from cybersecurity conferences over the past six years, I classify data identified in the papers and determine if there is a concrete benefit from sharing data publicly, specifically in terms of citations of the papers associated with those datasets. In addition, I focus on the benefits of making research data available in IMPACT to quantify the benefits of making other cybersecurity datasets public. I do this by focusing on citations before and after a dataset is a part of IMPACT.

#15 - Student driven design of a web tracking lab for privacy engineering

Marina Moore, Bruce Debruhl and Max Zinkus, ***Cal Poly San Luis Obispo***

In this poster, undergraduate teaching assistants share a novel lab that they developed and their experience in developing the lab. This lab was designed to teach the intricacies of server-side web tracking by creating a website that tracks users. We designed bots to visit each of the student websites multiple times, with varied http headers so they could gain insights about the bot 'users'. Students then applied server-side privacy techniques, including k-anonymity and differential privacy, to the data they collected and measured the impact on data usefulness. We developed this lab to apply offensive security education concepts to the realm of privacy. Offensive security education has been proven to work by getting students to think adversarially. In our lab, we applied this concept to privacy, getting students to collect large amounts of data and see what they could learn from this data, then try methods to protect hypothetical users. In a pilot of this course, we assessed students learning using an entry/exit knowledge survey of relevant skills. We find a notable increase in student confidence in technical privacy skills and analysis. This includes a statistically significant increase in confidence for the statement "I can identify techniques to maintain consumer privacy in a database."

POSTER DESCRIPTIONS

#16 - Deep-packet Inspection for Anomaly Detection of Industrial Control Systems

Mustafa Faisal, Xi Qin, Kelvin Mai and Alvaro Cardenas, ***University of Texas at Dallas***

The security of Industrial Control Systems (ICS) has a prominent place in cyber security because ICS are commonly used in critical infrastructures, such as power grid, water and chemical plants, etc. To identify abnormal events and attacks, we are currently working on developing deep-packet inspection tools for industrial networks to build models of the behavior of these systems. Our models have been applied to network communication datasets from a testbed of equipment used in real-world power generation substations. Our experiments are focusing on two well-known industrial network protocols: (1) Modbus/TCP and (2) DNP3. Our anomaly detection system is able to present the informative discrete state diagrams of ICS and spot abnormal states or transitions through unseen states or transition probabilities. With these functions, the goal of our system is to alert the operators of new unusual behavior in their networks and to provide them with enough contextual information so that they can remediate these issues.

#17 - The Secret Life of IoT Devices: A Security Analysis

Junia Valente and Alvaro Cardenas, ***University of Texas at Dallas***

We analyze over a dozen of IoT devices, and summarize vulnerabilities we found on them: including encryption problems on a smart toy and filesystem misconfigurations on consumer drones. We show that voice-enabled toys---targeting young children---pose new unanticipated threats. An attacker can inject malicious voice content and insult or ask young children to do unsafe things. Also, an attacker can obtain private-sensitive data (when the toy is lost or resold). We successfully tested these attacks. Further, we tested a variety of attacks in a new family of drones (U818A) released in 2016. Our concerns over safety (taking down a drone operated by someone else) and privacy (taking unauthorized pictures) alert us that even when a drone is purchased as a toy, cyber-attacks can have dangerous, real-world consequences. We conclude our discussion with steps/ and tools we used to find the vulnerabilities, highlight considerations vendors should take when designing their products, and share our experience in reporting the vulnerabilities to U.S. CERT and affected vendors following a responsible disclosure approach. Our contributions include several CVEs: CVE-2017-3209, CVE-2017-8865 through CVE-2017-8867.

#18 - Viewing Advanced Persistent Threats as Game-Playing Agents

Lindsay Von Tish, ***Lewis and Clark College***

Advanced Persistent Threats (or APTs) are net-based malicious actors. They are groups or organizations who can effectively and persistently compromise their targets for extended periods of time. Currently, the industry standard approach is on stopping APTs after they've attacked by detection and patching of vulnerabilities. Game theory has been used to explain or predict movements of international threat actors. The same principles of game theory can be applied to APTs to determine future actions. This presentation will present a way to model the behavior of APT based on risk tolerance, objectiveness, and ability. We model APTs as game-playing agents who receive payoffs for undetected attacks and incur costs for thwarted or detected attacks. Through use of our model, potential targets of APTs will be able to predict likely agents as well as methods of attack.

POSTER DESCRIPTIONS

#19 - Robust Principal Component Analysis for Anomaly Detection in Cyber Network Data
Melanie Jutras, ***Worcester Polytechnic Institute***

The goal of this research is to utilize Robust Principal Component Analysis (RPCA) for the purpose of anomaly detection in DNS network packet data. Computer network traffic meets all of the criteria for Big Data. When dealing with high dimensional data, Principal Component Analysis (PCA) is a common technique used for dimensionality reduction. Because traditional PCA is known to be sensitive to outliers, a robust version of PCA called RPCA is used. Through the use of a tuning parameter, RPCA can be used to separate the original data into two parts: regular network data and anomalous network data. This data science technique allows for tuning a model utilizing a very small amount of training data. The method described here is useful for cybersecurity because these types of problems are largely unsupervised and often involve high dimensional network data with sparse anomalies.

#20 - ArmorPLC : Diagnosing PLCs Against Cybersecurity Threats through Physical Process Monitoring and Record & Replay
Wenhui Zhang, ***Penn State***

Cyber threats are ubiquitous to manufacturing industry, which target vulnerable Programmable Logic Controllers(PLCs). In this paper, we discuss vulnerabilities in these PLCs. This paper also state threat models, detection and protection techniques. We implement physical process monitoring to detect the attacks such as, output value configuration comparison, timing comparison and using known I/O values for comparison and control flow logic of ST files. We also implemented record & replay technique for mitigation of various possible vulnerabilities. As part of evaluation, we use majority vote and are considering Byzantine failure. The record and replay system captures pin values of Pulse Width Modulation with sensitivity of 50 us. And we achieved false positive rate of 1% in our abnormal detection implementation with setting of 4 virtual PLCs.

#21 - Getting Harder to Catch: Analyzing the Evolution of China's Cyber Espionage Campaigns against the United States through a Case Study of APT1
Winnona Desombre, ***Tufts University***

The relationship between China and the United States is one of the thornier dynamics in international politics, complicated further by each country's growing cyber espionage and warfare capabilities. As early as 2007, the US-China Economic and Security Review Commission has labeled China's espionage efforts "the single greatest risk to the security of American technologies". However, as cyber security is a relatively new field, there is little precedence for pressing charges or taking action against individuals or groups conducting cyber attacks or espionage. This paper is composed of three parts: part one contains an overview of China-US relations within the context of the cyber realm and dilemmas in the international sphere regarding formulation of cyber security policy. Part two is a case study of APT1, a hacker unit attributed to the Chinese People's Liberation Army Unit 61398, a description of APT1's history, and an analysis of its cyber espionage campaigns. Part three reviews the general trends of APT1 within the context of the 2015 US-China Cyber Agreement and China-US relations regarding cyber security, and how policies set by the agreement is reason for optimism.

POSTER DESCRIPTIONS

#22 - Gateway based Multifactor Authentication for IoT devices

Yunshu Liu, ***Northeastern University***

Internet of Things (IoT) has changed the way we perform routine aspects of our life. IoT was exponentially accepted among the general populous as a ‘low-cost’ and ‘easy-to-use’ solution. ‘Internet’ is an integral part of ‘Internet of Things (IoT)’. IoT thus inherits security issues from the Internet, one such issue that we address in our research is insufficient authentication. This paper presents an approach to provide multifactor authentication to IoT devices while maintaining the fundamental ‘low-cost’ and ‘easy-to-use’ characteristics of IoT. The proposed model manages IoT devices over a private network and controls access to these devices by placing a gateway between the IoT private network and the home router. The gateway and authentication server as parts of our model perform resource intensive tasks like multifactor authentication, user management and IoT access management. This paper will discuss the implementation details as well as performance and security analysis of the proposed model. Contrary to most previous works, the proposed model does not require modification to the IoT device, router and application.

#23 - Design and Enforcement of DDoS mitigation mechanism using Blockchain and Smart Contracts

Prasanthi Akella, ***University of Texas at San Antonio***

DDoS attacks are in rise, with increasing strength and duration. Recent attacks hosted on KerbsSecurity.com, DNS provider Dyn have seen a different trend in attack mechanisms being used. As the number of IoT devices in use are increasing exponentially from past few years, it is one of the major advantage for attackers to avoid the cost of infrastructure incurred to host an attack. Previous attacks launched on target systems used limited set of botnets of compromised systems or unmanaged DNS servers on the web to generate the traffic. They used well known techniques to amplify, relatively small attack into a larger one. In contrast to those techniques, attackers are not using any amplification or reflection methods instead generating such huge traffic from large botnet of compromised devices. Attacks on KerbsSecurity.com, OVH both web hosting service providers witnessed a traffic of 665 Gigabits per second and 990 Gigabits per second respectively, a highest record so far. Akamai and CloudFlare are most popular cloud based DDoS protection services used by these systems to protect themselves against DDoS attacks. Even their services couldn’t react to the incident as expected immediately. On the other hand, such cloud based solutions are costly to implement and not all systems hosted online can afford to use them to protect themselves. Smart Contracts in the context of Ethereum Blockchain can serve as effective mitigation solution for DDoS attacks.

#24 - Blockchain-based Community ATM

Bahareh Mokarram Dorri, Mingmin Bai and Pablo Sanchez, ***University of Louisiana at Lafayette***

Digital currencies are revolutionizing technology, making it easier for consumers to transfer funds across the globe. In cryptocurrencies, the whole fund transfer process is instant, secure, and does not need the intervention of a middleman. Cryptocurrencies are increasingly being adopted in eCommerce. All the cryptocurrencies work based on the Blockchain technology that enables keeping track of all the transactions occurred on a cryptocurrency unit. Blockchain provides a decentralized mechanism to keep track of transactions and prove their validity. A smart contract is a protocol intended to facilitate, verify, and enforce the negotiation or performance of a cryptocurrency transaction. The aim of smart contracts is to secure transactions and reduce their associated costs. Smart contract is a piece of code running on top of blockchain that codifies the rules of a transaction. When the rules of a transaction are met, then the transaction is executed. In this project, we implemented a blockchain-based ATM web application. Through this application users can transfer Ether. The user who needs cash will find other users who already set their availability to pay money. After money exchange, ether transfers between their accounts on the Ethereum. We wrote a smart contract and based of on the application works great!

POSTER DESCRIPTIONS

#25 - Controller Area Network Intrusion Detection and Response System

*Linxi Zhang, **University of Michigan***

Controller Area Network(CAN) bus is a standard in-vehicle communications network protocol. However, CAN bus is subjected to attacks, due to the lack of enough security feature. Very little about automotive IDPS is currently publicly available. We provide a machine learning based intrusion detection system for in-vehicle CAN networks. Only ID portion of a CAN message is necessary. And the data sets collected form 2006 Honda Accord.

#26 - Analysis of Delay Patterns of Multiple Instances of DDoS Attacks Against CPUs and Memory

*Leena Radeke, Andrew Erickson, Dennis Guster and Paul Safonov, **St Cloud State University***

Comprehending the consequences of a DDoS attack is significant in developing defense mechanisms, particularly regarding memory usage within a cloud-based virtual host. The subsequent experiments administer a succession of tests establishing the pattern of degradation occurring as multiple instances of denial of service are instantiated. The C code program swapCrash.c is utilized in a sequence of tests to determine the effects of a DDoS attack. The first attack scenario evaluated the amount of time needed for the kernel to terminate a running instance of the swapCrash.c code. The second attack scenario evaluated the footprint of a DDoS attack, where three instances were running inside the system. The third attack scenario addressed a DDoS attack's impact on an end-user trying to complete a task as the attack was taking place. The experiment's output demonstrates a DDoS attack does not necessarily result in increased processing delay. This publication aims to observe a pattern in memory degradation after recurring attacks, which could be beneficial in generating new defense and detection techniques against elusive application-level DoS attacks. A major benefit of contemporary cloud architecture is virtualized hosts (VMs), which receives a logical slice of the usable physical resources. Only the affected VM will require a reboot in the case of a successful DDoS, indicating a cloud architecture is helpful in isolating the impact of a DDOS attack. Additionally, intrusion detection systems and preemptive testing on the host level are imperative to safeguarding the integrity of not only virtualized, but physical hosts as well.

#27 - Detection of Insider Threat Activities: A Data Analysis Approach

*Yanwen Wu and Hongmei Chi, **Florida A&M***

The inside threat against database management systems has become the prime cyber-security concern to public and private organizations. To detect and predict insider-threat problems, scholars have put forward technical, social or socio-technical approaches, relying on linguistic and sentiment analysis. While these approaches may make us better understand motivations behind insider threats and bring about more efficient monitoring, through the development of user profiles from certain social cues. In this work, we present a new direction to address this problem. With the test data collected from Enron emails as well as some training data, we use machine learning approach to identify insider threats by analyzing word texts. We can realize a significant precision and accuracy in text analysis, by recurring to two major comment classification methods, the Naïve Bayes Multinomial (NBM) and Support Vector Machines (SVM). Meanwhile, we implement the Median Absolute Deviation (MAD) method to identify cases where the threat level of a given person would be considered as an outlier compared to those of other persons being profiled, adopting psychosocial indicator words used by the FBI from the LIWC library.

POSTER DESCRIPTIONS

#28 - Designing SecDLC Hands-on Labs via CyberCEIGE

*Ra'Teema Stanley and Hongmei Chi, **Florida A&M***

The security development life cycle (SecDLC) model delivers a perpetual cycle of information security management and refinement. Using real-world examples and within SecDLC framework, we will ensures each hands-on lab for preserving, monitoring, and improving security practices, policies, and standards in private and public sectors. Each hands-on lab will contain all four stages of SecDLC , comparing and contrasting them to existing security development models. In this poster, CyberCIEGE, an innovative computer-based tool to teach information assurance concepts, is adopted to design the SecDLC hands-on lab, by using this tool, students can be trained to be cyber security professionals who solve security issues within SecDLC framework.

#29 - A comparative study on Java method-level patterns and method-level software metrics in vulnerability prediction

*Kazizakia Sultana and Byron J. Williams, **Mississippi State***

Ensuring secure code in the early stage of software development can reduce the likelihood of inducing vulnerabilities and save resources during testing. Traditional software metrics have been used for vulnerability prediction but are unable to precisely isolate the problematic areas in the codebase. In this study, we mine Java nano-patterns (method-level design constructs) patterns and then compare their vulnerability prediction performance with software metrics. Nano-patterns are similar in nature to design patterns, but they can be automatically recognized and extracted from source code. The results of this study can assist developers in assessing their software security and identifying potentially vulnerable code commits prior to release. To obtain this insight, we studied reported security vulnerabilities for two major releases of Apache Tomcat. We used the Naïve Bayes machine learning technique to predict vulnerabilities using nano-patterns as features. We applied the same technique using method-level software metrics as features and then compared their performance with nano-patterns. We found that nano-patterns have a lower false negative rate for classifying vulnerable methods and have higher recall in predicting vulnerable code than the traditional software metrics. On the other hand, traditional software metrics present higher precision than nano-patterns.

#30 - Multi-factor Continuous Authentication of Smart Phone users using Support Vector Machine

*Anshu Bhattarai, **Tennesse Tech University***

Most authentication systems (password and biometric feature based) use one time static authentication methods. Such systems are susceptible to masquerade attacks, where unauthorized users can take over user's identity after initial authorization and then compromise user's security and privacy. A real time continuous authentication system provides better security control where the user is continuously authenticated based on user's behavior after initial authorization. Monitoring more user features have shown to yield more accurate results. For continuous authentication of smart phone users, in this work, we evaluate micro movements, orientation and grasp of user's hand, as a set of behavioral features, which can be easily collected from smart phone sensors like accelerometer, gyroscope, and magnetometer to continuously authenticate users. We demonstrate the use of Support Vector Machine to design a continuous authentication system that yields better results with usage of smart phones.

facebook

</>

CYBERSECJOBS

www.cybersecjobs.com

@cybersecjobsusa
cybersecjobs
cybersecjobs
linkedin.com/company/cybersecjobs

Cybersecjobs.com is a veteran-owned career site and hiring event company for cyber security professionals and students.

Equipping you with job search tools beyond a campus recruiting experience prepares you for career success, not just your first professional position. One of those tools is career sites, the number two source of hire for employers in 2016.*

We provide the information you need to help you find the career that best suits your needs.

We offer:

- Intelligence that informs you to make better career choices
- Public and Private profile settings so you control your visibility to employers
- Educational content so you understand how to job search more successfully
- Job Alerts so you can search more efficiently

**Silk Road's 2016 Top Sources of Hire Report*

Google

g.co/SecurityPrivacyEngJobs

Are you ready to help us fight the good fight?

Are you passionate about building systems to protect Google and its users from attacks? Do you like to break things — and then fix them?

Join Google Security & Privacy Engineering to build secure software solutions; conduct cutting-edge research; and use a wealth of tools, languages, and frameworks.

Our mission is to keep Google and its millions of users safe, secure, and happy.

IBM Security

Cybersecurity is one of the most critical issues of our generation.

IBM Security is looking for applicants with strong business or technical skills, a passion for technology and software, strong teaming skills and leadership potential.

If you want to help protect the world's data and transform the security industry, **we want to hear from you.**

1.5 Million unfilled IT security jobs **globally projected by 2020**

- + Be a part of something big. Help us make the world a safer place.
- + Tackle the increasingly sophisticated security challenges faced by 10,000+ IBM Security clients.
- + Help organizations disrupt targeted attacks and make more informed business decisions.
- + Deploy security innovations, and discover new ways to detect, prevent and respond to today's complex threats.
- + Access IBM's global knowledge and expertise to stay ahead.

Careers with IBM Security:
http://www.ibm.com/employment/security

DiversityInc 2016 TOP 50 COMPANIES FOR DIVERSITY®

IBM®

© Copyright IBM Corporation 2016

intel®
AMAZING WORKS HERE
NO ONE ELSE SEES THE WORLD LIKE YOU DO. WE'VE BEEN LOOKING FOR THAT.

INTEL CORPORATION IS A PROUD SPONSOR OF WICYS

We currently have BS, MS and PhD opportunities for internships and full-time positions in the areas of: Cybersecurity, Research & Development, Information Security, Engineering, Software, IT, Sales, Marketing and Manufacturing. Join us at our Social Event and Career Fair to learn more!

Come Meet Us!

March 22nd 7pm | Mentoring Social

March 23rd 3pm | Career Fair

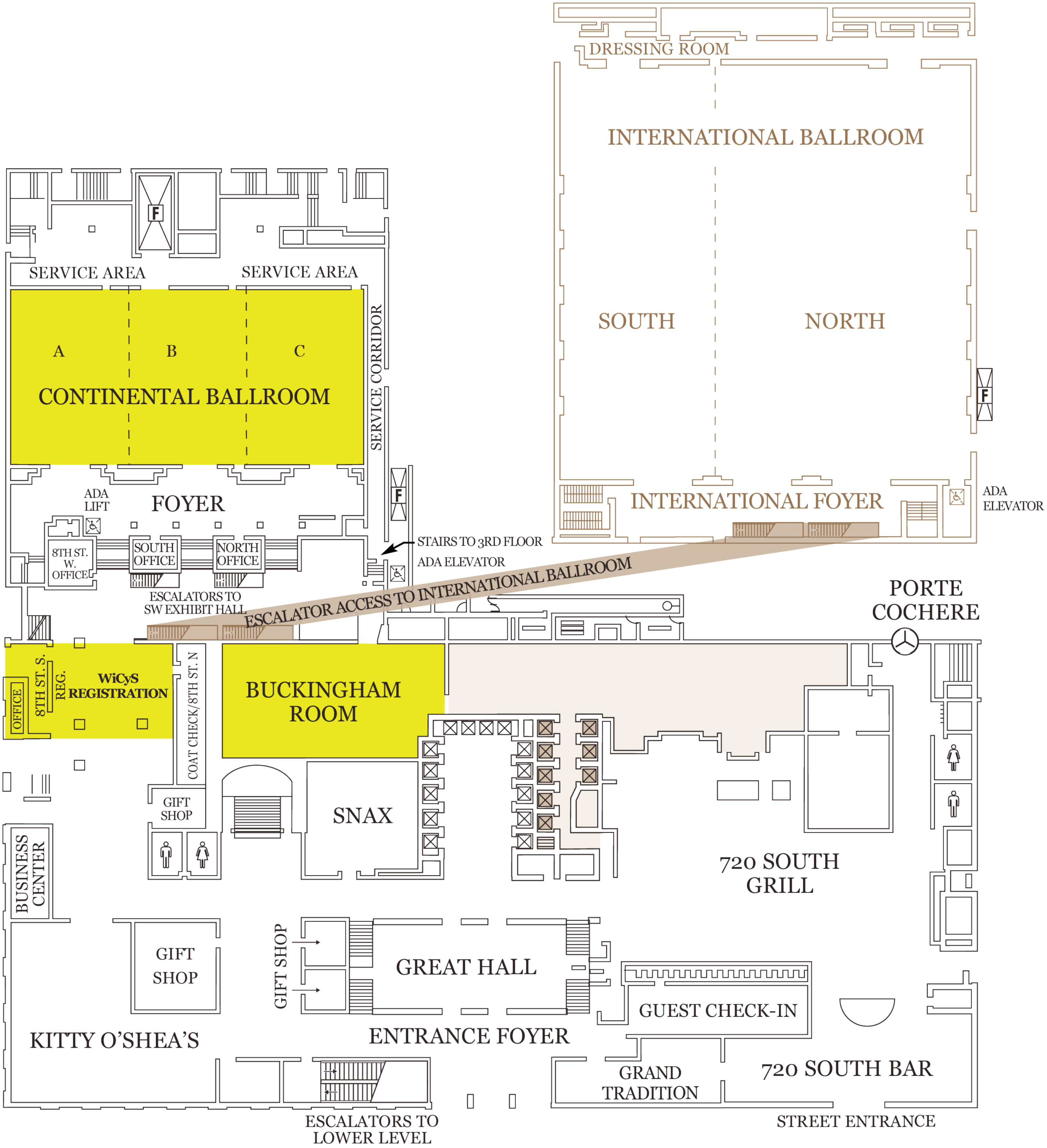
Innovation isn't easy. Or quick to come by. So ours is a challenging workplace where teams are diverse, competitive and continually searching for tomorrow's technology and the brilliant minds to create it. Join us.

jobs.intel.com

Photo by Brittainy Newman

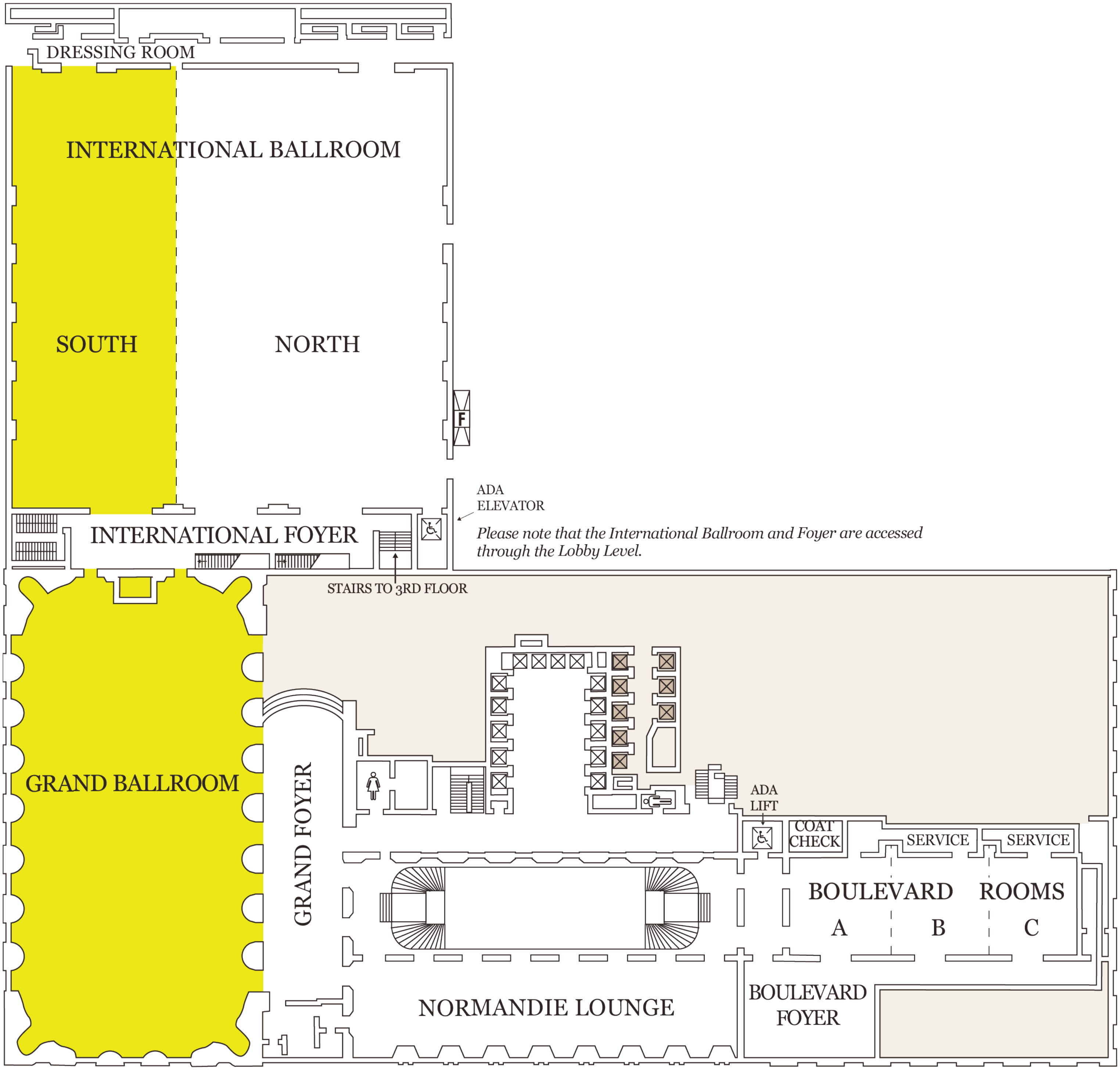
MAPS

LOBBY LEVEL



MAPS

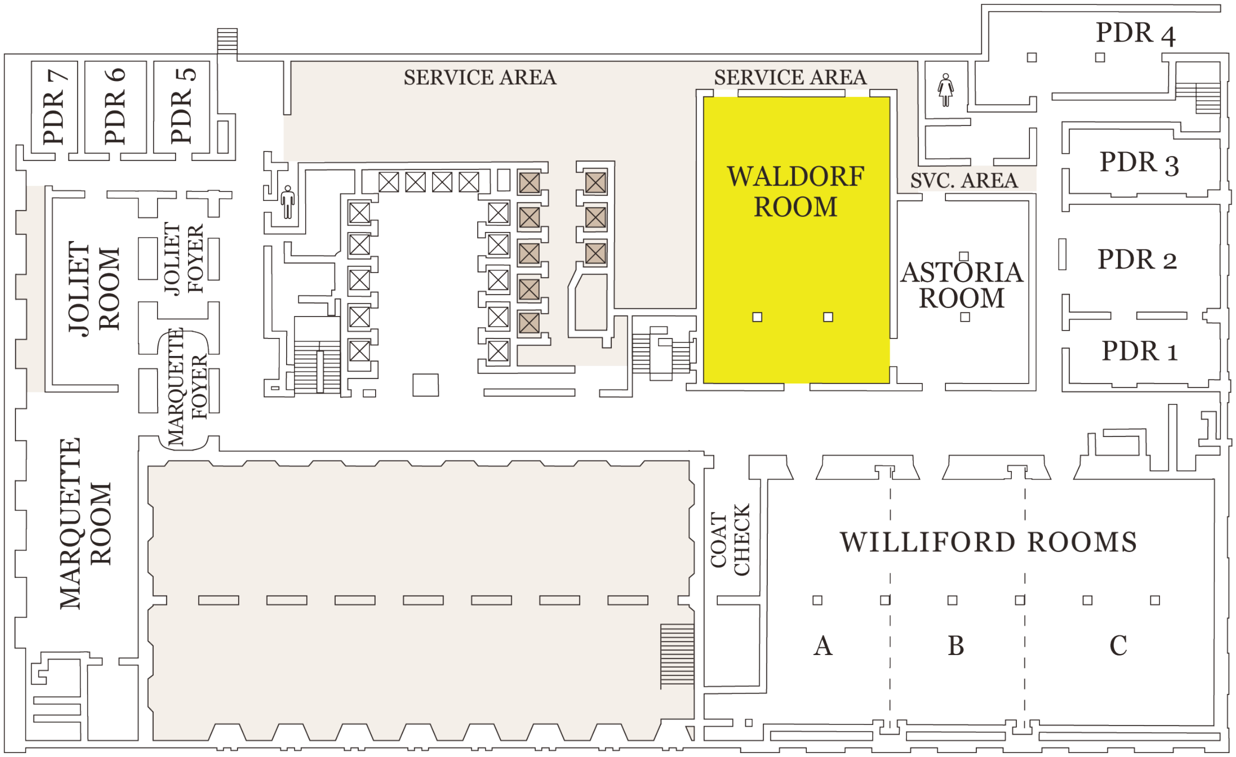
SECOND FLOOR



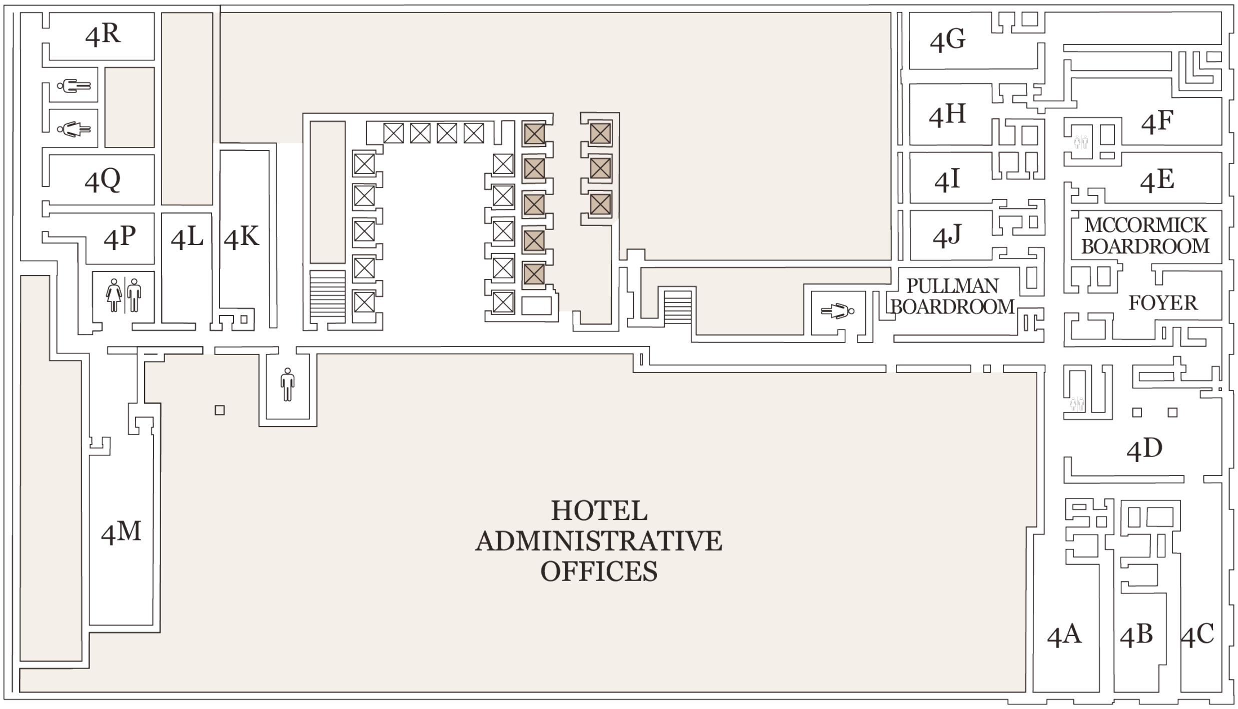
Please note that the International Ballroom and Foyer are accessed through the Lobby Level.

MAPS

THIRD FLOOR

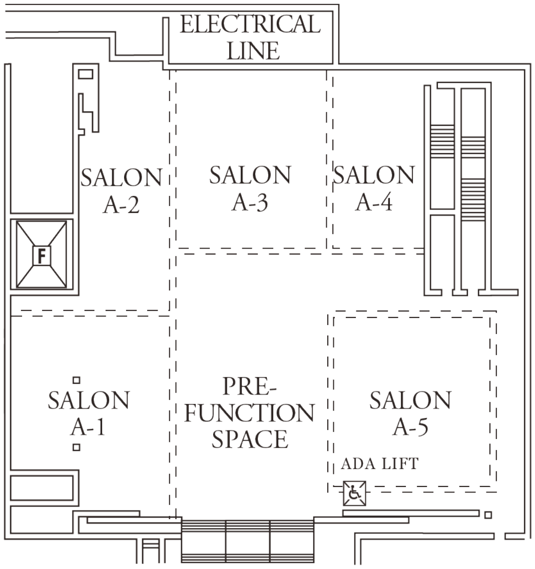


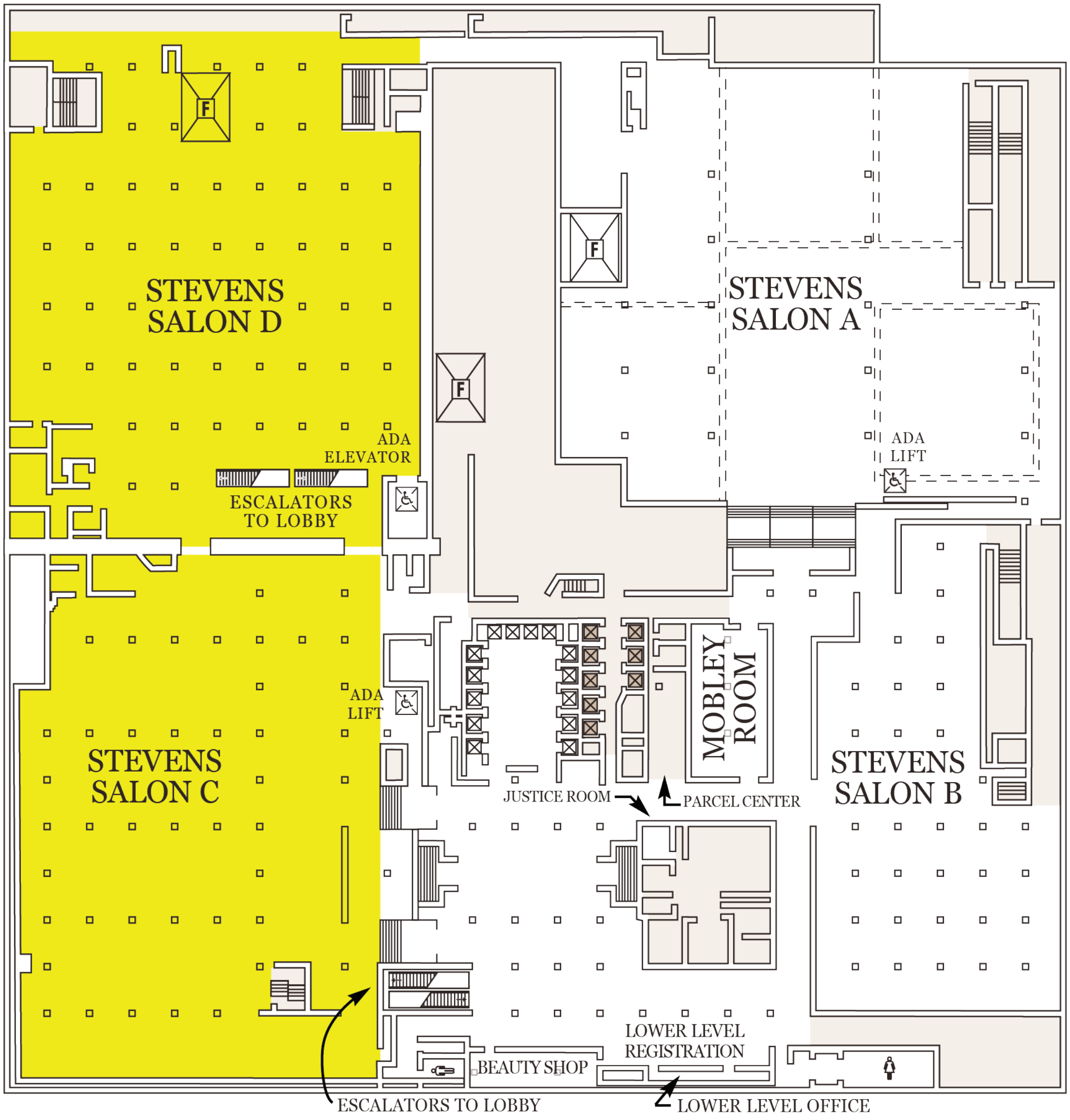
FORTH FLOOR



MAPS

LOWER LEVEL





NOTES

CEROC
Cybersecurity Education, Research and Outreach Center

Thank You To Our Partners!

Illinois Institute of Technology

STRATEGIC PARTNERS

Cisco

facebook

Fidelity Investments

DIAMOND PARTNERS

Bank of America

CERT | Software Engineering Institute Carnegie Mellon University

Central Intelligence Agency

CSSIA National Support Center for Systems Security and Information Assurance

CYBERSECJOBS

Google

IBM

intel

paloalto networks

pwc

Raytheon

R·I·T Computing Security

acm SIGSAC

Symantec

UTD Center for Engaging Women in Cyber Security

PLATINUM PARTNERS

aetna

Booz | Allen | Hamilton

ini Information Networking Institute Carnegie Mellon

CME Group

Georgia Tech College of Computing

Georgia Tech Research Institute

KPMG

Kroll

Northrop Grumman

protiviti Risk & Business Consulting. Internal Audit.

Southern New Hampshire University

TARGET

W Master of Cybersecurity & Leadership University of Washington | Tacoma

Walmart

WPI

GOLD PARTNERS

airbnb

Allstate

AT&T

Comerica Bank

ENDGAME.

National CyberWatch Center

splunk>

State Farm

SWAMP Software Assurance Marketplace

W University of Washington | Bothell Master of Science in Cyber Security Engineering

VISA

SILVER PARTNERS

bringa

Capitol Technology University

Carnegie Mellon University Heinz College Information Systems • Public Policy • Management

CRA-W Computing Research Association Women

cww cyberwatch west

EY Building a better working world

General Dynamics Information Technology

Homeland Security Intelligence and Analysis

Indiana University Security and Privacy in Informatics, Computing, and Engineering

Micro Focus

NCL

NOKIA

Pace University Seidenberg School of Computer Science and Information Systems

SANS

shopify

Stephen F. Austin State University Nacogdoches, Texas

Towson University

BRONZE PARTNERS

alight

Bay Path University

BISHOP FOX.

Michigan State University

EC-Council | Academia Preparing the Next Generation of Cybersecurity Experts

DSU Dakota State Graduate School

HALOCK

McAfee Together is power.

Northeastern University