# 3rd International Workshop on IoT and Security (*IoT&Security*)

Co-located with IEEE DASC 2024

November 5-8, 2024 - Boracay Island, Malay, Philippines

https://cyber-science.org/2024/dasc/index.html

## *Technical description*

The pervasiveness of IoT devices and applications in everyday life has rendered their security a critical requirement. Security of such devices poses various challenges. Firstly, manufacturers often fail to employ security-by-design approaches, resulting in products that expose vulnerabilities which are difficult to remedy or unlikely to be addressed. Secondly, many IoT devices lack sufficient computing power to run antivirus or other detection mechanisms, and some even prevent installation of such software. Finally, the heterogeneity inherent in IoT, encompassing diverse applications, hardware, and software, expands the attack surface while complicating the deployment of comprehensive security solutions.

Despite the security provided by IoT enabling technologies (e.g., communication protocols) or intrusion prevention systems, attackers continue to find ways to compromise devices or their communication channels. Unlike laptop and desktop computers, which undergo frequent on-off cycles, many IoT devices such as webcams and wireless routers operate 24/7 without supervision, making them particularly vulnerable to various attacks, including those aimed at recruiting devices for botnets. This not only jeopardizes the security of IoT networks themselves but also poses a threat to remote systems targeted by attacks launched from infected IoT devices.

Moreover, IoT-based systems handling sensitive data (e.g., healthcare information systems) must promptly respond to malicious activities to prevent unauthorized data exfiltration. As such, IoT networks must be equipped with robust security mechanisms such as intrusion detection systems, intrusion prevention systems, attack reaction systems, and proactive defense mechanisms.

We invite both academic and industrial researchers to submit research papers as either original works, discussion papers, or except for already published papers.

Possible topics include, but are not limited to:

- Intrusion Detection Systems
- Malware/Botnet detection
- Security for VANETS/MANETS

- Security for IoT-based systems (industrial control, healthcare monitoring, Cyber Physical Systems, domotic)
- Security for cloud-based IoT applications
- Security at the edge/fog
- Attack detection and countermeasures
- Game theory for the IoT security
- Security resources placement strategies
- Security for software defined IoT networks
- Security for narrowband IoT networks
- Security for SCADA-based systems
- IoT firmware analysis
- Automatic exploit generation for IoT devices
- Side channel attacks for IoT devices
- Cryptography for IoT
- Tamperproofing techniques for IoT

## *Important Dates*

| | |
|---|---|
| Papers Submission Due: | July 15, 2024 |
| Authors Notification: | August 15, 2024 |
| Camera-ready Submission: | September 15, 2024 |

## *Submission and review process*

Authors are invited to submit either full papers, which may represent exhaustive and completed works, and short papers, which are suggested for presenting work in progress, extended abstracts, software prototypes, or general overviews of research projects. Workshop submissions must be in PDF format, written in English and formatted according to the IEEE camera-ready standard format (double column, 10pt font size). Full paper pages are minimum 4 and should not exceed 6 pages (up to 8 pages with an additional charge of $100 per extra page).

All papers will be peer reviewed by at least two members of the program committee. The workshop expects to present at least five accepted papers.

## *Plans for dissemination*

We will employ various dissemination strategies to advertise the IoT&Security workshop, including targeted email advertisements to relevant mailing lists of researchers active in the field and social media campaigns.

## *History of the Workshop*

The IoT&Security workshop, co-located within the DASC conference, is now in its third edition, following two successful previous editions.

## *Organizers*


Claudia Greco, University of Calabria, Italy claudia.greco@dimes.unical.it

Carmelo Felicetti, University of Calabria, Italy carmelo.felicetti@unical.it

Sandeep Pirbhulal, Norwegian Computing Center, Norway sandeep@nr.no

Shantanu Pal, Deakin University, Australia shantanu.pal@deakin.edu.au

# *3rd International Workshop on IoT and Security (IoT&Security)*

# CALL FOR PAPERS

## *Scope and topics of the workshop*

The proliferation of IoT devices in everyday human life has made their security a critical requirement. Currently, those devices are not very secure because of several reasons. First, manufacturers do not account much for security, releasing products that are vulnerable to attacks, thus leaving users with security issues that are unlikely to be resolved. Second, many IoT devices do not have enough computing power to run an antivirus or even allow one to install an antivirus. Finally, the heterogeneity which characterizes the IoT in terms of applications, hardware, and software, expands the attack surface, while at the same time increasing the difficulty of deploying all-encompassing security solutions. Despite some sort of security provided by IoT enabling technologies (e.g., communication protocols), or by intrusion prevention systems (e.g., network firewalls), attackers still find ways to compromise devices, or the communication between them. Unlike laptop and desktop computers (which have frequent on-off cycles), many IoT devices such as webcams and wireless routers operate 24/7 unattended. This makes IoT devices particularly prone to various attacks, such as attacks aiming at recruiting devices for botnets. This makes IoT networks dangerous not only for themselves but also for remote systems that are victims of attacks launched by infected IoT devices. Moreover, IoT-based systems that handle sensitive data (e.g., healthcare IS) need to promptly react to malicious activities in order to prevent private data from leaving the network. IoT networks, thus, must be equipped with some sort of security mechanism, such as intrusion detection systems, intrusion prevention systems, attack reaction systems, proactive defense mechanisms, etc.

We invite both academic and industrial researchers to submit research papers as either original works, discussion papers, or excerpts of already published papers.

Possible topics include, but are not limited to:

- Intrusion Detection Systems (Machine learning based IDS; Host-based IDS; Network-based IDS; Anomaly-based IDS; Signature-based IDS; Specification-based IDS; Distributed IDS; Privacy preserving IDS)
- Malware/Botnet detection
- Security for VANETS/MANETS
- Security for IoT-based systems (industrial control, healthcare monitoring, Cyber Physical Systems, domotic)
- Security for cloud-based IoT applications
- Security at the edge/fog
- Attack detection and countermeasures
- Game theory for the IoT security
- Security resources placement strategies
- Security for software defined IoT networks
- Security for narrowband IoT networks
- Security for SCADA-based systems
- IoT firmware analysis
- Automatic exploit generation for IoT devices
- Side channel attacks for IoT devices
- Cryptography for IoT
- Tamperproofing techniques for IoT

## *Important Dates*

| | |
|---|---|
| Papers Submission Due: | July 15, 2024 |
| Authors Notification: | August 15, 2024 |
| Camera-ready Submission: | September 15, 2024 |

## *General Co-Chairs*

Claudia Greco, University of Calabria, Italy
Carmelo Felicetti, University of Calabria, Italy
Sandeep Pirbhulal, Norwegian Computing Center, Norway
Shantanu Pal, Deakin University, Australia

## *Program Committee*

Michele Ianni, University of Calabria, Italy
Amit Kumar Singh, National Institute of Technology Patna, India
Andrea Pugliese, University of Calabria, Italy
Areeba Umair, Federico II University, Italy
Elio Masciari, Federico II University, Italy
Gianluca Lax, University of Reggio Calabria, Italy
Gwanggil Jeon, Incheon National University, Korea
Lin Yang, Huazhong Agricultural University, China
Marco Fisichella, L3S Research Center of Leibniz University, Germany
Mohammad Mehedi Hassan, King Saudi University, Saudi Arabia
Niccolo' Marastoni, University of Verona, Italy
Zia Ush Shamszaman, Teesside University, United Kingdom