You have been warned: Abusing 5G's Warning and Emergency Systems

Evangelos Bitsikas and Christina Pöpper

Annual Computer Security Applications Conference (ACSAC) 2022, Austin TX, USA
Introduction

Mobile voice communication
Efficient voice to reach billions
Focus shifts to mobile data
Mobile broadband and emerging expansion
Unified connectivity fabric for the next decade

1980s
Analog voice AMPS, NMT, TACS

1990s
Digital voice D-AMPS, GSM, IS-95 (CDMA)

2000s
Mobile data WCDMA/HSPA+, CDMA2000/EV-DO

2010s
Mobile broadband LTE, LTE Advanced, Gigabit LTE

Wireless Edge
5G New Radio (NR)

https://www.qualcomm.com/news/onq/2019/09/5g-launches-globally-what-comes-next
Public Warning System (PWS)

Earthquake and tsunami warning

this is a ETWS test message

STEP 01
Government releases Public Warning Cell Broadcast Message

STEP 02
Alert goes to a Cell Broadcast Entity (CBE)
CBE authenticates originator's credentials and forwards to carriers

STEP 03
Call carrier receives alert at their respective Cell Broadcast Center (CBC) and routes alert to appropriate cell towers

STEP 04
Cell phones within CBC reception area receive alert

Malicious interference with PWS may aim at:
- Criminal activities
- Fraud
- Political goals
- Terrorism
→ Risk of disasters and human life loss
The Current State

Ballistic missile warning sent in error by Hawaii authorities

By Jolyn Rosa

Mistaken Pickering, Ont. nuclear alert sparked panic, emails show

[a] Lee et al.: This is Your President Speaking: Spoofing Alerts in 4G LTE Networks. MobiSys 2019
Network Structure

Core Network
CBCF = Cell Broadcast Center Function
CBC = Cell Broadcast Center
PWS-IWF = Public Warning System Interworking Function
AMF = Access and Mobility Management Function

External Entities
CBE = Cell Broadcast Entity
NG-RAN = Radio Access Network
UE = User Equipment
Emergency System

You have been warned: Abusing 5G's Warning and Emergency Systems
Evangelos Bitsikas and Christina Pöpper
Annual Computer Security Applications Conference (ACSAC) 2022, Austin TX, USA

1. Emergency Broadcast Request
2. NonUEN2MessageTransfer (Write-Replace-Warning Request NG-RAN)
3. NonUEN2MessageTransfer (Write-Replace-Warning Confirm NG-RAN)
4. Emergency Broadcast Response
5. Write-Replace-Warning Request
6. Write-Replace-Warning Response
7. User Alerting
6. Cell Broadcast Delivery
8. NonUEN2InfoNotify (Write-Replace-Warning Indication NG-RAN)
9. Record successful and failed message deliveries in trace record
Paging Procedure

You have been warned: Abusing 5G’s Warning and Emergency Systems
Evangelos Bitsikas and Christina Pöpper
Annual Computer Security Applications Conference (ACSAC) 2022, Austin TX, USA

SIB6 -> Earthquake and Tsunami Warning System (ETWS) Primary
SIB7 -> Earthquake and Tsunami Warning System (ETWS) Secondary
SIB8 -> Commercial Mobile Alert System (CMAS)

RRC idle/inactive

RRC active

Broadcast Transmissions

SIB 6,7,8

Released Connection

Paging with P-RNTI

DRX Cycle

Paging Occasion

DRX Cycle

Paging Occasion

Paging with P-RNTI

SIB 6,7,8

UE

gNodeB

A Ka

Control and User-Plane Connection

SI Modification Period

Paging Occasion

SI Modification Period

Paging Occasion

Paging with P-RNTI

SIB 6,7,8

UE

gNodeB
Motivation & Contributions

WHY?

- We found unresolved and unaddressed flaws in Emergency/Alerting System
- Flaws and attacks were only investigated for 4G

So, we:

- Determine the main reasons why the Emergency System has vulnerabilities and investigate its security posture in 5G Standalone ecosystem
- Carry out the attacks using commercial software (Amarisoft) with various configurations
  - Prior work evaluated attacks using open-source software (e.g., srsLTE/srsRAN)
- Delve into different attack variations of warning spoofing and suppression
- Explore potential countermeasures
Security Flaws

Directly associated:
1. Insecure broadcast messages (SIB 6,7,8)
2. Inconsistent storing of MIB messages
3. Unprotected paging messages
4. Lack of acknowledgements/verifications used in warning system

Indirectly associated:
1. Insecure broadcast messages (SIB 1,2,..)
2. Unverified measurements\(^{[b]}\)
3. Unprotected Signal Radio Bearer (SRB) messages in RRC

\(^{[b]}\) Bitsikas, Pöpper: Don’t hand it over: Vulnerabilities of the handover procedure of cellular telecommunications. ACSAC 2021
Attacks without MitM

Suppression: \( D_{supp} (Attach) \approx D_{spoof} (Attach) + t_{rec,supi} + t_{rach,ran} \)
MitM-based Attacks

You have been warned: Abusing 5G’s Warning and Emergency Systems
Evangelos Bitsikas and Christina Pöpper
Annual Computer Security Applications Conference (ACSAC) 2022, Austin TX, USA

Suppression: \[ D_{\text{supp}} \ (\text{MitM}) \approx D_{\text{spoof}} \ (\text{MitM}) + t_{\text{rec,upi}} + t_{\text{rach,ran}} \]
You have been warned: Abusing 5G’s Warning and Emergency Systems
Evangelos Bitsikas and Christina Pöpper
Annual Computer Security Applications Conference (ACSAC) 2022, Austin TX, USA

Requirements:
(1) Set cell_barred of MIB to ‘barred’,
(2) intra_freq_reselection of MIB to ‘notAllowed’, and
(3) cell_reserved for operator use of SIB 1 to ‘reserved’.

Suppression: $D_{\text{supp}}(Barr) \approx t_{barr} + t_{\text{rec, supi}} + t_{\text{rach, ran}}$

Signal Strength: $\delta_i \geq 10dB$ (100% success rate)

Limitation: Already active devices may not be affected

Other variation: Overshadowing is also possible[c]

[c] Yang et al.: Hiding in Plain Signal: Physical Signal Overshadowing Attack on LTE, USENIX Security 2019
Impact

You have been warned: Abusing 5G’s Warning and Emergency Systems
Evangelos Bitsikas and Christina Pöpper
Annual Computer Security Applications Conference (ACSAC) 2022, Austin TX, USA

| PWS Attack               | Complexity | Impact | Attack Duration (s) |
|--------------------------|------------|--------|---------------------|
| Spoofing (MitM)          | High       | High   | $D_{spoof}(MitM) \geq 55$ |
| Spoofing (non-MitM)      | Medium     | Low    | $D_{spoof}(Attach) \leq 43$ |
| Suppression by DoS (MitM)| High       | Medium | $D_{supp}(MitM) \geq 58$ |
| Suppression by DoS       | Medium     | Low    | $D_{supp}(Attach) \leq 46$ |
| (non-MitM)               |            |        |                     |
| Suppression by barring   | Low        | High   | $D_{supp}(Barr) \in Q^+$ |

Spoofing time (MitM): $D_{spoof}(MitM) \geq 55$ sec

Spoofing time (Attach): $D_{spoof}(Attach) \approx 40 - 43$ sec

Responsible Vulnerability Disclosure to GSMA (CVD-2022-0054), FCC, FEMA, CISA & ENISA
Countermeasures

You have been warned: Abusing 5G’s Warning and Emergency Systems
Evangelos Bitsikas and Christina Pöpper
Annual Computer Security Applications Conference (ACSAC) 2022, Austin TX, USA

Partial PKI-based countermeasure

Signing warning-based SIB broadcasts to avoid spoofing

Suppression and barring attacks are still possible

Replays are possible within a legitimate time frame, but difficult

Full PKI-based countermeasure

Architectural modifications needed

Client-based countermeasure

Post-Quantum

Full RRC and NAS protection

Monitoring and attack detection
Takeaway Points

- No straightforward solution to fully protect the emergency system
- Spoofing and suppression variations with realistic impact
- We must avoid making next generation of networks equally vulnerable
- We must maintain a reliable system in case of emergency incidents (e.g., severe climate emergencies)

FCC Acts to Strengthen the Security of Nation's Alerting Systems