Tittle : SigOver + alpha

Subtitle : -Signal overshadowing attack on LTE and its applications-

Summary : As Long-Term Evolution (LTE) communication is based on over-the-air signaling, a legitimate signal can potentially be counterfeited by a malicious signal. Although most LTE signaling messages are protected from modification using cryptographic primitives, broadcast messages and some of the unicast messages are unprotected. In this talk, we would like to introduce a signal injection attack that exploits the fundamental weakness of unprotected messages in LTE and modifies a transmitted signal over the air.

This attack, which is referred to as signal overshadowing (named SigOver) overwrites a portion of the legitimate signal to inject manipulated signal into the victim while the victim is connected to a legitimate cellular network. In most aspects, SigOver attack is superior to FBS (Fake Bas Station) and MitM (Man-in-the-Middle) attack, in terms of Efficiency, Effectiveness, and Stealthiness. Thus, Sigover results in new attacks exploiting broadcast channel and unicast channel. For example, SigOver attack on the broadcast messages can affect a large number of nearby UEs simultaneously such as signaling storm, Denial-Of-Service, downgrading attack, location tracking, and fake emergency alert. SigOver attack on unicast channel can silently hand over victims to FBS and perform MitM attack.

Sigover attack is currently zero-day. Since it exploits the fundamental problems in LTE physical signal, it will remain effective until 3GPP standards change.

Description : In detail, we talk about the implementation of the SigOver, the first practical realization of the signal overshadowing attack on the LTE broadcast signals, using a low-cost Software Defined Radio (SDR) platform and open-source LTE library. The SigOver attack was tested against 10 smartphones connected to a real-world network, and all were successful. The experimental result shows that the SigOver overshadows the target signal and causes the victim device to decode it with 98% success rate with only 3 dB power difference from a legitimate signal. On the other hand, attacks utilizing an FBS have only 80% success rate even with 35 dB power difference. This implies that the SigOver can inconspicuously inject any LTE message and hand over victims to FBS for the Man-in-the-Middle attack.

Presentation Snapshot :

1. Overview on LTE Architecture including structure, security aspects, and types of messages. Broadcast messages and some of the unicast messages are unprotected; thus they have a fundamental weakness.

2. Introduction of SigOver Attack, attack vectors, detailed implementational design, and issues on performing the attack. SigOver attack can manipulate unprotected LTE signals.

3. Comparison with FBS (Fake Base Station) Attacker and MitM (Man-in-the-Middle) Attacker, in terms of Efficiency, Effectiveness, and Stealthiness. In most aspects, SigOver is superior than FBS and MitM attacker.

4. Possible exploitations of broadcast channel using SigOver Attacks, such as signaling storm, Denial-Of-Service, downgrading attack, location tracking, and fake emergency alert.

5. Possible exploitations of unicast channel using SigOver Attacks. An attacker can manipulate every individual unprotected downlink messages. As the whole injection process is silent, this results in whole new types of attacks.

6. For example, an attacker can silently hand over victims to the fake base station. Once the victim is connected to the FBS, attacks including Man-in-the-Middle attack are possible.