Program Agenda

8th Annual **HOT TOPICS** *in the* **SCIENCE OF SECURITY** ***(HoTSoS)***

APRIL 13-15, 2021 | *virtually hosted by* THE NATIONAL SECURITY AGENCY

https://hotsos.org

Monday, April 12

0800 - 1800 Check out the virtual platforms and test your settings

Tuesday, April 13

0900 - 0930 Networking, log into the platform and chat with other attendees

0930 - 1000 Welcome and Opening Remarks
General Chair: *Adam Tagert (National Security Agency)*
Program Co-Chairs: *Özgür Kafali (University of Kent)*
Ahmad Ridley (National Security Agency)

1000 - 1100 **KEYNOTE: Securing Data in Clouds: Making the Most of Trusted Hardware**
Nick Felts (National Security Agency)

1100 - 1115 **BREAK / NETWORKING ON GATHER**

SESSION 1: Cloud Security

1115 - 1140 Formal Foundations for Intel SGX Data Center Attestation Primitives
Muhammed Usama Sardar, Rasha Faqeh, Christof Fetzer (TU Dresden)

1140 - 1205 A Secure and Formally Verified Linux KVM Hypervisor
Shih-Wei Li, Xupeng Li, Ronghui Gu, Jason Nieh, John Zhuang Hui (Columbia University)

1205 - 1250 Work-In-Progress Discussion Session: JavaScript Attacks
Ross Copeland and Drew Davidson (University of Kansas)

1250 - 1400 **LUNCH & NETWORKING**
Preview posters in Gather

SESSION 2: To Err is to Be Human

1400 - 1445 Work-In-Progress Discussion Session: Election Security
**Natalie Scala, *Josh Dehlinger, **Paul L. Goethals*
**Towson University, **USMA*

1445 - 1530 Work-In-Progress Discussion Session: Phishing
**Dennis Roellke, *Salvatore Stolfo, *George Litvinov, **Shlomo Herschkopp, †Mark Seiden*
**Columbia University, **Allure Security, †Internet Archive*

1530 - 1600 **BREAK**

SESSION 3: Student Presentations

1600 - 1620	Analysis of the Impact of Varying Statistical RF Fingerprint Features on IoT Device Classification *Asia Mason (Morgan State University)*
1620 - 1640	MAZE: A Secure Cloud Storage Service Using Moving Target Defense and Secure Shell Protocol (SSH) Tunneling *Vasco Xu and Sherif Khattab (University of Pittsburgh)*
1640 - 1700	Performance improvement of anomaly detection on IoT network *Latha Suryavanshi Karakos and Jumoke Ladeji-Osias (Morgan State University)*
1700 - 1720	The Uighurs and Politics of identity In China *Camille Catania (University of Kent)*
1720 - 1740	Vulnerability Evaluation and Prioritization for Cyber Resilient Systems *Omer Keskin, Nick Gannon, Brian Lopez, Unal Tatar (University at Albany)*

1740 - 1900 **The Student Presentation Happy Hour**
Location: Gather

Wednesday, April 14

0930 - 0935 **Welcome**
Adam Tagert (National Security Agency)

0935 - 1030 **KEYNOTE: Spectre Attacks: Exploiting Speculative Execution - and why the heck is the computer speculating anyway?**
Werner Haas (Cyberus Technology)

1030 - 1045 **BREAK**

SESSION 4: Flanking the Defense

1045 - 1110	Leveraging EM Side-Channel Information to Detect Rowhammer Attacks **Zhenkai Zhang, */**Zihao Zhan, **Daniel Balasubramanian, †Bo Li, **Peter Volgyesi, **Xenofon Koutsoukos* **Texas Tech University, **Vanderbilt, University,* *†University of Illinois at Urbana-Champaign*
1110 - 1135	Counting Broken Links: A Quant's View of Software Supply Chain Security *Dan Geer, Bentz Tozer, John Speed Meyers (In-Q-Tel)*
1135 - 1220	Work-In-Progress Discussion Session: Device Profiling **Tushar Jois, **Claudia Moncaliano, †Khir Henderson, *Aviel D. Rubin* **Johns Hopkins University, **JHU APL, †Morgan State University*

1220 - 1300 **LUNCH & NETWORKING**

1300 - 1400 **KEYNOTE: Why rigorous underpinnings for cyber security education and training matter? Experiences from CyBOK: the Cyber Security Body of Knowledge**
Awais Rashid (University of Bristol)

1400 - 1415 **BREAK**

SESSION 5: Humans aren't only Users

1415 - 1440	Can Advanced Type Systems Be Usable? An Empirical Study of Ownership, Assets, and Typestate in Obsidian *Michael Coblenz, **Jonathan Aldrich, **Brad Myers, **Joshua Sunshine *University of Maryland, **Carnegie Mellon University
1440 - 1505	Adversarial Thinking - Teaching Students to Think Like a Hacker Frank Katz (Georgia Southern University)
1505 - 1550	Work-In-Progress Discussion Session: Practices in Software Development *Leysan Nurgalieva, **Alisa Frik, *Gavin Doherty *Trinity College Dublin, Ireland, **UC Berkeley

1550 - 1730	**POSTER SESSION ON GATHER**
2000 - 2130	Hard Problem Discussions

Thursday, April 15

0930 - 0935	**Welcome** *Adam Tagert (National Security Agency)*
0935 - 1030	**KEYNOTE: Working with academia at the UK National Cyber Security Centre** *Paul Waller (GCHQ)*
1030 - 1045	**BREAK**

SESSION 6: Saving the Physical World from Cyber

1045 - 1110	Verified Hardware/Software Co-Assurance: Enhancing Safety and Security for Critical Systems *David Hardin (Collins)*
1110 - 1135	überSpark: Practical, Provable, End-to-End Guarantees on Commodity Heterogenous Interconnected Computing Platforms *Amit Vasudevan, **Petros Maniatis, †Ruben Martins, *Anton Dimov Hristozov, *Bruce Krogh, *†Raffaele Romagnoli *SEI, CMU; **Google Research; †CSD, CMU; *†ECE, CMU
1135 - 1220	Work-In-Progress Discussion Session: Railway Infrastructure *Himanshu Neema, *Leqiang Wang, *Xenofon Koutsoukos, **CheeYee Tang, **Keith Stouffer *Vanderbilt University, **NIST

1220 - 1320	**LUNCH & NETWORKING**

SESSION 7: Go Where I Send Thee

1320 - 1405	Work-In-Progress Discussion Session: Studying App Reviews *Vaibhav Garg, *Hui Guo,**Nirav Ajmeri, *Munindar P. Singh *NCSU, **University of Bristol
1405 - 1430	ZeRØ: Zero-Overhead Resilient Operation Under Pointer Integrity Attacks *Mohamed Tarek, *Miguel Arroyo, *Evgeny Manzhosov, */**Simha Sethumadhavan *Columbia University, **Chip Scan
1430 - 1455	Insights for Systems Security Engineering from Multilayer Network Models *Adam Williams, Gabriel C. Birch, Susan Caskey, Elizabeth Fleming, Thushara Gunda, Thomas Adams, Jamie Wingo (Sandia)*

1455 - 1525 **BREAK**

SESSION 8: Potpourri for 1,000

1525 - 1550 AI-Powered Ransomware Detection Framework
Subash Poudya and Dipankar Dasgupta (Univ. of Memphis)

1550 - 1615 On Managing Vulnerabilities in AI/ML Systems
**Jonathan Spring, *April Galyardt, *Allen Householder, **Nathan M. VanHoudnos*
**CERT/CC, SEI, CMU; **SEI, CMU*

1615 - 1700 Work-In-Progress Discussion Session: Attestation and Game Theory
**Shanto Roy, *Salah Uddin Kadir, **Yevgeniy Vorobeychik, *Aron Laszka*
**University of Houston, **Washington University in St. Louis*

1700 - 1715 **Closing Remarks**

SYMPOSIUM ADJOURNED