The 8th Biannual

CYBER SECURITY SUMMIT

UNIVERSITY OF CALIFORNIA

October 23, 2019
UC Santa Barbara

Agenda

8:00-9:00am	**BREAKFAST & CHECK-IN**
9:00-9:15am	**WELCOME** DAVID RUSTING, Systemwide CISO, UCOP
9:15-9:30am	**ICE BREAKER: Rochambeau!** Participants will have the opportunity to share their concerns about cybersecurity, to impress each other with their knowledge, and to get to know their colleagues on a deeper level with this activity.
9:30-10:15am	**KEYNOTE — Understanding the Threat: Malicious Software, Malicious Actors, and the Promise of Artificial Intelligence** GIOVANNI VIGNA, Professor, UC Santa Barbara Cyber attacks are becoming more sophisticated and widespread. Malicious actors compromise the computing infrastructure of organizations to steal their data, abuse their computing resources, or compromise their business processes. Some recent research approaches leverage artificial intelligence and machine learning in order to proactively fix vulnerabilities, detect anomalous behavior, and track the evolution of malicious programs. Vigna will discuss these promising new techniques, including their complex application and why they might provide a false sense of security.
10:15-10:30am	**BREAK**
10:30-11:15am	**Creating, Weaponizing, and Detecting Deep Fakes** SHRUTI AGARWAL, PhD Student, Computer Science, UC Berkeley During the past few years, the startling rise of fake news—in which everyone from individuals to nation-sponsored entities can produce and distribute misinformation—has been implicated in many troubling trends. Fake news leads to a misinformed public and serves as an existential threat to democracy and an instigator of violence. Rapid advances in machine learning are making it easier than ever to create sophisticated and compelling fake images, videos, and audio recordings, increasing the power and danger of fake news. Agarwal will provide an overview of how these deep fakes are created—and detected.
11:15am-12:00pm	**Practice to Prevent: Creating, Delivering, and Learning from Incident Response Tabletop Exercises** RICHARD SPARROW, Acting Chief Information Security Officer, Penn State Annual tabletop exercises are often a required part of incident response plans. Some institutions may see these exercises as a compliance box that needs to be checked. However, they are actually an opportunity to identify gaps, improve processes, increase performance, and build highfunctioning teams. In this session, Sparrow will discuss how Penn State has leveraged tabletop exercises to positively impact incident response and develop teams that work closely to address the complexities that arise during an actual incident.

Agenda

12:00-1:30pm	**NETWORKING LUNCH**
1:30-2:00pm	**ACTIVITY: Table Trivia** Another opportunity to get to know your fellow attendees and build teamwork skills that enhance cybersecurity planning and performance.
2:00-2:45pm	**"Things That Go Boom": Threats to Industrial Control Systems and Critical Infrastructure** SERGIO CALTAGIRONE, Vice President, Dragos Some threats go bad, some threats go "boom"—and that difference is critical. Caltagirone will discuss the current threat landscape involving industrial control systems that provide reliable power, clean drinking water, oil and gas, manufactured goods, food, and many other products and services critical to modern civilization. After the scary stuff, Caltagirone will discuss what is, and what is not, being done about the problem and the outlook for the future.
2:45-3:00pm	**BREAK**
3:00-3:45pm	**Lessons Learned From Building CISA's First Phishing Assessment Service** KELLY THIELE, Information Security Specialist, Cybersecurity and Infrastructure Security Agency This part-technical, part-behavioral analysis presentation shares insights and lessons learned during Thiele's work as the Team Lead in the Cybersecurity and Infrastructure Security Agency's (CISA) first externally facing phishing assessment service. She will discuss how CISA built their program by filling a need to balance the testing of technical controls necessary to prevent successful phishing attacks and the testing of the human behavioral response when presented with a phishing email. Thiele will examine the challenges of creating objective, repeatable, and scalable phishing assessments that support anti-phishing awareness training, including metrics that can inform senior leadership risk management decisions.
3:45-4:00pm	**WRAP-UP** DAVID RUSTING, Systemwide CISO, UCOP

UC CYBER-RISK
COORDINATION CENTER

C3 is delighted
to welcome
these accomplished
speakers to
UC Santa Barbara.

Speakers

GIOVANNI VIGNA

Professor, University
of California at Santa Barbara

Giovanni Vigna is a Professor of Computer Science at the University of California in Santa Barbara and co-founder of Lastline, Inc. Research. His interests include malware analysis and anti-malware solutions, vulnerability assessment, binary analysis, and web and mobile phone security. Vigna served as Program Chair of the International Symposium on Recent Advances in Intrusion Detection (2003), the ISOC Symposium on Network and Distributed Systems Security (2009), and the IEEE Symposium on Security and Privacy (2011). The annual Capture the Flag hacking contest he runs, iCTF, involves dozens of teams around the world. Vigna is also an IEEE fellow and a senior member of the ACM.

SHRUTI AGARWAL

PhD Student, University
of California at Berkeley

Shruti Agarwal is a PhD student in the Department of Electrical Engineering and Computer Science at the University of California at Berkeley. Her primary research interests are multimedia forensics, image analysis, machine learning, and computer vision. Prior to enrolling in her PhD program, she worked as a software developer on the Adobe Illustrator team in India where she was responsible for algorithm designing, coding, technical brainstorming, and technical design. Agarwal earned her BS and MS in Computer Science from the Indian Institute of Technology (IIT) Delhi, India and Harcourt Butler Technology Institute (HBTI), India, respectively.

Speakers

RICHARD SPARROW

Acting Chief Information Security Officer, Penn State

As Penn State's Acting Chief Information Security Officer, Richard Sparrow oversees security operations, privacy, information security compliance, and identity and access management. Previously, Sparrow served as the Director of Security Operations in Penn State's Office of Information Security, leading a team of IT security professionals that advanced security services, provided security consulting and architecture, and developed enterprise security operations. Sparrow's current projects focus on transforming threat detection, implementing an information-centric cybersecurity strategy, ensuring operational excellence, and designing incident response testing and training exercises.

SERGIO CALTAGIRONE

Vice President, Dragos

With over 15 years of experience in information security, Caltagirone "hunts evil" as Vice President at Dragos, protecting industrial control systems and critical infrastructure worldwide. He is also Technical Director at the worldwide counter-human trafficking nonprofit Global Emancipation Network. Caltagirone previously led cybersecurity missions at both the National Security Agency (NSA) and Microsoft, beginning both of their cyber threat intelligence missions. Co-author of "The Diamond Model of Intrusion Analysis," Caltagirone also contributes to numerous cybersecurity books and periodicals.

KELLY THIELE

Information Security Specialist, Cybersecurity and Infrastructure Security Agency (CISA)

Kelly Thiele is an information security specialist for the Cybersecurity and Infrastructure Security Agency (CISA) and leads the Phishing Campaign Assessment program for CISA's Vulnerability Management division. Since 2012, Thiele has also been a key program lead for CISA's network vulnerability scanning service. Prior to joining CISA, Thiele earned an MS in International Affairs and a BS in Economics from the Georgia Institute of Technology. She is also an alumna of the Joint Forces Staff College's Joint C4I/Cyber Staff and Operation Course and a graduate of the National Science Foundation's CyberCorps Scholarship for Service program.

Save the Date

The 9th Biannual

CYBER SECURITY SUMMIT

April 15, 2020
UC Berkeley

The University of California Cyber-Risk Coordination Center (C3) has already begun planning the ninth Biannual Cyber Security Summit.

We welcome your suggestions about possible topics and speakers. Please contact uccybersummit@ucop.edu.

Thank you to our Fall 2019 Cyber Security Summit Sponsors!

Dasher Technologies

e+ Where Technology Means More®

proofpoint.

cisco

FIREEYE