2nd International Workshop on IoT and Security (*IoT&Security*)

Co-located with IEEE DASC 2023
Abu Dhabi, UAE, November 13 - 17, 2023
https://icnetlab.org/cyber-science2023/dasc/index.html

IMPORTANT DATES

Papers Submission due	July 15, 2023
Authors Notification	September 15, 2023
Camera-ready Submission	September 30, 2023

SCOPE

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 do not 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 increases 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.

TOPICS

The main 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

SUBMISSION AND CAMERA READY PREPARATION
Please refer to the conference submission link below:
https://icnetlab.org/cyber-science2023/dasc/papersubmission/index.html

GENERAL CHAIRS
Antonella Guzzo, University of Calabria, Italy
Michele Ianni, University of Calabria, Italy
Sebastian Schrittwieser, University of Vienna, Austria
Kaitai Liang, Delft University of Technology, Netherlands

PROGRAM COMMITTEE
Amit Kumar Singh, National Institute of Technology Patna, India
Andrea Pugliese, University of Calabria, Italy
Antonino Rullo, University of Calabria, Italy
Areeba Umair, Federico II University, Italy
Carmelo Felicetti, University of Calabria, Italy
Claudia Greco, University of Calabria, Italy
Edoardo Serra, Boise State University, USA
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