P1 Security

Priority One Security

2022

Training Description

TS-201 Telecom Security hands-on course

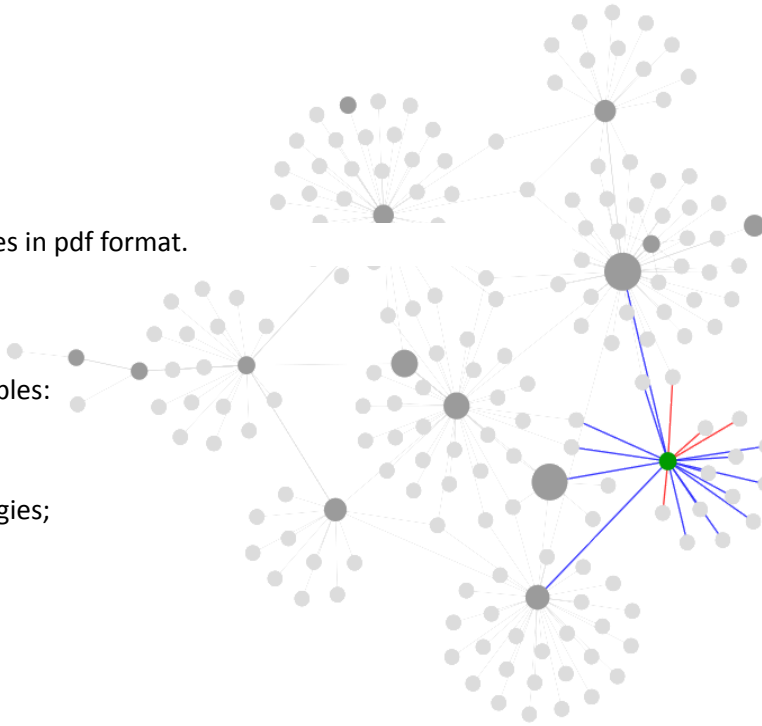
TS-201 Telecom Security hands-on course

Description of training

This training provides an in-depth knowledge of telecom security problems and their roots in the telecom systems focused on SIGTRAN, SS7, GPRS and GRX technologies as well as attacks against telecom network elements, architecture and design of various 3GPP releases.

Duration

Unique version: 3 days.



Attendees will receive

- Training material: copy of the presenter's slides in pdf format.

Prerequisites for training

- Basic knowledge of telecom & network principles:
  - What is 2G, 3G;
  - OSI network layers;
  - Basic knowledge of telecom technologies;
  - Basic knowledge of Linux.
- Good knowledge and usage of Wireshark;
- Good IT security background;
- Internet Access *(preferred but optional*).

Covered in this training

This is a practical SS7 and telecom security training. It aims at understanding the theory and practice of attacks and protections of telecom signalling networks, in the context of security and fraud.

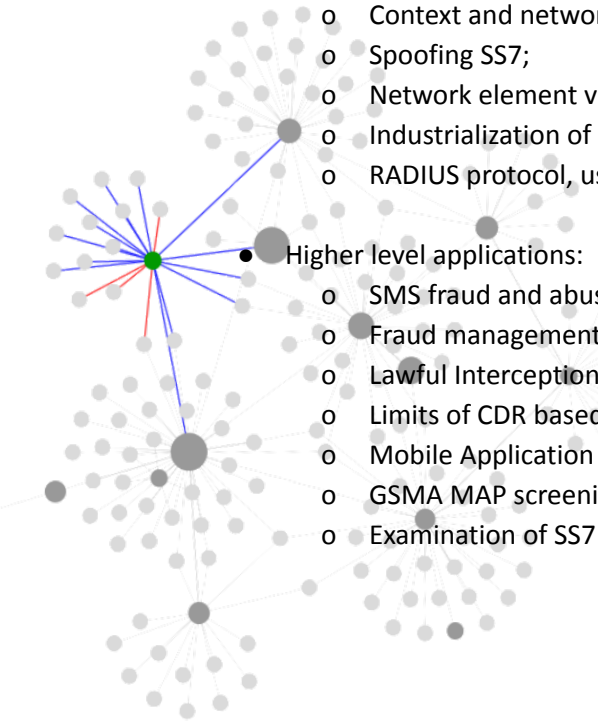
This training provides engineers who already have an established knowledge, either in telecom or IT security, to understand and evaluate security problems within an SS7 and telecom-signaling environment.

- SS7 Security:
  - SS7 basics and possibilities;
  - SS7 protocols description;
  - Telecom signalling networks architectures;
  - SS7 external access SS7Map review;
  - SS7 low level protocols analysis;
  - Low level SS7 packets analysis, sniffing and network tracing;
  - Signalling attacks;
  - SS7 and SIGTRAN
  - Low level peering
  - SCTP scan usage a

2022

- Scanning SS7 networks - from MTP to SCTP and upper SS7;
- SS7 upper level protocols (User Adaptation layers);
- Network elements and their functions, HLR, VLR, STP, SCP, BTS, GGSN, SGSN, MSC, 3G alternatives.

- Telecom signalling vulnerabilities:
  - Network elements underlying technologies;
  - Identifying signalling and core network equipment: proprietary OS, Windows-based, Linux-based;
  - 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) infrastructures;
  - SS7 signalling equipment vulnerabilities;
  - Crafting SS7 packets (MSU) by hand;
  - Context and network layers;
  - Spoofing SS7;
  - Network element vulnerability research: discovering zero days in SS7 equipment;
  - Industrialization of vulnerability scanning in SS7 & SIGTRAN context;
  - RADIUS protocol, usage and possible attacks.



- Higher level applications:
  - SMS fraud and abuses;
  - Fraud management systems (FMS) and FRA;
  - Lawful 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.