Don’t Hand it Over: Vulnerabilities in the Handover Procedure of Cellular Telecommunications

Evangelos Bitsikas and Christina Pöpper
Annual Computer Security Applications Conference (ACSAC) 2021, Virtual, USA
Cellular Networks

Don’t Hand it Over: Vulnerabilities in Handover Procedure of Cellular Telecommunications
Evangelos Bitsikas and Christina Pöpper
Annual Computer Security Applications Conference (ACSAC) 2021, Virtual, USA

Motivation

The lack of proper security measures when the user/subscriber relocates from one network cell to another.

Some security issues that started in 2G era continue to affect the current 5G standards and implementations.

Handover exploitation may be used as a steppingstone for other attacks.

Encryption and Integrity-protection are not enough to secure mobility management.
Contributions

1. First study that covers handover attacks in such a depth.
2. First study that includes actual 5G handover exploitation in the standalone setup.
3. Different handover types, services and conditions are covered.
4. All handovers that are based on measurements can be exploited.
5. Handover attacks can result in Denial-of-Service, Man-in-the-Middle attacks and information disclosure.
**Mobility Management**: is the fundamental technology that allows the serving networks to maintain the connection and services of a network subscriber, as this subscriber changes locations and points of attachment.
Handover Phases:

1. **Preparation Phase** corresponds to the handover decision, information exchange between cells and resource reservation.

2. **Execution Phase** corresponds to the actual mobile connection to the target cell.

3. **Completion Phase** consists of the establishment of bearers and the release of the old resources.
System Information (SI) messages are broadcast messages that are transmitted by the base station in order to facilitate certain network operations.

System Information messages are separated into:

• Master Information Block (MIB), and
• System Information Blocks (SIB)
UE Connection
Measurement report (MR) is the collection of signal metrics that is sent to the serving base station in order to evaluate the condition of the connection in terms of quality and strength.

Measurement Report Metrics on 5G
- Reference Signal Received Power (RSRP)
- Reference Signal Received Quality (RSRQ)
- Signal to Interference and Noise Ration (SINR)

Measurement Report Metrics on LTE
- Reference Signal Received Power (RSRP)
- Reference Signal Received Quality (RSRQ)
## Handover Classifications

<table>
<thead>
<tr>
<th>Intra Base Station</th>
<th>Intra-HO</th>
<th>Inter Base Station</th>
<th>Inter-HO</th>
</tr>
</thead>
</table>

### Inter-HO handover cases for all Radio Access Technologies:

<table>
<thead>
<tr>
<th>Source Network</th>
<th>Within the Source Network</th>
<th>Target Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>5G RAN</td>
<td>Intra-RAT, Intra/Inter-AMF Xn or N2</td>
<td>5G RAN: Intra-RAT, Intra-AMF N2</td>
</tr>
<tr>
<td>E-UTRAN</td>
<td>Intra-RAT, Intra/Inter-MME X2 or S1</td>
<td>5G RAN: Intra-RAT, Intra-AMF N2</td>
</tr>
<tr>
<td>UTRAN/GERAN</td>
<td>Intra/Inter RAT, Intra/Inter SGSN A/Gb or Lu mode</td>
<td>5G RAN: Intra-RAT, Intra-AMF N2</td>
</tr>
</tbody>
</table>

**Conditional Handovers (CHO)**

**CU-DU gNodeB Handovers**
Inter-HO Example

5G Inter-HO with N2 interface

1. Measurement Report
2. Handover decision via N2
3. Handover Required
4. Handover Request
5. Handover Request ACK
6. Handover Command (RRC Reconfiguration)
7. Handover Command (RRC Reconfiguration) [9, Direct or Indirect Data Forwarding to target]
8. RAN Status Transfer
9. RACH procedure
10. Handover Confirm (RRC Reconfiguration Complete)

14. UE Context Release

5G Inter-HO with Xn interface

1. Measurement Report
2. Handover Decision
3. Handover Request
4. Handover Admission Control
5. Handover Request ACK
6. Handover Command (RRC Reconfiguration)
7. RAN Status Transfer
8. Data Forwarding
9. RACH procedure
10. Handover Confirm (RRC Reconfiguration Complete)

13. UE Context Release
11. Path Switch Request
12. Path Switch Request ACK

Don’t Hand it Over: Vulnerabilities in Handover Procedure of Cellular Telecommunications
Evangelos Bitsikas and Christina Pöpper
Annual Computer Security Applications Conference (ACSAC) 2021, Virtual, USA
Vulnerabilities

Security flaws and inadequacies in Intra-HO and Inter-HO cases:

A. Insecure Broadcast Messages (MIB, SIBs)
B. Unverified Measurement Reports
C. Missing Cross-Validation in Preparation Phase
D. RACH initiation without verification
E. Missing Recovery Mechanism
F. Difficulty of distinguishing network failures from attacks
Attacker’s Setup & Steps

Attacker’s setup:

- Equipment for one or more malicious base station(s)
- Malicious software for base station, Core Network and UE operations
- Very high signal power
- Replay of MIB and SIB messages of the affected cell

Attacker’s configurations:

- Cell Identifier
- Downlink frequency (dl_ARFCN)
- Tracking Area Identity (MMC + MNC + TAC)
- PRACH Root Sequence Index
- Type of service

Steps:

1. Initial Reconnaissance
2. Determining the network structure
3. Selecting the target-victim
4. Configuring the false base station
5. Handover Exploitation
Impact Cases

Intra-HO attack case

Cell 1

Cell 2

MR₁

SIB₁

MIB₁

Inter-HO attack case

Cell 1

Cell 2

MR₁

SIB₁

MIB₁
Exploitation (Intra-HO)

Forced Disconnection

Malicious Attachment

Cell 1  Cell 2

SIB₁  MIB₁

RRC Reconfiguration

Cell 1  Cell 2

Attachment

Don’t Hand it Over: Vulnerabilities in Handover Procedure of Cellular Telecommunications
Evangelos Bitsikas and Christina Pöpper
Annual Computer Security Applications Conference (ACSAC) 2021, Virtual, USA
Exploitation Results (Intra-HO)

Denial-of-Service

MitM Relay

OR

Don’t Hand it Over: Vulnerabilities in Handover Procedure of Cellular Telecommunications
Evangelos Bitsikas and Christina Pöpper
Annual Computer Security Applications Conference (ACSAC) 2021, Virtual, USA
Vulnerabilities:

A. Insecure Broadcast Messages (MIB, SIBs)
B. Unverified Measurement Reports
C. Missing Cross-Validation in Preparation Phase
D. RACH initiation without verification
E. Missing Recovery Mechanism
F. Difficulty of distinguishing network failures from attacks
Exploitation (Inter-HO)

Forced Disconnection

Malicious Attachment

Don’t Hand it Over: Vulnerabilities in Handover Procedure of Cellular Telecommunications
Evangelos Bitsikas and Christina Pöpper
Annual Computer Security Applications Conference (ACSAC) 2021, Virtual, USA
Exploitation Results (Inter-HO)

Denial-of-Service

Attach Reject Messages

Cell 1

Cell 2

Cell 1

Cell 2

DoS

MitM Relay

Cell 1

Cell 2

MitM
Vulnerabilities:

A. Insecure Broadcast Messages (MIB, SIBs)
B. Unverified Measurement Reports
C. Missing Cross-Validation in Preparation Phase
D. RACH initiation without verification
E. Missing Recovery Mechanism
F. Difficulty of distinguishing network failures from attacks
Handover attacks may lead to network failures, such as:

- PCI confusions and conflicts
- X2/Xn errors
- Handover errors
- Timer expirations and resource exhaustion
- Base station outages due to handover failures [46]
Traffic Variations

- Three tested scenarios: Calls, SMS and mobile data usage.
- Calls were slightly more susceptible to MitM instead of DoS.
- Differences in smartphone behavior were observed.
Don’t Hand it Over: Vulnerabilities in Handover Procedure of Cellular Telecommunications
Evangelos Bitsikas and Christina Pöpper
Annual Computer Security Applications Conference (ACSAC) 2021, Virtual, USA

Impact

Handover Vulnerabilities

- Denial-of-Service (User)
- Man-in-the-Middle (User)
- Information Disclosure (User)
- Network Damages
Countermeasures

- UE-based approaches for false base station detection.
- Enriched measurement reports and verification.
- Public Key Infrastructure for system info messages. \[49\]
- Encrypted system queries.
- Encryption and Integrity-protection, especially for all NAS and RRC messages.
- A combination of the above!

\[49\] Singla et al. Look Before You Leap: Secure Connection Bootstrapping for 5G Networks to Defend Against Fake Base-Stations. Asia CCS'21
Handovers can be exploited and remain unmitigated to date in all generations.

Solving the security issues may not be straightforward.

UE response to attacks may vary based on the service or smartphone device.

Handover attacks may impact the network when on a large scale.

Handover attacks are feasible, so we need a way to make our systems/networks more secure!
Thank You!
Questions?