IEEE MeditCom

IEEE International Mediterranean Conference on Communications and Networking
5-8 July 2021 // Athens, Greece

Special Session

Securing Future Networks

Organizing Projects	PANDORA (https://www.pandora-edidp.eu/) PALANTIR (https://www.palantir-project.eu/) 5GENESIS (https://5genesis.eu/) ASSURED (https://www.project-assured.eu/) INSPIRE5GPLUS (https://www.inspire-5gplus.eu/) SPHINX (https://sphinx-project.eu/) CYRENE (https://www.cyrene.eu/)
Structure	2.5 h, 1 Keynote speaker, 6 papers
Organizers	Georgios Gardikis, Nikos Drosos, Space Hellas SA (ggar@space.gr, ndrosos@space.gr) Valerio Frascolla, Intel Deutschland GmbH (valerio.frascolla@intel.com) Thanassis Gianetsos, Ubitech Ltd (agiannetsos@ubitech.eu) Diego Lopez, Telefónica I+D (diego.r.lopez@telefonica.com) Michail-Alexandros Kourtis, NCSR "Demokritos" (akis.kourtis@iit.demokritos.gr) Evangelos Markakis, Hellenic Mediterranean University (markakis@pasiphae.eu) Sofoklis Efremidis, Gruppo Maggioli SpA (sofoklis.efremidis@maggioli.it)

Background and Motivation

5G systems, and even more so future communication network technologies, bring a new rich set of features and capabilities, which, in addition to their technical and business value, are also accompanied with various side-effects, one of the most important of which is the drastic increase in the attack surface, compared to legacy network infrastructures. Some of these capabilities, which, under certain circumstances, may introduce new vulnerabilities and increase the probability of a security incident, are: software-defined infrastructures (emphasising vulnerabilities associated with softwarisation); slicing and multi-tenancy (resulting in threats related to violation of slices isolation); multi-actor service paradigms and infrastructure sharing (raising privacy and availability concerns); and complex and multi-tier architectures (introducing new threats at the control and management planes).

In addition, in 5G and future networks, not only the probability of a security incident increases, but also its expected impact and severity. The connection of more and more devices to the network, many of which track personal data, while others support critical operations (as in Intelligent Transport Systems/connected cars or e-health), implies that security incidents can lead to severe privacy breaches and in some special cases even life-threatening situations.

This situation calls for a more effective and efficient cybersecurity approach in future networks, not only addressing their new threats, but at the same time leveraging their unprecedented capabilities - such as service agility, dynamic network service deployment and edge processing- to introduce a new generation of security architectures and services.

Topics of Interest

This special session aims at bringing together network and security engineers to discuss challenges associated to, but not limited to, the following topics:

- *Trust and attestation for Virtual Network Functions (VNFs)*
- *SDN security*
- *Network slice isolation and security*
- *Security assessment of multi-tenant network infrastructures and neutral host deployments*
- *Security Information and Event Management (SIEM) evolution for future networks*
- *Virtualisation of security functions*
- *Big Data Analytics for incident detection and classification, Endpoint Detection and Reponse*
- *AI for cybersecurity at the edge*
- *Zero-trust architectures*
- *5G Managed Security Services*
- *Integrity assurance for cyber-physical systems and embedded devices*
- *Endpoint Detection and Response*
- *Threat Intelligence sharing*
- *Security Orchestration, Automation and Reponse (SOAR)*
- *Standardization and Validation of cyber-security technologies and trust techniques*