P1 Security

Priority One Security

2019

Training Description

TS-270 LTE Security and Insecurity

TS-270 LTE Security and Insecurity

Description of training

Learn about modern telecom, mainline and mobile, systems and networks for 4G LTE mobile network service. Understand the security mechanism of LTE and the Evolved Packet Core network security and vulnerabilities. Learn in detail the various problems that may happen in LTE networks and define a plan of study to become an LTE Network auditor.

Duration
Unique version: 2 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

- 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;
- Internet Access *(preferred but optional*).

Covered in this training

- LTE Introduction;
- LTE Security architecture;
- LTE Network elements overview and security roles & functions;
- LTE Communication security, cryptography and key management;
- Study of LTE protocols:
  - S1AP;
  - X2AP;
  - Diameter;
  - GTP-C;
  - GTP-U;
  - GTP v2;
  - GTP';
  - NAS.
- Typical attacks on LTE infrastructure;
- Recap of SS7 attack scenarios and comparison to 4G;
- Role of legacy in LTE security;

- Network elements and their functions: HSS, DRA/DEA, MME, PCRF, eNodeB, PGW, SGW;
- DRA remote and RCE compromise via Diameter;
- Vulnerabilities in VoLTE;
- Analysis of Generic LTE Network element and vulnerabilities:
- Diameter security and comparison to SIGTRAN and Radius protocols;
- Diameter fuzzing and scanning;
- Diameter in a roaming context;
- NAS security, protocol review and known attacks;
- SCTP protocol basics, scanning and attack scenarios;
- SGW – PGW infrastructure and design and GTPv2 scanning and fuzzing;
- S1AP interface protocol study and known vulnerabilities;
- Attack scenarios over the S1AP interface;
- Attacking O&M (OAM & Management) of network elements;
- GRX / IPX compromise case studies, architecture and design and known vulnerabilities;
- Scenarios of attack of LTE network:
    - Radio-based, subscriber role;
    - Infrastructure-based, transmission or RAN vector;
    - Internal-based attack;
    - Interconnect based attack scenarios.