

Preface

The goal of Hot Topics in the Science of Security (HoTSoS) is bringing together researchers, practitioners, and thought leaders from government, industry, and academia, and to provide a forum for dialogue focused on developing and advancing scientific foundations in cybersecurity. The unique technical emphasis of HoTSoS is building a foundational science of security. Specifically, incorporating scientific methods, data gathering and analysis, experimental approaches, mathematical models, and the interactions among them to create a scientific basis for security.

The 7th Annual HotSoS Symposium, hosted by The University of Kansas, was held virtually September 22–24, 2020 after a several month COVID-19 delay. The symposium included a mix of invited talks, presentations of refereed papers, a work in progress/work already published session, a poster session, and a special workshop session with the goal of providing the authors and the security community with early, in-depth feedback on new unpublished research.

As in previous years, HotSoS 2020 focuses on problems related to:

- Scalability and composability in the construction of secure systems,
- Policy-governed collaboration for handling data across different domains of authority while ensuring security and privacy,
- Security metrics and improved measurement tools, to guide choice-making in security engineering and response,
- Resilient architectures that can deliver service despite compromised components,
- Analysis of human behavior, encompassing users, operators, and adversaries, to support improved cybersecurity design.

Submissions were subject to a rigorous reviewing process, and ultimately 12 out of 17 papers submitted to the symposium were accepted, including one systemization of knowledge paper. In addition, 6 papers submitted to the special workshop session were accepted. The program also included 20 posters that were presented during the poster sessions.

We are grateful to Joshua Guttman, Michael Hicks, Andrew Gacek, and Lyle Paczkowski for giving keynote talks at HoTSoS and we thank the members of the program committee for all their work. We thank Jason Hayden for helping with logistics and moving HoTSoS from April to September in one day. We would like to express our appreciation to Katie Dey for her outstanding support including managing the web site, interfacing with ACM, scheduling, and generally keeping us on the right path. Finally, we thank Adam Tagert and Heather Lucas for helping with conference organization and acknowledge the National Security Agency (NSA) for their continual support of the science of security community.

Drew Davidson & Baek-Young Choi – Program Chairs
Perry Alexander – General Chair

HoTSoS 2020

Lawrence, Kansas, USA
September 22-24, 2020

Sponsored by *National Security Agency*

Organized in cooperation with *ACM SIGSAC*

General Chair

Perry Alexander – The University of Kansas

Program Co-Chairs

Drew Davidson – The University of Kansas

Baek-Young Choi – University of Missouri, Kansas City

Publications Chair

Koyel Pramanic – The University of Kansas

Local Arrangements Co-Chairs

Katie Dey – Vanderbilt University

Jason Hayden – The University of Kansas

NSA Liasons

Heather Lucas

Adam Tagert

Graphic Design

Amy Karns – Vanderbilt University

Program Committee

Drew Davidson	The University of Kansas
Baek-Young Choi	University of Missouri, Kansas City
Adam Tagert	National Security Agency
Alexandru Bardas	The University of Kansas
Gul Agha	University of Illinois at Urbana-Champaign
Nirav Ajmeri	North Carolina State University
Bo Luo	The University of Kansas
Fengjun Li	The University of Kansas
Vaibhav Rastogi	Google
Lorenzo De Carli	Worcester Polytechnic Institute
Alvaro Cardenas	The University of California, Santa Cruz
Heechul Yun	The University of Kansas
Eric Clemons	Department of Defense
Ehab Al-Shaer	UNC Charlotte
Perry Alexander	The University of Kansas
Homa Alemzadeh	University of Virginia

Table of Contents

Simulation Testbed for Railway Infrastructure Security and Resilience Evaluation	1
<i>Himanshu Neema¹, Xenofon Koutsoukos¹, Bradley Potteiger², and Cheegee Tang³</i>	
@PAD: Adversarial Training of Power Systems Against Denial of Service Attacks	9
<i>Ali I Ozdagli, Carlos Barreto, and Xenofon Koutsoukos</i>	
The More the Merrier: Adding Hidden Measurements for Anomaly Detection and Mitigation in Industrial Control Systems	18
<i>Jairo Giraldo¹, David Urbina², Cheegee Tang³, and Alvaro Cardenas⁴</i>	
RUCKUS: A Cybersecurity Engine for Performing Autonomous Cyber-Physical System Vulnerability Discovery at Scale	28
<i>Bradley Potteiger, Jacob Mills, Daniel Cohen, and Paul Velez</i>	
Exploring Hackers Assets: Topics of Interest as Indicators of Compromise	38
<i>Mohammad Alramahi, Izzat Alsmadi, and Joshua Davenport</i>	
Cyber Threat Modeling and Validation: Port Scanning and Detection ..	42
<i>Eric Vugrin, Jerry Cruz, Christian Reedy, Thomas Tarmann, and Ali Pinar</i>	
Can We Use Software Bug Reports to Identify Software Vulnerability Strategies	52
<i>Farzana Ahamed Bhuiyan, Raunak Shakya, and Akond Rahman</i>	
Automated Influence and the Challenge of Cognitive Security	62
<i>Sarah Rajtmajer and Daniel Susser</i>	
Neutralizing Manipulation of Critical Data by Enforcing Data-Instruction Dependency	71
<i>Chandra Sharma, Nathan Miller, and George Amariuca</i>	
Ghostbusting: Mitigating Spectre with Intraprocess Memory Isolation ...	82
<i>Ira Jenkins, Prashant Anantharaman, Rebecca Shapiro, J Peter Brady, Sergey Bratus, and Sean Smith</i>	
WOLF: Automated Machine Learning Workflow Management Framework for Malware Detection and Other Applications	93
<i>Sohaib Kiani, Sana Awan, Fengjun Li, and Bo Luo</i>	

A Formal Security Analysis of Zigbee	101
<i>Li Li¹, Proyash Podder², and Endadul Hoque¹</i>	
Poster: A Curated Dataset of Security Defects in Scientific Software Projects	112
<i>Justin Murphy, Elias T. Brady, Shazibul Islam Shamim, and Akond Rahman</i>	
Poster: A Preliminary Taxonomy of Techniques Used in Software Fuzzing	114
<i>Raunak Shakya and Akond Rahman</i>	
Poster: A Raspberry Pi Sensor Network for Wildlife Conservation	116
<i>Andrew Arnold, Paul Corapi, Michael Nasta, Kevin Wolgast, and Thomas A. Babbitt</i>	
Poster: Accelerating Block Propagation in PoW Blockchain Networks with Pipelining and Chunking (PiChu)	119
<i>Kaushik Ayinala, Baek-Young Choi, and Sejun Song</i>	
Poster: An Infrastructure for Faithful Execution of Remote Attestation Protocols	121
<i>Adam Petz</i>	
Poster: An seL4-based Architecture for Layered Attestation	122
<i>Grant Jurgensen, Michael Neises, and Perry Alexander</i>	
Poster: An Uncertain Graph-based Approach for Cyber-security Risk Assessment	124
<i>Hoang Hai Nguyen</i>	
Poster: Application of the Armament Cyber Assessment Framework	126
<i>Aidan McCarthy, Liam Furey, Keagan Smith, Daniel Hawthorne, and Raymond Blaine</i>	
Poster: Approaches to Ethical Hacking: Expanding Conceptual Frameworks for Research	128
<i>Danielle Alexander, Rebecca Labitt, and Asher Rodriguez</i>	
Poster: Decentralized Backup and Recovery of TOTP Secrets	129
<i>Conor Gilsean, Noura Alomar, and Andrew Huang</i>	
Poster: Do Configuration Management Tools Make Systems More Secure? An Empirical Research Plan	131
<i>Md Rayhanur Rahman, William Enck, and Laurie Williams</i>	
Poster: Exploiting DRAM Bank Mapping and HugePages for Effective Denial-of-Service Attacks on Shared Cache in Multicore	133
<i>Michael Bechtel and Heechul Yun</i>	

VI

Poster: How to Swap Instructions Midstream: An Embedding Algorithm For Program Steganography	135
<i>Ryan Gabrys, Luis Martinez, and Sunny Fugate</i>	
Poster: Improving Architectures for Automating Network Security Using Specification-Based Protocols	137
<i>Khir Henderson and Kevin Kornegay</i>	
Poster: Resilient Multi-Robot Target Pursuit	139
<i>Jiani Li¹, Waseem Abbas¹, Xenofon Kousoukos¹, and Mudassir Shabbir²</i>	
Poster: Time Series Anomaly Detection in Medical Break The Glass	141
<i>Qais Tasali, Nikesh Gyawali, and Eugene Y. Vasserman</i>	
Poster: Tokens of Interaction: Psycho-physiological Signals, A Potential Source of Evidence of Digital Incidents	143
<i>Nancy Mogire</i>	
Poster: Toward Just-in-Time Patching for Containerized Applications	145
<i>Olufogorehan Tunde-Onadele, Yuhang Lin, Jingzhu He, and Xiaohui Gu</i>	
Poster: Using Intel SGX to Improve Private Neural Network Training and Inference	147
<i>Ryan Karl, Jonathan Takeshita, and Taeho Jung</i>	
Poster: Vulnerability Trends in Web Servers and Browsers	149
<i>M S Raunak¹, Richard Kuhn², Richard Kogut¹, and Raghu Kacker²</i>	
Author Index	150

Simulation Testbed for Railway Infrastructure Security and Resilience Evaluation

Himanshu Neema¹, Xenofon Koutsoukos¹, Bradley Pottleiger², and Cheeyee Tang³

¹Vanderbilt University, ²Johns Hopkins Applied Physics Lab, ³National Institute of Standards and Technology

@PAD: Adversarial Training of Power Systems Against Denial of Service Attacks

Ali I 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 Giraldo¹, David Urbina², Cheeyee Tang³, and Alvaro Cardenas⁴

¹University of Utah, ²University of Texas at Dallas, ³National Institute of Standards and Technology, ⁴The 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

Vanderbilt University

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 Bug Reports 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

Neutralizing Manipulation of Critical Data by Enforcing Data-Instruction Dependency

Chandra Sharma, Nathan Miller, and George Amariucaí

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

The University of Kansas

A Formal Security Analysis of Zigbee

Li Li¹, Proyash Podder², and Endadul Hoque¹

¹Syracuse University, ²Florida International University,

Poster: A Curated Dataset of Security Defects in Scientific Software Projects

Justin Murphy, Elias T. Brady, Shazibul Islam Shamim, and Akond Rahman

Tennessee Technological University

Poster: A Preliminary Taxonomy of Techniques Used in Software Fuzzing

Raunak Shakya and Akond Rahman

Tennessee Technological University

Poster: A Raspberry Pi Sensor Network for Wildlife Conservation

Andrew Arnold, Paul Corapi, Michael Nasta, Kevin Wolgast, and Thomas A.
Babbitt

United States Military Academy

**Poster: Accelerating Block Propagation in PoW
Blockchain Networks with Pipelining and
Chunking (PiChu)**

Kaushik Ayinala, Baek-Young Choi, and Sejun Song

University of Missouri, Kansas City

Poster: An Infrastructure for Faithful Execution of Remote Attestation Protocols

Adam Petz

The University of Kansas

Poster: An seL4-based Architecture for Layered Attestation

Grant Jurgensen, Michael Neises, and Perry Alexander

The University of Kansas

Poster: An Uncertain Graph-based Approach for Cyber-security Risk Assessment

Hoang Hai Nguyen

University of Illinois Urbana Champaign,

Poster: Application of the Armament Cyber Assessment Framework

Aidan McCarthy, Liam Furey, Keagan Smith, Daniel Hawthorne, and
Raymond Blaine

The United States Military Academy

Poster: Approaches to Ethical Hacking: Expanding Conceptual Frameworks for Research

Danielle Alexander, Rebecca Labitt, and Asher Rodriguez

Simmons University

Poster: Decentralized Backup and Recovery of TOTP Secrets

Conor Gilsonan, Noura Alomar, and Andrew Huang

UC Berkeley

Poster: Do Configuration Management Tools Make Systems More Secure? An Empirical Research Plan

Md Rayhanur Rahman, William Enck, and Laurie Williams

North Carolina State University

**Poster: Exploiting DRAM Bank Mapping and
HugePages for Effective Denial-of-Service
Attacks on Shared Cache in Multicore**

Michael Bechtel and Heechul Yun

The University of Kansas

**Poster: How to Swap Instructions Midstream:
An Embedding Algorithm For Program
Steganography**

Ryan Gabrys, Luis Martinez, and Sunny Fugate

Naval Information Warfare Center

Poster: Improving Architectures for Automating Network Security Using Specification-Based Protocols

Khair Henderson and Kevin Kornegay

Morgan State University

Poster: Resilient Multi-Robot Target Pursuit

Jiani Li¹, Waseem Abbas¹, Xenofon Kousoukos¹, and Mudassir Shabbir²

¹Vanderbilt University, ²Information Technology University, Lahore, Pakistan

Poster: Time Series Anomaly Detection in Medical Break The Glass

Qais Tasali, Nikesh Gyawali, and Eugene Y. Vasserman

Kansas State University

**Poster: Tokens of Interaction:
Psycho-physiological Signals, A Potential Source
of Evidence of Digital Incidents**

Nancy Mogire

University of Hawaii

Poster: Toward Just-in-Time Patching for Containerized Applications

Olufogorehan Tunde-Onadele, Yuhang Lin, Jingzhu He, and Xiaohui Gu

North Carolina State University

Poster: Using Intel SGX to Improve Private Neural Network Training and Inference

Ryan Karl, Jonathan Takeshita, and Taeho Jung

University of Notre Dame

Poster: Vulnerability Trends in Web Servers and Browsers

M S Raunak¹, Richard Kuhn², Richard Kogut¹, and Raghu Kacker²

¹Loyola University Maryland, ²National Institute of Standards and Technology

