Reversing Telecom Platforms for Security

Who Should Attend?

This course is aimed at engineers who want to learn about contemporary Telecom and mobile system reverse engineering, the operation of core Telecom infrastructure within the context of Telecom and Mobile Network operators, and how core telecom infrastructure operates — down to the usage of this service by operators' mobile apps and handset manufacturers' platforms. Participants will see how all these technologies mesh together and learn how to make sense of the protocols and applications, from the mobile handset (Android, apps, platform) and enterprise applications (iPBX) all the way to Core Network.

Course Scope

1. Handsets & Subscriber Applications.
   - Mobile Phone Usage of the Network and Applications (CS, USSD, SMS, Packet-switched/Data, VAS) — We will look into the protocols used by mobile phones, analyse them, and detail where security problems can appear. Using OsmocomBB, we will analyse live networks around the conference.
   - Proprietary Apps and their Interface to Telecom Systems — By reversing some proprietary apps, we will see how non-standard interfaces are used within the mobile network. We will use frameworks for both static analysis (dead code, binary form) and dynamic analysis (live running apps, within existing phones/handsets).
   - Samsung Android Platform (Android + Proprietary Extensions) — We will look into Samsung Android platform specifics and security.
   - Access Network Protocol Analysis — We will look into the network protocols that are used by mobile handsets with the mobile network.
2. PBX, Femtocell, and Enterprise Access Methods.
   - M2M Connection Reverse Engineering.
   - Corporate Data/Packet-switched Mobile Broadband Connection Analysis — We will analyse and reverse common access setups and protocols to look for the vulnerabilities within these networks. We will look into multiple solutions for corporate access to the network. If time permits, we will look into existing 3G/4G access kits and their vulnerabilities.
   - Alcatel Lucent OmniPCX iPBX — We will look into the typical setup and vulnerabilities of modern PBX for enterprise access. We will look into the embedded operating system of PBX by extracting it from the hardware.
   - Commercial SIP Implementation Reverse Engineering and Vulnerability Analysis.
   - Hardware Embedded SIP TA Audit and Reverse Engineering.
   - Femtocell Security Vulnerabilities and Reverse Engineering.
3. Core Network Protocols and Network Elements.
   - We will dig into Core Network protocols, reverse engineer some specified and some proprietary Telecom Core Network protocols.
   - The training will show the various attack surfaces for these networks and show the impact of vulnerabilities for each network element.
   - Legacy Core Network Element Analysis; Nokia DX200 Core Network Element (legacy,

monolithic)—description and analysis.
  - Huawei MGW8900 Core Network Element (legacy, monolithic, VxWorks + FPGA) — description, analysis, and reverse engineering.
  - Huawei HSS / MSC Core Network Element (ATCA, recent, Linux + FPGA) — description, analysis, and reverse engineering.
  - ZTE Core Network Element (ATCA, recent, Linux) — description, analysis, and reverse engineering.

Prerequisites

- Basic knowledge of Telecom and network principles; 2G, 3G, 4G; OSI network layers; basic knowledge of Telecom technology.
- Laptop with Linux installed either in a VM or native. Backtrack or Ubuntu with reverse engineering and hacking tools recommended.
- Understand and be able to use Wireshark and Linux for reverse engineering (strings, knowledge of tools in Backtrack for reverse engineering).
- Mobile phone (Android recommended) and working SIM card with sufficient credit for voice, SMS, and data.
- Additional SIM cards recommended.
- Legal IDA Pro license recommended.

Training Structure

Five-day training divided into logical sessions.

Methodology

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