Telecom Security Risks

Who Should Attend?

This course is aimed at managers, engineers, and operation teams who want to understand how Telecom security and fraud works, and how attackers can abuse the system and threaten Mobile Network Operators, fixed-lines operators, VoIP providers, and any other Telecom-related company.

Course Scope

1. Introduction to Telecom Security.
2. Telecom Fraud: descriptions and case studies.
   - A Bit of History: from the First Frauds to the Latest.
   - General Principles and Underlying Laws of Telecom Frauds.
   - Fraud Management Systems (FMS) and FRA.
   - Limits of CDR-based Fraud Detection and Security.
   - Telecom Fraud from a Legal Standpoint.
   - Fraud and Institutions (GSMA, 3GPP, CFCA, Fight FAS, I3).
   - Fraud and Law Enforcement.
   - Deep inside Fraud Case Studies.
3. Telecom Security Introduction.
   - Availability: from Crash to Denial of Service.
   - Confidentiality: What do the Operators have at Stake?
   - Integrity: How Secure and Trustworthy are We?
   - Billing: Protecting Revenue from Leakage, Collection, and Traceability.
   - Underlying technologies, Risks, and Organisation.
   - Legal Interception (LI), CALEA, Legal Requirements, and Related Systems.
4. Telecom Security Attacks and Problems.
   - Introduction to Case Studies and Generic List.
   - Practical SIM Fraud (case study).
   - Attacking the Signalling Network: risks and attacks on SS7 and SIGTRAN.
   - Privacy Attacks and HLR Requests: danger ahead.
   - Country-Wide Denial of Service.
   - User-Targeted Denial of Service.
   - VoIP-related Attacks and Security Risks.
   - Manipulating Operators' Networks.
   - Attack on the Radio: GSM, 3G / UMTS, 4G / LTE / LTE Advanced; User-centered attacks: from SMS and MMS High-profile Attacks; Mobile Malware and Application: the Smartphone Security Challenge.
5. Telecom Security Risk Mitigation.
   - Network-centric Mitigation.
   - End-user-centric Mitigation.
   - Systemic and Organisational Security Measures.
   - Reducing your Footprint and Attack Surface.
   - Organisational Security and Procedures.

- Auditing Telecom Security: the proactive protection Planning Telecom Security—drawing the way.
- Monitoring Telecom Security: reactive qualities.

Prerequisites

Basic knowledge of Telecom and network principles: 2G, 3G, 4G, and OSI network layers.

Training Structure

Two-day training divided into logical sessions.

Methodology

Instructor-led training.