CPSIoTSec'24: Sixth Workshop on CPS&IoT Security and Privacy

CPSIoTSec'24: Sixth Workshop on CPS&IoT Security and Privacy

Kassem Fawaz
kfawaz@wisc.edu
University of Wisconsin–Madison
Madison, WI, USA

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

ABSTRACT

The sixth Workshop on CPS & IoT Security and Privacy is set to take place in Salt Lake City, UT, USA, on October 18, 2024, in conjunction with the ACM Conference on Computer and Communications Security (CCS'24). 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 full research papers, work-in-progress submissions, and one-page abstracts. The workshop program includes eight full-length papers on the security and privacy of CPS/IoT, alongside six shorter papers that present original or work-in-progress research. Furthermore, the workshop will feature one distinguished keynote presentation by Prof. Alvaro Cardenas, a world-renowned expert in CPS security. The talk will offer insights into how the state of CPS security has evolved since 2007. The complete CPSIoTSec'24 workshop proceedings are available at https://doi.org/10.1145/3658644.3691550.

CCS CONCEPTS

• **Security and privacy**;

KEYWORDS

cyber physical systems, internet of things, security, privacy

ACM Reference Format:
Kassem Fawaz and Magnus Almgren. 2024. CPSIoTSec'24: Sixth Workshop on CPS&IoT Security and Privacy. In *Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security (CCS '24), October 14–18, 2024, Salt Lake City, UT, USA.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3658644.3691550

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 a 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 government 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. We specifically asked for the following types of submissions.

- Long papers that include a) Original research on a CPS/IoT security and privacy topic, b) Systematization of Knowledge of CPS/IoT security and privacy;
- Short papers that include original work-in-progress research on a CPS/IoT security and privacy topic;
- 1-page abstracts that include demos/interesting findings or insights on CPS/IoT security and privacy, which should be accompanied by a hands-on demo during the workshop.

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 '24, October 14–18, 2024, Salt Lake City, UT, USA

ACM ISBN 979-8-4007-0636-3/24/10.
https://doi.org/10.1145/3658644.3691550

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

3 ORGANIZATION

3.1 Program Committee Chairs

- Kassem Fawaz, University of Wisconsin–Madison
- Magnus Almgren, Chalmers University of Technology

3.2 TPC Members

(1) Alessandro Brighente, University of Padua
(2) Amir Rahmati, Stony Brook University
(3) Awais Rashid, University of Bristol
(4) Cristina Alcaraz, University of Malaga
(5) Gang Tan, Penn State
(6) George Stergiopoulos, University of the Aegean
(7) Gerhard Hancke, City University of Hong Kong
(8) Habiba Farrukh, Purdue University
(9) Kassem Fawaz, University of Wisconsin-Madison
(10) Le Guan, University of Georgia
(11) Luis Garcia, University of Utah
(12) Luis Salazar, UC Santa Cruz
(13) Magnus Almgren, Chalmers University of Technology
(14) Marina Krotofil, MaK Security
(15) Marios Anagnostopoulos, Aalborg University
(16) Mauro Conti, University of Padua
(17) Mikael Asplund, Linköping University
(18) Monowar Hasan, Washington State University
(19) Muslum Ozgur Ozmen, Purdue University & Arizona State University
(20) Nils Ole Tippenhauer, CISPA Helmholtz Center for Information Security
(21) Pablo Picazo-Sanchez, Halmstad University, Halmstad, Sweden
(22) Peng Liu, The Pennsylvania State University
(23) Rishabh Khandelwal, University of Wisconsin–Madison
(24) Sachin Kumar Singh, University of Utah
(25) Saman Zonouz, Georgia Institute of Technology
(26) Sara Rampazzi, University of Florida
(27) Shimaa Ahmed, Visa Research
(28) Sokratis Katsikas, Norwegian University of Science & Technology
(29) Sridhar Adepu, University of Bristol
(30) Stefano Longari, Politecnico di Milano
(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 Chairs

- Pablo Picazo-Sanchez, Halmstad University
- Masoom Rabbani, COSIC, KU Leuven, Belgium

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
- Roshan Thomas, MITRE
- Yuqing Zhang, University of CAS

4 STATISTICS

We received thirty-one submissions, encompassing nineteen full papers and twelve shorter work-in-progress papers. 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, where all the reviewers converged on a decision for each submission. Reviewers were encouraged to be positive and consider the submission's contributions to the community, even if the scores were on the lower side. Ultimately, the workshop program will comprise eight full papers (42% acceptance rate) and six short papers (50% acceptance rate). In addition, the program will feature one distinguished keynote presentation by Prof. Alvaro Cardenas, a world-renowned expert in CPS security. The talk will offer insights into how the state of CPS security has evolved since 2007.

5 CPSIOTSEC'24 SCHEDULE

The workshop schedule has four sessions separated by coffee breaks and lunch. The first session includes welcome remarks, a keynote presentation, and one long presentation. The second session includes three long presentations. After lunch, the third session includes six short presentations. The fourth session includes four presentations and the final remarks. Full papers get a 20-minute slot (including QA), and short papers get a 15-minute slot (including QA). The program will end with the award to the best full paper of CPSIoTSec'24. 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 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.