# CATCHING The CATCHERS:

## IMSI-CATCHER CATCHER


Ryan Abdi

Tarbiat Modares University

Supervised By D. Abadi

https://www.modares.ac.ir/~abadi

abadi@modares.ac.ir

*Tarbiat Modares University*


June, 2023

# Introduction

## IMSI Catchers, Stringrays, Fake Base Stations, Drt-Boxes

- **Fake Devices** Simulating a part or complete cellular network
- **Identification** and **Tracking** of mobile devices in the Radio Coverage Area
- **Interception** of mobile User Data and radio Signalling Data
- **Downgrade** mobile users to lower generation networks(Weaker)
- Battery Drain
- DoS

# Introduction

## IMSI Catchers, Stringrays, Fake Base Stations, Drt-Boxes

- **Fake Devices** Simulating a part or complete cellular network
- **Identification** and **Tracking** of mobile devices in the Radio Coverage Area
- **Interception** of mobile User Data and radio Signalling Data
- **Downgrade** mobile users to lower generation networks(Weaker)
- Battery Drain
- DoS

# Introduction

## IMSI Catchers, Stringrays, Fake Base Stations, Drt-Boxes

- **Fake Devices** Simulating a part or complete cellular network
- **Identification** and **Tracking** of mobile devices in the Radio Coverage Area
- **Interception** of mobile User Data and radio Signalling Data
- **Downgrade** mobile users to lower generation networks(Weaker)
- Battery Drain
- DoS

# Introduction

## IMSI Catchers, Stringrays, Fake Base Stations, Drt-Boxes

- **Fake Devices** Simulating a part or complete cellular network
- **Identification** and **Tracking** of mobile devices in the Radio Coverage Area
- **Interception** of mobile User Data and radio Signalling Data
- **Downgrade** mobile users to lower generation networks(Weaker)
- Battery Drain
- DoS

# Introduction

## IMSI Catchers, Stringrays, Fake Base Stations, Drt-Boxes

- **Fake Devices** Simulating a part or complete cellular network
- **Identification** and **Tracking** of mobile devices in the Radio Coverage Area
- **Interception** of mobile User Data and radio Signalling Data
- **Downgrade** mobile users to lower generation networks(Weaker)
- Battery Drain
- DoS

# Introduction

## IMSI Catchers, Stringrays, Fake Base Stations, Drt-Boxes

- **Fake Devices** Simulating a part or complete cellular network
- **Identification** and **Tracking** of mobile devices in the Radio Coverage Area
- **Interception** of mobile User Data and radio Signalling Data
- **Downgrade** mobile users to lower generation networks(Weaker)
- Battery Drain
- DoS

# Introduction

## IMSI Catchers, Stringrays, Fake Base Stations, Drt-Boxes

- **Fake Devices** Simulating a part or complete cellular network
- **Identification** and **Tracking** of mobile devices in the Radio Coverage Area
- **Interception** of mobile User Data and radio Signalling Data
- **Downgrade** mobile users to lower generation networks(Weaker)
- Battery Drain
- DoS

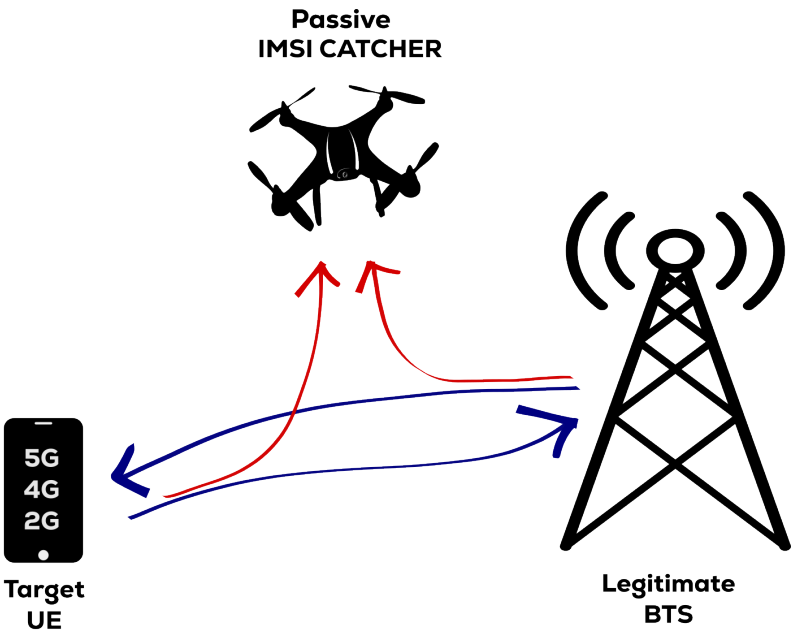
# Introduction

## IMSI Catchers Types

- **Passive**
  - Does not **Interact** with mobile phones or networks
  - **Silent** (difficult to detect) to mobile users and networks
- **Active**
  - **Control** mobiles phones as a master-slave architecture (**Interaction**)
  - More powerful
  - **Can Be Detected**

# Introduction

## IMSI Catchers Types

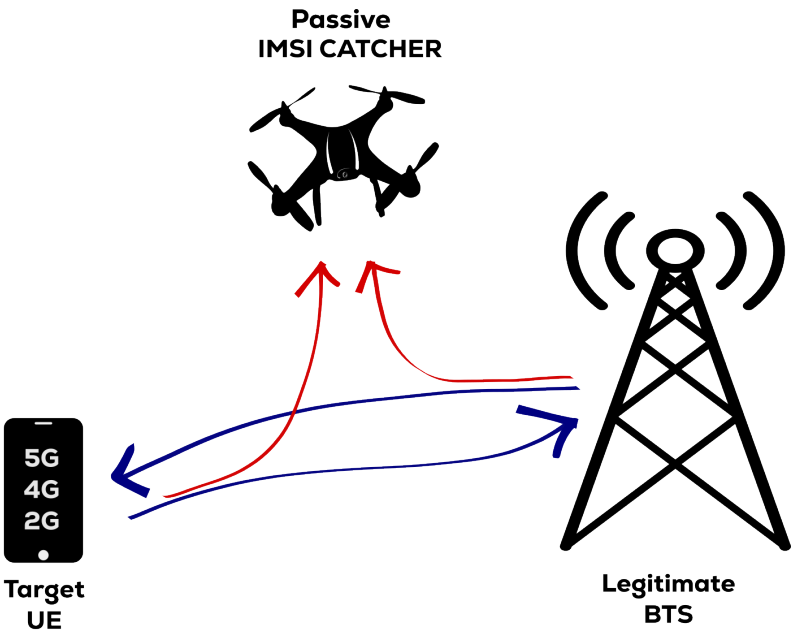



- **Passive**
  - Does not **Interact** with mobile phones or networks
  - **Silent** (difficult to detect) to mobile users and networks

- **Active**
  - **Control** mobiles phones as a master-slave architecture (**Interaction**)
  - More powerful
  - **Can Be Detected**

# Introduction

## IMSI Catchers Types

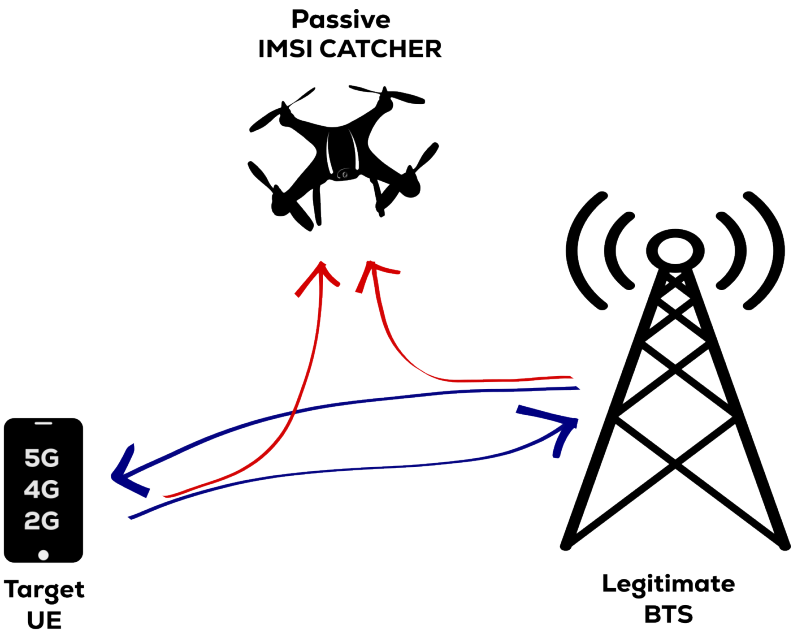



- **Passive**
  - Does not **Interact** with mobile phones or networks
  - **Silent** (difficult to detect) to mobile users and networks

- **Active**
  - **Control** mobiles phones as a master-slave architecture (**Interaction**)
  - More powerful
  - **Can Be Detected**

# Introduction

## IMSI Catchers Types

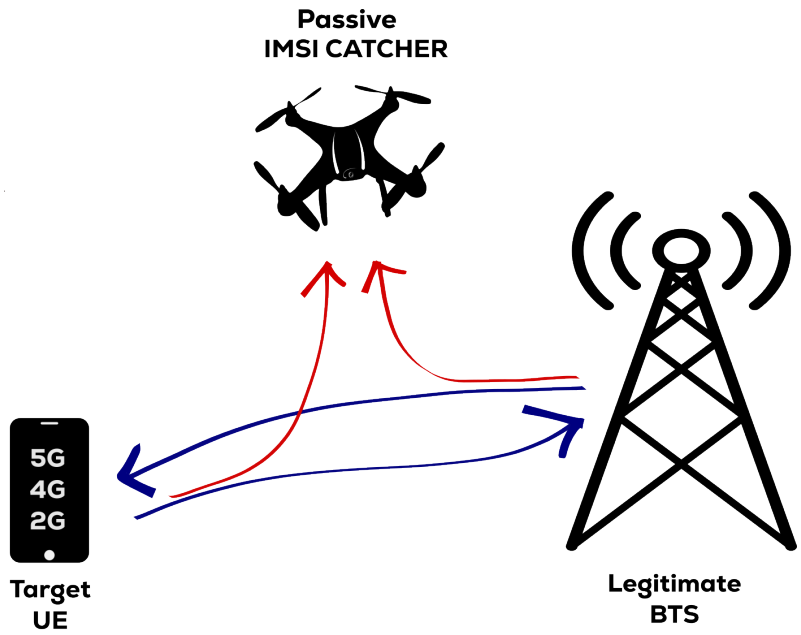


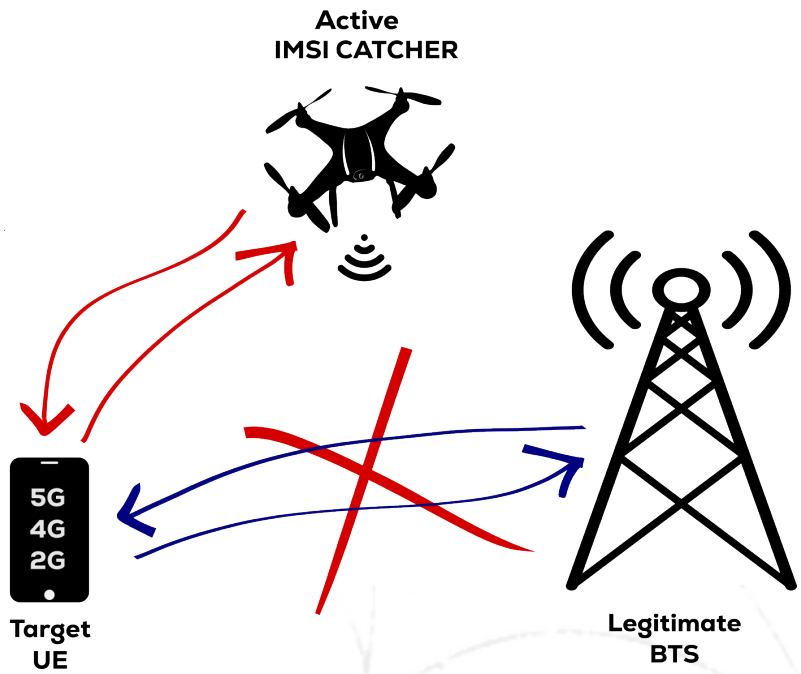

- **Passive**
  - Does not **Interact** with mobile phones or networks
  - **Silent** (difficult to detect) to mobile users and networks

- **Active**
  - **Control** mobiles phones as a master-slave architecture (**Interaction**)
  - More powerful
  - **Can Be Detected**

# Introduction

## IMSI Catchers Types



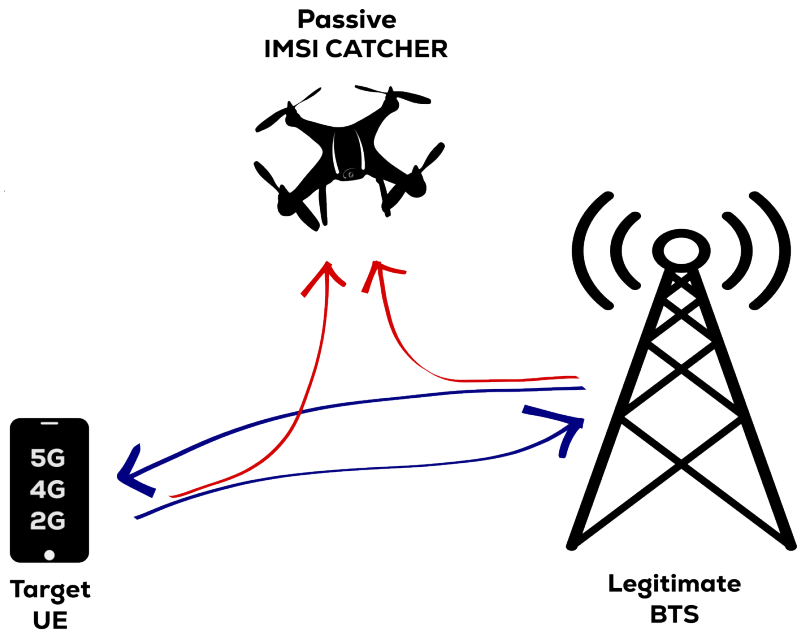



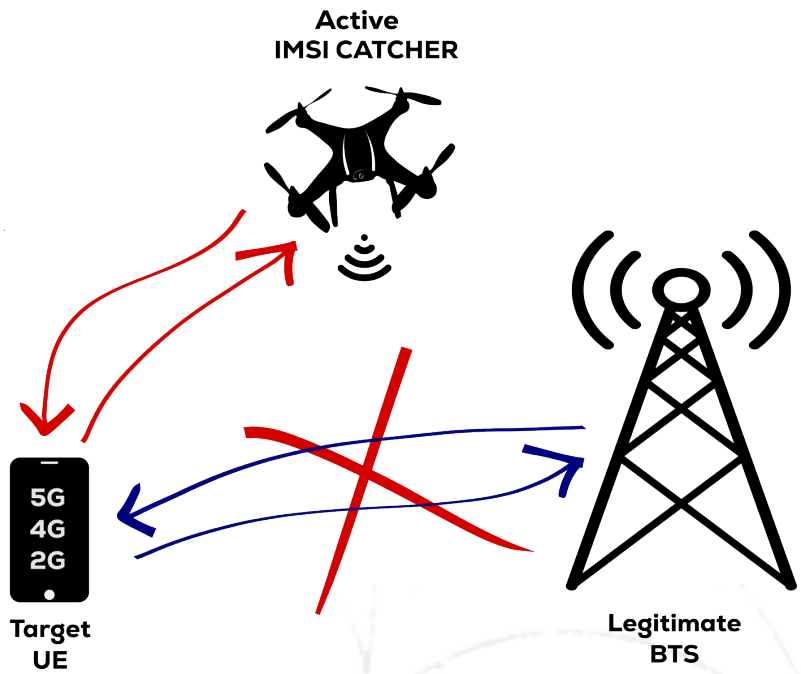

- **Passive**
  - Does not **Interact** with mobile phones or networks
  - **Silent** (difficult to detect) to mobile users and networks

- **Active**
  - **Control** mobiles phones as a master-slave architecture (**Interaction**)
  - More powerful
  - **Can Be Detected**

# Introduction

## IMSI Catchers Types



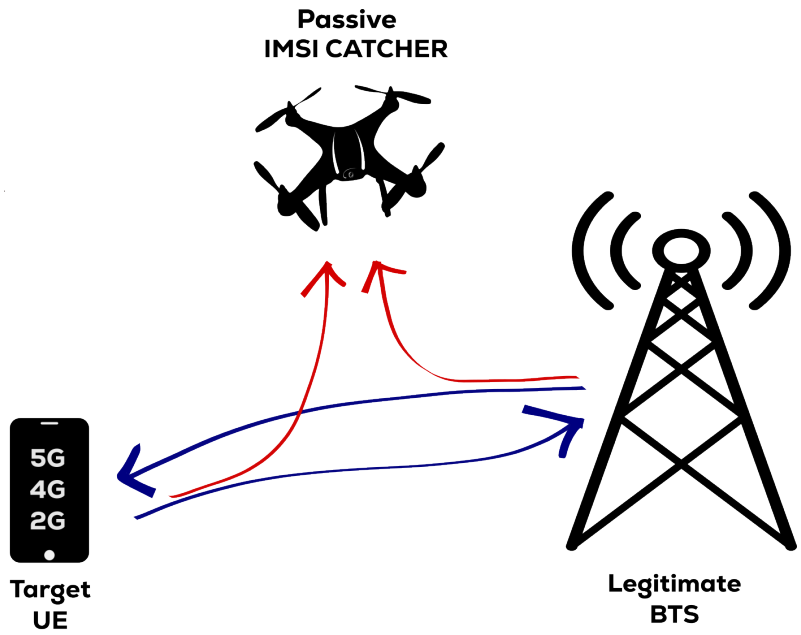



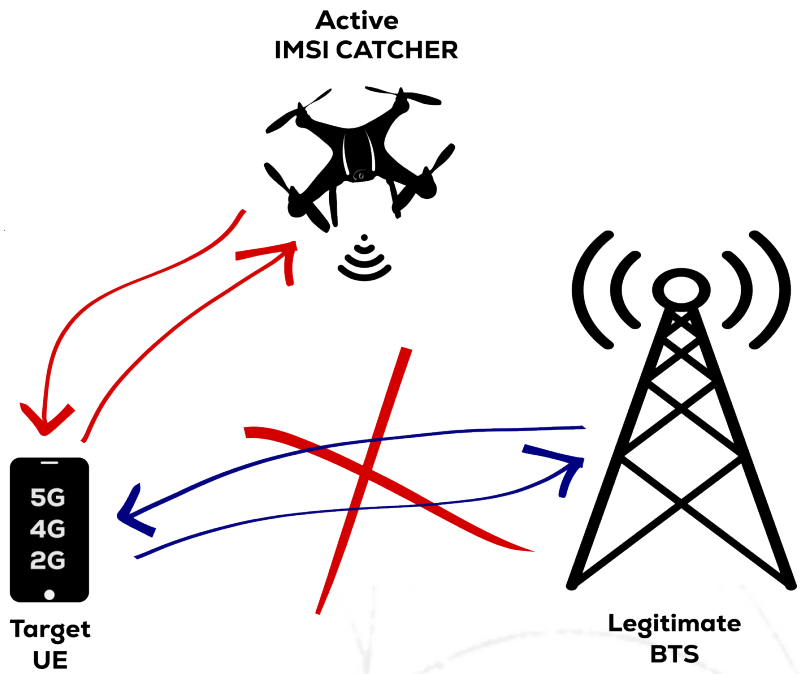

- **Passive**
  - Does not **Interact** with mobile phones or networks
  - **Silent** (difficult to detect) to mobile users and networks

- **Active**
  - **Control** mobiles phones as a master-slave architecture (**Interaction**)
  - More powerful
  - **Can Be Detected**

# Introduction

## IMSI Catchers Types



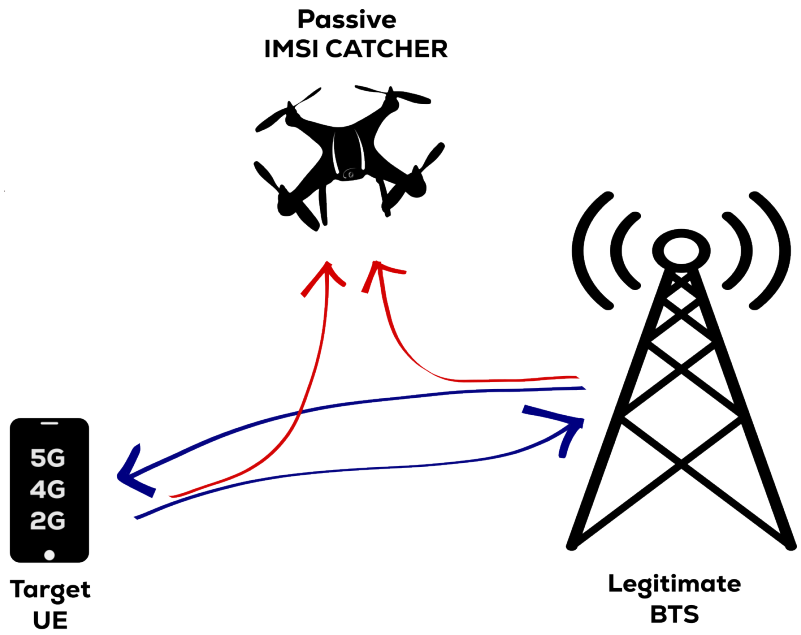



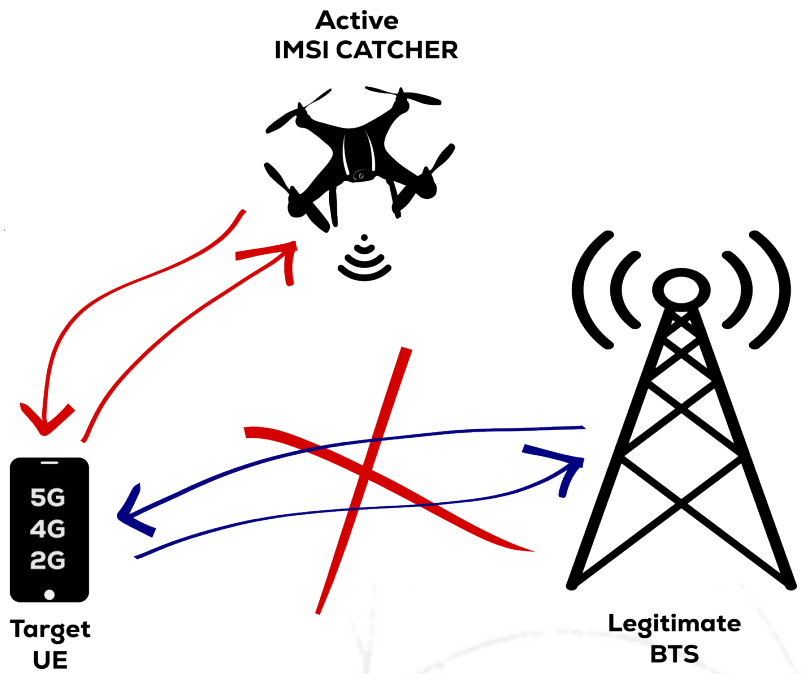

- **Passive**
  - Does not **Interact** with mobile phones or networks
  - **Silent** (difficult to detect) to mobile users and networks

- **Active**
  - **Control** mobiles phones as a master-slave architecture (**Interaction**)
  - More powerful
  - **Can Be Detected**

# Introduction

## IMSI Catchers Types



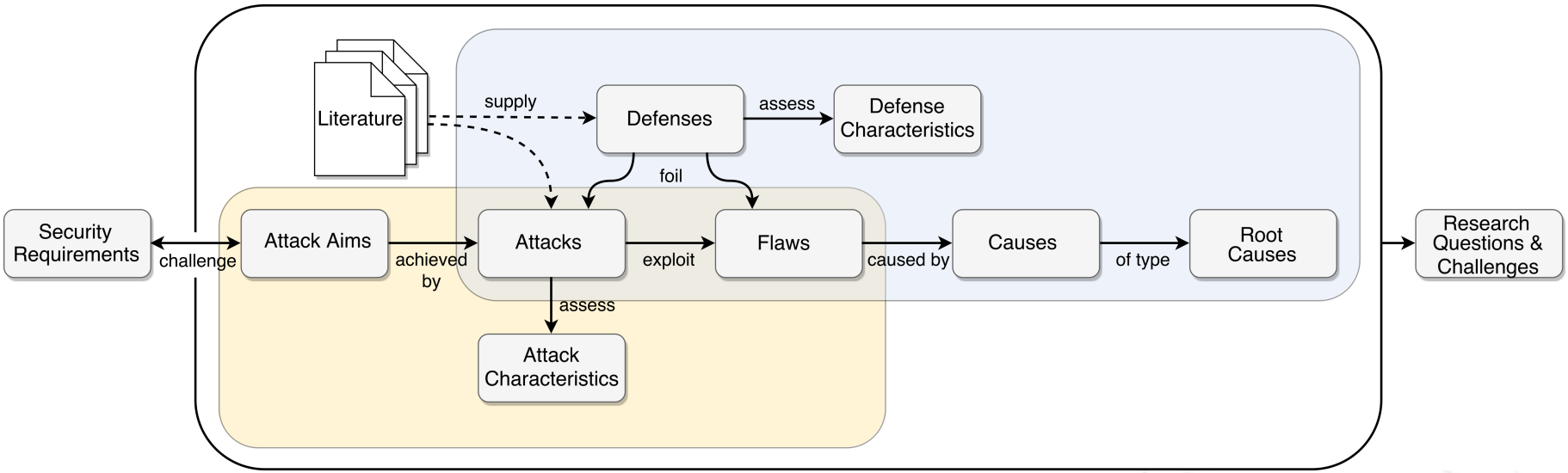




- **Passive**
  - Does not **Interact** with mobile phones or networks
  - **Silent** (difficult to detect) to mobile users and networks

- **Active**
  - **Control** mobiles phones as a master-slave architecture (**Interaction**)
  - More powerful
  - **Can Be Detected**

# Methodology of Systemization

## The Way We Think




**Systematization Methodology Applied Throughout This Work.**[1]

[1] David Rupprecht et al. "On Security Research Towards Future Mobile Network Generations". In: *IEEE Communications Surveys Tutorials* (2018).

# Methodology of Systemization

## Attacks By Their Aim

| Aim | Attack | Attacker Capabilities | | Target | | Technology | | | | Range |
|---|---|---|---|---|---|---|---|---|---|---|
| | | Passive | Active | User | Network | 2G | 3G | 4G | 5G | |
| Privacy | Unauthenticated IMSI Request (IMSI Catcher)[2] | ● | ● | ✓ | ✗ | ● | ● | ● | ? | Cell |
| Privacy | Unauthenticated IMEI Request[3] | ● | ● | ✓ | ✗ | ● | ● | ○ | ? | Cell |
| Privacy | Location/Tracking Area not Allowed (Downgrade)[4] | ● | ● | ✓ | ✗ | ○ | ● | ● | ? | Cell |
| Privacy | Measurement Reports Localization [2] | ● | ● | ✓ | ✗ | ○ | ○ | ● | ? | Cell |
| Secrecy | MitM IMSI Catcher | ● | ● | ✓ | ✗ | ● | ○ | ○ | ? | Cell |
| Fraud | Fake Base Station SMS Spam[5] | ● | ● | ✓ | ✗ | ● | ◐ | ○ | ? | Cell |

**Categorization Of Attacks By Their Aim.**

● yes, applicable, needed for attack
◐ partially/supportive/optional
○ no, not applicable, or does not apply

? property unknown

[2] A Shaik et al. "Practical attacks against privacy and availability in 4G/LTE mobile communication systems". In: *NDSS*. 2017.

[3] Stig F Mjølsnes and Ruxandra F Olimid. "Easy 4G/LTE IMSI catchers for non-programmers". In: *Computer Network Security*. 2017.

[4] Wanqiao Zhang and Haoqi Shan. "LTE redirection: Forcing targeted LTE cellphone into unsafe network". In: *Proc. Defcon*. 2016.

[5] Zhenhua Li et al. "FBS-Radar: Uncovering Fake Base Stations at Scale in the Wild.". In: 2017.

# Methodology of Systemization

## Causes and Root Causes

| Root Cause | Cause | Attack |
|---|---|---|
| Specification Issue | Unsecured Pre-Authentication Traffic | Location/Tracking Area not Allowed (Downgrade) |
| | | Measurement Reports Localization |
| | | Unauthenticated IMEI Request |
| | | Unauthenticated IMSI Request (IMSI Catcher) |
| | Non-Existing Mutual Authentication | MitM IMSI Catcher |
| | | Fake Base Station SMS Spam |
| | Weak Cryptography | |
| | Resource Usage Asymmetry | |
| | Insecure Inter-Network Protocol | |
| Implementation Issue | Insecure Implementation | |
| | Leaky Implementation | |
| Protocol Context Discrepancy | Cross-Layer Information Loss | |
| | Accounting Policy Inconsistency | |
| Wireless Channel | Channel Characteristics | |

**Categorization of Attacks By Their Root Cause[6].**

[6] Rupprecht et al., "On Security Research Towards Future Mobile Network Generations".

# Solution

## Challenges And Research Questions

| Cause | Detect | | Mitigation | Challenges | Research Questions |
|---|---|---|---|---|---|
| | User Side | Network Side | | | |
| **Unsecured Pre-Authentication Traffic** | 1. Smartphone App<br>2. Baseband Firewalls | Network Structure | Protocol Change | Non-Backward-Compatible | Abandoning pre-authentication |
| **Non-Existing Mutual Authentication** | 1. Smartphone App<br>2. Baseband Firewalls<br>3. Content of The SMS | Phase Out GSM | Fixed in 3G, 4G, 5G | The Phone Still "Speak" GSM | Downgrade Protection Scheme |

**Categorization of Defenses.**

# Thank You

## So Much

### Any Questions?