Call for Papers

6th Annual **HOT TOPICS** *in the* **SCIENCE OF SECURITY** ***(HoTSoS)***

APRIL 2-3, 2019 | NASHVILLE, TENNESSEE

https://hotsos.org

Overview

Submissions are solicited for the 6th Annual Hot Topics in the Science of Security (HoTSoS) Symposium, which will be held April 2-4, 2019 at the Wyatt Center on the Peabody Campus of Vanderbilt University in Nashville, Tennessee. This symposium solicits original and solid scientific work in security and privacy which examines the scientific foundations of trustworthy systems for security and privacy, and it can be generalized across multiple domains with quantifiable evidence for advancing security objectives. The symposium program will include invited talks, refereed papers, panels, tutorials, and posters. The poster session will include a poster competition on developing security metrics. The papers will appear in the conference proceedings to be published by ACM Press.

Themes

We invite submissions on any topic related to science of security that aligns with the conference scope and goals listed above. The 2019 HoTSoS will highlight the following themes:

- **Resilient Architectures** for designing and analyzing system architectures that deliver required service in the face of compromised components,
- **Scalability and Composability** for automating the construction of provably secure systems from components with known security properties,
- **Policy-Governed Secure Collaboration** for handling data across different domains of authority while ensuring security and privacy,
- **Security-Metrics-Driven Development and Evaluation** for guiding choice-making in security engineering and response by assuring or predicting the security properties of cyber systems,
- **Understanding and Accounting for Human Behavior**, including modeling users, operators, and adversaries, to for enabling the design, modeling, and analysis of systems with specified security properties,
- **Privacy Policy Enforcement** for enabling the use (i.e., collect, store, and share) of data in accordance with requirements, and
- F**oundations for the Security of Cyber-Physical Systems Security and Resilience**, including applications to the Internet of Things.

Important Dates

Full Paper/Tutorial/Talk Submissions:	January 7, 2019
General Poster Submissions:	February 8, 2019
SecMetrics Comp. Poster Submissions:	February 8, 2019
Full Paper/Tutorial/Talk Decisions:	February 18, 2019
Camera Ready:	February 25, 2019
Conference:	April 1-3, 2019

Scope, Vision, & Topics of Interest

HoTSoS brings together researchers, practitioners, and thought leaders from government, industry, and academia. The conference provides a forum that facilitates technical dialogue and exchange of experiences about the development and advancement of scientific foundations in cyber security and privacy. The technical emphasis of HoTSoS is on scientific methods, data gathering and analysis, metrics and measurements, experimental approaches, mathematical models, and the interactions among those approaches to build a foundational science of security. The HoTSoS vision is one of engaging and growing a community—including researchers and skilled practitioners from diverse disciplines—that is focused around the advancement of scientific methods. The following topics (but are not limited to) are of interest of the 2019 HotSoS:

- The scientific foundation for secure and resilient system development.
- Verification and quantification of cyber resilience
- Resiliency with/for Software Defined Networking.
- Autonomous cyber defense
- Security and resiliency metrics
- Measuring the robustness of Machine Learning and AI Techniques
- Resilient decision-making for cyber defense
- Privacy verification and quantification
- Analyzing cyber and cyber-physical systems of complex interdependent components
- Quantifiable compositional verification
- Characterizing security properties that require quantum phenomena
- Information flow and data provenance in supply chain
- Privacy preserving data analysis
- privacy-supporting architecture for big data
- Quantitive risk assessment
- Resilient and dynamic cyber deception and counter-deception
- Attackers' attribution
- Resilient algorithms for verification and monitoring of Cyber-physical systems
- Mathematical models for evaluating privacy risk
- Human Factors for Cybersecurity
- Testbeds and experimentation for measuring cyber security and resiliency

NATIONAL SECURITY AGENCY · UNITED STATES OF AMERICA

acm In-Cooperation

acm SIGSAC

VANDERBILT UNIVERSITY®

Call for Papers

6th Annual **HOT TOPICS** *in the* **SCIENCE OF SECURITY** ***(HoTSoS)***

HOTSOS 2019

APRIL 2-3, 2019 | NASHVILLE, TENNESSEE

https://hotsos.org

Submission Requirements

FULL PAPERS/TUTORIALS. Submissions of full papers or tutorial proposals must be made by the deadline of **Monday, January 7, 2019 EST** through https://easychair.org/conferences/?conf=hotsos2019 by specifying the submission category to be one of the following. Nominations or proposals for government or industry talks can be sent directly to the program chairs via email at hotsoschairs@cps-vo.org.

- **Full Papers.** A submission of full paper should be at most 10 pages in the double-column ACM format* including the bibliography or, alternatively, 9 pages not including the bibliography. The paper may have optional appendices, but reviewers are not required to read them. All submissions must be in PDF format.
- **Tutorial Proposals.** A submission of tutorial proposal should be at most 2 pages in the double-column ACM format* including the bibliography. A submission should include a detailed syllabus of material to be presented. All submissions must be in PDF format.

GENERAL AND SECMETRICS POSTERS. If you are interested in participating in the general poster session or the security metrics poster competition, please upload a submission of your poster abstract by the deadline of **Friday, February 8, 2019 EST** through https://cps-vo.org/hotsos19/poster-cfp. Poster abstracts will be included in the ACM proceedings and must be submitted in the double-column ACM format*. The posters will be displayed on the conference website.

- **General Posters.** Each extended abstract submission should be at most 2 pages including the bibliography.
- **SecMetrics Competition Posters.** Each abstract submission should be at most 2 pages including the bibliography. The SecMetrics abstract should include the following sections: the metric definition and modeling (what to measure), measurement methodology (how), scope/application (where), verification and validation, and benefit and cost. The poster evaluation criteria of this competition includes the following importance, accuracy, practicality, applicability/scope, and validation robustness.

Simultaneity. Submissions must not have been published previously, and may not be submitted in parallel to any other journal or conference/workshop with published proceedings. The program chairs reserve the right to consult confidentially with other chairs and responsible parties if a double submission is suspected.

ACM Template: https://www.overleaf.com/gallery/tagged/acm-official#.WIayAktG3v0

Please send any questions about topics or submission requirements to hotsos2019@cps-vo.org

General Chair



XENOFON KOUTSOUKOS is a professor of Computer Science, Computer Engineering, and Electrical Engineering in the Department of Electrical Engineering and Computer Science at Vanderbilt University. He is also a Senior Research Scientist in the Institute for Software Integrated Systems (ISIS). Before joining Vanderbilt in 2002, Koutsoukos was a Research Staff Member in the Xerox Palo Alto Research Center, working in the Embedded Collaborate Computing Area. Between 1993 and 1995, he joined the National Center for Space Applications, Hellenic Ministry of National Defense, Athens, Greece as a computer engineer in the areas of image processing and remote sensing. Koutsoukos's research work is in the area of cyber-physical systems with emphasis on formal methods, distributed algorithms, diagnosis and fault tolerance, and adaptive resource management. He has published numerous journal and conference papers and he is co-inventor of four US patents.

Program Co-Chairs



ALVARO CARDENAS is a Eugene McDermott Associate Professor of Computer Science at the University of Texas at Dallas. He holds M.S. and Ph.D. degrees from the University of Maryland, College Park. Before joining UT Dallas he was a postdoctoral scholar at the University of California, Berkeley, and a research staff at Fujitsu Laboratories of America in Sunnyvale California. His research interests focus on cyber-physical systems and IoT security and privacy. He is the recipient of the NSF CAREER award, the 2018 faculty excellence in research award from the Erik Johnson School of Engineering and Computer Science, the Eugene McDermott Fellow recognition at the University of Texas at Dallas, and best paper awards from the IEEE Smart Grid Communications Conference and the U.S. Army Research Conference.



EHAB AL-SHAER is a Professor and the Director of the Cyber Defense and Network Assurability (CyberDNA) Center in the School of Computing and Informatics at University of North Carolina Charlotte. His primary research areas are network security, security management, fault diagnosis, and network assurability. Prof. Al-Shaer edited/co-edited more than 10 books and book chapters, and published about 100 refereed journals and conferences papers in his area. Prof. Al-Shaer is the General Chair of ACM Computer and Communication 2009-2010 and NSF Workshop in Assurable and Usable Security Configuration, August 2008. Prof. Al-Shaer received his MSc and Ph.D. in Computer Science from the Northeastern University (Boston, MA) and Old Dominion University (Norfolk, VA) in 1998 and 1994 respectively.

Organizing Committee

Publications Chair: ZHENKAI ZHANG, Vanderbilt University

Local Arrangements Chair: KATIE DEY, Vanderbilt University

NSA Liasons: HEATHER LUCAS and **TIM THIMMESCH**

Graphic Design: AMY KARNS, Vanderbilt University