1200 G Street, NW
Suite 500
Washington, DC 20005

P: 202-628-6380
W: www.atis.org

October 30, 2020

James Wiley
Public Safety and Homeland Security Bureau
Federal Communications Commission
45 L Street NE
Washington, DC 20554

Re: ATIS Report on Mitigating Wireless Emergency Alert (WEA) False Base Station Attacks

Dear James:

The Alliance for Telecommunications Industry Solutions (ATIS) Wireless Technologies and Systems Committee (WTSC) is pleased to provide the attached *ATIS Report on Mitigating Wireless Emergency Alert (WEA) False Base Station Attacks* (ATIS-0700046). This report addresses a potential False Base Station Attack exploit, in which one or more well-placed false base stations broadcasting fraudulent WEA are placed in a crowded venue placed by a malicious actor(s). The report also provides an evaluation of possible mitigation techniques in 4G Long Term Evolution (LTE) networks.

Due to the nature of this information and its potential misuse by bad actors, ATIS requests that the Commission not release this information publicly. While any single piece of information in this report may not be considered highly sensitive, the aggregation of this information – which includes mitigation techniques together with analyses of vulnerabilities, comparisons of their effectiveness, and industry conclusions – into a single source raises the effective sensitivity of all parts of the report. ATIS also requests that the Commission consider the potential risk involved in making this report available beyond those with the need to know within the Commission.

If you have any questions or would like further information, please do not hesitate to contact the undersigned. ATIS WTSC would be happy to arrange a call to provide addition information about the report.

Sincerely,

Thomas Goode
ATIS General Counsel

cc: Mark Younge, ATIS WTSC Chair
Don Zelmer, ATIS WTSC Vice Chair
Peter Musgrove, ATIS WTSC SN Chair
Terri Brooks, ATIS WTSC SN Vice Chair
Steve Barclay, ATIS Sr. Director, Global Standards Development
Katie Bagwill, ATIS Coordinator, Global Standards Development

ATIS STANDARD

ATIS-0700046

ATIS Report on Mitigating Wireless Emergency Alert (WEA) False Base Station Attacks

TECHNICAL REPORT

As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global ICT companies to advance the industry's most pressing business priorities. ATIS' nearly 200 member companies are currently working to address the All-IP transition, 5G, network functions virtualization, big data analytics, cloud services, device solutions, emergency services, M2M, cyber security, network evolution, quality of service, billing support, operations, and much more. These priorities follow a fast-track development lifecycle — from design and innovation through standards, specifications, requirements, business use cases, software toolkits, open source solutions, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). The organization is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of the oneM2M global initiative, a member of the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org.

Notice of Disclaimer & Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OFMERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

> NOTE - The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. By publication of this standard, no position is taken with respect to whether use of an invention covered by patent rights will be required, and if any such use is required no position is taken regarding the validity of this claim or any patent rights in connection therewith. Please refer to [http://www.atis.org/legal/patentinfo.asp] to determine if any statement has been filed by a patent holder indicating a willingness to grant a license either without compensation or on reasonable and non-discriminatory terms and conditions to applicants desiring to obtain a license.

ATIS-0700046, *ATIS Report on Mitigating Wireless Emergency Alert (WEA) False Base Station Attacks*

Published by

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

Copyright © 2020 by Alliance for Telecommunications Industry Solutions
All rights reserved.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher. For information contact ATIS at 202.628.6380. ATIS is online at < http://www.atis.org >.

ATIS-0700046

ATIS Report on Mitigating Wireless Emergency Alert (WEA) False Base Station Attacks

Alliance for Telecommunications Industry Solutions

Approved October 6, 2020

Table of Contents

Table of Tables

Table of Figures

1 Executive Summary

The Wireless Emergency Alert (WEA) system is responsible for the dissemination of critical and often life-saving information to the public. All stakeholders involved in this system from the Alert Originators, to the Federal Emergency Management Agency (FEMA), to the Participating Commercial Mobile Service Providers (CMSPs), need to be cognizant of possible risks to that system, including the existence of possible malicious intent to disseminate false information to the public with the purpose of doing harm. At the same time, the important information carried in the WEA messages being communicated via this system should be available to all mobile device users, in a timely manner, whenever possible. The perceived benefits of any potential security measures should be analyzed and balanced against any identified impacts to the WEA service that they may cause from the perspective of delaying or inhibiting any mobile devices from being able to process and present alerts to the user, as well as impacts to any other parts of the WEA system.

This report addresses a potential False Base Station Attack exploit which, in theory, uses one or more well-placed false base stations broadcasting fraudulent WEA in a crowded venue, such as a sports stadium, placed by a malicious actor or actors. These actors may be an individual or fringe group of individuals with the intent to disrupt the event[1]. A false base station may be able to divert User Equipment (UE) to monitor the System Information Broadcasts (SIBs) it is broadcasting rather than listening to available authentic base station. The described exploit allows a false base station to broadcast a WEA message containing false information that is then received by the UE and may be presented to the user, appearing to the user as an authentic WEA. A demonstration of this exploit is described in [Ref 1].

The scope of this report analyses the false base station exploit and provides an evaluation of possible mitigation techniques in 4G Long Term Evolution (LTE) networks, per the focus of the University of Colorado study. The scenario being studied focuses on UEs in an idle (not connected) state. False WEA delivery to UEs in the active/connected mode would be more challenging to execute than an attack on idle mode UEs per the description in Section 3.2 of the University of Colorado report. Security mechanisms are in place in 4G LTE to mitigate the possibility of attaching to a false base station when switching to a connected state. Further enhancements are being added for 5G.

This report describes several potential mitigation techniques and evaluates each mitigation technique based on the following potential impacts:

1) Standards impacts, including the standards bodies (e.g., 3GPP, ATIS) and specifications impacted (to include estimated standardization timelines)
2) Development impacts to all Alert System stakeholders (Alert Originators, FEMA, Participating CMSPs)
3) Deployment Complexity and Impacts
4) Impacts to Alert Presentation at the Mobile Device:
    a. Delay in the user being presented the WEA
    b. WEA delivery success rate
    c. Presentation of a WEA for legacy mobile devices (i.e., devices that are not able to be upgraded)
    d. Ability of roaming subscribers to receive WEA messages
    e. Ability of non-service initialized (NSI) devices for receiving WEA messages

Finally, each mitigation technique is evaluated to further narrow using various additional criteria, including:

1) The degree to which the mitigation technique fully addresses the False Base Station Attack exploit
2) The degree of vulnerability of the mitigation technique to be circumvented
3) The degree of risk of adverse impacts or other unintended consequences to users and/or the WEA service overall
4) Complexity of the mitigation technique
5) Standards Impacts, including Standards Development Organization(s)(SDO) impacts and estimated standardization timelines
6) Deployment Considerations, including Testability

[1] Risks from sophisticated and/or state-sponsored actors are not addressed in this report.

Following the application of the evaluation criteria described above, Section 8 presents the results of the analysis. The mitigation technique[s] remaining after applying the evaluation criteria are:

MT1: Digital signatures w/NAS based key distribution

MT7: Application Layer Digital signatures

Finally, this report takes a more holistic look at the problem statement, the expectations, and realities in the field. Clause 9 discusses the types of field configurations that are likely to be deployed in a flagship venue. These configurations, combined with the limited number of UEs expected to be in idle mode during a major event (e.g., a major sporting event), would substantially reduce the percentage of mobile devices that would be vulnerable to this exploit. This fact, coupled with the lack of confirmation of the imminent threat by any other means (stadium siren, announcement, etc.), further lower the chances of success of this exploit.

Clause 9 goes on to discuss the identified negative impacts to mobile users that may result from deploying a mitigation technique, including additional delay in receiving possible life-saving WEAs, and the chance that authentic WEAs will not be presented to the user. The impacts of deploying any mitigation technique are ubiquitous throughout the WEA system—the impacts will apply universally to all alerts and all users in any location receiving a WEA broadcast.

Based on the analysis of the threat from a rogue actor, the consensus is that the False Base Station Attack theorized by the University of Colorado does not constitute grounds for taking these risks of delays or non-presentation of authentic WEAs posed to users by the deployment of a mitigation technique.

In conclusion, to preserve the integrity of WEA system and maintain user confidence in WEA, no mitigation technique should be deployed due to the risk of the loss of conveying important information in a timely manner to users for a known imminent threat to life or property, in return for attempting to address a potential risk that carries an uncertain chance of success.

2 Introduction

This report is produced to address concerns of the potential risks of exploits employing false WEA for nefarious purposes such as to trigger public panic or false alarm. A demonstration of this exploit is described in [Ref 1].

While there is limited chance of success for the False Base Station Attack from a rogue malicious actor (i.e., individual or small group), ATIS and its participating CMSPs are not in a position to fully address risks of the False Base Station Attack threat if there are more sophisticated actors and/or state-sponsored threats. Sophisticated attacks are likely to overcome any mitigation put in place. A complete risk/threat analysis of these sophisticated actors requires input from intelligence agencies within the U.S. government including the Department of Defense.

One potential mitigation is the use of digital signature to address the attacks discussed in the University of Colorado study; however, there are a number of other potential risks to WEA that were identified in the FCC Communications Security, Reliability, and Interoperability Council (CSRIC V) Working Group 2 report on WEA Security[2]. Digitally signing WEA was not one of the recommendations out of that Report as there are other risks that are much more probable, impactful, and have higher risk exposure.

During the creation of this report, a study previously performed by 3GPP was reviewed to leverage the findings of that work. This 3GPP study focuses on Public Warning System (PWS) Security. The 3GPP study can be found in [Ref 2].

The following sections of this report advise the reader of the following for each proposed mitigation technique:

1) Requirements, architecture and technical description.
2) Evaluation: Ability to fully address the False Base Station Attack, including the Replay Attack[3]
3) Testability
4) Potential impacts (See Executive Summary)

[2] https://transition.fcc.gov/bureaus/pshs/advisory/csric5/WG2_WEA-Sec-Sub_FinalReport_0316.docx

[3] The Replay Attack could occur should a signing mitigation technique with no included timestamp nonce be deployed. The Replay Attack may allow a false base station to re-send a previously valid WEA at a later time when that WEA is no longer valid or active.

3 References

[Ref 1] *This is Your President Speaking: Spoofing Alerts in 4G LTE Networks* by Lee, Lee, Lee, Im, Hollingsworth, Wustrow, Grunwald and Ha, MobiSys '19, June 17-21, 2019, Seoul, Korea

[Ref 2] 3GPP TR 33.969, *Study on Security aspects of Public Warning System (PWS)*

[Ref 3] 3GPP TS 22.268, *Public Warning System (PWS) requirements*

4 Acronyms & Abbreviations

3GPP	3rd Generation Partnership Project
ATIS	Alliance for Telecommunications Industry Solutions
CA	Certificate Authority
CBC	Cell Broadcast Center
CBE	Cell Broadcast Entity
CMAS	Commercial Mobile Alert Service
CMSP	Commercial Mobile Service Provider
CN	Core Network
EEWS	Earthquake Early Warning System
HeNodeBs	Home eNodeBs
FEMA	Federal Emergency Management Agency
FIFO	First In First Out
LTE	Long Term Evolution
MME	Mobility Management Entity
NAS	Non-Access Stratum
NWS	National Weather Service
PLMN	Public Land Mobile Network
PWS	Public Warning System
RAN	Radio Access Network
RRC	Radio Resource Controller
RSS	Received Signal Strength
SDO	Standards Development Organization
SIB	System Information Block
UE	User Equipment
USGS	United States Geological Survey
USIM	Universal Subscriber Identity Module
WEA	Wireless Emergency Alert

WHAM	WEA Handset Action Message

5 Potential Mitigation Techniques

Each Mitigation Technique subsection below includes the following:

- Details, Requirements and Architecture
- Evaluation: Does the technique fully address the False Base Station Attack
- Testability, indicating the technical feasibility and difficulty level of testing the technique

The mitigation technique known as Last Mile Security for WEA was reviewed but not included in this report. In this mitigation technique, the security of PWS, or WEA as called in this document, is handled by last mile entities, which are the Core Network (CN) and the Radio Access Networks (RAN) in the serving Public Land Mobile Network (PLMN). While some aspects of the mitigation technique were discussed by 3GPP, the technique has not been developed to the extent necessary to allow the analysis required in this report.

5.1 Mitigation Technique #1–Digital signatures with NAS based key distribution

5.1.1 Introduction

This mitigation technique is based on digital signatures for integrity protection of WEA messages.

5.1.2 Details, Requirements, & Architecture

See the mitigation technique described in Section 6.1 in [Ref 1], which relies on the NAS based key distribution as described in Clause 7.3 in [Ref 2].

This technique uses the Non-Access Stratum (NAS) signaling exchanged between the operator network and the mobile device during the registration process to exchange public keys known only to the wireless operator and the mobile device. Integrity protection is offered via the NAS signaling method of public key exchange for LTE. Such public keys can be distributed/updated to core network nodes by pre-configuration or by network signaling from the Cell Broadcast Center (CBC). It is assumed that the signing of WEA alerts can occur at the 3GPP Cell Broadcast Entity (CBE), which is the Commercial Mobile Service Provider (CMSP) gateway in the ATIS WEA architecture. Individual WEA messages are digitally signed by the CMSP gateway after receipt of the alert from the FEMA Federal Alert Gateway. The mobile devices are able to verify the digital signature sent with each WEA message by using a stored public key from the NAS exchange during registration. If the digital signature is verified, the mobile device proceeds with normal WEA processing (i.e., determine its location and present the alert to the user if the device is determined to be within the alert area).

5.1.3 Evaluation

If a false base station were to broadcast a WEA alert to a mobile device that supports this technique, the false base station would not know the key(s) distributed by the wireless operator network, and therefore, would not be able to include a verifiable digital signature in the false alert. Mobile devices that supported this technique would not be able to verify the alerts from a false base station; therefore, these devices may not present the false alerts to the user, subject to policy.

Legacy devices (i.e., those that do not support this mitigation technique) would ignore the NAS key exchange during the registration process. Legacy devices would also ignore the digital signature when it is sent with a WEA alert, as the signature would be viewed by the device as an unknown parameter, and in such cases, the device would proceed with normal processing of the WEA alert upon receipt.

This technique involves changes in the network and changes to mobile devices. No development changes would be needed for the Alert Originators or for the FEMA Federal Alert Gateway.

If this technique were implemented in the operator network, users of NSI devices that support this technique would not be presented digitally signed messages, unless the device preconfigured key is still valid, as the NAS procedure for key exchange requires a subscription to allow for mobile device registration to the wireless operator's network.

Note that users of legacy NSI devices (i.e., those devices not supporting this mitigation technique and without a subscription) will still be vulnerable to receiving false base station alerts if this mitigation technique were implemented by the operator.

If the digital signature verification fails, or if there was no signature included in the WEA alert (e.g., legacy broadcast from a roaming network that did not support this mitigation technique), the mobile device would detect an error (see Section 7.2).

5.1.4 Testability

Testing of this technique would require careful planning, standardization, development, implementation, and testing within the wireless operator network. CMSP gateways, Mobility Management Entity (MMEs), eNodeBs, Home eNodeBs, and new devices would require changes and need testing to ensure the viability of this technique. Neither FEMA nor Alert Originators would be required to be involved in testing this technique in operator networks.

5.2 Mitigation Technique #2 – Accepting WEA alerts only from authenticated networks (client-only approach)

5.2.1 Introduction

This mitigation technique is a client-only approach in which the UE accepts WEA alerts after it has authenticated/registered with a network.

5.2.2 Details, Requirements, & Architecture

See the mitigation technique described as *Accepting only secure Commercial Mobile Alert Service (CMAS)* in Section 6.2 in [Ref 1].

5.2.3 Evaluation

Client-only mitigation techniques may be fooled by a resourceful attacker. In this particular mitigation technique, the resourceful attacker may succeed by acting as a proxy so that the UE has a notion that the network is authenticated. This technique is fundamentally flawed, as a false base station may pose as an authenticated network, broadcasting the same System Information Block (SIB)12 WEA information as the network with which the UE has registered. Valid subscribers, including roamers whose UEs support this technique and whose UEs authenticate/register to the operator network, will continue to be vulnerable to receiving false base station alerts. Roamers whose UEs do not support this mitigation technique, as well as users with legacy devices that do not support this mitigation technique, will remain vulnerable to receiving alerts from false base stations, The only users protected from receiving false alerts by this technique will be those with NSI devices and those temporarily in the unauthenticated state due to a number of conditions such as a UE attempting to attach to a network, a UE undergoing idle exit, or a UE in the middle of a handover. This technique requires no changes to network nodes, no changes to the FEMA Federal Alert Gateway, and no changes to Alert Originators; however, changes would be required to mobile devices such that they would prohibit the presentation of WEA alerts to the user while they were in an unauthenticated/unregistered state.

If this technique were implemented in devices, users of NSI devices that support this technique would be protected from receiving alerts from false base stations. Note that users of legacy NSI devices (i.e., those devices not supporting this mitigation technique and without a subscription) will still be vulnerable to receiving false base station alerts.

5.2.4 Testability

No network node testing is required for this mitigation technique. Only devices would need to be tested with this technique to see if they adhere to the requirement that WEA alerts are not to be presented to users when the UEs are in the unauthenticated/unregistered state.

5.3 Mitigation Technique #3–LTE eNodeB fingerprinting (client-only approach)

5.3.1 Introduction

This mitigation technique is also a client-only approach where the UE creates fingerprints of the eNodeBs used and authenticated in normal operation. The characteristics of the eNodeB broadcasting the WEA will be compared against the fingerprint.

5.3.2 Details, Requirements, & Architecture

See the mitigation technique described as *LTE eNodeB fingerprinting* in Section 6.2 in [Ref 1].

5.3.3 Evaluation

Client-only mitigation techniques may be fooled by a resourceful attacker. In this particular mitigation technique, a resourceful attacker may succeed in creating a false radio environment around the UE by replicating the transmission patterns of genuine eNodeBs.

This technique relies on the UE monitoring the SIB transmission patterns of eNodeBs which it detects in its environment and presumably storing this information for later use upon receipt of a WEA alert. While the details of how such a client-only solution would actually be implemented within a UE are not described in Section 6.2 in [Ref 1], the premise of LTE eNodeB fingerprinting is that the UE will, upon receipt of a WEA alert, perform a comparison of the SIB pattern associated with the eNodeB or HeNodeB transmitting the alert to a list of previously stored patterns in the UE. How such patterns are recognized and stored in the UE is critical to the evaluation of this mitigation technique.

The potential UE complexity of supporting LTE eNodeB fingerprinting for WEA will depend on the answer to a number of questions including the following:

(1) What are the criteria for storing information in the UE regarding eNodeB SIB transmission patterns?
(2) Will the UE store information about every eNodeB it detects, or just for those on which it registers?
(3) Will the detection include Home eNodeBs (HeNodeBs) small cells (assuming there is some differentiator in the SIB signaling between eNodeBs and HeNodeBs)?
(4) Is a First In First Out (FIFO) algorithm the most appropriate for the UE to use for the storage and subsequent deletion (upon reaching some maximum threshold for storage) of LTE fingerprinting patterns?
(5) Will the pattern information be stored only when in the home network or also when roaming?
(6) Is the fingerprinting information stored in the UE to be used for any other application beyond WEA?
(7) Does the UE already perform fingerprinting in which case an existing capability can be leveraged to assist with WEA?
(8) For how long should the UE store pattern information associated with a particular eNodeB or Home eNodeB?
(9) Does the time storage requirement differ for eNodeBs and Home eNodeBs detected in the home network and in roaming networks?
(10) For what length of time might a false base station have to transmit SIB information for a UE to be able to detect and store the false base station SIB pattern as a valid LTE fingerprint?
(11) How does the length of time in item 10 above compare to the length of time that a valid temporary small cell, cell on wheels, or cell on wings (drone, blimp) would have to transmit SIB information to be recognized as a valid LTE fingerprint?
(12) Does the risk of vastly larger power levels of macrocells drowning out microcells in their immediate vicinity affect the LTE eNodeB fingerprinting technique?

A thorough evaluation of this mitigation technique would be very difficult to complete without answers to the above questions or at least a limiting set of assumptions.

One of the highest risk use cases for false base station alerts is in a large stadium environment in which a large number of people can simultaneously be “manipulated” by a false alert. It is in this stadium environment that operators may choose to deploy temporary cell sites which may include a mix of fixed small cells, cells on wheels, or even cells on wings (drones, blimps) to assist with coverage. It is arguable that in this highest risk environment for false alerts, LTE fingerprinting may have its largest challenges due to the lack of advance time for a UE to detect and store valid SIB patterns for cell sites that may not be turned on until close to the time of a large event. If the LTE fingerprinting technique is to cause a UE not to present a received WEA alert because the detected SIB pattern for the WEA alert was not a “recognized SIB pattern”, then the danger exists that valid WEA alerts broadcast to an alert area that includes the stadium would not be presented to users. This highlights the inherent risk of LTE fingerprinting, i.e., that perfectly valid alerts will be quashed by the UE if a pattern match is not found.

If this technique were implemented in devices, users of NSI devices that support this technique would be protected from receiving alerts from false base stations to the same extent as users of devices with subscriptions. Note that users of legacy NSI devices (i.e., those devices not supporting this mitigation technique and without a subscription) will still be vulnerable to receiving false base station alerts.

5.3.4 Testability

No network node testing is required for this mitigation technique, as this is a client-only approach. Only devices would need to be tested with this technique to see if they adhere to the requirement that WEA alerts are not to be presented to users when the UEs do not detect a recognized SIB LTE fingerprint pattern in the SIB for the received WEA alert. Device testing in the real-world environment for this mitigation technique is expected to be very complex.

5.4 Mitigation Technique #4 – LTE eNodeB location verification

5.4.1 Introduction

This mitigation technique involves the UE measuring eNodeB Received Signal Strength (RSS) to determine of the estimated distance from the broadcasting eNodeB.

5.4.2 Details, Requirements, & Architecture

This mitigation technique follows the mitigation technique described as *Providing an eNodeB's location* in Section 6.2 in [Ref 1]. While this mitigation technique is labeled as a “client-only” approach in [Ref 1], it requires UE consultation of an internet-connected database of cell site locations and thus loses the purported advantages of other truly client-only approaches.

The UE consults an internet-connected database to determine whether any base station(s) exist at approximately the estimated distance from the UE. If any such WEA broadcasting base stations exist near this estimated distance, the base station is deemed to be at a feasible distance from the UE and therefore the WEA will be further processed by the UE when it is received. If there are no such WEA broadcasting base stations near this estimated (feasible) distance, the WEA will be discarded by the UE.

5.4.3 Evaluation

This mitigation technique may be fooled by a resourceful attacker. In this particular mitigation technique, a resourceful attacker may succeed in fooling the UE's base station location estimation mechanisms by adjusting its transmission power, thus influencing the measured RSS at the UE. This could ultimately mean that the UE may estimate that the false base station is at a feasible distance, thus producing a false positive (feasible) result.

This mitigation technique as described in [Ref 1] relies on the UE having access to online base station location data , access to an onboard UE location service (e.g., GPS), and a good radio propagation model to estimate the distance between the UE and the broadcasting base station based on the measured. For access to the base station location data the UE needs to be connected and have access to the internet when a WEA alert is received. This technique requires internet queries from the UE to a cell site location database upon receipt of each WEA alert. Substantial network traffic proportional to the size of the broadcast area will be generated in the wireless operator networks to support queries generated from every UE supporting this technique within the broadcast area upon receipt of each WEA alert. In addition, the deployment of COWS/COLTS/Cell on Wings may not be included in such a database in a timely manner and thus may be missed for mobile devices connected to these base stations. The description in [Ref 1] references cellmapper.net as a potential source of information for cell site locations noting the concern regarding COWS/COLTS/Cell on Wings. The trustworthiness of the source of cell site location data would need to be evaluated, and perhaps each operator could establish a trusted source for querying for such information.

However, special consideration would be needed for the handling of NSI mobiles that support this technique, and which are not necessarily associated with a particular operator.

Mitigation of the onerous UE network query requirement to determine base station locations upon receipt of a WEA alert could possibly be achieved by having the UEs obtain and store an onboard database of nearby cell site locations for areas in which they rove. This onboard UE database would be consulted upon receipt of a WEA alert instead of querying an external database. However, there are many issues with this concept. First, how much data would be stored in such an onboard UE database? How often would it be updated (thus requiring generation of network traffic)? Would the updating of onboard data be time-based, location-based, and roaming status-based? How reliable could the base station location information be given the dynamic nature of the deployment of base stations (including macrocells, microcells, and temporary base stations such as cells on wheels, and cells on wings meant to fill in coverage for large events and during times of disaster when other base stations may be out of service)?

The algorithm in the UE for deciding whether or not one or more feasible base stations exist for transmitting the alert will be complex and will be subject to error/uncertainty. In a rural area with macrocells spread out over a large distance, this technique would appear to have the best chance of success, as few base station choices with likely a large degree of distance variation may prove relatively easy to distinguish from a nearby small cell false base station. However, in an urban environment with a large number of macrocells and an even larger number of microcells in close proximity, distinguishing distance variations may prove difficult and render this technique unreliable. If the algorithm is developed to be too exacting on UE-to-base station location comparisons, then there could be a large number of false negatives in distance feasibility determination, and the consequence would be not presenting valid WEA alerts to the user. If the algorithm is developed to be too lax on UE-to-base station location comparisons, then there could be a large number of false positives in distance feasibility determination, and the consequence would be allowing alerts from false base stations to be presented to users.

If this technique were implemented in devices, users of NSI devices that support this technique would be protected from receiving alerts from false base stations to the same extent as users of devices with subscriptions. Note that users of legacy NSI devices (i.e., those devices not supporting this mitigation technique and without a subscription) will still be vulnerable to receiving false base station alerts.

5.4.4 Testability

Both UE and network node testing would be required for this mitigation technique. The network node testing would involve testing queries and responses at one or more base station location databases as well as testing the methods for dynamically changing the data in such network databases. The UE testing would involve testing queries and responses to the network base station location database(s) upon receipt of a WEA alert by the UE. The UE testing would also involve testing of the algorithm decision-making reliability for determination of UE-to-base station distance feasibility for this technique. The above assumes a real-time query from the UE to a base station location database when the UE receives a WEA alert.

If the onboard UE database were to be pursued, testing of both the UE and the network base station databases would need to be done. The onboard UE database method would likely lead to more complexity in both UE and network development and testing due to the potential need for onboard UE database updates at some time-based, location-based, and roaming status-based intervals.

5.5 Mitigation Technique #5 – Not accepting WEA during cell reselection

5.5.1 Introduction

In this mitigation technique the UE does not accept WEAs during a cell reselection procedure.

5.5.2 Details, Requirements, & Architecture

Clause 4.6.4 of TS 22.268 [Ref 3] contains a requirement that UEs shall, subject to regional or national regulations, be capable of receiving and displaying PWS messages in limited service state. In the technique it is assumed that this requirement applies when a UE has no USIM or is in limited service state because there is no allowed PLMN available to attach to and that this requirement does not apply when a UE is going through a procedure of reselecting a cell. The referenced TS 22.268 [Ref 3] requirement does not apply in the United States.

Cell reselection occurs when a UE is losing its connectivity with a cell it has registered on. Measurements data of neighboring cells may make the UE decide to reselect a neighbor cell to camp on. However, as long as the UE remains in Radio Resource Control (RRC)_IDLE mode it won't register on the cell and will merely camp on this cell (unless it selected a cell in a different Tracking Area, or it needs to go to RRC_CONNECTED mode). This state is effectively a limited service state and makes the UE vulnerable to receiving WEA messages from any neighbor cell, including cells from a false base station.

The mitigation technique relies on the ability of a UE to be aware that it has just left a cell it was registered on and shall therefore not be susceptible to receiving WEA messages. The UE shall resume receiving WEA messages after it has registered on a cell.

5.5.3 Evaluation

When the UE is in the process of cell reselection it will not receive any WEA messages, but that also excludes genuine WEA messages. As long as the UE remains in idle mode and does not register on a reselected cell; it will merely camp on it and this may not be limited to a very short period of time. The UE will not receive WEA messages until it registers with a network provider on a new cell.

5.5.4 Testability

No network node testing is required for this mitigation technique. Only devices would need to be tested with this technique to see if they adhere to the requirement that WEA alerts are not to be presented to users when the UEs are in the state of cell reselection.

5.6 Mitigation Technique #6 – Detecting false base stations

5.6.1 Introduction

In a cybersecure system, protection is generally the first line of defense. Nevertheless, protection is necessary but not sufficient. It is so because attack and protection are like arms race, meaning that attackers constantly try to bypass existing protection mechanisms.

Therefore, detection has become an essential part in today's cybersecurity. Irrespective or in addition to the protection mechanisms described in this document that might eventually be adopted, it is highly important that there exists also a detection mechanism.

In that light, the kind of detection mechanism that is relevant to WEA security is the detection of false base stations, which are the root cause of the problem.

5.6.2 Details, Requirements, & Architecture

This mitigation technique proposes to use a network-based false base station framework as described in Annex E of 3GPP TS 33.501 (3GPP 5G security standard). The framework is very general, the basic idea being to (re)use the measurement reports sent by mobile phones to the network for detecting false base stations. Those measurement reports are already sent by mobile phones to the network for purposes like handover and self-organizing networks. The framework enables the new security use case of false base station detection by using existing data in the network.

In a 4G/LTE network, the network can configure UEs by sending measurement configuration in RRC messages, called reconfiguration and resume, for measurements in RRC_CONNECTED state. If the UEs are capable of doing logged measurements, the network can also configure those UEs to collect logs even during RRC_IDLE state by sending an RRC message called logged measurement configuration. If the network wants to collect non-usual reports, it can do while having least effect on UEs in terms of service interruption or power consumption by distributing the measurement load among various UEs. Figure 1 shows the corresponding procedures.

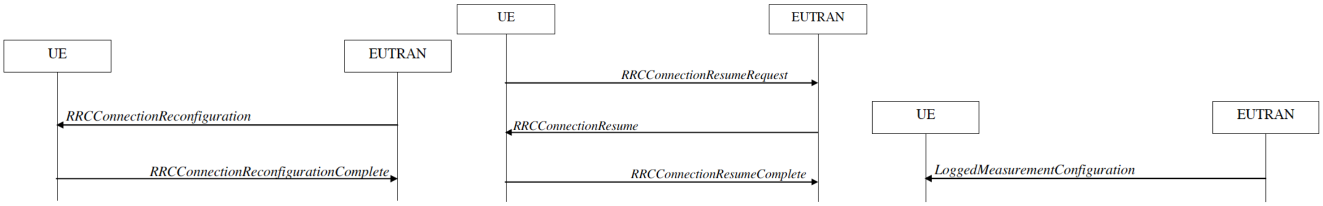

UE
EUTRAN
RRCConnectionReconfiguration
RRCConnectionReconfigurationComplete
UE
EUTRAN
RRCConnectionResumeRequest
RRCConnectionResume
RRCConnectionResumeComplete
UE
EUTRAN
LoggedMeasurementConfiguration

Figure 1 – Measurement configuration in a 4G/LTE network

The UEs measure accordingly and send a report to the network in an RRC message called measurement report. The network can fetch logged measurements using an RRC UE information procedure. Figure 2 shows the corresponding procedures.

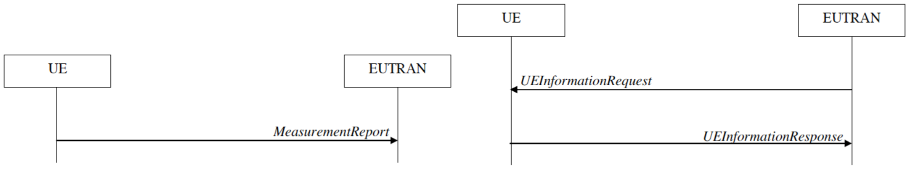


Figure 2 – Measurement reporting in a 4G/LTE network

The detection logic can make use of data points like PCI, RSRP, RSRQ, CGI (including MCC, MNC) and so on to detect false base stations, e.g., phased out RATs (e.g., phased out 2G/GSM networks), unexpected cell IDs, unfeasible location continuity, jump of authentication regions, irregular signaling loads, etc.

5.6.3 Evaluation

The detection of false base stations offers a general defense tool against WEA attacks.

It is also pertinent to observe that a 4G/LTE network can use this mechanism to collect measurements on intra 4G/LTE frequency, inter 4G/LTE frequency, inter RAN 5G/NR, 3G/UTRA, 2G/GERAN, and WLAN frequencies among others. In other words, 4G/LTE network can monitor all generations of false base stations from 2G to 5G.

The necessity of a generic detection mechanism becomes more evident when protection mechanisms are evaded, if not by a rookie attacker, by a resourceful attacker.

One example is when an attacker does downgrade attack 2G and evades the protection mechanism. In this case, a detection mechanism would be able to detect this attack simply by detecting a 2G cell or by obtaining CGI reports.

Another example is when an attacker wants to create panic in a Network A by using false WEA messages. The Network A has deployed WEA protections, while some other network has not. A resourceful attacker augments a false base station with a legitimate but ill-intentioned core network in another network and lures UEs. Since UEs cannot tell by themselves whether they are supposed to be in Network A or another network, the UEs will have no means to validate WEA messages coming from another network. Nevertheless, detection mechanism in the Network A will not only detect the presence of the attack in radio network level, but also in core network level.

This solution provides a means of detecting the root cause of attack, so must be coupled with additional mitigation strategies to defend against false WEA attacks.

5.6.4 Testability

The detection efficacy can be tested with normal UEs and normal network, by configuring one of existing cells with non-conformant parameters (PCI, power) or by operating an SDR on the field.

5.7 Mitigation Technique #7 – Digital signatures at the Application Layer

5.7.1 Introduction

3GPP studied various mitigation techniques in Rel-12 (TR 33.969) that relies on the CMSA to sign the PWS messages and identified a number of issues with network-based approaches:

- Legacy networks that are not upgraded cannot support Signed WEA
  - Depending on the mitigation technique, there is impact on RAN as well as core network nodes
  - Consumes additional radio resources – messages for key management and increased message size for signature
- Device impact is also larger (e.g., impacts the cellular network stack and OS/App layers)
- Recovering from any future security (e.g., algorithm) compromise may also require that all CMSP networks are upgraded to recover
- Key management and distribution is also complex

3GPP study concluded that no normative work will be pursued

- Without 3GPP standardization, it is not practical to pursue network-based approaches

With App Layer based approach, impacts on the CMSP as well as lower layers can be minimized

- Once the message is signed, it cannot be changed. Therefore, any necessary encoding of the message needs to be performed before signing
- Mitigation technique can be specified in ATIS specifications with minimum impact to 3GPP specifications

5.7.2 Details, Requirements and Architecture

Referring to Figure 3, WEA Client is preconfigured with one Root Certificate Authority (CA) public key and two Subsidiary CA (WEA CA) public keys:

- Public Key of Root CA – Root CA issues certificates for WEA CA's
  - Optionally used to a) revoke a compromised WEA CA; b) update public key of WEA CA
- Public Key of WEA CA1 (primary CA) and Public Key of WEA CA2 (backup CA)
  - WEA CA2 proposed as a backup in the unlikely event WEA CA1 is compromised – key update requires a long period of time

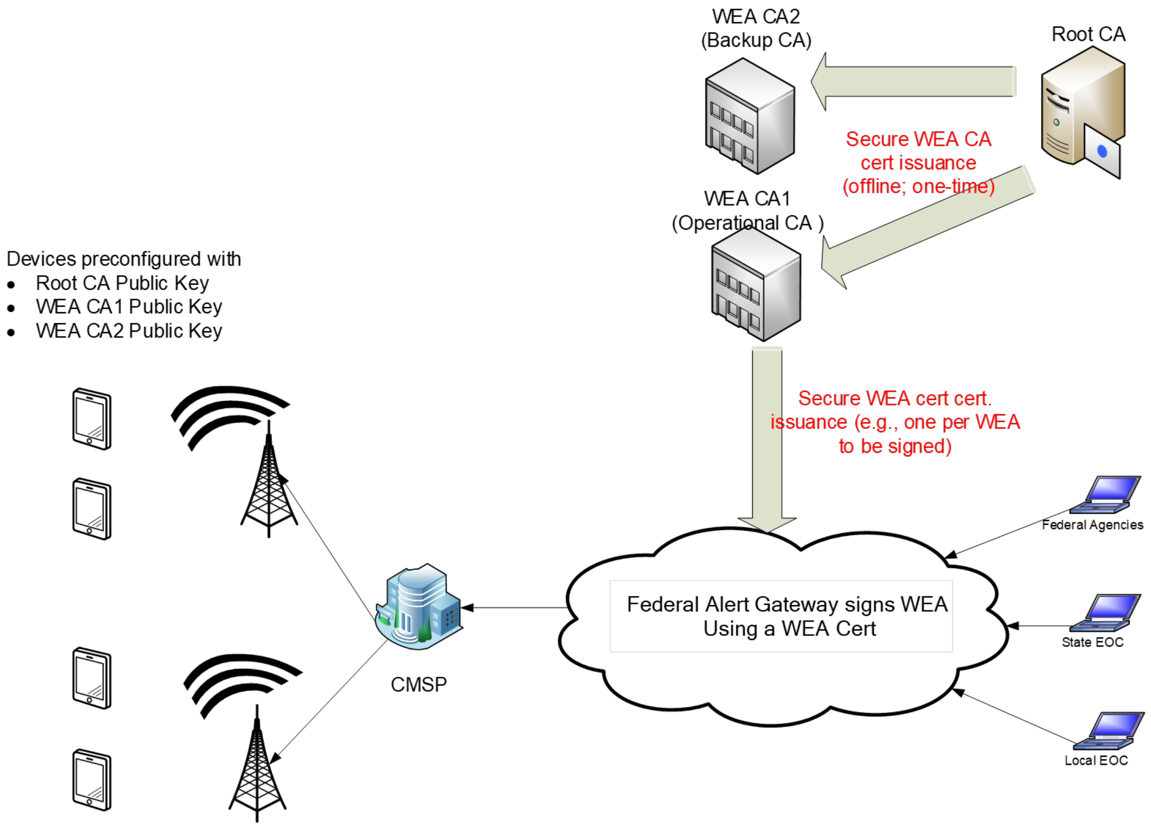

WEA CA2
(Backup CA)
Root CA
Secure WEA CA cert issuance (offline; one-time)
WEA CA1
(Operational CA)
Devices preconfigured with
• Root CA Public Key
• WEA CA1 Public Key
• WEA CA2 Public Key
Secure WEA cert cert. issuance (e.g., one per WEA to be signed)
Federal Agencies
Federal Alert Gateway signs WEA Using a WEA Cert
State EOC
CMSP
Local EOC

Figure 3 – Architecture of the Digital signatures at the Application Layer

Federal Alert Gateway (FEMA/IPAWS) obtains WEA Certificate (WEA Cert) from operational WEA CA

- WEA Cert is used by the Federal Alert gateway to sign the WEA messages
- WEA CA's may be operated by FEMA/IPAWS or a trusted 3rd party

Federal Alert Gateway signs the WEA message using the private key of the WEA Cert and distributes the Signed WEA (which includes WEA Cert) to the CBEs of CMSA using existing C refence point

- Signed WEA includes, the message, signature and the WEA Cert used to sign the message
- The format for Signed WEA is FFS (e.g., whether to use existing message format or define a new message format)

Using the Public Key of WEA Cert, WEA Client verifies the signature on the Signed WEA

- If the verification is successful, then presented to the user
- It is FFS what the device does when signature verification fails
  - ignores WEA or
  - present to the user with a warning indicating that the authenticity of the WEA is suspect

As mentioned earlier, WEA Client is preconfigured with the necessary public key(s) of the CA

- Authorized public keys of the root CA, WEA CA1 and WEA CA2 may be published by the Federal Alert Gateway (e.g., on a website)
- Device OEMs include it in their WEA client implementation
  - e.g. at device manufacturing time

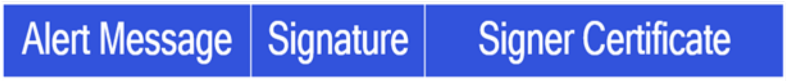
The preconfigured public key of CA1 or CA2 may be updated after device is manufactured using the WEA Handset Action Message (WHAM) Signed WEA message

- WHAM message is signed using the Root CA public key and is broadcast to the device
- May be used to revoke an existing WEA CA public key at the device and/or to configure the WEA client with a new WEA CA public key
- Root CA public key is not updatable
- It is FFS whether WEA CA revocation and updating is one or two operations

5.7.3 Evaluation

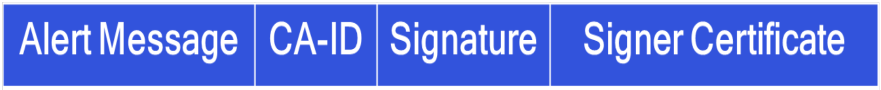
There are several possible signed WEA formats. CA-ID is 8-bits and identifies the CA that issues the WEA Cert and signature algorithm used (e.g., 6 bits for CA identifier and 2 bits for signature algorithms). Nonce is a 32-bit time stamp value (e.g., in seconds from epoch).

Option 1: one CA; one signature algorithm; no replay protection. Note: either replay protection is not needed or WEA client relies other ways to provide some form of replay protection (e.g., other fields within the Alert to identify replayed messages).



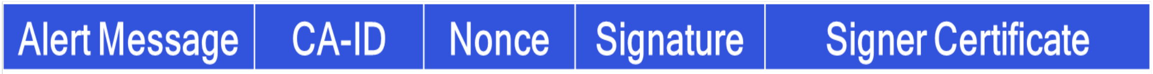
Alert Message	Signature	Signer Certificate

Option 2: Multiple CA and Signature algorithms; no replay protection. This option is analyzed assuming that a) CA and signature algorithm agility is needed to recover from potential future compromise of CA / signature algorithms; b) replay protection is not needed.



Alert Message	CA-ID	Signature	Signer Certificate

Option 3: Multiple CA and Signature algorithm; Nonce (e.g., timestamp) for replay.



Alert Message	CA-ID	Nonce	Signature	Signer Certificate

Assuming 128-bit level of security:

- Many choices available but space used for security shall be as small as possible (to allow for as much space as possible for the actual Alert message)

- Choices for Digital Signature Algorithms (DSA) (c.f. 3GPP TR 33.969)
  - DSA (Finite Field Crypto based) or ECDSA (Elliptic Curve Crypto based)
  - Signature Size = 512-bits (64 bytes)

- ECDSA is proposed as the signature algorithm
  - ECC is considered faster and public keys are smaller compared to DSA

Assuming Option 2 and Implicit Certificates, total security overhead of Signed WEA:

- CA-ID is 8 bits. 6 bits for Federal Alert Gateway CA identifier and 2 bits for signature algorithm
- Signature is 512 bits
- Size of Implicit Certificate is 257 bits
- Total Size required for security is at least 777 bits (~98 bytes)
  - Disclaimer: This is a preliminary estimate which may change based on further analysis
- If this is not possible, we may further study the potential to accept reduced level of security (e.g., 112-bit level security instead of 128-bit thus saving few bytes)
- If replay protection is needed, 4 bytes nonce is needed (~102 bytes)

5.7.4 Testability

During the device certification phase, some carriers verify WEA implementation for every single device type including relevant 3GPP specs, ATIS standards, and carrier specific requirement. This is performed for all WEA types via either captive lab network or a simulator platform (e.g., Rohde & Schwarz, KeySight, etc.). Some carriers will also test WEA on live network using Exercise and CMPS defined alerts.

If the signing is done outside a carrier’s network, it may require additional complexity to perform this test.

6 Impacts

This section addresses the following aspects with a series of tables to allow for a simpler comparison among all mitigation techniques:

- Stakeholder Development Impacts
- Alert Presentation/Mobile User Impacts
- Standards Impacts (3GPP and ATIS)

Table entries include notes when needed for more detailed explanation.

6.1 Stakeholder Development Impacts

The table below indicates which stakeholders will need to engage in development in order to move this technique into the field. Development time may vary, and would be followed by testing, integration testing, and end-to-end testing. Development would not begin until completion of any related ATIS and 3GPP specifications.

Any technique requiring mobile device updates will depend on market penetration time following completion of development and testing.

	MT1 Digital signatures w/NAS based	MT2 Accepting WEA alerts only from	MT3 LTE eNodeB fingerprinting	MT4 LTE eNodeB location verification	MT5 Not accepting WEA during cell reselection	MT6 Detecting false base stations	MT7 App Layer Digital signatures

	key distribution	authenticated networks					
Federal Alert Gateway							✓[1]
CMSP Gateway	✓			✓		✓	✓[1]
Mobile Device	✓	✓	✓	✓	✓		✓

Table 1 Stakeholder Development Impacts

Note 1: Depends on the location of Certification Agent

6.2 Alert Presentation/Mobile User Impacts

Impacts can range from minor to significant and are somewhat subjective as to where they lie in that range. As an example, an increased latency of a few seconds may not be seen as significant for a thunderstorm warning but would be very significant in the case of an Earthquake Early Warning System (EEWS) alert.

If any category of mobile device is able to process and present alerts under a particular field scenario now, but would be unable to do the same following the deployment of any of the mitigation techniques described in this report, this impact is addressed here. If no impact is indicated in the table for a given mobile device category, the mobile device's ability, or lack thereof, to process any given alert today will not change with the deployment of that mitigation technique.

In the table below:

1) Additional latency may be introduced.
2) Legacy (non-upgradable) mobiles show a check under a given mitigation technique if that technique will impact the current ability of that device to receive, process or present an alert.
3) Roaming devices show a check under a given mitigation technique if that technique will impact the current ability of that device to receive, process or present an alert.
4) NSI devices show a check under a given mitigation technique if that technique will impact the current ability of that device to receive, process or present an alert.

	MT1 Digital signatures w/NAS based key distribution	MT2 Accepting WEA alerts only from authenticated networks	MT3 LTE eNodeB fingerprinting	MT4 LTE eNodeB location verification	MT5 Not accepting WEA during cell reselection	MT6 Detecting false base stations	MT7 App Layer Digital signatures
Latency (range)	✓[1]			✓[2]	✓[3]		✓[1]
Legacy Mobiles							
Roamers							
NSI	✓[4]						

Table 2 Alert Presentation/Mobile User Impacts

Note 1: There will be additional transmission delay due to the additional information bits, as well as processing delay due to the decryption process. The exact values are unknown.

Note 2: Latency may be introduced due to the query from the UE to the base station location database.

Note 3: Latency equal to the length of the cell selection period will be introduced. This may not be limited to a brief period of time.

Note 4: NSI devices that support this mitigation technique would not receive the digitally signed messages unless the device preconfigured key is still valid.

6.3 Standards Specification Impacts (3GPP and ATIS)

The check marks in this table indicate the standards groups with responsibility for one or more specifications that will require modifications to support the mitigation technique.

Even with the identification of specifications that would be impacted, timelines would be difficult to establish with any certainty. Some standards groups have dependencies on other groups. An example of this would be a 3GPP WG which deals with the information carried by signaling which depends on another 3GPP WG to specify the signaling or container within with that information is carried.

	MT1 Digital signatures w/NAS based key distribution	MT2 Accepting WEA alerts only from authenticated networks	MT3 LTE eNodeB fingerprinting	MT4 LTE eNodeB location verification	MT5 Not accepting WEA during cell reselection	MT6 Detecting false base stations	MT7 App Layer Digital signatures
ATIS	✓	✓	✓	✓	✓		✓
3GPP					✓		✓

Table 3 Standards Specification Impacts

7 Evaluation of Mitigation Techniques

7.1 Gating Evaluation Criteria

The first step following the analysis of the mitigation techniques is to narrow the list of mitigation techniques. For this reason, the following criteria have been applied:

1) The degree to which the mitigation technique fully addresses the False Base Station Attack exploit
2) The degree of vulnerability of the mitigation technique to be circumvented
3) The degree of risk of adverse impacts or other unintended consequences to users and/or the WEA service overall
4) Complexity of the mitigation technique
5) Standards Impacts, including SDO(s) impacts and estimated standardization timelines
6) Deployment Considerations, including Testability

The first three criteria are considered the most critical, and were the basis for the removal of the following mitigation techniques from further evaluation:

1) MT2: Accepting WEA Alert only from Authenticated Networks
2) MT3: LTE eNodeB fingerprinting
3) MT4: LTE eNodeB location verification
4) MT5: Not Accepting WEA During Cell Reselection
5) MT6: Detecting False Base Stations

All critical inputs to the UE's decision-making process for techniques MT2, MT3, and MT4 can be generated by a false base station and therefore spoofed by that same false base station. MT5 carries the risk of unacceptable latency of alert presentation for imminent danger alerts. MT6 is not sufficient to fully address the original problem, as it detects the root cause of attacks, specifically the false base station, but does not directly mitigate the attack.

7.2 User Protection Techniques Not Addressed

During the evaluation of the mitigation techniques, it became apparent that there are scenarios in which there exists the possibility of having authentic WEAs not presented by UEs. To minimize this possibility, proposals such as establishing a grace period to ensure all network elements for all carriers could be updated, or the possibility of having the WEA presented with an indication that the WEA might not be authentic. Each of these proposals would reduce the perceived benefits of any deployed mitigation technique. Any WEA presented with an indication that the WEA might not be authentic also carries a strong possibility of lowering consumer and Alert Originator confidence in the WEA system.

For these reasons, the analysis and evaluation of the mitigation techniques does not include these proposals. It should be noted that this exclusion of a grace period or an indication to the user that a WEA might not be authentic increases the possibility of having authentic alerts received by the UE but not presented.

8 Results of Analysis

8.1 Summary of Mitigation Technique Evaluation

Following the application of the evaluation criteria and other methods described in clause 7, the mitigation techniques remaining are:

MT1: Digital signatures w/NAS based key distribution

MT7: Application Layer Digital signatures

Although these mitigation techniques are different, they share a common underlying approach of digitally signing the alert. The analysis of the best location for signing (Federal Alert Gateway, CMSP Gateway, or CBC) and the CA is for further study, as each option has advantages and disadvantages.

In this section we will discuss the fundamental digital signature approach and its potential impact on the existing WEA (i.e., WEA 3.0 and prior).

As indicated in the analysis of MT1 and MT7, there needs to be a method by which various keys are updated. Although there are well-known techniques to do so, they will all add complexity to the existing WEA system which could negatively impact the delivery of life saving WEA messages. Both 3GPP and ATIS standards will be needed to pursue any digital signature technique.

WEA 3.0 supports an extended message length of 360 characters, two languages, and the sending of alert area coordinates. The addition of a digital signature will further increase the size of SIB12 content. The SIB is a critical operational element of 4G and 5G, and it was originally intended for system operation and not for large amounts of user data. In addition, there is a danger that there will be a substantial delay in receiving all the SIB12 segments by the device, which will delay the presentation of WEA to the user. Additional delay could also be incurred if any of the keys need to be updated. Finally, there is a delay due to processing of digital signatures that could also impact the device's battery life. The bottom line is that digital signature will add complexity, delay, and adversely impact the device's battery life. The precise impact cannot be evaluated at this time until the mitigation techniques are studied in much greater details.

Potential roaming exploits may exist with MT1 and MT7. This is for further study.

9 Conclusions

Clause 8 in this report conveys the final evaluation of the mitigation techniques following the evaluation exercise. The intent of this clause is to take a more holistic look at the problem statement, the expectations, and realities in the field.

9.1 Closer Look at the Exploit

The University of Colorado paper details a particular scenario of a crowded outdoor venue (Clause 5.4), claiming 90% effectiveness of the False Base Station Attack. However, the University of Colorado's hypothetical illustration (Fig. 17 in Ref 1) of the attack describes a venue with a single carrier's base station and four rogue base stations. The reality of deployments in this type of venue would likely be quite different.

Venues that are able to attract and accommodate the size crowd needed to provide the context for an effective attack of this type are considered flagship venues. This means that potential deployments would provide for high-capacity service for all attendees to the best of the carrier's ability. These potential deployments, at a minimum, would configure a number of cell sites, including temporary capacity enhancements using "Cell on Wheels/Wings/Trucks" (COWS/COLTS) throughout the venue to provide low latency and high capacity. The number of authentic base stations vying for the UEs would significantly reduce the ability of false base stations to attract UEs. The rogue base stations would likely also need to spoof at least three top-tier carriers, not just a single carrier, as indicated in the University of Colorado's hypothetical illustration, in order to attempt an attack on the full capacity of the stadium.

Given that this attack specifically focuses on UEs in the idle state, the number of vulnerable mobiles for which the rogue base stations could exploit would be significantly reduced due to the large percentage of UEs that would be in a connected state for voice calls or video streaming, or regularly transitioning to a connected state for data exchanges (inbound and outbound) for every email, social media interaction, background apps, and texting exchange throughout the event.

Another critical factor to consider is the user's behavior upon receiving an imminent threat alert. Alert Originators stress that social scientists report that users will attempt to validate an alert before taking action; that is, users check the validity through multiple sources. As an example, the Missile Alert Test exercise performed on January 13th, 2018 in Hawaii [reference] did not result in the level of panic possible for this critical alert because users are "programmed" to expect to be able to confirm this type of information even while they may be also planning their plan of action. In Hawaii, the absence of air-raid sirens called into question the validity of the alert. In a crowded venue, such as the Super Bowl, announcements would confirm the alert as well as conveying information for a safe, but speedy exit from the premises, and sirens would sound off in the area. In addition, almost all users engage in some form of social media and would be checking for confirmation from these and other sources, including family members, friends, public safety and news social media feeds, and even those sitting near them in the venue.

In summary, the deployed cellular configurations and user behavior in flagship venues would substantially reduce the percentage of mobile devices that could be affected by this type of attack. End users will question the validity of an alert with the lack of confirmation of the imminent threat by any other means, decreasing the success of the exploit.

These factors alone comprise effective mitigation of the risk, **without the addition of possible negative impacts to users**.

9.2 Impacts to Users

As seen in the clause above, flagship venue deployment, as well as user behavior limit the effectiveness of this exploit, meaning that the number of users that might benefit by the deployment of a mitigation technique is substantially lower than the estimate put forth in the University of Colorado paper [Ref 1]. In this clause, we look at the possible impacts to users from the deployment of a mitigation technique.

Additional delay will be introduced for WEA. This may produce significant consequences for WEA with critical timing needs, such tornado warnings from the National Weather Service (NWS) or the earthquake early warnings from the United States Geological Survey (USGS).

Throughout the evaluation of the mitigation techniques, concerns were expressed about the possibility of having authentic alerts not being presented to the user because security information that is expected by the UE in order to validate the WEA is not received. Depending on the specific mitigation technique in question, this could occur because a network element has not been fully upgraded to provide the needed security information.

9.3 Recommendation

Based on the analysis of the threat from a rogue actor, the consensus is that the False Base Station Attack theorized by the University of Colorado study does not constitute grounds for taking the risks of delays or non-presentation of authentic WEAs posed to users by the deployment of a mitigation technique.

In conclusion, to preserve the integrity of WEA and maintain user confidence in WEA, no mitigation technique should be deployed due to the risk the loss of conveying important information in a timely manner to users for a known imminent threat to life or property in return for attempting to address a potential risk that carries an uncertain chance of success.