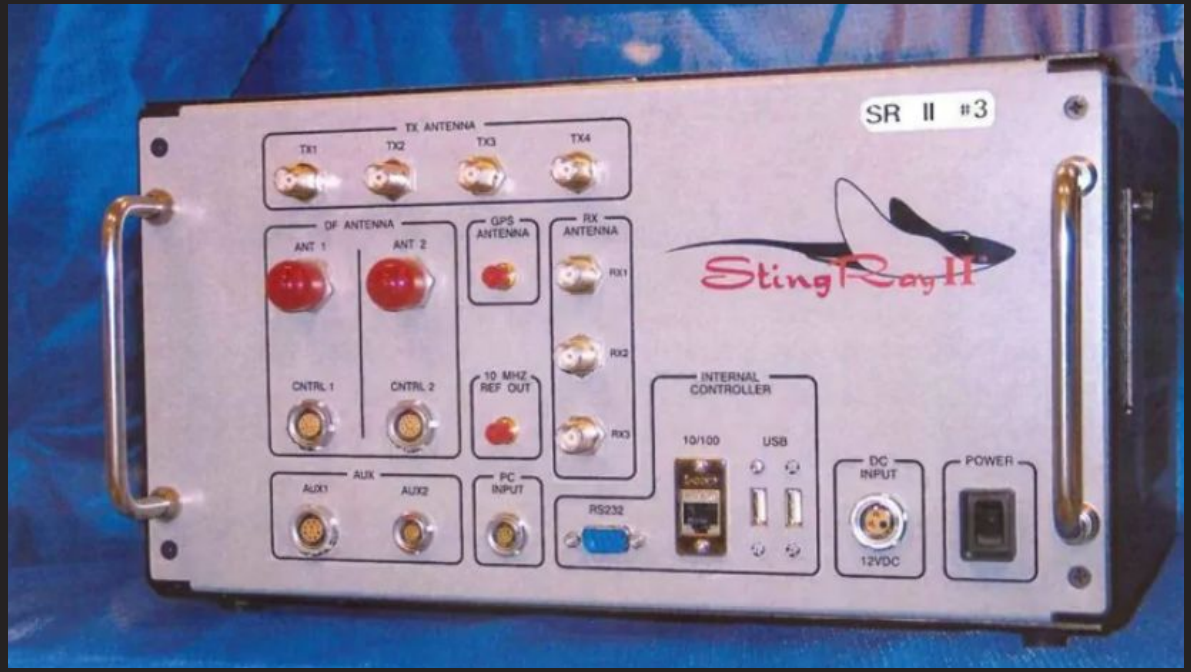
ENIGMA

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

Yomna Nasser
@rival_elf

What is an IMSI-catcher?



SPY VS. SPY —

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.

CYRUS FARIVAR - 4/3/2018, 12:27 PM

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**

(Photo: Facebook)

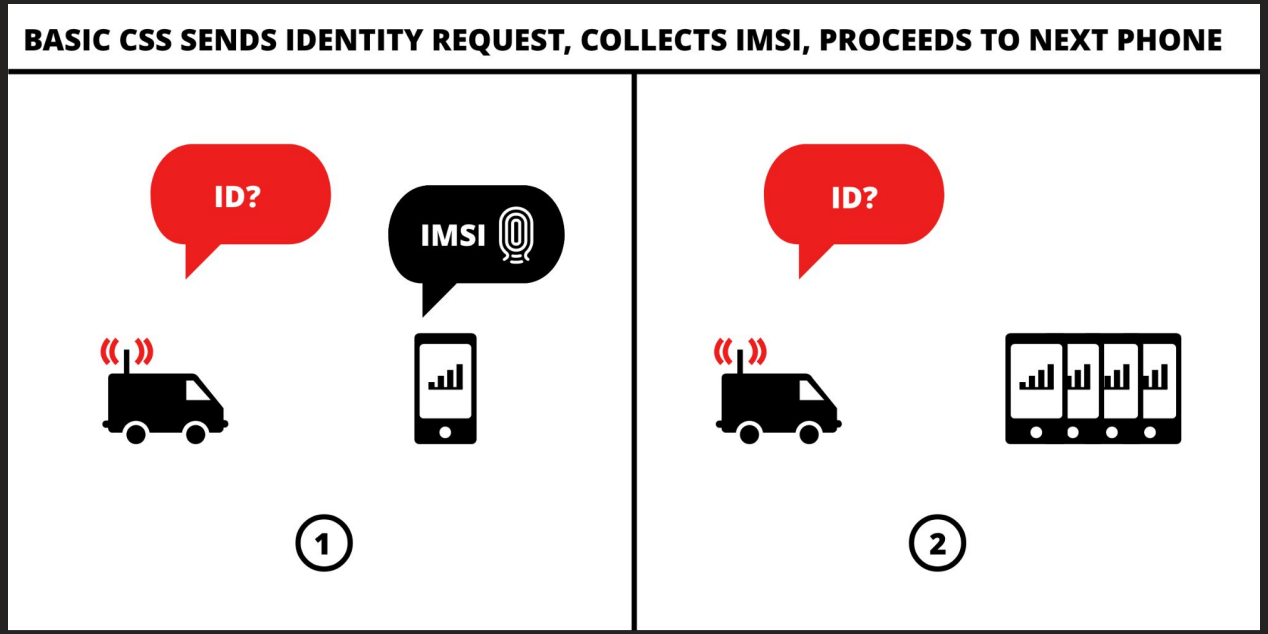
Detroit — Federal investigators are using a cellphone snooping device designed for counter-terrorism to hunt undocumented immigrants amid President Donald Trump’s immigration crackdown, according to federal court records obtained by The Detroit News.

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

Terminology

- Base station
- GSM (2G)
- LTE (4G)
- 5G

The original (GSM) IMSI-catcher



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

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

Spoofing Presidential Alerts

SIB-10	ETWS (Earthquake and Tsunami Warning System) information (Primary notification)
SIB-11	ETWS (Earthquake and Tsunami Warning System) information (Secondary notification)
SIB-12	Commercial Mobile Alert Service (CMAS) information.

What about digital certificates?

Insecure Connection Bootstrapping in Cellular Networks: The Root of All Evil

Syed Rafiul Hussain
Purdue University
hussain1@purdue.edu

Mitziu Echeverria
University of Iowa
mitziu-echeverria@uiowa.edu

Ankush Singla
Purdue University
asingla@purdue.edu

Omar Chowdhury
University of Iowa
omar-chowdhury@uiowa.edu

Elisa Bertino
Purdue University
bertino@purdue.edu

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?

Insecure Connection Bootstrapping in Cellular Networks: The Root of All Evil

Syed Rafiul Hussain
Purdue University
hussain1@purdue.edu

Mitziu Echeverria
University of Iowa
mitziu-echeverria@uiowa.edu

Ankush Singla
Purdue University
asingla@purdue.edu

Omar Chowdhury
University of Iowa
omar-chowdhury@uiowa.edu

Elisa Bertino
Purdue University
bertino@purdue.edu

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

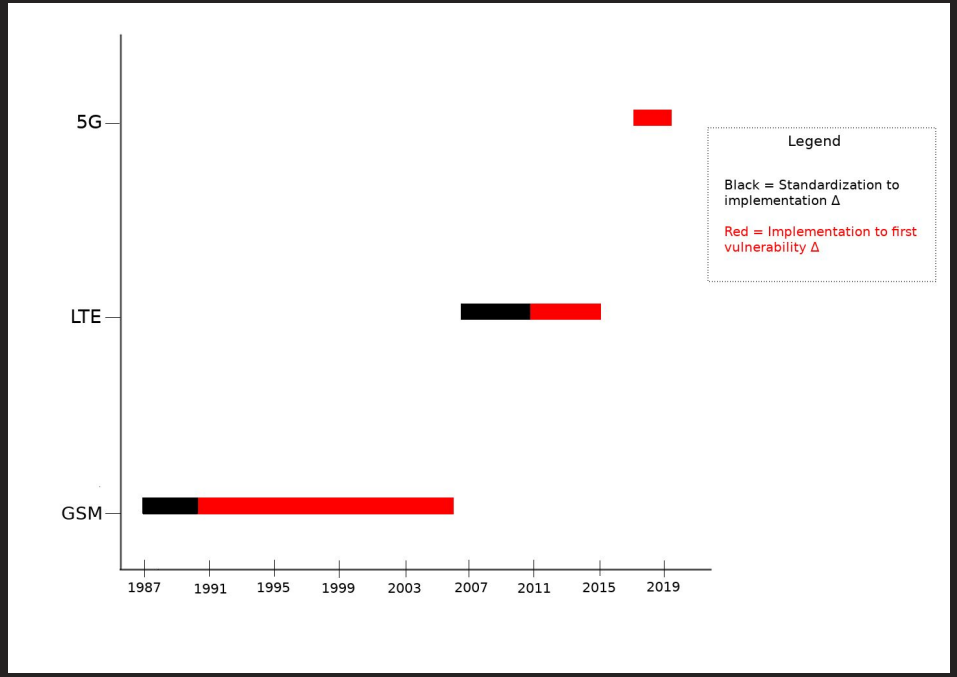
Challenges in cell network security research

- 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



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

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?