P1 Security

Priority One Security

2019

Training Description

TS-501 5G Telecom Security hands-on course

TS-501 5G Telecom Security hands-on course

Description of training

With 5G Proofs of Concepts and early test deployment, Market adoption and direction in terms of usage are set or appearing; and operators are preparing massive deployment.

This 5G Training Session (TS-501) will help security and telecom professionals get an understanding of the key concepts of 5G, their security, the implementation of such architectures and the impact in terms of related risks.

Duration
Unique version: 3 days.

Attendees will receive

- Training material: copy of the presenter's slides through Intralinks Web platform tool for a one Year duration after the training's delivery.

Prerequisites for training

- Good knowledge of 4G architectures (LTE & EPC)
- Basic knowledge of telecom & network principles:
    - What is 2G, 3G;
    - OSI network layers;
    - Basic knowledge of telecom technologies.
- Good knowledge and usage of Wireshark;
- Internet Access.

Covered in this training

- Introduction
- Different 5G architectures and impact on security
    - 5G cell non-standalone deployment within a 4G network
    - 5G standalone deployment
- Components of 5G deployments and danger areas:
    - UDM and AUSF
    - PCF and AF
    - AMF, SMF and UPF
    - gNB (DU-CU)
- Impact of new 5G protocols in terms of security:
    - S1AP and X2AP extensions
    - NGAP, XnAP, E1AP and F1AP
    - PFCP
    - Service Based Architecture, HTTP/2, JSON

- 5G roaming and interconnect security
    - N32 interface
    - HTTP/2, TLS, JSON Web Encryption and JOSE
- Slicing in 5G network
    - Benefits in each part of the network (RAN, transport, Core, applications...)
    - Complexity and security risks
- Infrastructure level deployment, security & risk of NFV (Network Functions Virtualization)
    - Hypervisor, OS and container security
    - MANO (Management and Orchestration) solutions
- Risks and attacks on isolation in a 5G multi-tenant environment (Slicing, NFV, SDN)
- MEC (Mobile Edge Computing / Multi-access Edge Computing) and security
- 5G subscribers connection security principles
    - Protection of subscribers permanent identities
    - New 5G-AKA authentication procedure
    - Better security enforcement for roaming subscribers
    - Terminal and baseband architectures
- Testbeds and experimentation platform
    - open-source and commercial solutions
- Closing remarks and debrief