The attacks aren't alright: Large-Scale Simulation of Fake Base Station Attacks and Detections

Thijs Heijligenberg, David Rupprecht, Katharina Kohls

August 13, 2024

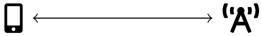
Simulation of Fake Base Station Attacks and Detections

Simulation of $\underbrace{\text{Fake Base Station}}_{①}$ Attacks and Detections

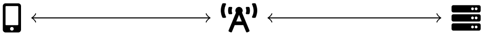
$\underbrace{\text{Simulation}}_{\textcircled{2}}$ of $\underbrace{\text{Fake Base Station}}_{\textcircled{1}}$ Attacks and Detections

$$\underbrace{\text{Simulation}}_{②}\text{ of }\underbrace{\text{Fake Base Station}}_{①}\text{ Attacks and }\underbrace{\text{Detections}}_{③}$$

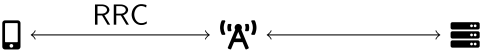
Mobile networks



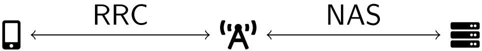
Mobile networks



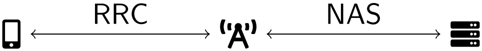
Mobile networks



Mobile networks

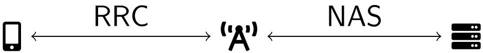


Mobile networks



- RRC: Control radio connection

Mobile networks



- RRC: Control radio connection
- NAS: Control network connection (mobile and data)

Idle and connected modes

Two modes for being ”in” the mobile network:

Idle and connected modes

Two modes for being "in" the mobile network:**Idle**:

- Listening for call notifications

Idle and connected modes

Two modes for being "in" the mobile network:**Idle**:

- Listening for call notifications
- Configuration is broadcast (plaintext)

Idle and connected modes

Two modes for being ”in” the mobile network:**Idle**:

- Listening for call notifications
- Configuration is broadcast (plaintext)

Connected:

- Active session for data transmission

Idle and connected modes

Two modes for being ”in” the mobile network:**Idle**:

- Listening for call notifications
- Configuration is broadcast (plaintext)

Connected:

- Active session for data transmission
- Encrypted, authenticated, ...

Idle and connected modes

Two modes for being "in" the mobile network:**Idle**:

- Listening for call notifications
- Configuration is broadcast (plaintext)

Connected:

- Active session for data transmission
- Encrypted, authenticated, ...
- Configuration is sent directly

(re)selection

When do you get a new cell?

(re)selection

When do you get a new cell?

Selection: find a suitable cell initially (idle)

(re)selection

When do you get a new cell?

Selection: find a suitable cell initially (idle)

Reselection: find a suitable cell if necessary (idle)

(re)selection

When do you get a new cell?

Selection: find a suitable cell initially (idle)

Reselection: find a suitable cell if necessary (idle)

Handover: transfer your active connection (connected)

Fake base stations

An attacker-operated base station with:

Fake base stations

An attacker-operated base station with:

1. The same country/operator code

Fake base stations

An attacker-operated base station with:

1. The same country/operator code
2. The right frequency (band)

Fake base stations

An attacker-operated base station with:

1. The same country/operator code
2. The right frequency (band)

Goal: the UE (re)selects to the cell

Fake base stations

An attacker-operated base station with:

1. The same country/operator code
2. The right frequency (band)

Goal: the UE (re)selects to the cell

Connection: report a different "tracking area"

Fake base stations

An attacker-operated base station with:

1. The same country/operator code
2. The right frequency (band)

Goal: the UE (re)selects to the cell

Connection: report a different ”tracking area”

Various attacks

Reasons & solutions

Reasons:

Reasons & solutions

Reasons:

- Idle $\implies$ no session $\implies$ no security

Reasons & solutions

Reasons:

- Idle $\implies$ no session $\implies$ no security
- Fallback

Reasons & solutions

Reasons:

- Idle $\implies$ no session $\implies$ no security
- Fallback
- Pre-shared keys

Reasons & solutions

Reasons:

- Idle $\implies$ no session $\implies$ no security
- Fallback
- Pre-shared keys

Solution in 5G!

Why simulate?

An attack requires:

- Reselection to the fake base station

Why simulate?

An attack requires:

- Reselection to the fake base station
- I.e. the signal is stronger

Why simulate?

An attack requires:

- Reselection to the fake base station
- I.e. the signal is ~~stronger~~ better with the configured offsets

Why simulate?

An attack requires:

- Reselection to the fake base station
- I.e. the signal is ~~stronger~~ better with the configured offsets
- Depends on transmission power, the configuration, and placement

Why simulate?

An attack requires:

- Reselection to the fake base station
- I.e. the signal is ~~stronger~~ better with the configured offsets
- Depends on transmission power, the configuration, and placement

Tests must be large-scale to be representative.

Why simulate?

An attack requires:

- Reselection to the fake base station
- I.e. the signal is ~~stronger~~ better with the configured offsets
- Depends on transmission power, the configuration, and placement

Tests must be large-scale to be representative.

Real-life tests are illegal/unethical...

Complications

- Specification → Implementation

Complications

- Specification → Implementation→ Configuration

Complications

- Specification → Implementation→ Configuration
- Signal propagation is hard

Complications

- Specification → Implementation→ Configuration
- Signal propagation is hard
- Define success?

Simulation results

Transmission power:

Simulation results

Transmission power:

- Large effect
- COTS: 15-30%
- "real": 75%+

Simulation results

Placement:

Simulation results

Placement:

- Large variance
- Trend: 7-13%
- Hard to get right

Detection

- Fake base stations in 4G and below will **never** be ”solved”

Detection

- Fake base stations in 4G and below will **never** be ”solved”
- Detection: same evaluation problems as before

Detection

- Fake base stations in 4G and below will **never** be "solved"
- Detection: same evaluation problems as before
- Simulation!

Detection methods

Tracking Area updates

Detection methods

Tracking Area updates

- Detect weird behaviour

Detection methods

Tracking Area updates

- Detect weird behaviour
- Dabrowski et al. (2016)

Detection methods

Tracking Area updates

- Detect weird behaviour
- Dabrowski et al. (2016)
- Inconsistent...

Detection methods

Tracking Area updates

- Detect weird behaviour
- Dabrowski et al. (2016)
- Inconsistent...

Measurement reports

Detection methods

Tracking Area updates

- Detect weird behaviour
- Dabrowski et al. (2016)
- Inconsistent...

Measurement reports

- Use available data

Detection methods

Tracking Area updates

- Detect weird behaviour
- Dabrowski et al. (2016)
- Inconsistent...

Measurement reports

- Use available data
- Idea is in specs

Detection methods

Tracking Area updates

- Detect weird behaviour
- Dabrowski et al. (2016)
- Inconsistent...

Measurement reports

- Use available data
- Idea is in specs
- "Hard" problem

Conclusion

- Fake base station attacks are suitable

Conclusion

- Fake base station attacks are suitable
- Simulation: get actual numbers

Conclusion

- Fake base station attacks are suitable
- Simulation: get actual numbers
- Test proposed solutions at scale

Conclusion

- Fake base station attacks are suitable
- Simulation: get actual numbers
- Test proposed solutions at scale