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

Evangelos Bitsikas and Christina Pöpper

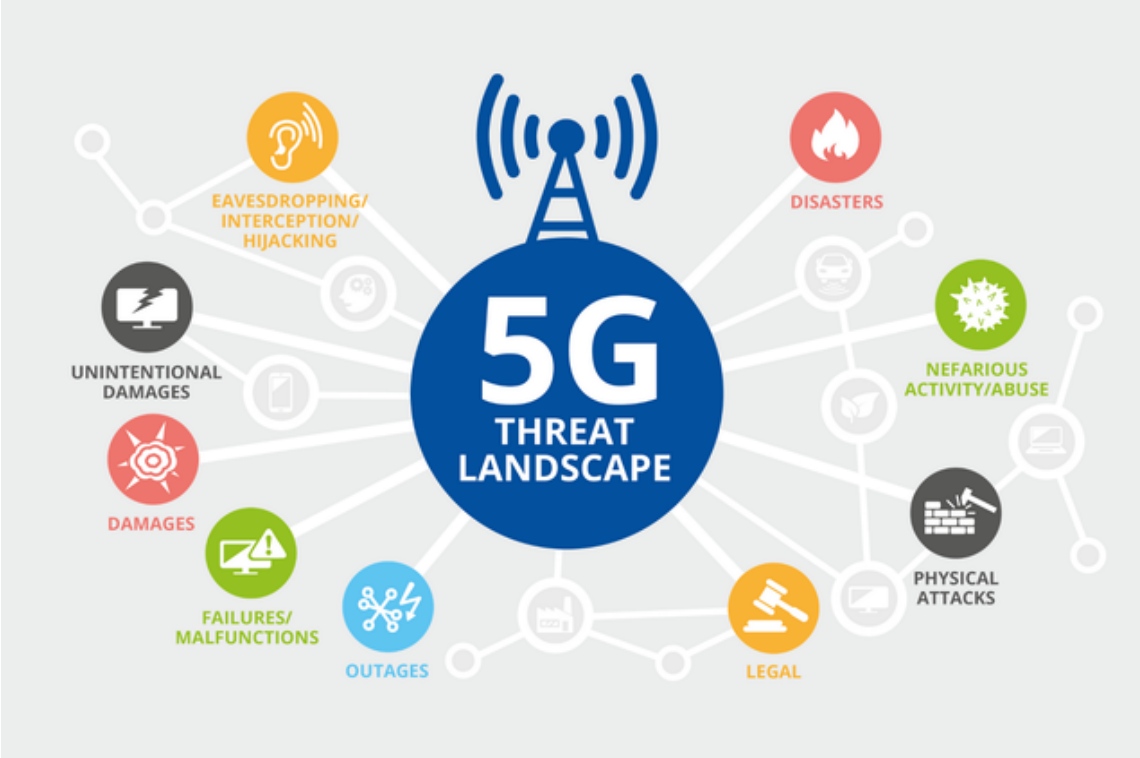
Annual Computer Security Applications Conference (ACSAC) 2021, Virtual, USA

جامعة نيويورك أبوظبي
NYU ABU DHABI

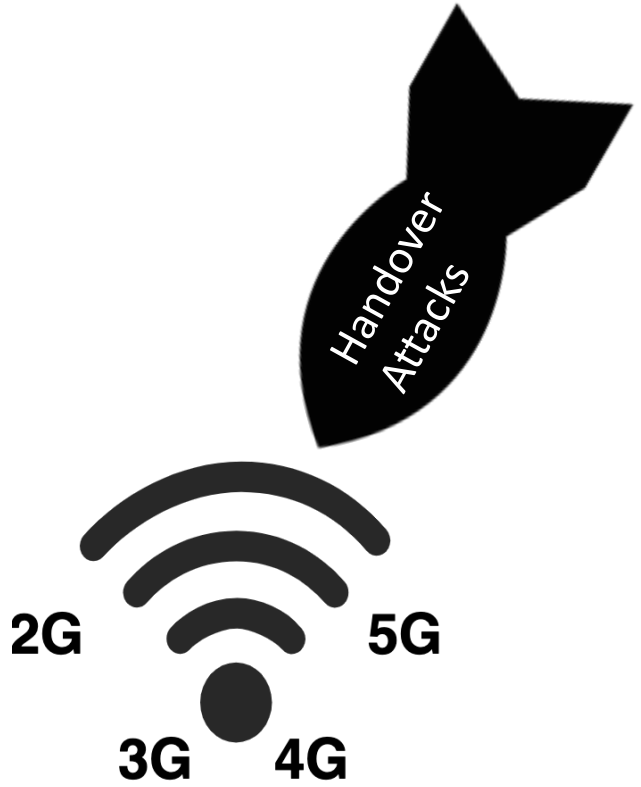
CSP-lab
Cyber Security and Privacy Lab

CENTER FOR
CYBER SECURITY

Cellular Networks



Source: https://www.enisa.europa.eu/news/enisa-news/updated-enisa-5g-threat-landscape-report-to-enhance-5g-security



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.

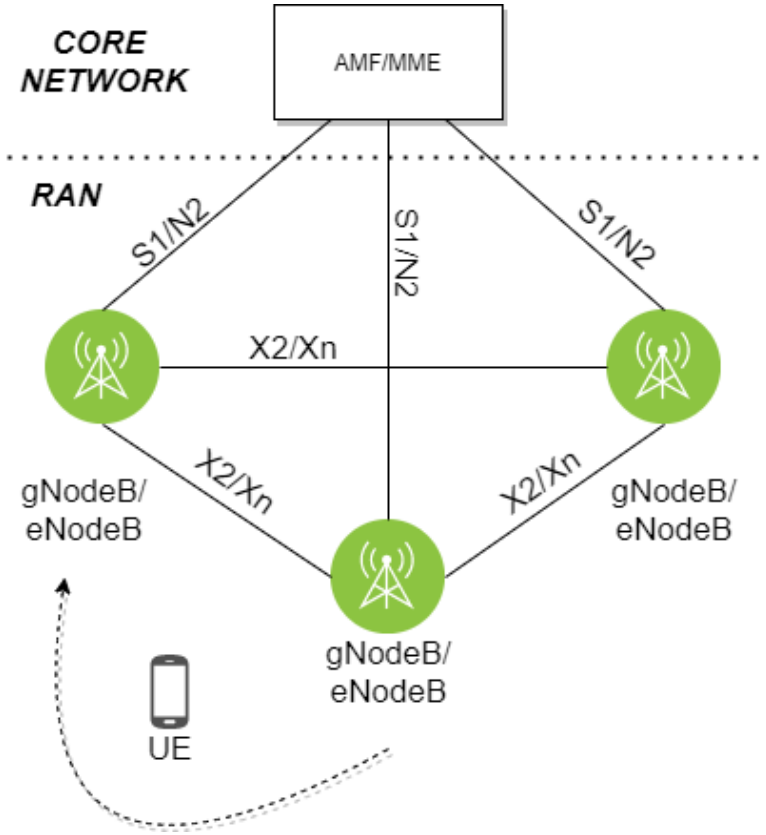
Encryption and Integrity-protection are not enough to secure mobility management.

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

***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.



Handovers

Handover Phases:

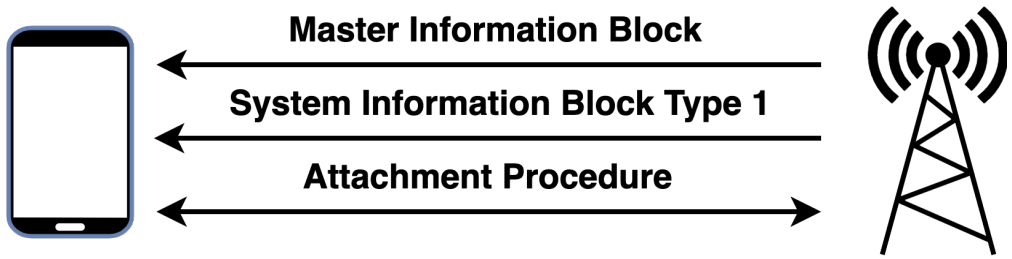
1. *Preparation Phase* corresponds to the handover decision, information exchange between cells and resource reservation.
2. *Execution Phase* corresponds to the actual mobile connection to the target cell.
3. *Completion Phase* consists of the establishment of bearers and the release of the old resources.

System Information

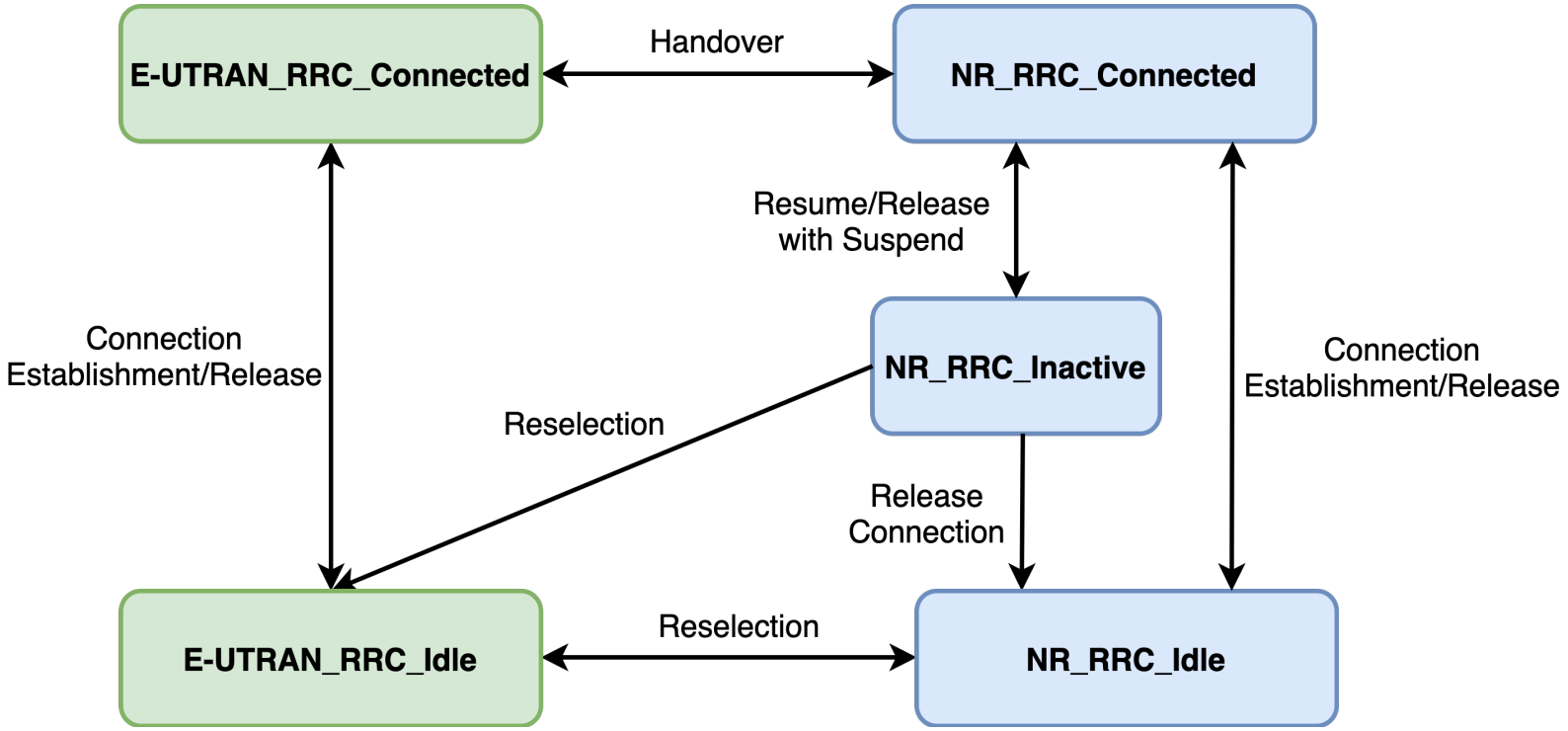
System Information **(SI)** messages are broadcast messages that are transmitted by the base station in order to facilitate certain network operations.

System Information messages are separated into:

- Master Information Block (MIB), and
- System Information Blocks (SIB)



UE Connection



Measurement Reports

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)

Message: Measurement Report

Data:

```
{
  message c1: measurementReport: {
    criticalExtensions c1: measurementReport-r8: {
      measResults {
        measId 3,
        measResultPCell {
          rsrpResult 53,
          rsrqResult 33
        },
        measResultNeighCells measResultListEUTRA: {
          {
            physCellId 2,
            measResult {
              rsrpResult 59,
              rsrqResult 26
            }
          }
        }
      }
    }
  }
}
```

Handover Classifications

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

Intra Base Station ⟶ **Intra-HO**

Inter Base Station ⟶ **Inter-HO**

Inter-HO handover cases for all Radio Access Technologies:

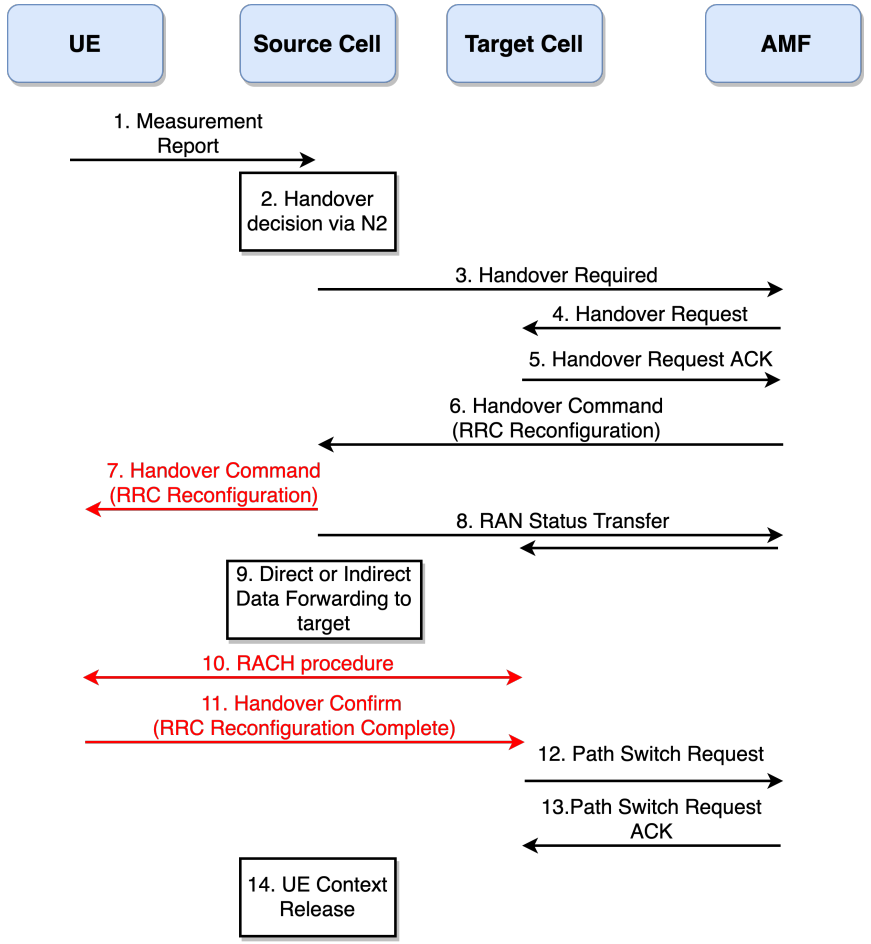
		Target Network			
		Within the Source Network	5G RAN	E-UTRAN	UTRAN / GERAN
Source Network	5G RAN	Intra-RAT Intra/Inter-AMF Xn or N2	Intra-RAT Inter-AMF N2	Inter-RAT (with or w/o N26 interface)	Inter-RAT through SRVCC (Call only)
	E-UTRAN	Intra-RAT Intra/Inter-MME X2 or S1	Inter-RAT (with or w/o N26 interface)	Intra-RAT Inter-MME S1	Inter-RAT (with or w/o SGW relocation, direct or indirect tunneling)
	UTRAN/ GERAN	Intra/Inter RAT Intra/Inter SGSN A/Gb or Iu mode	–	Inter-RAT (with or w/o SGW relocation, direct or indirect tunneling)	Intra/Inter RAT Inter SGSN A/Gb or Iu mode

Conditional Handovers (CHO) ✓

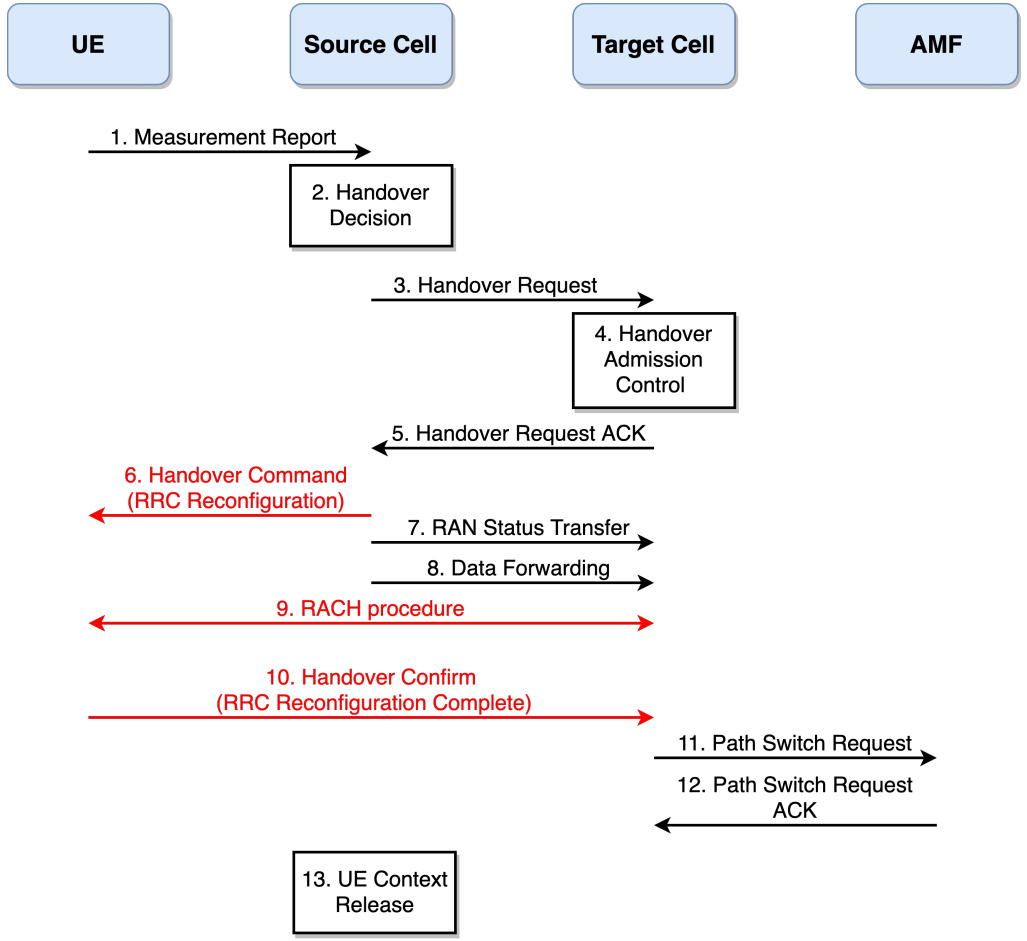
CU-DU gNodeB Handovers ✓

Inter-HO Example

5G Inter-HO with N2 interface



5G Inter-HO with Xn interface



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:

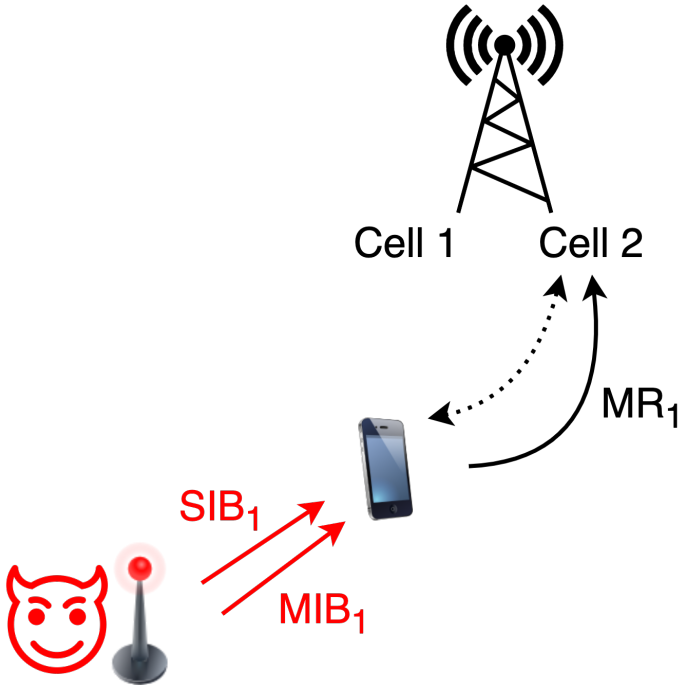
- Cell Identifier
- Downlink frequency (dl_ARFCN)
- Tracking Area Identity (MMC + MNC + TAC)
- PRACH Root Sequence Index
- Type of service

Steps:

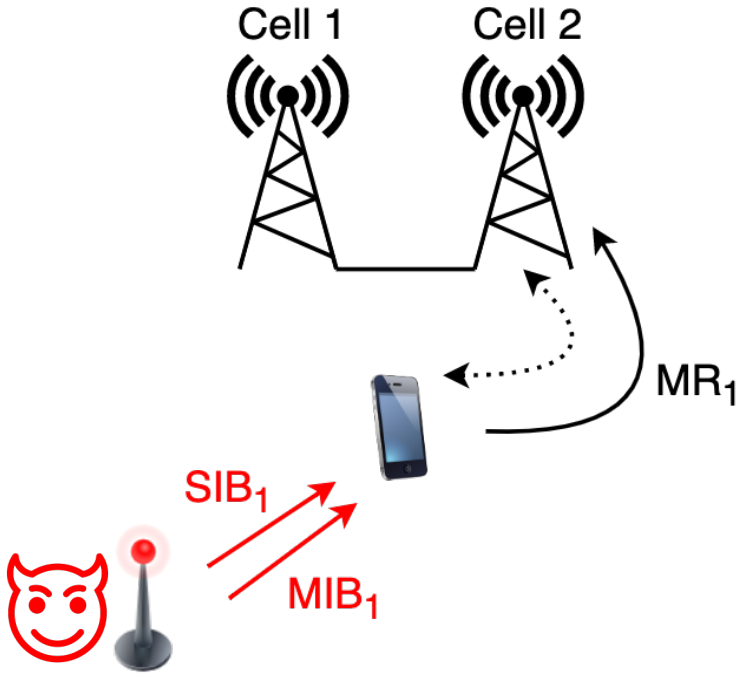
1. Initial Reconnaissance
2. Determing the network structure
3. Selecting the target-victim
4. Configuring the false base station
5. Handover Exploitation

Impact Cases

Intra-HO attack case



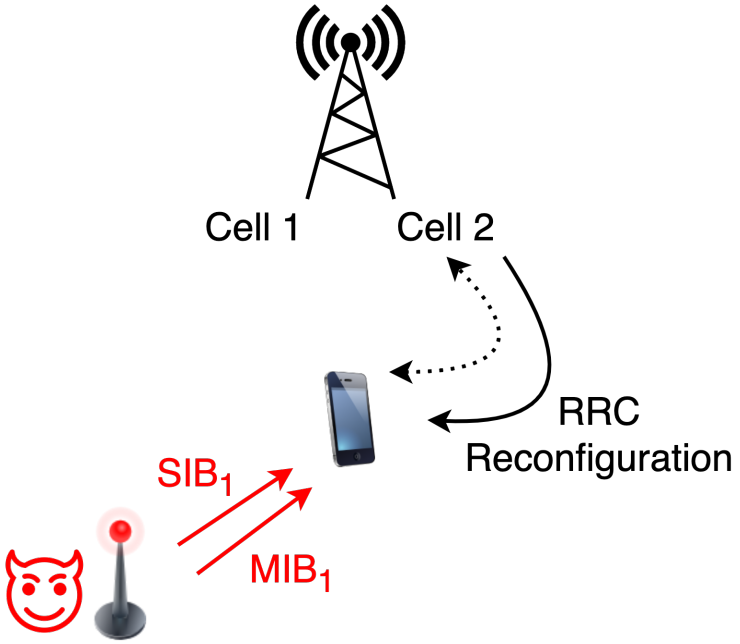
Inter-HO attack case



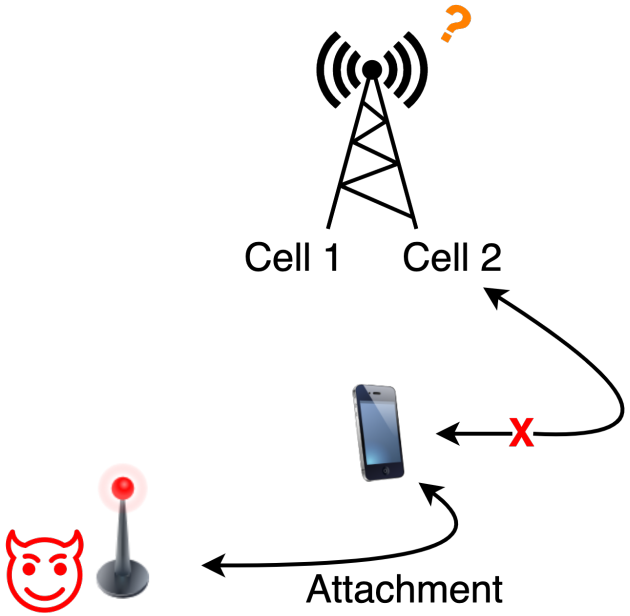
Exploitation (Intra-HO)

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

Forced Disconnection



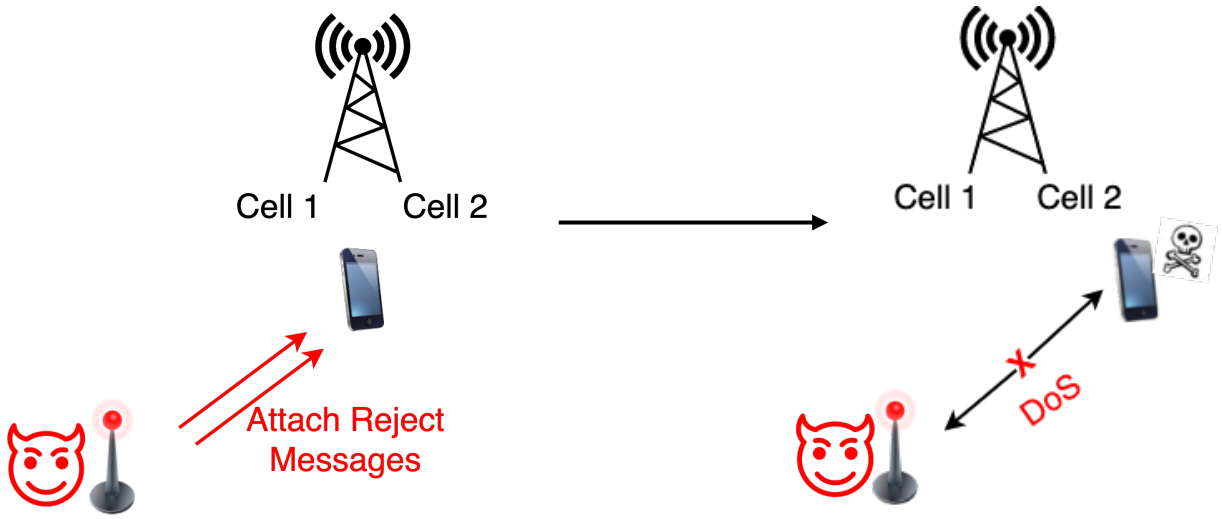
Malicious Attachment



Exploitation Results (Intra-HO)

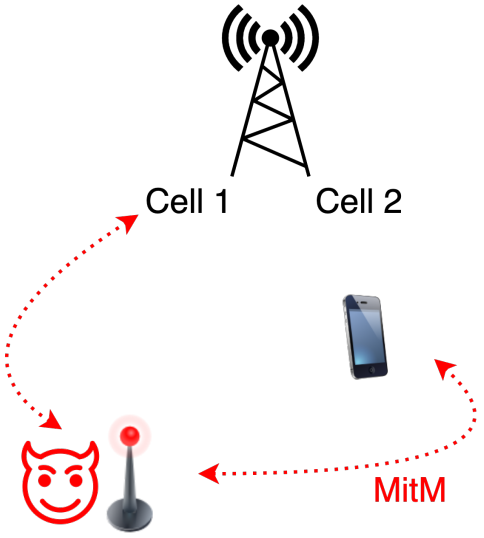
Don't Hand it Over: Vulnerabilities in Handover Procedure of Cellular Telecommunications
Evangelos Bitsikas and Christina Pöpper
Annual Computer Security Applications Conference (ACSAC) 2021, Virtual, USA

Denial-of-Service



OR

MitM Relay

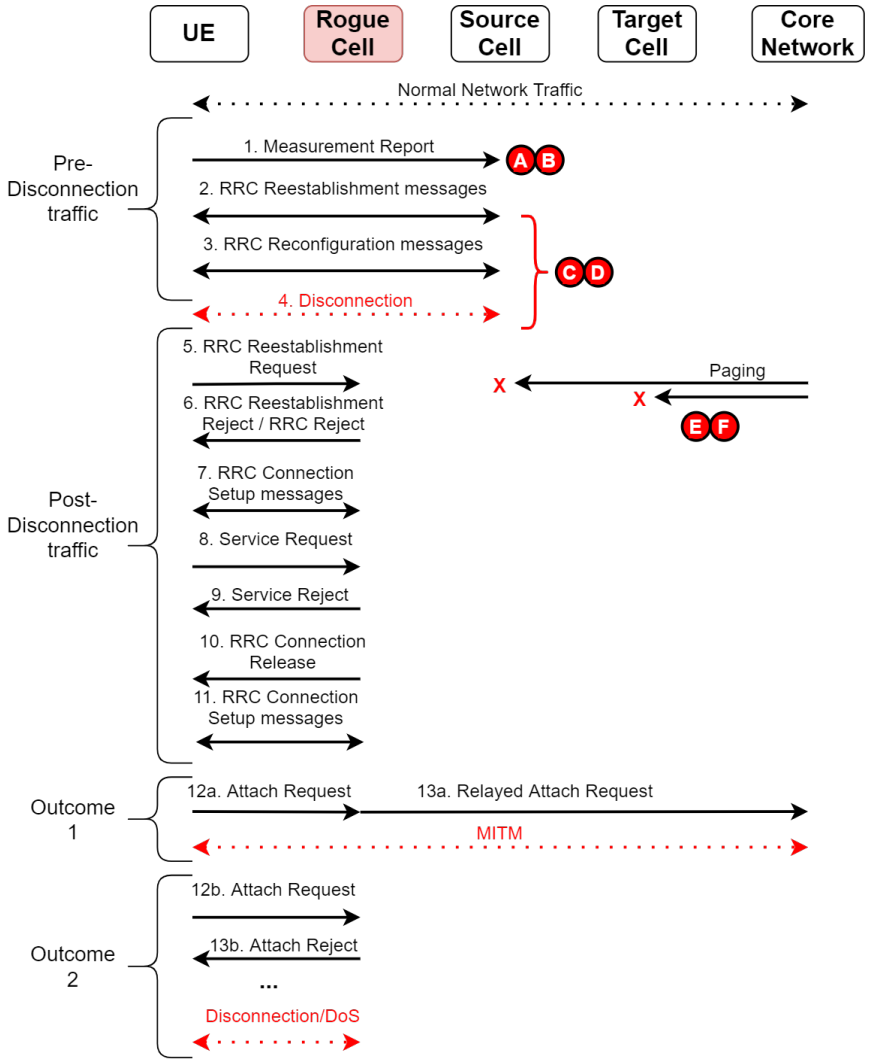


Exploitation Traffic (Intra-HO)

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:

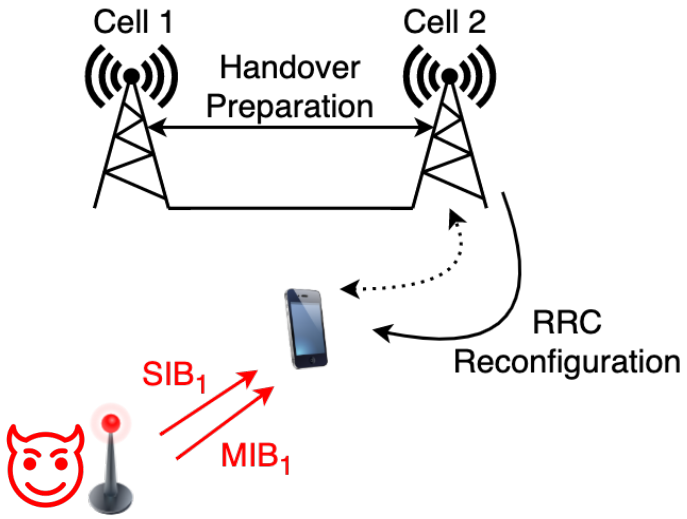
A. Insecure Broadcast Messages (MIB, SIBs)
B. Unverified Measurement Reports
C. Missing Cross-Validation in Preparation Phase
D. RACH initiation without verification
E. Missing Recovery Mechanism
F. Difficulty of distinguishing network failures from attacks



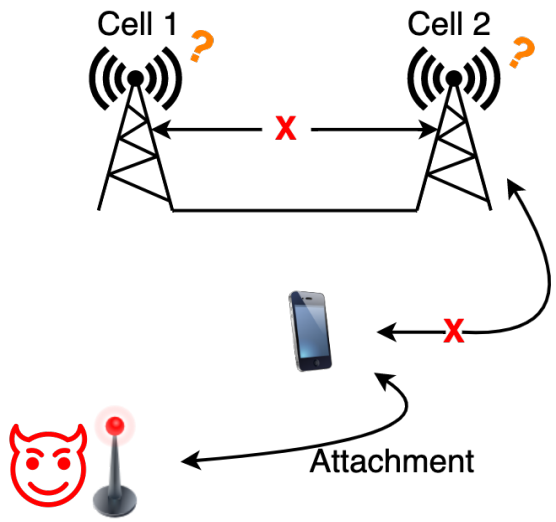
Exploitation (Inter-HO)

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

Forced Disconnection

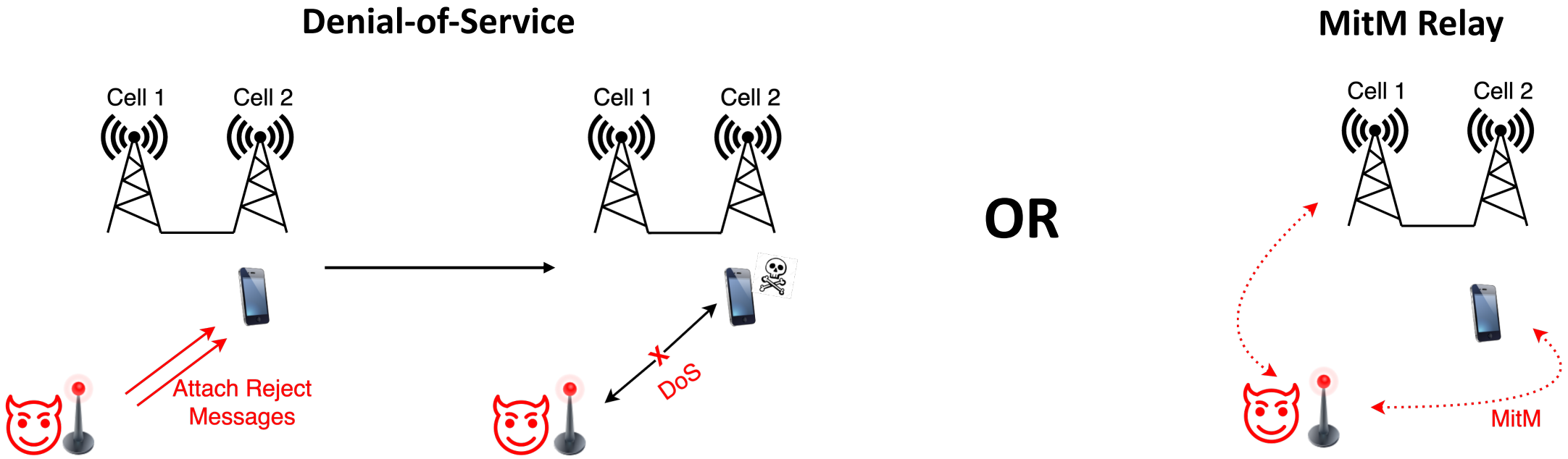


Malicious Attachment



Exploitation Results (Inter-HO)

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

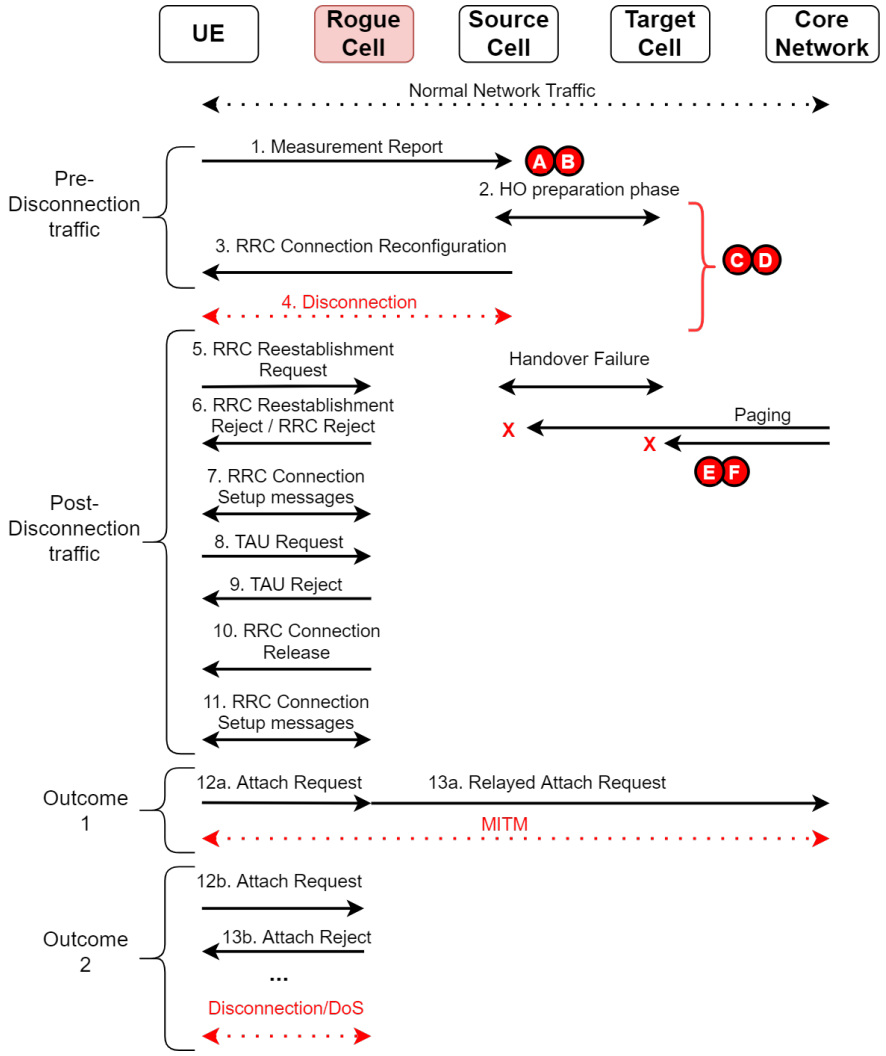


Exploitation Traffic (Inter-HO)

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



Network Implications

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]

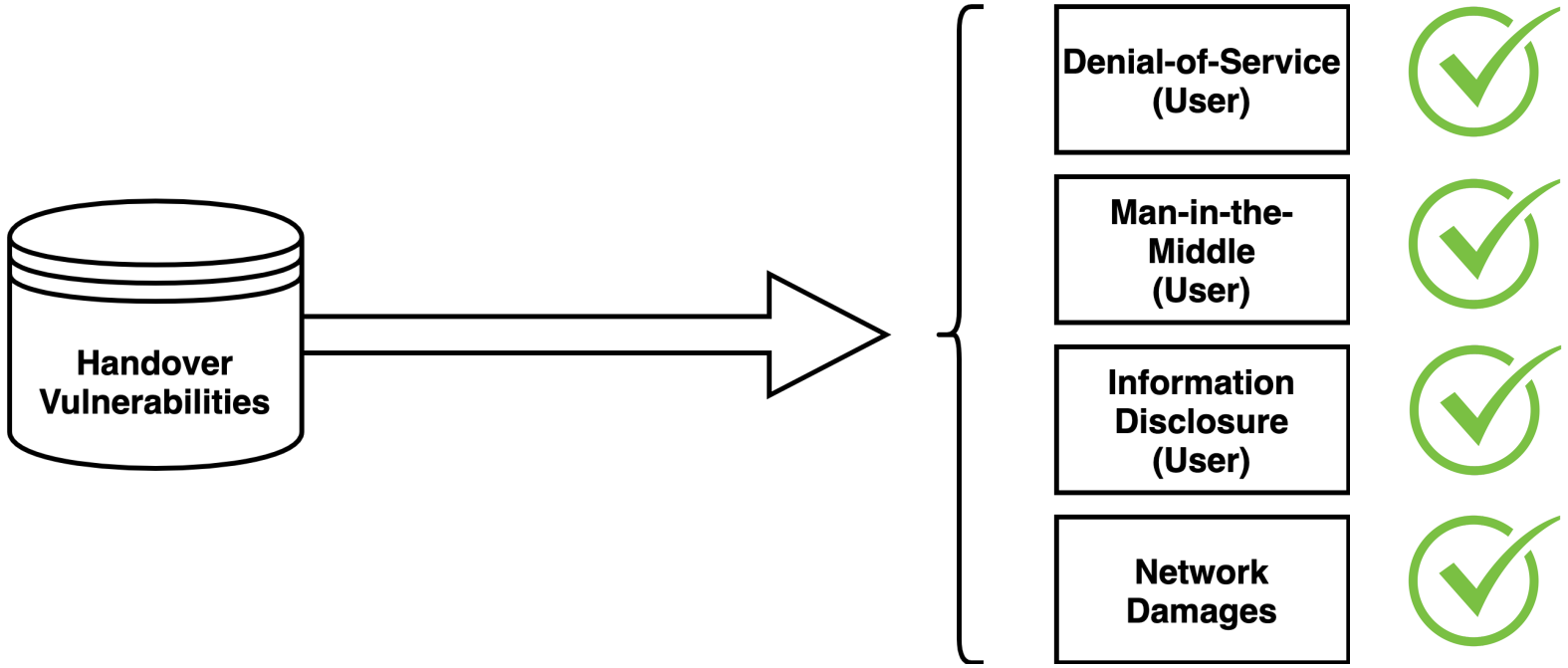
[46] Shaik et al. On the Impact of Rogue Base Stations in 4G/LTE Self Organizing Networks. Wisec'18

Traffic Variations

Device	Chipset	OS	Model	Release	MitM Susceptibility	DoS Susceptibility
Huawei P40 Pro 5G	Huawei Kirin 990 5G	Android 10	ELS-NX9	2020	High	High
One Plus 6	Snapdragon 855	Android 10	One Plus A6000	2019	High	High
Samsung Note 10 5G	Snapdragon 845	Android 10	SM-N976Q	2018	Medium	High
Apple iPhone 5	Apple A6 (32 nm)	iOS 10	A1428	2012	Medium	High

- 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.

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 Infrastucture 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

Takeaway Points

1. Handovers can be exploited and remain unmitigated to date in all generations.
2. Solving the security issues may not be straightforward.
3. UE response to attacks may vary based on the service or smartphone device.
4. 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?

جامعة نيويورك أبوظبي

NYU ABU DHABI

CSP-lab

Cyber Security and Privacy Lab

CENTER FOR CYBER SECURITY