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

0600 - 1600 Check out the virtual platforms and test your settings

Tuesday, April 13

0700 - 0730 Networking, log into the platform and chat with other attendees

0730 - 0800 Welcome and Opening Remarks
General Chair: *Adam Tagert (National Security Agency)*
Program Co-Chairs: *Özgür Kafali (University of Kent)*
Ahmad Ridley (National Security Agency)

0800 - 0900 **KEYNOTE: Securing Data in Clouds: Making the Most of Trusted Hardware**
Nick Felts (National Security Agency)

0900 - 0915 **BREAK / NETWORKING ON GATHER**

SESSION 1: Cloud Security

0915 - 0940 Formal Foundations for Intel SGX Data Center Attestation Primitives
Muhammed Usama Sardar, Rasha Faqeh, Christof Fetzer (TU Dresden)

0940 - 1005 A Secure and Formally Verified Linux KVM Hypervisor
Shih-Wei Li, Xupeng Li, Ronghui Gu, Jason Nieh, John Zhuang Hui (Columbia University)

1005 - 1050 Work-In-Progress Discussion Session: JavaScript Attacks
Ross Copeland and Drew Davidson (University of Kansas)

1050 - 1200 **LUNCH & NETWORKING**
Preview posters in Gather

SESSION 2: To Err is to Be Human

1200 - 1245 Work-In-Progress Discussion Session: Election Security
**Natalie Scala, *Josh Dehlinger, **Paul L. Goethals*
**Towson University, **USMA*

1245 - 1330 Work-In-Progress Discussion Session: Phishing
**Dennis Roellke, *Salvatore Stolfo, *George Litvinov, **Shlomo Herschkopp, †Mark Seiden*
**Columbia University, **Allure Security, †Internet Archive*

1330 - 1400 **BREAK**

SESSION 3: Student Presentations

1400 - 1420	Analysis of the Impact of Varying Statistical RF Fingerprint Features on IoT Device Classification *Asia Mason (Morgan State University)*
1420 - 1440	MAZE: A Secure Cloud Storage Service Using Moving Target Defense and Secure Shell Protocol (SSH) Tunneling *Vasco Xu and Sherif Khattab (University of Pittsburgh)*
1440 - 1500	Performance improvement of anomaly detection on IoT network *Latha Suryavanshi Karakos and Jumoke Ladeji-Osias (Morgan State University)*
1500 - 1520	The Uighurs and Politics of identity In China *Camille Catania (University of Kent)*
1520 - 1540	Vulnerability Evaluation and Prioritization for Cyber Resilient Systems *Omer Keskin, Nick Gannon, Brian Lopez, Unal Tatar (University at Albany)*

1540 - 1700 **The Student Presentation Happy Hour**
Location: Gather

Wednesday, April 14

0730 - 0735	**Welcome** *Adam Tagert (National Security Agency)*
0735 - 0830	**KEYNOTE: Spectre Attacks: Exploiting Speculative Execution - and why the heck is the computer speculating anyway?** *Werner Haas (Cyberus Technology)*
0830 - 0845	**BREAK**

SESSION 4: Flanking the Defense

0845 - 0910	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*
0910 - 0935	Counting Broken Links: A Quant's View of Software Supply Chain Security *Dan Geer, Bentz Tozer, John Speed Meyers (In-Q-Tel)*
0935 - 1020	Work-In-Progress Discussion Session: Device Profiling **Tushar Jois, **Claudia Moncaliano, †Khir Henderson, *Aviel D. Rubin* **Johns Hopkins University, **JHU APL, †Morgan State University*

1020 - 1100	**LUNCH & NETWORKING**
1100 - 1200	**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)*
1200 - 1215	**BREAK**

SESSION 5: Humans aren't only Users

1215 - 1240	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
1240 - 1305	Adversarial Thinking - Teaching Students to Think Like a Hacker Frank Katz (Georgia Southern University)
1305 - 1350	Work-In-Progress Discussion Session: Practices in Software Development *Leysan Nurgalieva, **Alisa Frik, *Gavin Doherty *Trinity College Dublin, Ireland, **UC Berkeley

1350 - 1530	**POSTER SESSION ON GATHER**
1800 - 1930	Hard Problem Discussions

Thursday, April 15

0730 - 0735	**Welcome** *Adam Tagert (National Security Agency)*
0735 - 0830	**KEYNOTE: Working with academia at the UK National Cyber Security Centre** *Paul Waller (GCHQ)*
0830 - 0845	**BREAK**

SESSION 6: Saving the Physical World from Cyber

0845 - 0910	Verified Hardware/Software Co-Assurance: Enhancing Safety and Security for Critical Systems *David Hardin (Collins)*
0910 - 0935	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
0935 - 1020	Work-In-Progress Discussion Session: Railway Infrastructure *Himanshu Neema, *Leqiang Wang, *Xenofon Koutsoukos, **CheeYee Tang, **Keith Stouffer *Vanderbilt University, **NIST

1020 - 1120	**LUNCH & NETWORKING**

SESSION 7: Go Where I Send Thee

1120 - 1205	Work-In-Progress Discussion Session: Studying App Reviews *Vaibhav Garg, *Hui Guo,**Nirav Ajmeri, *Munindar P. Singh *NCSU, **University of Bristol
1205 - 1230	ZeRØ: Zero-Overhead Resilient Operation Under Pointer Integrity Attacks *Mohamed Tarek, *Miguel Arroyo, *Evgeny Manzhosov, */**Simha Sethumadhavan *Columbia University, **Chip Scan
1230 - 1255	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)*

1255 - 1325 **BREAK**

SESSION 8: Potpourri for 1,000

1325 - 1350 AI-Powered Ransomware Detection Framework
Subash Poudya and Dipankar Dasgupta (Univ. of Memphis)

1350 - 1415 On Managing Vulnerabilities in AI/ML Systems
**Jonathan Spring, *April Galyardt, *Allen Householder, **Nathan M. VanHoudnos*
**CERT/CC, SEI, CMU; **SEI, CMU*

1415 - 1500 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*

1500 - 1515 **Closing Remarks**

SYMPOSIUM ADJOURNED