LTE Security and Insecurity

Who Should Attend?

This training is aimed at Telecom core engineers. In this course, the participant will learn about LTE 4G mobile network service, LTE security mechanisms, Evolved Packet Core network security and vulnerabilities, and potential LTE network problems. Finally, the participant will define a plan of study to become a LTE Network auditor.

Course Scope

1. LTE Introduction.
2. LTE Security Architecture.
3. LTE Network Elements Overview, Security Roles, and Functions.
4. LTE Communication Security, Cryptography, and Key Management.
5. Study of LTE Protocols.
   - S1AP.
   - X2AP.
   - Diameter.
   - GTP-C.
   - GTP-U.
   - GTPv2.
   - GTP’.
   - NAS.
6. Typical Attacks on LTE Infrastructure.
7. Recap of SS7 attack scenarios and comparison to 4G.
8. Role of Legacy in LTE Security (CS Fallback, CSFB vs. VoLTE).
9. Network elements and their functions: HSS, DRA/DEA, MME, PCRF, eNodeB, PGW, SGW.
10. DRA remote and RCE compromise via Diameter.
11. Vulnerabilities in VoLTE.
12. Analysis of Network Elements and Vulnerabilities.
    - Generic LTE network element vulnerabilities.
    - Huawei LTE SAE EPC HSS: structure, vulnerabilities, and services.
    - Huawei LTE SAE RAN MME: role and attacks.
    - Ericsson LTE SAE RAN eNodeB: vulnerabilities, integration, provisioning, and hardware attacks.
    - Huawei LTE SAE EPC UGW (SeGW, S-GW, PDN GW): role and structure.
13. Diameter Security and Comparison to SIGTRAN and Radius Protocols.
14. Diameter Fuzzing and Scanning.
15. Diameter in a Roaming Context.
16. NAS Security, Protocol Review and Known Attacks.
17. SCTP Protocol Basics, Scanning and Attack Acenarios.
18. SGW – PGW Infrastructure and Design, and GTPv2 Scanning and Fuzzing.
19. S1AP Interface Protocol Study and Known Vulnerabilities.
20. Attack Scenarios over the S1AP Interface.
21. Attacking O&M (OAM & Management) of Network Elements.

22. GRX / IPX Compromise Case Studies, Architecture and Design, and Known Vulnerabilities.
23. Scenario of LTE Network Attack.
    - Radio-based; role of the subscriber.
    - Infrastructure-based, Transmission or RAN vector.
    - Internal-based attack.
    - Interconnect-based attack scenarios.
24. The Next Steps to Becoming a LTE Network Auditor.

Prerequisites

In order to fully understand the course, each participant needs:

- Basic knowledge of Telecom & network principles:
  - 2G, 3G, and 4G.
  - OSI network layers.
  - Basic knowledge of Telecom technologies.
- Laptop with Linux installed either in a VM or native, Backtrack or Ubuntu (reverse engineering and hacking tools recommended).
- Good ability to use Wireshark.
- Basic skills and usage of Linux for reverse engineering (strings, knowledge of tools in a Backtrack for reverse engineering).
- Legal IDA Pro license optional, but strongly recommended.

Training Structure

Two-day training divided into logical sessions.

Methodology

Instructor-led training. Participants will receive evaluation access to a vulnerability scanner for Telecom infrastructure and a developer account for LTE mobile security platform.