P1 Security

Priority One Security

2022

Training Description

TS-502 Advanced training on 5G Security

TS-502 Advanced training on 5G Security

Duration
Unique version: 3 days.

Attendees will receive

- Training material: watermarked copy of the presenter's slides, specific source code for the training, temporary access to virtual machines for the duration of the training session

Prerequisites for training

- Good knowledge of the 5G architecture
- Basic knowledge of telecom & network principles:
    - What is 2G, 3G, 4G
    - OSI network layers
    - Basic knowledge of telecom technologies
- Good knowledge and usage of Wireshark
- Knowledge of scripting languages (Python is mostly used during the training)
- Internet Access

Covered in this training

- Free5GC and Open5GS Open Source projects presentation
- OpenAPI Specification Files for 3GPP 5G Core Network presentation
- P1 testbed access (using SSH)
- 5G Core Network Exposure: perspective, protocols, risks and countermeasures
- 5G attack scenarios (based on PTA coverage)
- P1 Security VKB Fuzzing Vulnerabilities
- Workshop: analyzing Open5GS from the RAN perspective
    - Generation of 5G NGAP/NAS standard messages in Python with pycrate
    - Use of the P1 gNodeB and UE emulator
    - NGAP and NAS fuzzing on Open5GS
- Workshop: hands-on 5GC pentest
    - Using curl and OpenAPI definitions
    - Using httpcore and httpx python libraries
    - Generation of 5G HTTP/2 requests

    - HTTP/2 scanning and fuzzing on Open5GS
- Demo: PTA 5GCN product presentation