IMS Security and Attacking Telecom Infrastructure

Who Should Attend?

This course is aimed at telecom core engineers who want to learn about modern telecom and mobile systems and networks in the context of IMS and NGN core networks. Along with its main benefits, we present the core evolutions of the legacy telecom networks into IMS networks and the reuse of IETF-based protocols in the context of IMS.

Course Scope

1. IMS Introduction.
2. IMS Benefits.
3. IMS Technologies.
4. The Root of IMS Technology.
5. IMS Security Architecture.
6. Study of IMS-specific Protocols.
   - SIP IETF.
   - SIP-I.
   - SIP-T Diameter.
7. Overview of other protocols still used in IMS.
   - GTP-C
   - GTP-U
   - GTPv2
   - GTP'.
8. Overview, Security Roles, and Functions of IMS Network Elements.
   - HSS.
   - CSCFs: I-CSCF, P-CSCF, S-CSCF.
   - BG/BGCF.
   - MGCF.
   - SGW.
9. Specific Network Elements in recent versions of IMS core networks.
   - SDP/SDR.
   - PCRF.
10. Security of different IMS planes.
    - Access.
    - Transport.
    - Control.
    - Application.
11. IMS Communication security.
12. Open Source IMS tools.
13. IMS network element fingerprinting.
14. Typical attacks on IMS infrastructure.
15. Role of legacy in IMS security.
    - Interconnection with SS7 signaling network element.
    - H248.

IMS Security and Attacking Telecom Infrastructure

16. Vulnerabilities of some Voice over IP protocols:
    - SIP-I.
    - SIP-T.
    - H323.
17. Analysis of Network Elements and vulnerabilities.
    - Generic IMS Network Element vulnerabilities.
18. Diameter security.
19. IMS Network Attack Scenario.
    - Radio-based, role of the subscriber.
    - Infrastructure-based, Transmission or RAN vector.
    - Internal-based, attack.
20. Next steps to becoming an IMS network auditor.

Prerequisites

- Basic knowledge of telecom & network principles:
    - 2G, 3G, 4G.
    - OSI network layers.
    - Telecom technology.
- Thorough knowledge and usage of Wireshark.
- Basic skills and usage of Linux for reverse engineering (strings, knowledge of tools in BackTrack for reverse engineering).
- Legal IDA Pro license recommended, but optional.
- In addition, please bring a laptop with Linux installed either in a VM or native, BackTrack or Ubuntu (reverse engineering and hacking tools recommended).

Training Structure

Three-days training divided into logical sessions.

Methodology

Instructor-led training. The participants will receive access to a vulnerability scanner for telecom infrastructure.