Pre-authentication messages as a common root cause of cell network attacks

Yomna Nasser
@rival_elf
What is an IMSI-catcher?
Feds: There are hostile stingrays in DC, but we don’t know how to find them

There's also “anomalous activity”—probably stingrays—in other US cities, too.
ACLU sues Homeland Security over ‘stingray’ cell phone surveillance

Zack Whittaker  @zackwhittaker  /  8:00 am PST • December 11, 2019

Feds use anti-terror tool to hunt the undocumented

Robert Snell, The Detroit News  Published 10:49 p.m. ET May 18, 2017 | Updated 6:18 p.m. ET May 19, 2017

Detroit — Federal investigators are using a cellphone snooping device designed for counter-terrorism to hunt undocumented immigrants amid President Donald Trump’s immigration crackdown, according to federal court records obtained by The Detroit News.

An unsealed federal search warrant affidavit obtained by The News is the first public acknowledgment that agents are using secret devices that masquerade as a cell tower to find people who entered the U.S. illegally, privacy and civil liberties advocates said.
Terminology

- Base station
- GSM (2G)
- LTE (4G)
- 5G
The original (GSM) IMSI-catcher

BASIC CSS SENDS IDENTITY REQUEST, COLLECTS IMSI, PROCEEDS TO NEXT PHONE

1. ID?
2. IMSI
3. ID?
General attack types (from research)

- Communication interception/Eavesdropping (GSM)
- Location tracking
- Service denial
- Downgrading
Same root cause:
Pre-authentication messages
Spoofing Presidential Alerts

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

Gyhong Lee
University of Colorado Boulder
gyhong.lee@colorado.edu

Jihoon Lee
University of Colorado Boulder
jihoon.lee-1@colorado.edu

Jinsung Lee
University of Colorado Boulder
jinsung.lee@colorado.edu

Youngbin Im
University of Colorado Boulder
youngbin.im@colorado.edu

Max Hollingsworth
University of Colorado Boulder
max.hollingsworth@colorado.edu

Eric Wustrow
University of Colorado Boulder
ewust@colorado.edu

Dirk Grunwald
University of Colorado Boulder
dirk.grunwald@colorado.edu

Sangtae Ha
University of Colorado Boulder
sangtae.ha@colorado.edu

Session 8: Waiting for 7G
### Spoofing Presidential Alerts

<table>
<thead>
<tr>
<th>SIB-10</th>
<th>ETWS (Earthquake and Tsunami Warning System) information (Primary notification)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIB-11</td>
<td>ETWS (Earthquake and Tsunami Warning System) information (Secondary notification)</td>
</tr>
<tr>
<td>SIB-12</td>
<td>Commercial Mobile Alert Service (CMAS) information.</td>
</tr>
</tbody>
</table>
What about digital certificates?
What about digital certificates?

- Backwards compatibility
  - Radio packet size issues
What about digital certificates?

- Backwards compatibility
  - Radio packet size issues
- Where to put certs?
What about digital certificates?

- Backwards compatibility
  - Radio packet size issues
- Where to put certs?
- Roaming is hella difficult
What about digital certificates?

- Backwards compatibility
  - Radio packet size issues
- Where to put certs?
- Roaming is hella difficult
- Revocation challenges
- Replay attacks
What about digital certificates?
Challenges in cell network security research

- Closed source implementations
Challenges in cell network security research

- Closed source implementations
- $$$
Challenges in cell network security research

- Closed source implementations
- $$$
- Legal issues
Challenges in cell network security research

- Closed source implementations
- $$$
- Legal issues
- Sprawling specs
Challenges in cell network security research

- Closed source implementations
- $$$
- Legal issues
- Sprawling specs
- Huge variance across carriers
Cell network security research historically
This is Your President Speaking:
Spoofing Alerts in 4G LTE Networks

Gyuhong Lee*
University of Colorado Boulder
gyuhong.lee@colorado.edu

Jihoon Lee*
University of Colorado Boulder
jihoon.lee-1@colorado.edu

Jinsung Lee
University of Colorado Boulder
jinsung.lee@colorado.edu

Youngbin Im
University of Colorado Boulder
youngbin.im@colorado.edu

Max Hollingsworth
University of Colorado Boulder
max.hollingsworth@colorado.edu

Eric Wustrow
University of Colorado Boulder
ewust@colorado.edu

Dirk Grunwald
University of Colorado Boulder
dirk.grunwald@colorado.edu

Sangtae Ha
University of Colorado Boulder
sangtae.ha@colorado.edu
Conclusion + next steps

Conclusion:

- Pre-auth messages are what enable IMSI-catchers & more
Conclusion + next steps

Conclusion:
- Pre-auth messages are what enable IMSI-catchers & more

Next steps:
- Making research accessible
Conclusion + next steps

Conclusion:

- Pre-auth messages are what enable IMSI-catchers & more

Next steps:

- Making research accessible
- More authentication research
Conclusion + next steps

Conclusion:
- Pre-auth messages are what enable IMSI-catchers & more

Next steps:
- Making research accessible
- More authentication research
- More open source tools
Conclusion + next steps

Conclusion:
- Pre-auth messages are what enable IMSI-catchers & more

Next steps:
- Making research accessible
- More authentication research
- More open source tools
- More press & pressuring carriers
Questions?