DEMO – This is Your President Speaking: Spoofing Alerts in 4G LTE Networks

Max Hollingsworth, Gyuhong Lee, Jihoon Lee, Jinsung Lee,
Youngbin Im, Eric Wustrow, Dirk Grunwald, Sangtae Ha
University of Colorado Boulder
{max.hollingsworth,gyuhong.lee,jihoon.lee-1,jinsung.lee,youngbin.im,ewust,dirk.grunwald,sangtae.ha}@colorado.edu

ABSTRACT

4G LTE networks across the world (e.g., United States, Europe, and South Korea) use the same mechanism to broadcast emergency alerts. These alerts include AMBER, severe weather alerts, and the (unblockable) Presidential Alert in the US. We demonstrate the ability to spoof these alerts by forcing any 4G phone in the area of our malicious cell tower to receive and display a fabricated message. This demonstration uses a commercially-available software-defined radio, an LTE base station, and our modifications to the open-source NextEPC and srsLTE libraries to send the Presidential Alert to phones volunteered from the audience.

1 INTRODUCTION

The Warning, Alert, and Response Act of 2006 mandated that modern cell phones in the US receive and display emergency alerts. At this time, the 3GPP standard organization developed the Commercial Mobile Alert Service (CMAS) standard to define the delivery system for emergency alerts [1]. Some alerts, like AMBER and severe weather, are optional and can be disabled by the user. Other alerts, like the US Presidential Alert have no such optionality.

The first national test of the Presidential Alert was sent to all capable phones on Oct. 3, 2018 [8]. This test added to concern over the potential misuse of the alert system which had already entered the public eye due to a false alarm issued in Hawaii on Jan. 13, 2018 [9]. The alarm read, "BALLISTIC MISSILE THREAT INBOUND TO HAWAII. SEEK IMMEDIATE SHELTER. THIS IS NOT A DRILL." Although this message was caused by human error, not spoofing, it highlights the ability an attacker has to cause panic and disruption.

The LTE downlink carries alert messages, or CMAS messages, from the cell tower (referred to as eNodeB) to the cell phones (referred to as user equipment, or UE). A broadcast message, known as the System Information Block (SIB), carries the CMAS alert without encryption or authentication. Each eNodeB periodically broadcasts the SIB messages to the surrounding UEs. A UE requires the SIB message for the cell selection process, which the UE performs before mutual authentication with the eNodeB. Thus, the SIB is vulnerable to spoofing from a malicious eNodeB. Furthermore, even if a UE has completed its authentication process and securely communicates with an eNodeB, the UE is exposed to the security threat caused by broadcasts from other, possibly malicious, eNodeBs. This is due to the UE periodically gathering information from neighboring eNodeBs for potential (re)selection and handover.

SIB12 is the specific portion of the SIB that contains the CMAS alert [2]. The contents of the CMAS message is a simple GSM 7-bit encoding which is used in traditional Short Message Service (SMS) [6]. Any UE currently "camping", or synchronized, with an eNodeB will automatically decode all of the SIB messages and display the alert if the SIB12 is present. An attacker that can imitate eNodeB behavior closely enough to broadcast SIB12 has the capability to force any camping UE to decode and display a false CMAS alert. To the best of our knowledge, this is the first experimentally verified work that discloses the potentially formidable risk of CMAS spoofing. As a note, LTE networks currently deployed in most countries (including countries in Europe, United States, South Korea, etc.) have adopted public warning systems that follow the same architecture principles as CMAS [3], making them potential targets for the same attack.

In the full paper [4], the details of this spoofing attack of the Presidential Alert are further investigated using both commercially available hardware and modified open-source software.

2 SPOOF METHODOLOGY

A UE's vulnerability to the spoofed CMAS alert depends on whether it lies in *idle* or *active* mode, as seen in Figure 1. Our attack varies depending on the mode, so we discuss *idle* and *active* UEs separately.

2.1 Idle Mode UEs

Reference Signal Received Power (RSRP) is the power of the eNodeB's reference signals at the UE. A UE uses RSRP to make cell selection and handover decisions. Normally, when an *idle* UE performs cell selection (or reselection), it will associate with the eNodeB of the highest RSRP.

If the RSRP of a malicious eNodeB is the strongest, the UE will camp on the malicious eNodeB. The attacker does not need any of the UE's information (including security keys), which would normally be stored in the database of the network operator. Without having such user information the eNodeB will soon fail the UE's authentication process. However, the UE can receive a CMAS message transmitted by the malicious eNodeB during this process.

Since a UE attempts the authentication process up to five times before it listens to other frequency channels, the malicious eNodeB can leverage this period to send a CMAS message. The series of attach attempts and failures currently takes 42 seconds.

MobiSys '19, June 17–21, 2019, Seoul, Republic of Korea

ACM ISBN 978-1-4503-6661-8/19/06.
https://doi.org/10.1145/3307334.3328572

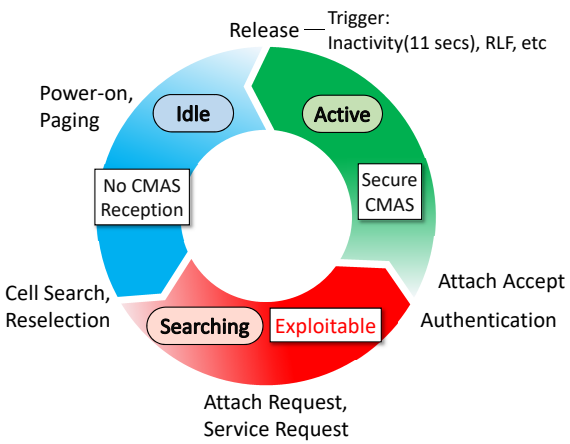

Figure 1: The Idle/Active life-cycle of a UE. The state of UE is moving counter clockwise. CMAS spoofing is possible while the UE performs a cell search, prior to successful authentication with a trusted eNodeB.

2.2 Active Mode UEs

When a UE is in *active* mode, it securely communicates with one serving eNodeB. If it finds another eNodeB with a higher RSRP than the existing serving eNodeB, the handover procedure triggers; the UE measures the RSRP of the candidate eNodeB and sends the measurement report to the serving eNodeB. The serving eNodeB then makes a handover decision based on the received measurement report. However, if the Mobility Management Entity (MME) of the UE's serving eNodeB does not identify the candidate eNodeB then the handover will eventually fail. Therefore, the handover procedure, even if caused by a malicious eNodeB, does not make a UE vulnerable to the CMAS spoofing attack.

As a consequence, in order to attack an active UE, the attacker first needs to disconnect the UE from its serving eNodeB. After the serving eNodeB releases the UE, it will immediately try to attach to the strongest eNodeB and become vulnerable in the same manner as described for *idle* UEs in section 2.1.

A communication error on an established radio link between the UE and its serving eNodeB is referred to as a Radio Link Failure (RLF). Both the UE and eNodeB can detect an RLF for various erroneous cases. One typical RLF is caused by reaching the maximum number of packet retransmissions. Jamming LTE signals can also lead to an RLF for active UEs [5, 7]. Without any special jamming technique, however, a malicious eNodeB can jam the communication between a UE and its serving eNodeB simply by transmitting at a much higher power than the serving eNodeB. The malicious eNodeB overwhelms the serving eNodeB's transmissions and causes an RLF. Once the RLF occurs, the UE releases its radio connection. At this time, the UE attempts to attach to the highest powered eNodeB, becoming vulnerable to spoofed CMAS messages.

3 DEMONSTRATION

The CMAS spoofing demonstration works on phones in *idle* and *active* modes. The equipment consists of a UE, a trusted eNodeB and Evolved Packet Core (EPC), a malicious eNodeB and EPC, and a faraday cage. Figure 2 shows the aforementioned trusted and malicious eNodeB and EPC. All wireless transmissions occur within the faraday cage to comply with US and South Korean laws. The UE initially authenticates to the trusted eNodeB, identical to the behavior of a normal cell phone. The malicious eNodeB then transmits on the same frequency as the trusted eNodeB, causing an RLF between the UE and the trusted network. Then, the UE attempts to connect to the higher-powered malicious eNodeB. The malicious eNodeB transmits the SIB12 message containing the false CMAS alert. Finally, the UE decodes and displays the alert for the user.

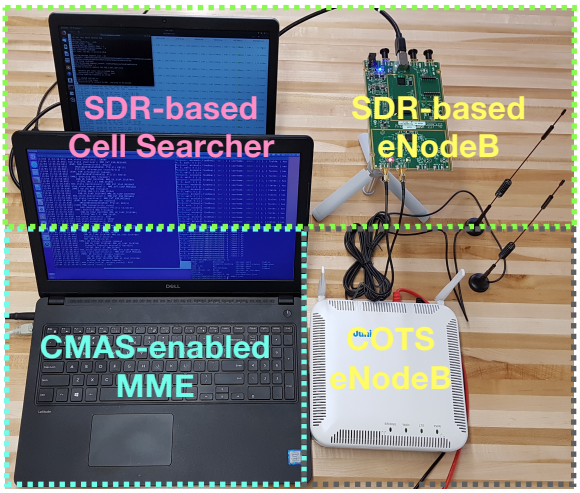

Figure 2: Our Presidential Alert Spoofer scans a cell, gathers operator information, and sends a fake Presidential Alert to both idle and active UEs. It consists of one SDR device, one COTS LTE eNodeB, and two laptops.

This spoofer demonstration has been tested on iOS and Android phones from all four major US carriers. Audience members may choose to participate in our demonstration by volunteering their phones to receive the spoofed alert. A video of the demo is available at https://youtu.be/XJ7FPYs2bIw.

REFERENCES

[1] 3GPP TS 23.041. Technical Specification Group Core Network and Terminals; Technical realization of Cell Broadcast Service (CBS) (Rel. 15). http://www.3gpp.org/dynareport/23041.htm, 2018.
[2] 3GPP TS 36.331. Technical Specification Group Radio Access Network; E-UTRA; Radio Resource Control (RRC) (Rel. 15). http://www.3gpp.org/dynareport/36331.htm, 2018.
[3] 5G Americas. Public Warning Systems in the Americas, 2018. https://goo.gl/yZ4R4L.
[4] G. Lee, J. Lee, J. Lee, Y. Im, M. Hollingsworth, E. Wustrow, D. Grunwald, and S. Ha. This is Your President Speaking: Spoofing Alerts in 4G LTE Networks. In *Proc. of ACM MobiSys*, 2019.
[5] M. Lichtman, R. P. Jover, M. Labib, R. Rao, V. Marojevic, and J. H. Reed. LTE/LTE-A jamming, spoofing, and sniffing: threat assessment and mitigation. *IEEE Communications Magazine*, 54(4):54–61, April 2016.
[6] C. Mulliner, N. Golde, and J.-P. Seifert. SMS of death: from analyzing to attacking mobile phones on a large scale. In *Proc. of USENIX conference on Security*, 2011.
[7] A. Shaik, J. Seifert, R. Borgaonkar, N. Asokan, and V. Niemi. Practical attacks against privacy and availability in 4G/LTE mobile communication systems. In *Proc. of NDSS*, 2016.
[8] The Washington Post. Cellphone users nationwide just received a 'Presidential Alert.' Here's what to know. https://goo.gl/KRfDjf, 2018.
[9] Wikipedia. Hawaii false missile alert. https://goo.gl/oD9ofx, 2018.