The CyberWire
621 East Pratt Street, suite 300
Baltimore MD 21202—3140
editor@thecyberwire.com
www.thecyberwire.com
@thecyberwire

Women in Cybersecurity Conference

March 27-28, 2015 Atlanta GA

The 2015 annual Women in Cybersecurity conference, organized by Tennessee Technological University and the National Science Foundation, met Friday and Saturday in Atlanta, Georgia, USA. The CyberWire is pleased to summarize its highlights below.

Debunking myths about security engineers. Facebook's Jenn Lesser Henley shared her personal history to encourage those attending the conference to expand their notion of who can become a security engineer. She came to security from an academic background in communications, but as someone who had a strong, longstanding love for mathematics. After working for PayPal earlier in her career she moved to Facebook, where she's now Director of Security Operations. She characterized this move as risky, but, both retrospectively and at the time, a risk worth taking. She finds her strategic responsibility for security across Facebook "fast-moving, challenging work." "The Internet is our shared space, and for it to be strong, it must be secure," Henley said. She predicts that there will be 1.4 million jobs in information security by 2020, and these jobs will be hard to fill. Given that diverse teams demonstrably perform better, why then don't more people — especially young women — go into security? Women have said they think the field lacks glamour, creativity, and the opportunity for collaborative work. But in fact, Henley argued, security offers all three. She encouraged people to think of security in terms of protectors and defenders, all of whom need empathy to do their work effectively. Empathy enables us to place problem solving in context. Henley sees encouraging signs that we're

headed in the right direction. Find a cheerleader, she advised, and said that there are plenty of them out there. She closed by challenging all to bring empathy to innovation.

In response to a question about how one might enter cyber security without being an engineer, Henley noted her own background and reminded all that cyber security is "a vast, multi-disciplinary field, with room for all." She offered some tips on communicating: have an ally, define your own response, and ask people how they handle difficult situations.

Security must be user-friendly by design. Google's Dr. Iulia Ion introduced the evening program. She noted the importance of making security easy to use, lest users simply bypass it. About a third of respondents to a Google survey reported a compromise, with the most common attack being password theft. Two-factor authentication, she noted, is one obviously important measure we should take, but we must also address account recovery. Google tries to contact users through multiple channels, and supports authentication with a risk analysis engine. She concluded with some common-sense (if counter-intuitive) observations on using physical devices in authentication: your phone, she said, is harder to steal than your password.

Cyber security is all about the numbers. Sherri Ramsay (of CyberPoint International) delivered a keynote on the state of the industry and about the role that women can, do, and should play in it. In the 1970s, when she was an undergraduate, there were few computer science programs, and few women majored in science, technology, engineering or mathematics (STEM). She reviewed the history of ARPANET, the early 1970s precursor of the Internet, pointing out that it was emphatically not designed for security. We all take advantage of the Internet's convenience as an open network of networks. The Internet, pervasive in daily (and economic) life and central to national security, drives the growth of cyber security as a career field. Our intellectual property is our greatest national asset, and it's easily exposed and stolen. There are now 2.2 billion Internet users, and some 200 thousand new pieces of malware appeared last year. The FBI, Ramsay commented, says it costs companies about $8.9m to remediate an intrusion, and a compromised company needs on average 243 days to clean up its networks. More than 1 billion pages of intellectual property were stolen last year. "So what more important job can there be," she asked students, "than protecting the Internet?" She challenged colleges to offer more cyber-relevant majors, and she challenged women to increase their participation in STEM fields. She closed with advice to students and those just beginning their careers: learn every day, have three mentors (and these will change over the course of one's career), "be hard to manage" (that is, challenge and question), and remember, "it's always right to do the right thing."

National Science Foundation opportunities. Victor Piotrowski of the National Science Foundation (NSF), en route to introducing Saturday's morning keynote, took the opportunity to draw students' attention to three major NSF cyber programs: Secure and Trusted Cyberspace (SaTC), CyberCorps Scholarships for Service (SFS), and Advanced Technological Education (ATE). (We include links to these programs in the "Dateline: Atlanta" section below.)

DHS cyber vision: industry, technology, and trust. Dr. Phyllis Schneck, Deputy Under Secretary for Cybersecurity and Communications for the National Protection and Programs Directorate (NPPD) at the US Department of Homeland Security (DHS), delivered the morning keynote. After expressing her gratification and "amazement" at seeing hundreds of women interested in cyber security gathered in one place, she described DHS's vision for infrastructure cyber protection, with particular emphasis on the Department's National Cybersecurity and Communications Integration Center (NCCIC). The NCCIC is the Government's 24/7 cyber watch center, with connections to other agencies as well as the private sector. She emphasized the importance of avoiding surprises, and the need to look at cyber challenges holistically while balancing security with privacy and civil liberties. Her vision for the future is the development of a security system in which machines can see attacks coming (the way meteorologists see storms approaching) and enable a response as fast and effective as the human immune system's

response to disease. We need, she said, to build trust, share and communicate for situational awareness, and then let the machines operate at speed.

Dr. Schneck encouraged students to pursue cyber security as a career, and described her own career arc as an example of the various paths one might take in such a career. Interagency partnership, she said, is fun and important, as is public-private partnership. She counseled against the all-too-common fear of trying a technical career. "It's always helpful to have a specific hard-core expertise, whether technical or policy, and it's important to keep up your technical chops." Keep learning. Don't be afraid to experiment, and make decisions that are good for you.

In response to a question, she said that she thought the biggest research and development gaps in the NIST Framework probably lie in risk assessment, because of its subjectivity. When another questioner asked whether women have to become comfortable with being uncomfortable, Schneck said yes — they should say what they think, and move on.

Lightning talks. The morning continued with short presentations on various topics.

- Stripe's **Karla Burnett** described the value of capture-the-flag exercises in developing security skills. These tend to encourage teamwork, and many can be done in a short period of time.
- **Tamara Shoemaker** of the Colloquium for Information System Security Education (CISSE) described CISSE's role in promoting cyber security education.
- Cigital's **Apoorva Phadke** advocated application security as an exciting career, saying that while ethical hacking for a living is cool, coming up with remediation solutions is even cooler.
- Facebook's **Meagan Kruman** described non-technical paths into cyber security — many of these run through geopolitics. She herself works on tracking threats to users, and her own background lies in languages and international affairs. She offered a brief, compelling case study of tracking Hong Kong's umbrella protests.
- Key Bank's **Kathy Peters**, an application security veteran, explained how to debrief development teams after you've subjected their work to security testing. Understand, she said, that development teams typically go through the five stages of grief when you confront

them with security testing results: denial, anger, bargaining, depression, and acceptance. So you need to make sure technical and management teams are on the same page. Stick to the facts. Keep emotions and prejudices out of the report. Avoid trigger words, like poor, weak, etc., and make your recommendations clear, concise, and, above all, actionable.

- **Priya Jain**, a Georgia Tech freshman, delivered an enthusiastic stem-winder on why freshmen make great cyber interns. "Our minds are basically empty," she exclaimed to widespread approval, and so "they're moldable" — companies who pass up offering freshmen internships are passing up a terrific opportunity to educate the kind of workforce they need. She urged first-year students to take a shot at internships — what have they got to lose?
- **Desiree Reagan**, a student at the University of Maryland University College, described OWASP's most wanted. Noting that even minor SQL injection attacks often cost about $200,000 to remediate, and are rising in frequency, she reported the results of an experimental SQLITE injection attack on EMR/EHR systems.
- **Deanne Wesley**, a member of the faculty at Forsyth Technical Community College, described the use of mock crime scenes in the computer forensics classroom, and explained how instructors can effectively use them to teach the full cycle of forensic investigation, from getting a warrant to doing the examination to finishing the report.
- The Michigan State Police's **Kelley Goldblatt** noted that almost every crime committed today has a cyber component. She described actual cases, highlighting the difference between state and Federal law enforcement, and emphasized the importance of information sharing.

Student poster sessions. The conference featured twenty-seven poster presentations, all worthy of the symposiasts' attention. Four of them were singled out for special recognition.

- **Top poster, graduate division: "Investigating the Factors Influencing Health Information Sharing on Online Social Networks,"** by Victoria Kisekka and Bich Vu, of the University at Buffalo. Vu and Kisekka isolated and defined seven key factors: information privacy concerns, information trust, access to personal health records, mobile device usage, health status, quality of physician-to-patient interaction, and online health information utilization.
- **Runner-up, graduate division: "Teaching Logic Flaws Using a Case Study on Cashier-as-a-Service Attacks**," by Lindsay Simpkins, North Carolina A&T State University. Simpkins described an approach to teaching logic flaws — testing for which is challenging because such flaws are resistant to detection by automated means — that uses real-world examples to introduce the field to undergraduates. Her module has been made available to other universities, and is readily adaptable to various curricula.
- **Top poster, undergraduate division: "Decision Times for Energy Fraud Detection in Smart Meters,"** by Christa Cody, Tennessee Technological University. Her research explored the use of decision trees to classify energy consumption data in ways that allow detection of potentially fraudulent activity.
- **Runner-up, undergraduate division: "Securing Embedded Systems with Spintronics,"** by Karolina Alvarez, Karen Lamb, Kenneth Jabon, and Wesley Brooks, the University of Illinois at Urbana-Champaign. Random-number generation is always a challenge for cryptographic applications; the researchers describe their use of spintronics to provide both a true random number generator and a physically unclonable function.

The adaptive individual. Microsoft's Angela McKay delivered the conference's closing keynote. She described her own career and life arc to illustrated the challenges of embracing individuality and adaptability. She went from communications modeling to cyber security, from Washington, DC, to Redmond, Washington. These moves involved dramatic cultural changes, but she found that, properly understood, her skills were transferable across corporate

cultures. The biggest cyber security challenge, she said, is people. We need a large, diverse, creative workforce. Looking at trends, she noted that Internet users in emerging nations now outnumber those from North America and Western Europe. We're seeing, she said, a future in which the global North is device-rich, the global South user-rich, and in which every company will be an IT company.

To engage that future, she urged students to "Own your uniqueness." You should be self-aware about your goals. You should cultivate the ability to see other people's distinctive individualities. Recognizing individuality is essential to building and leading teams. "And adaptability comes down to recognizing opportunities, and recognizing that skills are transferable. Be agile enough to change states rapidly," because cyber security inherently demands agility.

According to Ambareen Siraj, Founder and chair of the Women in Cybersecurity Conference, the call for the local hosting of the 2016 Women in Cybersecurity conference will be published in May this year and announced in July. If your organization is interested in becoming involved with this initiative, please refer to www.wicys.net or contact Dr. Siraj at asiraj AT tntech DOT edu.

the cyberwire

editor@thecyberwire.com
www.thecyberwire.com

@thecyberwire
+TheCyberWire

About The CyberWire

The CyberWire is supported by CyberPoint International and its community partners. We invite the support of other organizations with a shared commitment to keeping this informative service free and available to organizations and individuals across the globe.

Revised 8.4.15