# HotSoS 2018 Program

Submitted by Katie Dey on Thu, 02/15/2018 - 11:50am

## PROGRAM AGENDA

<table>
<thead>
<tr>
<th>MONDAY, APRIL 9</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>1830 - 2030 Evening Reception at The StateView Hotel</td>
<td>Fusion Patio</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TUESDAY, APRIL 10</th>
<th>Fusion C/D Foyer</th>
</tr>
</thead>
<tbody>
<tr>
<td>0730 - 1700 Registration</td>
<td></td>
</tr>
</tbody>
</table>

### SESSION 1

<table>
<thead>
<tr>
<th>Time</th>
<th>Session Details</th>
</tr>
</thead>
</table>
| 0830 - 0900 | **Welcome and Introduction**  
Symposium Co-Chairs: Laurie Williams and Munindar Singh |
| 0900 - 1000 | **Keynote:** Steve Lipner, Executive Director, SAFECODE  
*Foundational Cybersecurity Research: Report of a Study by NASEM* |
| 1000 - 1045 | **BREAK and POSTER SESSION** |

### SESSION 2

<table>
<thead>
<tr>
<th>Time</th>
<th>Session Details</th>
</tr>
</thead>
</table>
| 1045 - 1110 | **Paper Track: Vulnerabilities and Detection**  
**Tutorial/Industry Track (Synergy B)**  
(Fusion C/D)  
*Pooria Madani and Natalija Vlajic*  
University of York  
*Robustness of Deep Autoencoder in Intrusion Detection under Adversarial Contamination*  
* Dimitris Simos and *Rick Kuhn*  
SBA Research, *NIST*  
*Tutorial: Combinatorial Security Testing Course* |
1110 - 1135  Inger Anne Tøndel, *Tosin Daniel Oyetoyan, *Martin Gilje Jaatun and *Daniela S. Cruzes
Norwegian University of Science and Technology, *SINTEF Digital

Understanding the Challenges to Adoption of the Microsoft Elevation of Privilege Game

1135 - 1200  Ira Ray Jenkins, Sergey Bratus, Sean Smith and *Maxwell Koo
Dartmouth College, *Narf Industries


1200 - 1315  LUNCH

Lunch Presentation:
Erkang Zheng, Phil Gates-Idem and Matt Lavin
LifeOmic, Inc.

Building a Virtually Air-gapped Secure Environment in AWS

SESSION 3

1315 - 1415  Keynote: Ari Schwartz, Venable LLP

You've Got a Vuln, I've Got a Vuln, Everybody's Got a Vuln

1415 - 1515  Panel: Cybersecurity Framework Practitioners
Moderator: Nikola Vouk, Independent

Jeremy Maxwell, Allscripts
Andrew Porter, Merck
Alex Rogozhin, BB&T
Greg Witte, G2

1515 - 1600  BREAK and POSTER SESSION

SESSION 4

Paper Track: Secure Construction (Fusion C/D)

Tutorial/Industry Track (Synergy B)
1600 - 1625 Yao Dong, Ana Milanova and Julian Dolby, Rensselaer Polytechnic Institute, IBM
SecureMR: Secure MapReduce Computation Using Homomorphic Encryption and Program Partitioning

1625 - 1650 Bradley Potteiger, Zhenkai Zhang and Xenofon Koutsoukos, Vanderbilt University
Integrated Instruction Set Randomization and Control Reconfiguration for Securing Cyber-Physical Systems

1650 - 1715 Iness Ben Guirat and Harry Halpin, INSAT, INRIA
Formal Verification of the W3C Web Authentication Protocol

SESSION 5
1715 - 1800 BREAK

1800 Shuttle bus to the North Carolina Museum of Art. Meet in the hotel lobby. (Don't be late!)

1830 - 2100 Dinner at the North Carolina Museum of Art

WEDNESDAY, APRIL 11

0830 - 1530 Registration

SESSION 6
0900 - 1000 Keynote: David Burke, NAVAIR Cyber Warfare Detachment
Cyber Security for Aviation Weapon Systems
SESSION 7

**Paper Track: Applications and Risk Evaluation (Fusion C/D)**

1045 - 1110 Martha McNeil, Thomas Llanso and Dallas Pearson
Johns Hopkins University Applied Physics Laboratory
*Application of Capability-Based Cyber Risk Assessment Methodology to a Space System*

1110 - 1135 Daniela S. Cruzes, Martin Gilje Jaatun and Tosin Daniel Oyetoyan
SINTEF Digital
*Challenges and Approaches of Performing Canonical Action Research in Software Security*

?University of Texas at San Antonio, *Army Research Lab
*Quantifying the Security Effectiveness of Firewalls and DMZs*

1200 - 1315 **LUNCH**

SESSION 8

1315 - 1345 Michelle Mazurek, University of Maryland
NSA Fifth Annual Best Scientific Cybersecurity Paper Competition Winner
*You Get Where You're Looking For: The Impact of Information Sources on Code Security*

1345 - 1415 Daniel Gruss, Graz University of Technology
*Microarchitectural Attacks: From the Basics to Arbitrary Read and Write Primitives without any Software Bugs*

1415 - 1430 **BREAK**

1430 - 1530 **Keynote:** Ravi Sandhu, University of Texas at San Antonio
*An Access Control Perspective on the Science of Security*

1530 **Announcement of Winning Paper and Winning Poster**
Carl Landwehr and Adam Tagert

**Closing Remarks**
Laurie Williams and Munindar Singh