

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

Evangelos Bitsikas and Christina Pöpper

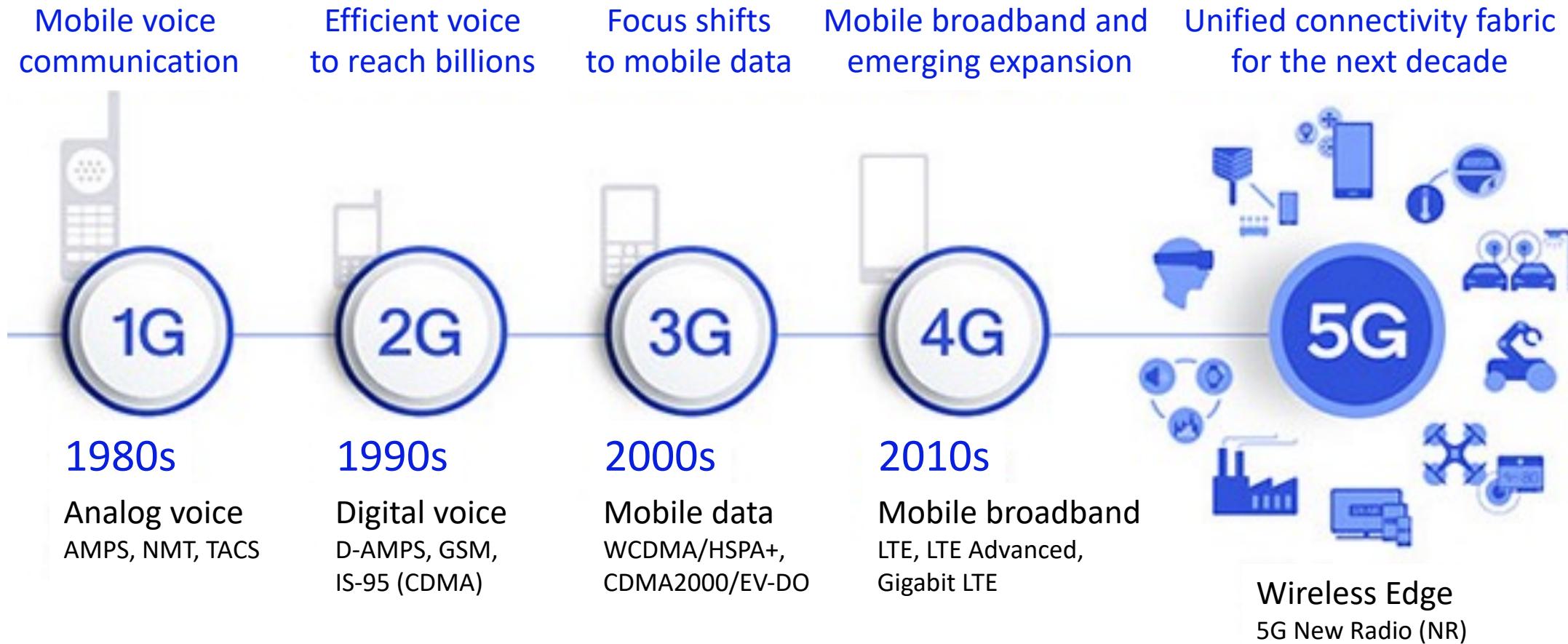
Annual Computer Security Applications Conference (ACSAC) 2022, Austin TX, USA

Introduction

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

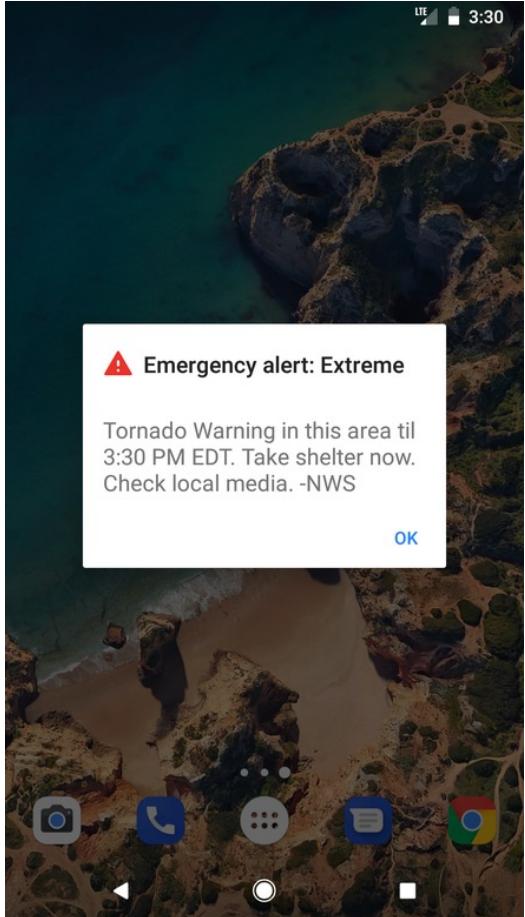


Public Warning System (PWS)

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



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

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

APAC JANUARY 13, 2018 / 1:57 PM / UPDATED 5 YEARS AGO

Ballistic missile warning sent in error by Hawaii authorities

By Jolyn Rosa

5 MIN READ

TORONTO | NEWS

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

MOTHERBOARD
TECH BY VICE

Researchers Demonstrate How U.S. Emergency Alert System Can Be Hijacked and Weaponized

With a pirate cell tower, it's easy to send fake emergency alerts warning of a terrorist attack, nuclear bomb, or other disaster.

Bongbong Marcos: Issuing 'emergency alerts' brings no advantage to me

By CNN Philippines Staff

Published Oct 7, 2021 3:52:54 PM

Latest from this section

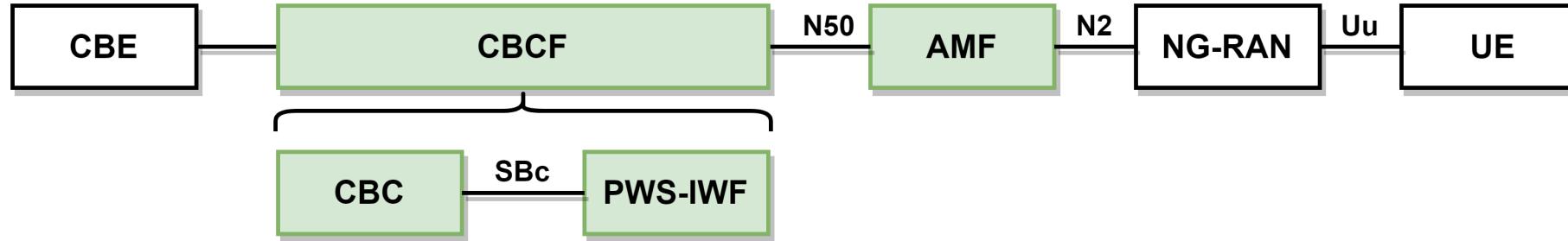
[a] Lee et al.: *This is Your President Speaking: Spoofing Alerts in 4G LTE Networks*. MobiSys 2019

Network Structure

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



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

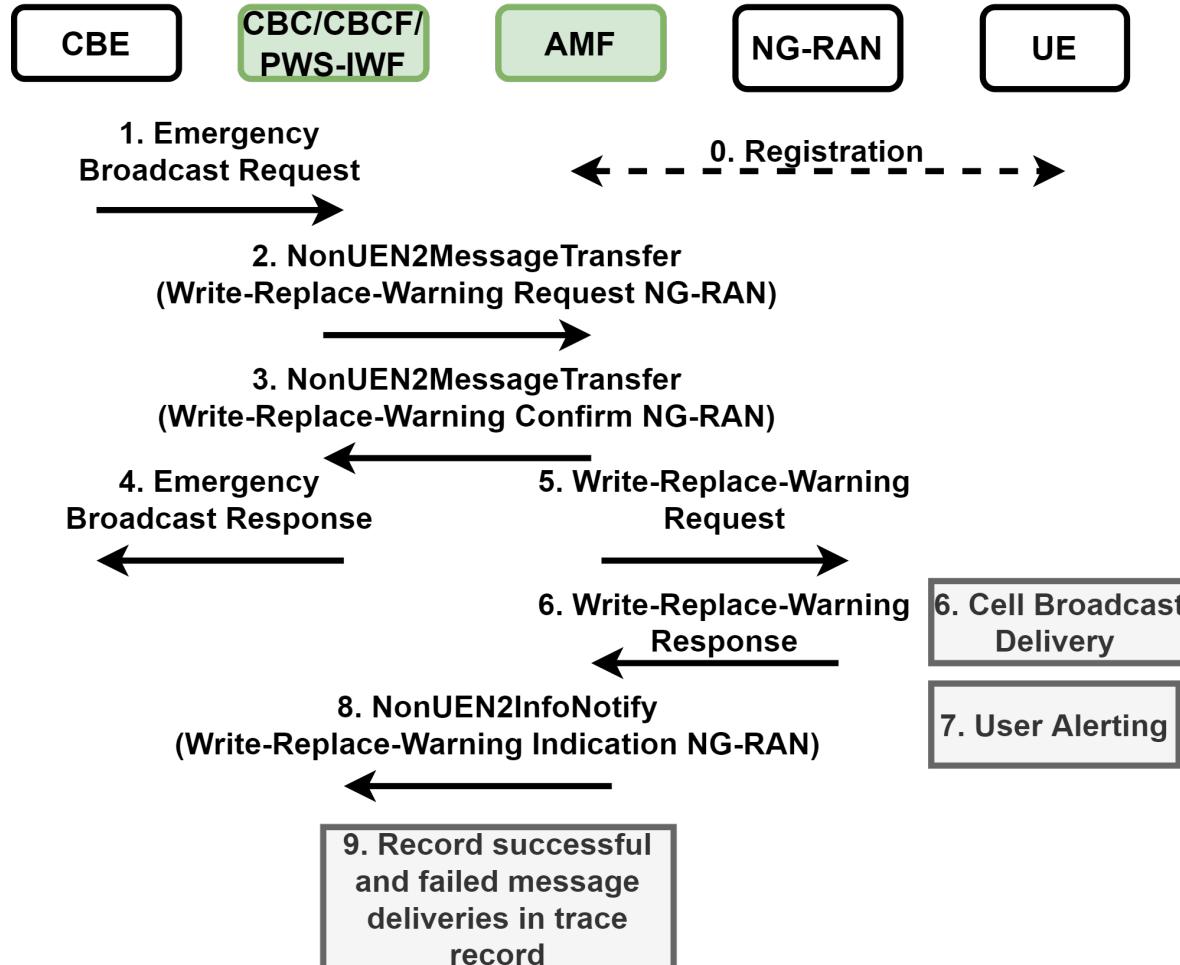
UE = User Equipment

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

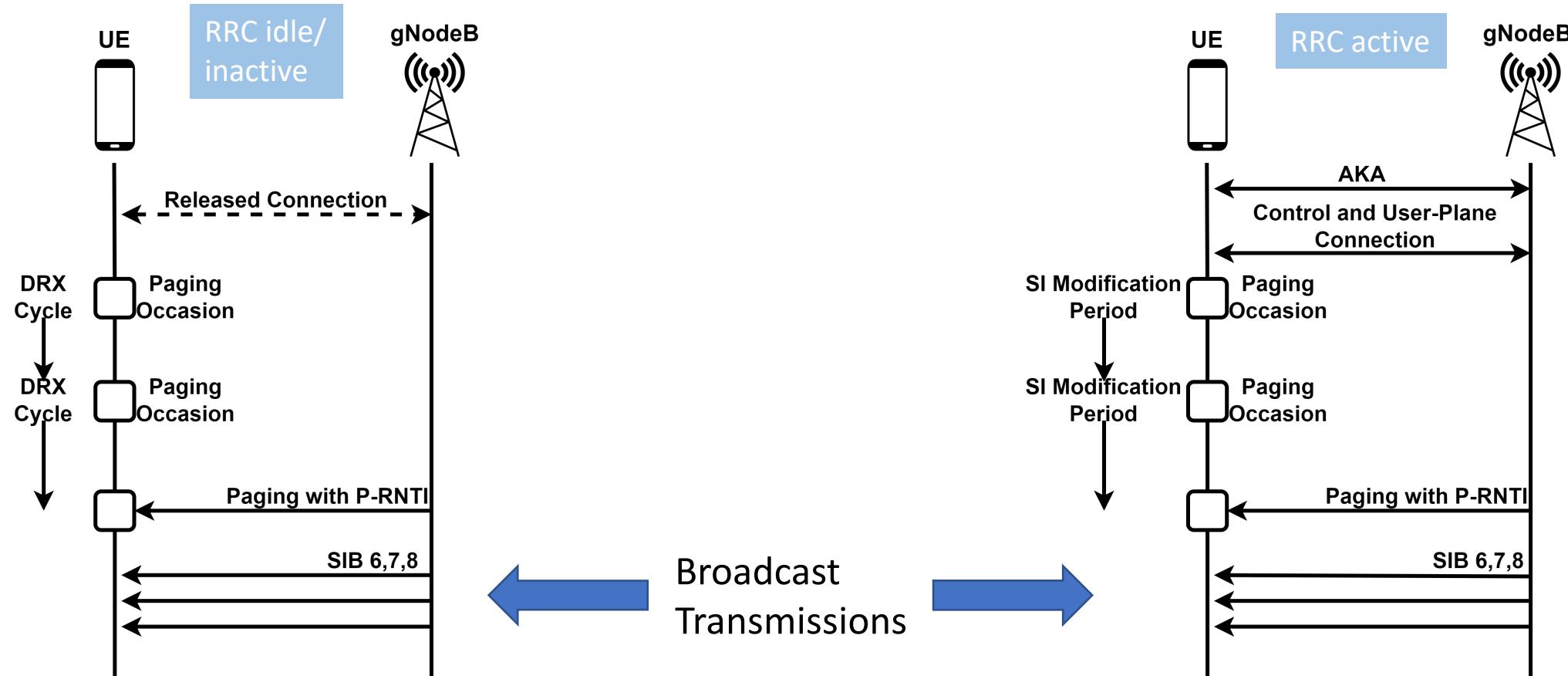


Paging Procedure

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)

Motivation & Contributions

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

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

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

Evangelos Bitsikas and Christina Pöpper

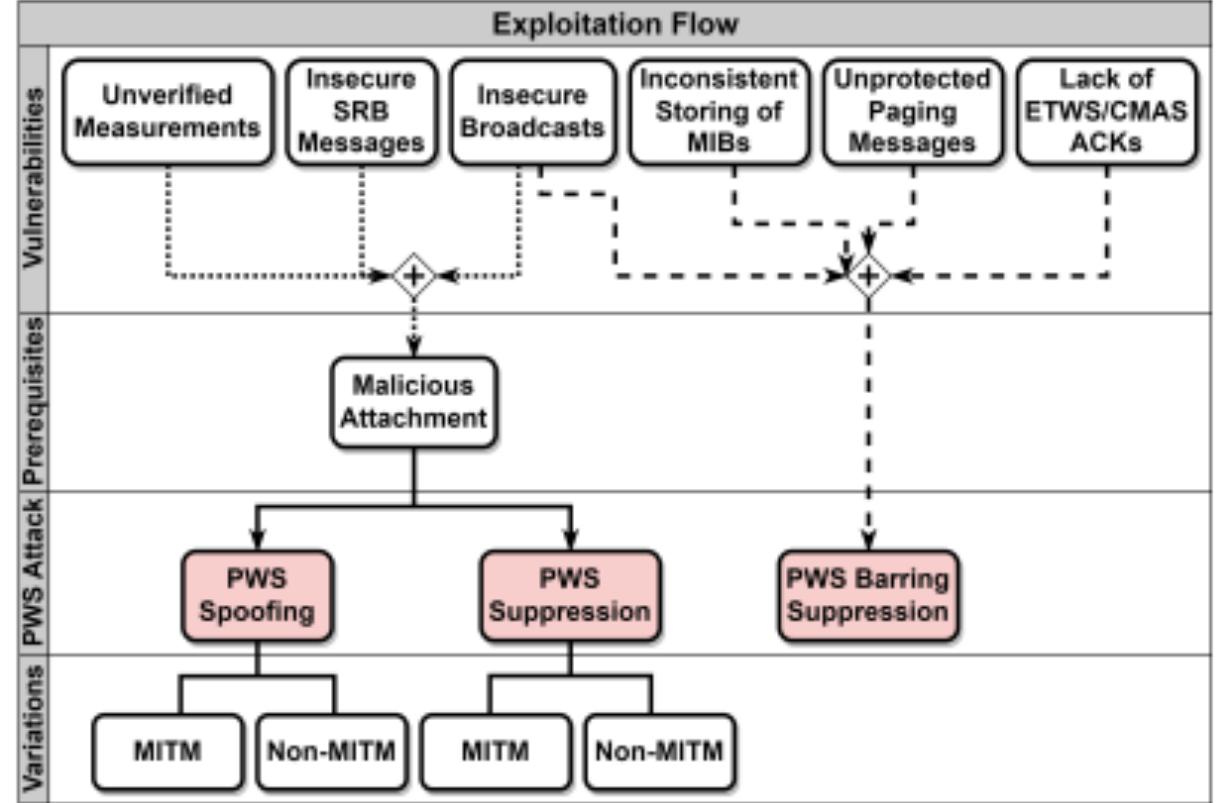
Annual Computer Security Applications Conference (ACSAC) 2022, Austin TX, USA

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.*

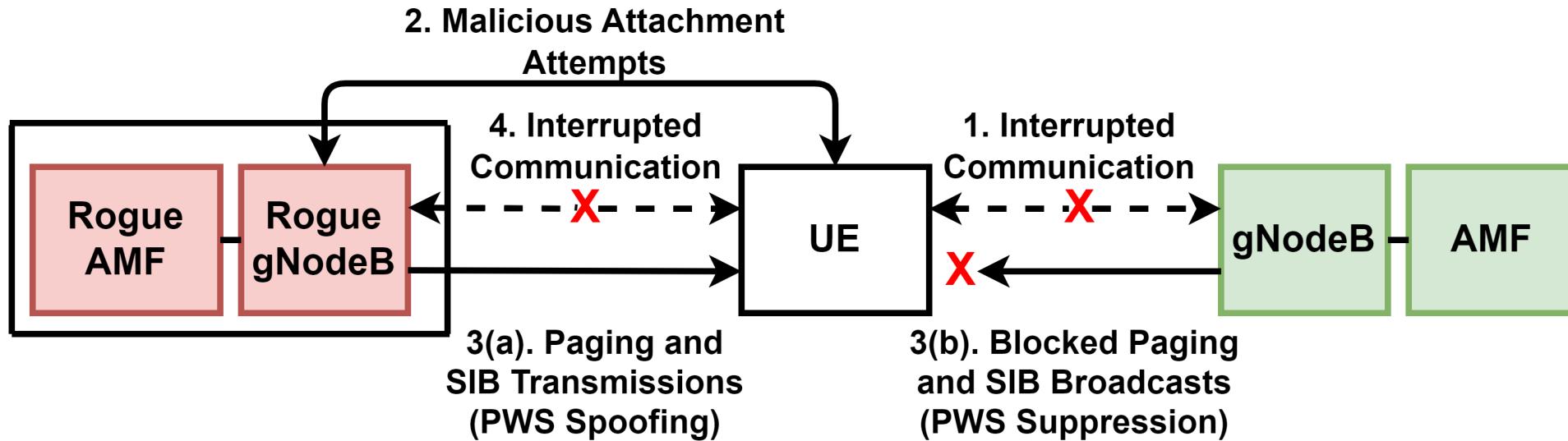
ACSAC 2021

Attacks without MitM

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



Spoofing: $D_{spoof}(\text{Attach})$

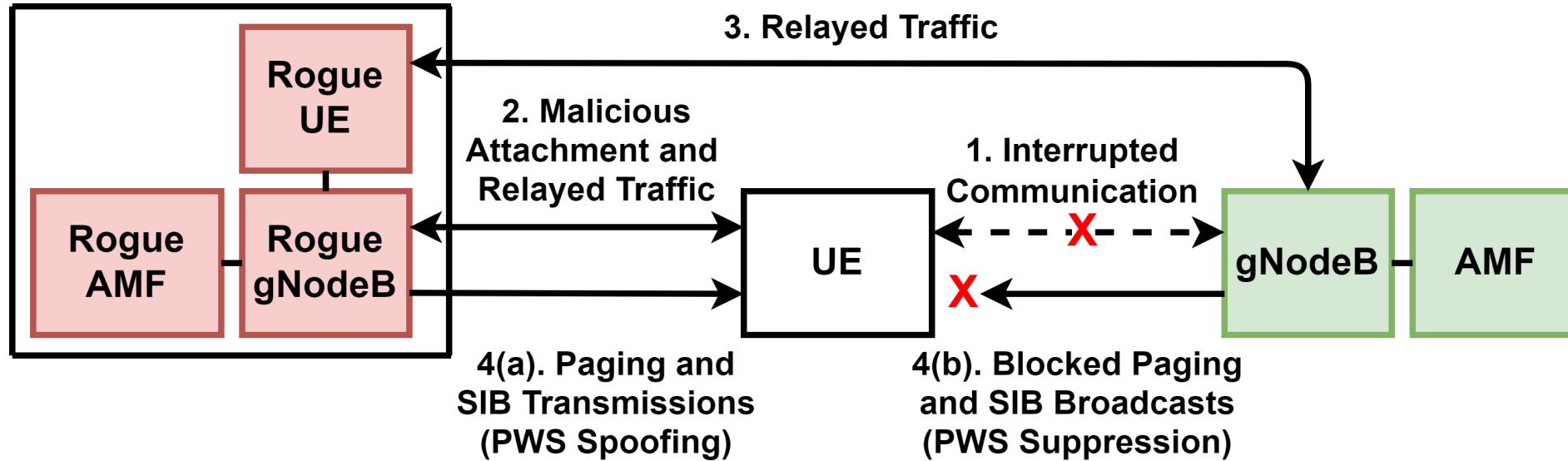
Suppression: $D_{supp}(\text{Attach}) \approx D_{spoof}(\text{Attach}) + t_{rec,supi} + t_{rach,ran}$

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



Spoofing: D_{spoof} (MitM)

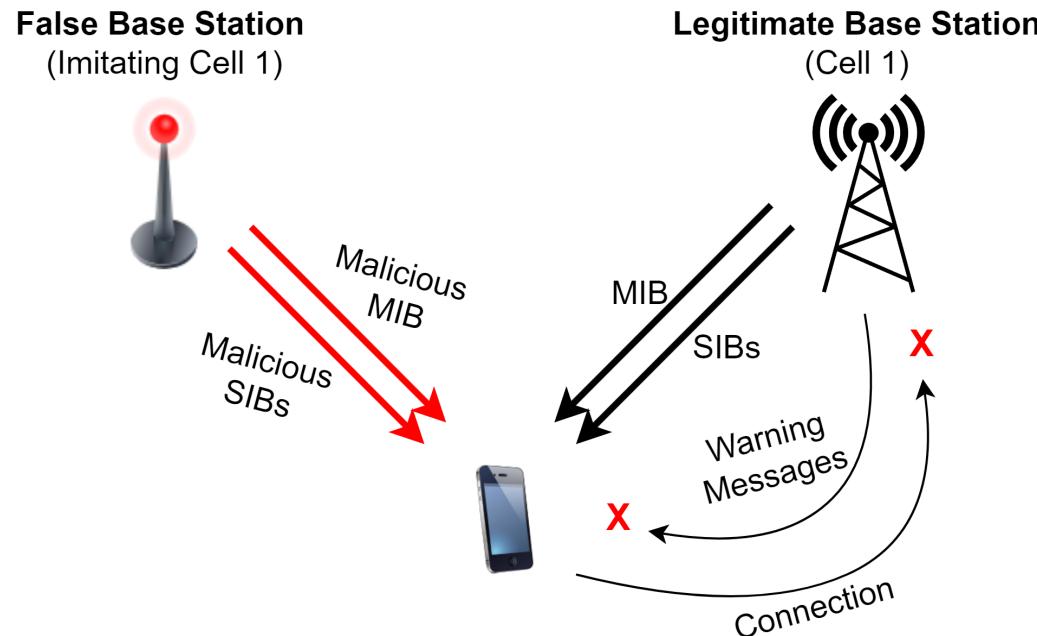
Suppression: D_{supp} (MitM) $\approx D_{spoof}$ (MitM) + $t_{rec,supi}$ + $t_{rach,ran}$

Barring Attack

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

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

Limitation: Already active devices may not be affected

Other variation: Overshadowing is also possible^[c]

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 (non-MitM)	Medium	Low	$D_{supp}(Attach) \leq 46$
Suppression by barring	Low	High	$D_{supp}(Barr) \in \mathbb{Q}^+$

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

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

$D_{spoof}(MitM) > D_{spoof}(Attach)$

$D_{supp}(MitM) > D_{supp}(Attach)$



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 ✗

Architectural modifications needed ✗

Post-Quantum ?

Client-based countermeasure

Full RRC and NAS protection

Monitoring and attack detection

Takeaway Points

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

- 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

Full Title: Amendment of Part 11 of the Commission's Rules Regarding the Emergency Alert System, et al., PS Docket No. 15-94 et al., Notice of Proposed Rulemaking

Document Type(s): Notice of Proposed Rulemaking

Bureau(s): Public Safety and Homeland Security

Description:

FCC launches a rulemaking to improve the security and reliability of the Emergency Alert System (EAS) and Wireless Emergency Alerts (WEA)

DA/FCC #: FCC-22-82

Docket/RM: 15-94, 15-91, 22-329

Document Dates

Released On: Oct 27, 2022

Adopted On: Oct 27, 2022

Issued On: Oct 27, 2022

Tags:

Cybersecurity - Disaster Response - Emergency Alert System - Emergency Communications - Network Reliability - Wireless Emergency Alerts

Thank You!
Questions?

*Evangelos Bitsikas
bitsikas.e@northeastern.edu*

جامعة نيويورك أبوظبي



N Northeastern University
Khoury College of
Computer Sciences