Telecom Security Hands-on Course

Who Should Attend?

This course is aimed at engineers with a background in Telecom or security who want to better understand and evaluate security problems within an SS7 and Telecom Signalling environment.

Course Scope

This course is a practical SS7 and Telecom security training both to learn the theory and practice hands-on attack and protection of Telecom signalling networks in the context of security and fraud.

1. SS7 Security.
   - SS7 Basics and Possibilities.
   - Description of SS7 protocols.
   - Telecom Signaling Network Architectures.
   - SS7 External Access and Geo-localisation over http (hands-on).
   - SS7 Low-level Protocols Analysis.
   - Low-level SS7 Packet Analysis, Sniffing and Network Tracing (hands-on).
   - Signalisation Attacks.
   - SS7 and SIGTRAN Audit Methodology.
   - Low-level Peering (M3UA and SCCP).
   - SCTP Scan Usage in Core Network Settings
   - Scanning SS7 Networks (MTP, SCTP, and upper SS7)(hands-on).
   - SCTP Netcat (Tool Discovery)
   - SS7 Higher-level Protocols (User Adaptation Layers).
   - M3UA Peering Analysis vs. M2PA (hands-on).
   - Links and Alerts (availability, warnings, and detection).
   - Network Elements, Functions, HLR, VLR, STP, SCP, BTS, GGSN, SGSN, MSC, 3G Alternatives.
2. Telecom Signalling Vulnerabilities.
   - Network Elements: Underlying Technologies.
   - Identifying Signalisation and Core Network Equipment: Proprietary OS, Windows-based, Linux-based, Solaris-based (case study and hands-on).
   - GPRS Signalling Technologies(GTP-C, GTP-U and GTP prime)and Known Vulnerabilities
   - Attacking GPRS and GTP-scanning.
   - Attack Scenarios and Case Studies from GRX and SCCP Providers
   - Attacking O&M (OAM & Management) Infrastructure.
   - SS7 Signalling Equipment Vulnerabilities.
   - Huawei De-bug Backdoor, aka Pseudmessage (case study)
   - Crafting SS7 Packets (MSU) by hand (hands-on).
   - Context and Network Layers.
   - Spoofing SS7 (hands-on).
   - Network Element Vulnerability Research: Discovering Zeroday in SS7 Equipment (hands-on).

- Mobile Reverse Engineering (hands-on).
- Industrialisation of Vulnerability Scanning in SS7 & SIGTRAN Context.
- RADIUS Protocol, Usage and Possible Attacks

3. Higher-level Applications.
   - SMS Fraud and Abuse.
   - SMSC (Kannel) Abuses (hands-on).
   - Fraud Management Systems (FMS) and FRA.
   - Legal Interception (LI) Systems.
   - Limits of CDR-based Fraud Detection and Security.
   - Mobile Application Part(MAP) Message Analysis and Attack Traffic
   - GSMA MAP screening recommendations(Cat1, Cat2, Cat3, Cat3+ and Cat SMS.
   - Examination of SS7 Attack Scenarios from National and International Perimeters.
4. Mobile Devices.
   - GAN/UMA.
   - Subscriber Identity Module.
   - GSM Authentication A3/A8.
   - Machine to machine (M2M) (Femtocell case study), Practical SIM Fraud (case study).

Prerequisites

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

Training Structure

Three-day training divided into logical sessions.

Methodology

Instructor-led training. Hands-on course with lab testing. Participants will receive a virtual machine with hands-on exercises and SIGTRAN/SS7 tools.