

## Workshop on IoT Security and Cyber Threat Intelligence (IoT-SCTI)

The IoT Security and Cyber Threat Intelligence (IoT-SCTI) Workshop will be held on Monday, December 4, 2023, in conjunction with the Annual Computer Security Applications Conference (ACSAC). ACSAC will be held at the AT&T Conference Center in Austin, Texas.

### Call for Papers:

The rapid proliferation of Internet of Things (IoT) devices has opened up new avenues for cyber attacks, making IoT security a critical concern. We invite researchers and practitioners to submit papers to our workshop focusing on IoT Security and IoT Cyber Threat Intelligence collection, analysis, validation, and application. The workshop aims to bring together experts and professionals to share their insights, discuss the latest findings, and explore novel techniques to enhance IoT Security and Cyber Threat Intelligence.

We encourage original and high-quality contributions, preliminary work, and novel ideas on topics, including but not limited to:

- Data Collection
  - IoT-specific honeypots and honeynets
  - Network and host-based intrusion detection systems for IoT
  - Web crawlers and scrapers for IoT threat information
  - Cyber threat intelligence feeds focusing on IoT
  - Darknet, social media, and other relevant source monitoring
  - Static and dynamic malware analysis for IoT
- Data Analysis and Correlation
  - Machine learning and data mining techniques for IoT threat analysis
  - IoT-specific threat actor profiling and attribution
  - Domain generation algorithms analysis for IoT malware
  - Identifying trends and patterns in IoT attacks and vulnerabilities
  - Correlating IoT threat data from multiple sources
- Data Validation
  - Evaluating the reliability and accuracy of IoT CTI sources
  - Addressing false positives and noise in IoT threat data
  - Assessing the effectiveness of IoT-specific threat detection methods
- Data Application
  - Developing and deploying countermeasures for IoT threats
  - Real-time IoT threat monitoring and alerting systems
  - Collaborative platforms for sharing and responding to IoT threats
  - Use cases of successful IoT CTI application in organizations

Submissions should be 5-10 pages, using the double-column ACM proceedings format (acmart) template available at <https://www.acm.org/publications/taps/word-template-workflow>, with the [sigconf, anonymous] options. Two additional pages can be used for the Appendix. Note that the reviewers are not expected to read the Appendix.

All submissions must be **anonymous**.

The submission website is at: <https://easychair.org/conferences/?conf=iotscti23>

## Publication

The accepted workshop papers and slides will be published on the ACSAC website with open access.

## Important Dates

Submission Deadline	September 15 22, 2023
Acceptance Notification	September 27, 2023
Final Manuscript due	October 4, 2023
Workshop Date	December 4, 2023

Further details about the workshop can be found on the workshop website:  
<https://www.acsac.org/2023/workshops/iot-scti/>

For any questions, please contact the Chair at: [alrawi@gatech.edu](mailto:alrawi@gatech.edu), [msalsabah@hbku.edu.qa](mailto:msalsabah@hbku.edu.qa)

## Organizing Committee

### General & Program Co-Chairs:

- Omar Alrawi, Georgia Tech
- Masha'el Al-Sabah, HBKU

### Program Committee Members include:

- Gong Chen, University of Georgia
- Savio Sciancalepore, Eindhoven University of Technology (TU/e)
- Afsah Anwar, University of New Mexico
- Zane Ma, Georgia Tech
- Yue Zhang, The Ohio State University
- Tj Oconnor, Florida Institute of Technology
- Sophie Stephenson, University of Wisconsin--Madison
- Jeman Park, Georgia Tech
- Berkay Celik, Purdue University
- Adwait Nadkarni, William and Mary
- David Mohaisen, University of Central Florida
- Luyi Xing, Indiana University Bloomington
- Hanan Hibshi, Carnegie Mellon University
- Brendan Saltaformaggio, Georgia Tech
- Amit Sikder, Georgia Tech
- Sonu Shankar, Phosphorus Cybersecurity
- Mohamed Nabeel, Qatar Computing Research Institute
- Marco Balduzzi, Trend Micro
- Xiaojing Liao, Indiana University Bloomington

## **Workshop Registration**

If you are interested in attending, please check off the appropriate box on the conference registration form and add in the IoT Security and Cyber Threat Intelligence (IoT-SCTI) Workshop fee.

For accepted papers, at least one author must register and attend.