# 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

0700 - 1700 Check out the virtual platforms and test your settings

## Tuesday, April 13

0800 - 0830 Networking, log into the platform and chat with other attendees

0830 - 0900 Welcome and Opening Remarks
General Chair: *Adam Tagert (National Security Agency)*
Program Co-Chairs: *Özgür Kafali (University of Kent)*
*Ahmad Ridley (National Security Agency)*

0900 - 1000 **KEYNOTE: Securing Data in Clouds: Making the Most of Trusted Hardware**
*Nick Felts (National Security Agency)*

1000 - 1015 **BREAK / NETWORKING ON GATHER**

---

**SESSION 1: Cloud Security**

---

1015 - 1040 Formal Foundations for Intel SGX Data Center Attestation Primitives
*Muhammed Usama Sardar, Rasha Faqeh, Christof Fetzer (TU Dresden)*

1040 - 1105 A Secure and Formally Verified Linux KVM Hypervisor
*Shih-Wei Li, Xupeng Li, Ronghui Gu, Jason Nieh, John Zhuang Hui (Columbia University)*

1105 - 1150 Work-In-Progress Discussion Session: JavaScript Attacks
*Ross Copeland and Drew Davidson (University of Kansas)*

---

1150 - 1300 **LUNCH & NETWORKING**
Preview posters in Gather

---

**SESSION 2: To Err is to Be Human**

---

1300 - 1345 Work-In-Progress Discussion Session: Election Security
**Natalie Scala, *Josh Dehlinger, **Paul L. Goethals*
**Towson University, **USMA*

1345 - 1430 Work-In-Progress Discussion Session: Phishing
**Dennis Roellke, *Salvatore Stolfo, *George Litvinov, **Shlomo Herschkopp, †Mark Seiden*
**Columbia University, **Allure Security, †Internet Archive*

---

1430 - 1500 **BREAK**

**SESSION 3: Student Presentations**

| | |
|---|---|
| 1500 - 1520 | Analysis of the Impact of Varying Statistical RF Fingerprint Features on IoT Device Classification<br>*Asia Mason (Morgan State University)* |
| 1520 - 1540 | MAZE: A Secure Cloud Storage Service Using Moving Target Defense and Secure Shell Protocol (SSH) Tunneling<br>*Vasco Xu and Sherif Khattab (University of Pittsburgh)* |
| 1540 - 1600 | Performance improvement of anomaly detection on IoT network<br>*Latha Suryavanshi Karakos and Jumoke Ladeji-Osias (Morgan State University)* |
| 1600 - 1620 | The Uighurs and Politics of identity In China<br>*Camille Catania (University of Kent)* |
| 1620 - 1640 | Vulnerability Evaluation and Prioritization for Cyber Resilient Systems<br>*Omer Keskin, Nick Gannon, Brian Lopez, Unal Tatar (University at Albany)* |

1640 - 1800 **The Student Presentation Happy Hour**
*Location: Gather*

# Wednesday, April 14

| | |
|---|---|
| 0830 - 0835 | **Welcome**<br>*Adam Tagert (National Security Agency)* |
| 0835 - 0930 | **KEYNOTE: Spectre Attacks: Exploiting Speculative Execution - and why the heck is the computer speculating anyway?**<br>*Werner Haas (Cyberus Technology)* |
| 0930 - 0945 | **BREAK** |

**SESSION 4: Flanking the Defense**

| | |
|---|---|
| 0945 - 1010 | Leveraging EM Side-Channel Information to Detect Rowhammer Attacks<br>**Zhenkai Zhang, */**Zihao Zhan, **Daniel Balasubramanian, †Bo Li, **Peter Volgyesi, **Xenofon Koutsoukos*<br>**Texas Tech University, **Vanderbilt, University,*<br>*†University of Illinois at Urbana-Champaign* |
| 1010 - 1035 | Counting Broken Links: A Quant's View of Software Supply Chain Security<br>*Dan Geer, Bentz Tozer, John Speed Meyers (In-Q-Tel)* |
| 1035 - 1120 | Work-In-Progress Discussion Session: Device Profiling<br>**Tushar Jois, **Claudia Moncaliano, †Khir Henderson, *Aviel D. Rubin*<br>**Johns Hopkins University, **JHU APL, †Morgan State University* |

| | |
|---|---|
| 1120 - 1200 | **LUNCH & NETWORKING** |
| 1200 - 1300 | **KEYNOTE: Why rigorous underpinnings for cyber security education and training matter? Experiences from CyBOK: the Cyber Security Body of Knowledge**<br>*Awais Rashid (University of Bristol)* |
| 1300 - 1315 | **BREAK** |

**SESSION 5: Humans aren't only Users**

1315 - 1340 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

1340 - 1405 Adversarial Thinking - Teaching Students to Think Like a Hacker
Frank Katz (Georgia Southern University)

1405 - 1450 Work-In-Progress Discussion Session: Practices in Software Development
*Leysan Nurgalieva, **Alisa Frik, *Gavin Doherty*
**Trinity College Dublin, Ireland, **UC Berkeley*

1450 - 1630 **POSTER SESSION ON GATHER**

1900 - 2030 Hard Problem Discussions

# Thursday, April 15

0830 - 0835 **Welcome**
*Adam Tagert (National Security Agency)*

0835 - 0930 **KEYNOTE: Working with academia at the UK National Cyber Security Centre**
*Paul Waller (GCHQ)*

0930 - 0945 **BREAK**

**SESSION 6: Saving the Physical World from Cyber**

0945 - 1010 Verified Hardware/Software Co-Assurance: Enhancing Safety and Security for Critical Systems
*David Hardin (Collins)*

1010 - 1035 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*

1035 - 1120 Work-In-Progress Discussion Session: Railway Infrastructure
*Himanshu Neema, *Leqiang Wang, *Xenofon Koutsoukos,*
***CheeYee Tang, **Keith Stouffer*
**Vanderbilt University, **NIST*

1120 - 1220 **LUNCH & NETWORKING**

**SESSION 7: Go Where I Send Thee**

1220 - 1305 Work-In-Progress Discussion Session: Studying App Reviews
*Vaibhav Garg, *Hui Guo,**Nirav Ajmeri, *Munindar P. Singh*
**NCSU, **University of Bristol*

1305 - 1330 ZeRØ: Zero-Overhead Resilient Operation Under Pointer Integrity Attacks
*Mohamed Tarek, *Miguel Arroyo, *Evgeny Manzhosov, */**Simha Sethumadhavan*
**Columbia University, **Chip Scan*

1330 - 1355 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)*

1355 - 1425 **BREAK**

**SESSION 8: Potpourri for 1,000**

1425 - 1450 AI-Powered Ransomware Detection Framework
*Subash Poudya and Dipankar Dasgupta (Univ. of Memphis)*

1450 - 1515 On Managing Vulnerabilities in AI/ML Systems
**Jonathan Spring, *April Galyardt, *Allen Householder, **Nathan M. VanHoudnos*
**CERT/CC, SEI, CMU; **SEI, CMU*

1515 - 1600 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*

1600 - 1615 **Closing Remarks**

**SYMPOSIUM ADJOURNED**