CPSIoTSec'23: Fifth Workshop on CPS & IoT Security and Privacy

Citation for the original published paper (version of record):

Almgren, M., Fernandes, E. (2023). CPSIoTSec'23: Fifth Workshop on CPS & IoT Security and Privacy. CCS 2023 - Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security: 3648-3650. http://dx.doi.org/10.1145/3576915.3624020

CPSIoTSec'23: Fifth Workshop on CPS & IoT Security and Privacy

Magnus Almgren
magnus.almgren@chalmers.se
Chalmers University of Technology
Gothenburg, Sweden

Earlence Fernandes
efernandes@ucsd.edu
University of California, San Diego
La Jolla, CA, USA

ABSTRACT

The fifth Workshop on CPS & IoT Security and Privacy is set to take place in Copenhagen, Denmark, on November 26, 2023, in conjunction with the ACM Conference on Computer and Communications Security (CCS'23). This workshop marks the amalgamation of two workshops held in 2019: one focused on the security and privacy of cyber-physical systems, while the other one centered on the security and privacy of IoT. The primary objective of this workshop is to create a collaborative forum that brings together academia, industry experts, and governmental entities, encouraging them to contribute cutting-edge research, share demonstrations or hands-on experiences, and engage in discussions.

This year, our call for contributions encompassed a broad spectrum, including mature research papers, work in progress submissions, and Systematization of Knowledge papers. The workshop program includes five full-length papers on the security and privacy of CPS/IoT, alongside five shorter papers that present original work-in-progress. Furthermore, the workshop will feature two distinguished keynote presentation, offering insights into the field, and a demonstration to provide a practical dimension to the discussions. The complete CPSIoTSec'23 workshop proceedings are available at: https://dl.acm.org/doi/proceedings/10.1145/3605758.

CCS CONCEPTS

• **Security and privacy**;

KEYWORDS

cyber physical systems, internet of things, security, privacy

ACM Reference Format:
Magnus Almgren and Earlence Fernandes. 2023. CPSIoTSec'23: Fifth Workshop on CPS & IoT Security and Privacy. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security (CCS '23), November 26–30, 2023, Copenhagen, Denmark.* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3576915.3624020

1 INTRODUCTION

Cyber-Physical Systems (CPS) and IoT devices seamlessly integrate computing and communication capabilities with real-world monitoring and actuation. In this context, security becomes a multifaceted challenge, demanding not only per-device considerations but also a full system perspective. Moreover, the landscape of CPS and IoT exhibits boundary conditions, such as lack of local computing resources, power-sources (battery-powered), and communication latency. Additionally, domain-specific knowledge is essential for comprehending potential attack vectors and the associated constraints, making it important for researchers from multiple interdisciplinary backgrounds to collectively address security and privacy concerns within the CPS/IoT domain.

In this context, the Workshop on CPS & IoT Security and Privacy serves as a vital forum for fostering collaborative discussions and knowledge sharing.

2 SCOPE AND TOPIC OF INTEREST

One of the goals of the workshop is to establish a collaborative forum that unites academia, industry experts, and governmental entities. For this year's workshop, we strongly encouraged papers that can point the research community to new research directions, and those that can set research agendas and priorities in CPS/IoT security and privacy. The goal was to create an engaging program that combines both mature research and ongoing work, along with hands-on experience. We expected all authors to consider diversity and inclusion, especially when preparing their own submission. We specifically asked for the following types of submissions.

- Original research papers on the security and privacy of CPS and IoT. For this category we encouraged both full papers for mature research and shorter papers for ongoing work.
- Systematization of Knowledge (SoK) papers on the security and privacy of CPS and IoT.
- Demos (hands-on or videos) of testbeds/experiences of CPS and IoT security and privacy research.

We sought submissions from multiple interdisciplinary backgrounds tackling security and privacy issues in CPS/IoT, including but not limited to the following topics.

- Mathematical foundations for secure CPS/IoT
- Control-theoretic approaches
- High assurance security architectures
- Security and resilience metrics
- Metrics and risk assessment approaches
- Identity and access management
- Privacy and trust
- Network security
- Game theory applied to CPS/IoT security
- Human factors, humans in the loop, and usable security
- Understanding dependencies among security, reliability and safety in CPS/IoT
- Economics of security and privacy
- Intrusion and anomaly detection
- Model-based security systems engineering
- Sensor and actuator attacks

CCS '23, November 26–30, 2023, Copenhagen, Denmark

ACM ISBN 979-8-4007-0050-7/23/11.
https://doi.org/10.1145/3576915.3624020

- CPS/IoT malware analysis
- CPS/IoT firmware analysis
- Hardware-assisted CPS/IoT security

3 ORGANIZATION

3.1 Program Committee Chairs

- Magnus Almgren, Chalmers University of Technology
- Earlence Fernandes, University of California, San Diego

3.2 TPC Members

(1) Alessandro Brighente, University of Padua
(2) Alvaro Cardenas, University of California, Santa Cruz
(3) Amir Rahmati, Stony Brook University
(4) Awais Rashid, University of Bristol
(5) Charalambos Konstantinou, KAUST
(6) Cristina Alcaraz, University of Malaga
(7) Ebelechukwu Nwafor, Villanova University
(8) Emil Lupu, Imperial College London
(9) Gang Tan, Penn State University
(10) George Stergiopoulos, University of the Aegean
(11) Gerhard Hancke, City University of Hong Kong
(12) Habiba Farrukh, Purdue University
(13) Hervé Debar, Telecom SudParis
(14) Le Guan, University of Georgia
(15) Luis Garcia, University of Southern California, Information Sciences Institute
(16) Marina Krotofil, Hamburg University of Technology
(17) Marios Anagnostopoulos, Aalborg University
(18) Mauro Conti, University of Padua
(19) Mikael Asplund Linköping University
(20) Monowar Hasan, Washington State University
(21) Muslum Ozgur Ozmen, Purdue University
(22) Nils Ole Tippenhauer, CISPA Helmholtz Center for Information Security
(23) Pablo Picazo-Sanchez, Halmstad University
(24) Peng Liu, The Pennsylvania State University
(25) Saman Zonouz, Georgia Institute of Technology
(26) Shahid Raza, RISE (Research Institutes of Sweden)
(27) Sokratis Katsikas, Norwegian University of Science & Technology
(28) Sridhar Adepu, University of Bristol
(29) Stefano Longari, Politecnico di Milano
(30) Takami Sato, University of California, Irvine
(31) Vasileios Gkioulos, Norwegian University of Science and Technology
(32) Weizhi Meng, Technical University of Denmark
(33) Yongkai Fan, State Key Laboratory of Media Convergence and Communication, China University of Communication
(34) Yuqing Zhang, National Computer Network Intrusion Protection Center, University of Chinese Academy of Sciences

3.3 Publicity Chair

- Pablo Picazo-Sanchez, Halmstad University, Sweden

3.4 Steering Committee

- Rakesh Bobba, Oregon State University
- Alvaro Cardenas, University of California, Santa Cruz
- Peng Liu, Penn State University
- Sibin Mohan, University of Illinois at Urbana-Champaign
- Awais Rashid, University of Bristol
- Gang Tan, Penn State University
- Nils Ole Tippenhauer, CISPA Helmholtz Center for Information Security
- Roshan Thomas, MITRE
- Yuqing Zhang, National Computer Network Intrusion Protection Center, University of Chinese Academy of Sciences

4 STATISTICS

We received twenty-three submissions, that encompassed twelve full papers, ten shorter work-in-progress papers, and one suggestion for a demonstration. The papers underwent a rigorous review process led by the TPC chairs, where the TPC consisted of 34 researchers with expertise in CPS or IoT Security and Privacy, or a combination of these domains. Each paper was assigned at least three reviewers.

The evaluation criteria for full papers included considerations of their significance, novelty, and technical quality. Authors were particularly encouraged to provide comprehensive details to facilitate reproducibility. The shorter work-in-progress papers did not need to meet the same rigorous evaluation standards, although they were still required to present evaluations with a credible path forward.

Following the review phase, a discussion stage ensued, during which potential shepherds were assigned to aid authors in refining their submissions, and recommendations were made regarding if some full papers should instead be considered as work-in-progress (one paper shifted category). Ultimately, the workshop program will be comprised of five full papers (42% acceptance rate), five short papers (45% acceptance rate) and one extended abstract with a demonstration. In addition, the program will feature two distinguished keynote presentation.

5 CPSIOTSEC'23 AGENDA

Table 1 includes the preliminary agenda (in European Central Time) planned for the current edition of the workshop. Full papers get a 30 minute slot (including QA) and short papers get a 20 minute slot (including QA). The program will end with the award to the best full paper of CPSIoTSec'23. We have a transparent process where the chairs will first select a subset of the papers presented physically at the workshop based on review scores and designate them as best paper candidates. Then, the audience will vote for the best one based on the presentation.

6 ACKNOWLEDGMENTS

The workshop chairs thank the steering committee, organizers, program committee, external reviewers, and authors of all submissions for their help in producing this exciting technical program. The chairs also want to acknowledge the support given by the Swedish Civil Contingencies Agency (MSB) through the projects RICS2 and RIOT.

9:00-9:15	Opening Remarks (Magnus Almgren)
9:15-10:00	Keynote 1: Security and privacy challenges for next generation communication and computational infrastructures and applications, Maria Kihl (Lund University, Sweden)
10:00-10:30	Break
10:30-12:20	Session 1: Assessment and Mitigation Strategies
	(full paper) Firmulti Fuzzer: Discovering Multi-process Vulnerabilities in IoT Devices with Full System Emulation and VMI
	(full paper) Water Risk-Proofed: Risk Assessment in Water Desalination
	(full paper) Remote Attestation of IoT Devices using Physically Unclonable Functions: Recent Advancements and Open Research Challenges
	(demo) From DDoSim to DDoSimQ: Enhancing DDoS Attack Simulations Through Full System Emulation
12:20-13:30	Lunch Break
13:30-15:30	Session 2: Adversarial Exploitation and Compiler Insights in Real-World Systems
	(full paper) Towards Adversarial Process Control on Inertial Sensor Systems with Physical Feedback Side Channels
	(full paper) Brain-Hack: Remotely Injecting False Brain-Waves with RF to Take Control of a Brain-Computer Interface
	(short paper) The Internet of Insecure Cows - A security analysis of wireless smart devices used for dairy farming
	(short paper) SweetCam: an IP Camera Honeypot
	(short paper) Towards PLC-specific Binary Analysis Tools: An Investigation of Codesys-compiled PLC Software Applications
15:30-16:00	Break
16:00-16:45	Keynote 2: IoT and Web, Friend or Foe? Security and Privacy of Internet of Things Apps, Musard Balliu (KTH, Sweden)
16:45-16:50	Short Break
16:50-17:30	Session 3: Device Identification and Anonymization
	(short paper) Granular IoT Device Identification Using TF-IDF and Cosine Similarity
	(short paper) Privacy through Diffusion: A White-listing Approach to Sensor Data Anonymization
17:30-17:45	Finish best paper voting process
17:45-18:00	Best paper announcement, Closing Remarks (Magnus Almgren)

Table 1: Agenda