Experimental Assessment of Private Information Disclosure in LTE Mobile Networks

Stig F. Mjølsnes and Ruxandra F. Olimid
Department of Information Security and Communication Technology, NTNU - Norwegian University of Science and Technology

Abstract

Open source software running on SDR (Software Defined Radio) devices now allow building a full-functional mobile network at low cost. These novel tools open up for exciting possibilities to analyse and verify by experiments the behaviour of existing and emerging mobile networks in new lab environments, for instance at universities. We use SDR equipment and open source software to analyse the feasibility of disclosing private information that is sent over the LTE access network. We verify by experiments that identity information can be obtained both passively, by listening on the radio link, and actively, by running considerable low detectable rogue base stations to impersonate the commercial network. Moreover, we implement a downgrade attack (to non-LTE networks) with minimal changes to the open source software.

Motivation & Contribution

- Disclosure of sensitive information in mobile networks has important consequences for both the privacy of subscribers and the security of commercial services.
- New tools have opened up the possibility to analyse by experiment the behaviour of all generations of cellular networks.
- We investigate, by experiment, information disclosure in LTE in 2 scenarios: passive attacks and active attacks.

Experimental Setup

General setup: computers running open source software, attached with SDR (Software Defined Radio) devices and antennas.

- Computers: Intel NUC DS425OWK (i5-4250U CPU@1.30GHz) and Lenovo ThinkPad T460s (i7-6600U CPU@2.30GHz), running 64-bit Ubuntu 14.04 kernel v3.19.0-61-low latency
- Handsets: Nexus 5 (Android v6.0.1) and Nexus 5X (Android v7.0)

Acknowledgements

The authors would like to thank post doc David Palmo at our department for providing some of the equipment necessary for the experiments and master students Christopher E. Otzen and Christian Sprøth for their help with some of the experiments.

Results

We sniffed the radio interface and intercepted parameters of a commercial mobile network in the Trondheim NTNU campus area:

- Figure 3 shows an example of cell search on a given frequency, listing cells that correspond to commercial eNodeBs in the area.
- Figure 4 shows a successfully decoded SIB1 (System Information Block 1) message. Notice the network identification parameters MCC (Mobile Country Code) and MNC (Mobile Network Code), the location area identifier and the cell identity. The cell is not barred and allows intra frequency reselection.
- Figure 5 shows a successfully decoded SIB5 (System Information Block 5) message. Notice the frequencies used in the area and their associated priorities.

Figure 2. HackRF One [1]
Figure 3. Commercial LTE Cells
Figure 4. Real capture of SIB1 (fragment)
Figure 5. Real capture of SIB5 (fragment)

Acknowledgements

The authors would like to thank post doc David Palmo at our department for providing some of the equipment necessary for the experiments and master students Christopher E. Otzen and Christian Sprøth for their help with some of the experiments.

References


Acronyms

- EMM: Equipment Management
- EPS: Evolved Packet System
- LTE: Long Term Evolution
- IMSI: International Mobile Subscriber Identity
- MNC: Mobile Network Code
- SDR: Software Defined Radio

Contact

Corresponding author: Ruxandra F. Olimid
Dept. of Information Security and Communication Technology
NTNU - Norwegian University of Science and Technology
Email: ruxandra.olimid@ntnu.no

Acknowledgements

The authors would like to thank post doc David Palmo at our department for providing some of the equipment necessary for the experiments and master students Christopher E. Otzen and Christian Sprøth for their help with some of the experiments.

References