1th International Workshop on IoT and Security (IoT&Security)

Technical description, focus and scope:

The pervasivity of IoT devices and applications into everyday life has made their security a critical requirement. Security of such devices is an issue because of several reasons. First, manufacturers often do not employ security-by-design approaches, releasing products that expose vulnerabilities which are hard to fix or unlikely to be addressed. Second, many IoT devices do not have enough computing power to run an antivirus or any other detection mechanism 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, 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 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 excerpt 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

Submission and review process

Authors are invited to submit either full papers, possibly already submitted to other conferences or journals, 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 papers should not exceed 8 pages (including bibliography).

Short papers must not exceed 3 pages.
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.

Dissemination
The workshop will be advertised and promoted through official and unofficial mailing lists, websites and social media platforms. An official website containing all the necessary information will be created and maintained.

Organizers
Antonella Guzzo, University of Calabria, Italy
Michele Ianni, University of Calabria, Italy
Antonino Rullo, University of Calabria, Italy
Angelo Furfaro, University of Calabria, Italy

CFP follows in the next page.

1th 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 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 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 excerpt 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: June 1, 2022
Authors Notification: July 1, 2022
Camera-ready Submission: July 15, 2022

Organizers

Antonella Guzzo, University of Calabria, Italy

Michele Ianni, University of Calabria, Italy
Antonino Rullo, University of Calabria, Italy
Angelo Furfaro, University of Calabria, Italy

Program Committee (tentative)

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