HotSoS 2020 Program Agenda

Submitted by willim1 on Wed, 03/04/2020 - 2:33pm

MONDAY, SEPTEMBER 21
1730 - 1930 Evening Reception at The Burge Union 1565 Irving Hill Rd. Lawrence, KS

TUESDAY, SEPTEMBER 22
0800 - 1730 Registration | Continental Breakfast (until 0830)

0830 - 0845 Chair's Opening Remarks
Symposium Chairs: Perry Alexander, Baek-Young Choi, and Drew Davidson

NSA Opening Remarks

0845 - 0945 Keynote Presentation: Access Control Verification for Everyone
Andrew Gacek, Amazon Web Services

0945 - 1000 BREAK

PAPER SESSION 1: CPS and Industrial Control
(20 minutes per paper with 10 minutes of flex in the block)
1000 - 1130 Simulation Testbed for Railway Infrastructure Security and Resilience Evaluation
*Himanshu Neema, *Xenofon Koutsoukos, **Bradley Potteiger, and ?Cheeyee Tang
*Vanderbilt University, **Johns Hopkins Applied Physics Lab, ?National Institute of Standards and Technology

@PAD: Adversarial Training of Power Systems Against Denial of Service Attacks
Ali Ozdagli, Carlos Barreto, and Xenofon Koutsoukos
Vanderbilt University
# The More the Merrier: Adding Hidden Measurements for Anomaly Detection and Mitigation in Industrial Control Systems
*Jairo Giraldo, **David Urbina, ?Cheeyee Tang, and ??Alvaro Cardenas
*University of Utah, **University of Texas at Dallas, ?National Institute of Standards and Technology, ??The University of California, Santa Cruz

# RUCKUS: A Cybersecurity Engine for Performing Autonomous Cyber-Physical System Vulnerability Discovery at Scale
Bradley Potteiger, Jacob Mills, Daniel Cohen, and Paul Velez
Johns Hopkins Applied Physics Lab

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>1130 - 1300</td>
<td><strong>LUNCH</strong></td>
</tr>
</tbody>
</table>
| 1300 - 1400| **Keynote Presentation: Is Hardware Root of Trust hard to do, and Trustworthy?**
Lyle Paczkowski, Sprint
| 1400 - 1415| **BREAK**                                  |

## WORKS IN PROGRESS (WiP) SESSION 1
<table>
<thead>
<tr>
<th>Time</th>
<th>Authors</th>
</tr>
</thead>
</table>
| 1415 - 1500| *Hao Xue, *Qiaozhi Wang, *Bo Lou, **Chao Lan, *Fenjun Li
*University of Kansas, **University of Wyoming
| 1500 - 1545| Jacob Fustos, Heechul Yun
University of Kansas
| 1545 - 1600| **BREAK**                                   |

## PAPER SESSION 2: Modeling
*(20 minutes per paper with 10 minutes of flex in the block)*
<table>
<thead>
<tr>
<th>Time</th>
<th>Title</th>
</tr>
</thead>
</table>
| 1600 - 1730| Exploring Hackers Assets: Topics of Interest as Indicators of Compromise
Mohammad Alramahi, Izzat Alsmadi, and Joshua Davenport
Texas A&M, San Antonio
Cyber Threat Modeling and Validation: Port Scanning and Detection
Eric Vugrin, Jerry Cruz, Christian Reedy, Thomas Tarman, and Ali Pinar
Sandia National Laboratories

Can We Use Software Bugs to Identify Software Vulnerability Strategies
Farzana Ahamed Bhuiyan, Raunak Shakya, and Akond Rahman
Tennessee Technological University

Automated Influence and the Challenge of Cognitive Security
Sarah Rajtmajer and Daniel Susser
Pennsylvania State University

1730 - 1900  POSTER SESSION

WEDNESDAY, SEPTEMBER 23

0800 - 1630  Registration | Continental Breakfast (until 0830)

0830 - 0930  Keynote Presentation: Trust Engineering with Cryptographic Protocols
Joshua Guttman, WPI/MITRE

0930 - 0945  BREAK

WORKS IN PROGRESS (WiP) SESSION 2

0945 - 1030  *Sohaib Kiani, *Fengjun Li, **Chao Lan, and *Bo Luo
*University of Kansas, **University of Wyoming

1030 - 1115  Ryan Karl, Jonathan Takeshita, and Taeho Jung
University of Notre Dame

1115 - 1130  BREAK

1130 - 1230  Keynote Presentation: Evaluating Fuzz Testing (and other technologies)
Michael Hicks, University of Maryland
1230 - 1400  LUNCH

WORKS IN PROGRESS (WiP)
SESSION 3

1400 - 1445  Tsion Yimer, Md Tanvir Arafim, and Kevin Kornegay
             Morgan State University

1445 - 1530  Sana Awan, Fenjun Li, Bo Luo
             University of Kansas

1530 - 1545  BREAK

PAPER SESSION 3: Systems

1545 - 1715  Neutralizing Manipulation of Critical Data by Enforcing
             Data-Instruction Dependency
             Chandra Sharma, Nathan Miller, and George Amariucai
             Kansas State University

             Ghostbusting: Mitigating Spectre with Intraprocess
             Memory Isolation
             Ira Jenkins, Prashant Anantharaman, Rebecca Shapiro, J
             Peter Brady, Sergey Bratus, and Sean Smith
             Dartmouth College

             WOLF: Automated Machine Learning Workflow
             Management Framework for Malware Detection and Other
             Applications
             Sohaib Kiani, Sana Awan, Fengjun Li, and Bo Luo
             University of Kansas

             A Formal Security Analysis of Zigbee
             *Li Li, **Proyash Podder, and *Endadul Hoque
             *Syracuse University, **Florida International University

1715 - 1730  Announcement of Winning Paper and Winning
             Poster
             Adam Tagert

             Closing Remarks
             Perry Alexander

SYMPOSIUM ADJOURNED
HotSoS 2020 Agenda