Active Exploitation Framework for Mobile Network Protocols Using Specialized Tactical Hardware

Tri Sumarno, Muhammad Mustafa Fagan

tri@noz.co.id fagan@noz.co.id

ABSTRACT

This Research presents the design and implementation of a state-of-the-art Active Exploitation Framework for Mobile Network Protocols, utilizing advanced tactical hardware, including USRP 2901, alongside multi-generation cellular stacks such as OpenBTS (2G), Osmocom (2G/3G), Open5GS (4G/5G), and srsRAN (4G/5G). The proposed framework enables comprehensive analysis of signaling behavior across heterogeneous radio access technologies and core network architectures, providing a unified, high-fidelity monitoring platform that facilitates cutting-edge technology research in mobile network security, interoperability, and performance evaluation.

Three major modules are developed:

SIM Swap Module, which evaluates real world attack surfaces involving subscriber identity exposure, mobility triggered authentication events, and GSM based distribution automation systems using PSOC based implementations. This includes passive IMSI collection on the Um interface, roaming based reauthentication scenarios, and GSMbased automation communication models.

Intercept Module, which implements lawful intercept architectures through HLR→HSS migration and UDM interworking, relay type network interception during packet forwarding (UPF, PGW, SGSN, MGW, IMS core), and MSISDN to IMSI mapping using OsmocomBB based probing on tactical SDR hardware.

Peripheral Module, The Peripheral Module implements sophisticated attack vectors at the Physical Layer (Layer 1). These attacks are particularly challenging to detect due to their low-level operation, which bypasses conventional protocol-based security monitoring mechanisms. For instance, an adversary could deploy a rogue gateway that disrupts network routing, floods the network with traffic, or in advanced scenarios executes Remote Code Execution (RCE) by exploiting vulnerabilities in baseband processors or network infrastructure through carefully crafted radio signals.

The framework provides researchers, telecom engineers, and security analysts with a reproducible methodology for evaluating protocol level threats, mobility management behavior, subscriber identity exposure, signaling interception points, and LI architecture compliance in modern telecom environments.

Keyword : SIM Swap, IMSI Collection, Lawful Intercept, Physical Layer Attack, Telecom Security.