Security

Ryan Abdi

Tarbiat Modares University

Supervised By D. Mokari

https://modares.ac.ir/~nader.mokari

nader.mokari@modares.ac.ir

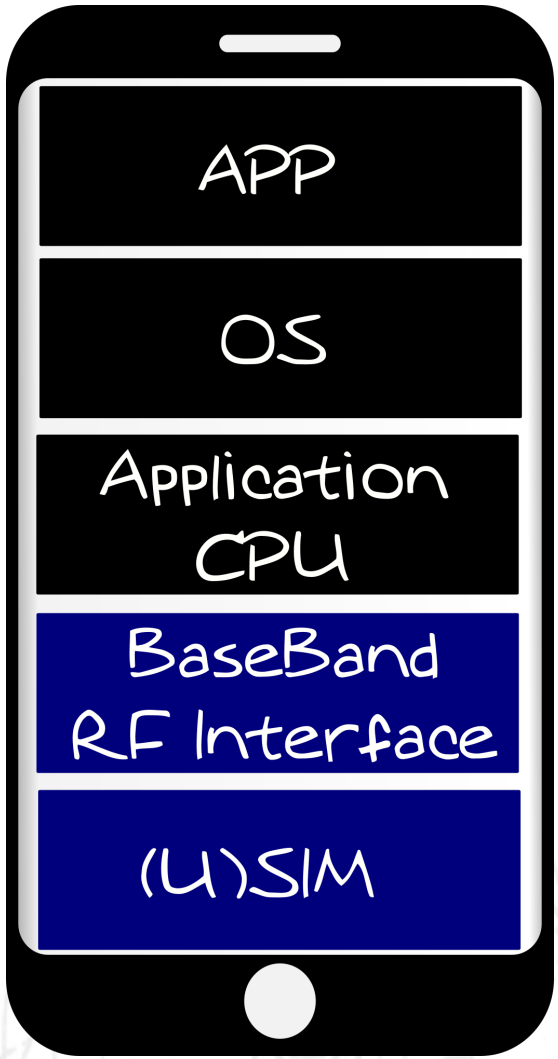
Tarbiat Modares University

Fall 2022

Background

User Equipment (UE)^{4G}

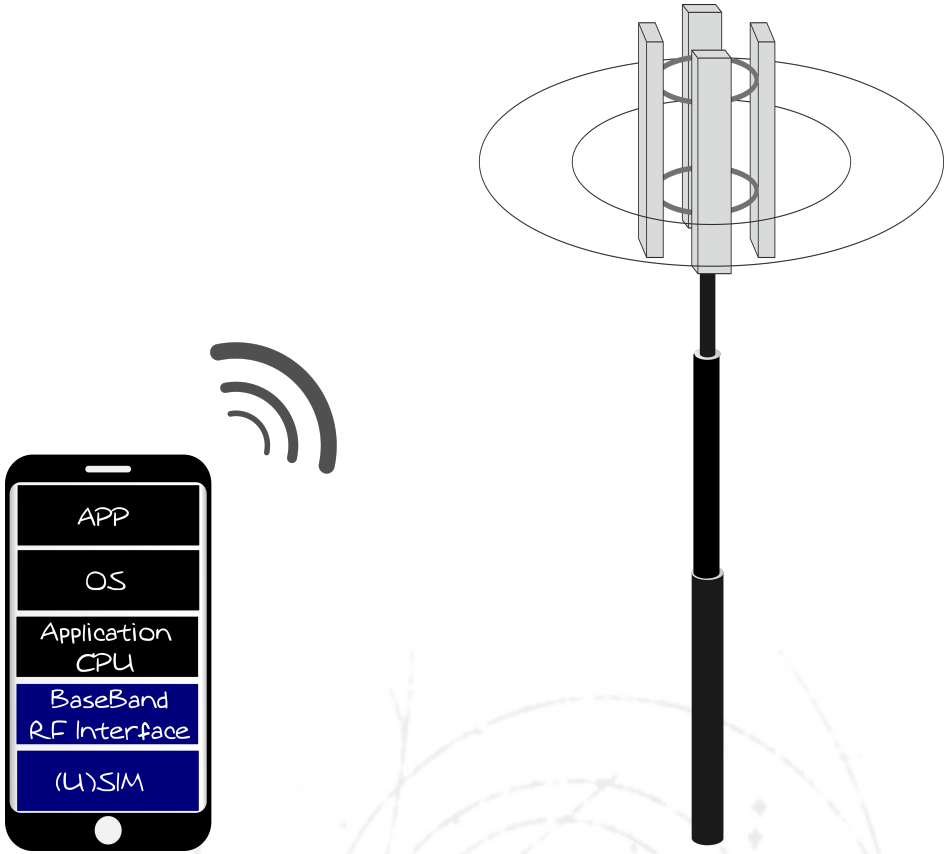
- (UE)^{4G} communicates with the network and consumes its services.
- The baseband processor implements the mobile protocol stacks
- (SIM)^{2G}, (USIM) $^{3G/4G}$
  - identifies a customer
  - stores the authentication information
    - IMSI
    - secret long-term symmetric key used for encryption and authentication
  - People know your MSISDN



Background

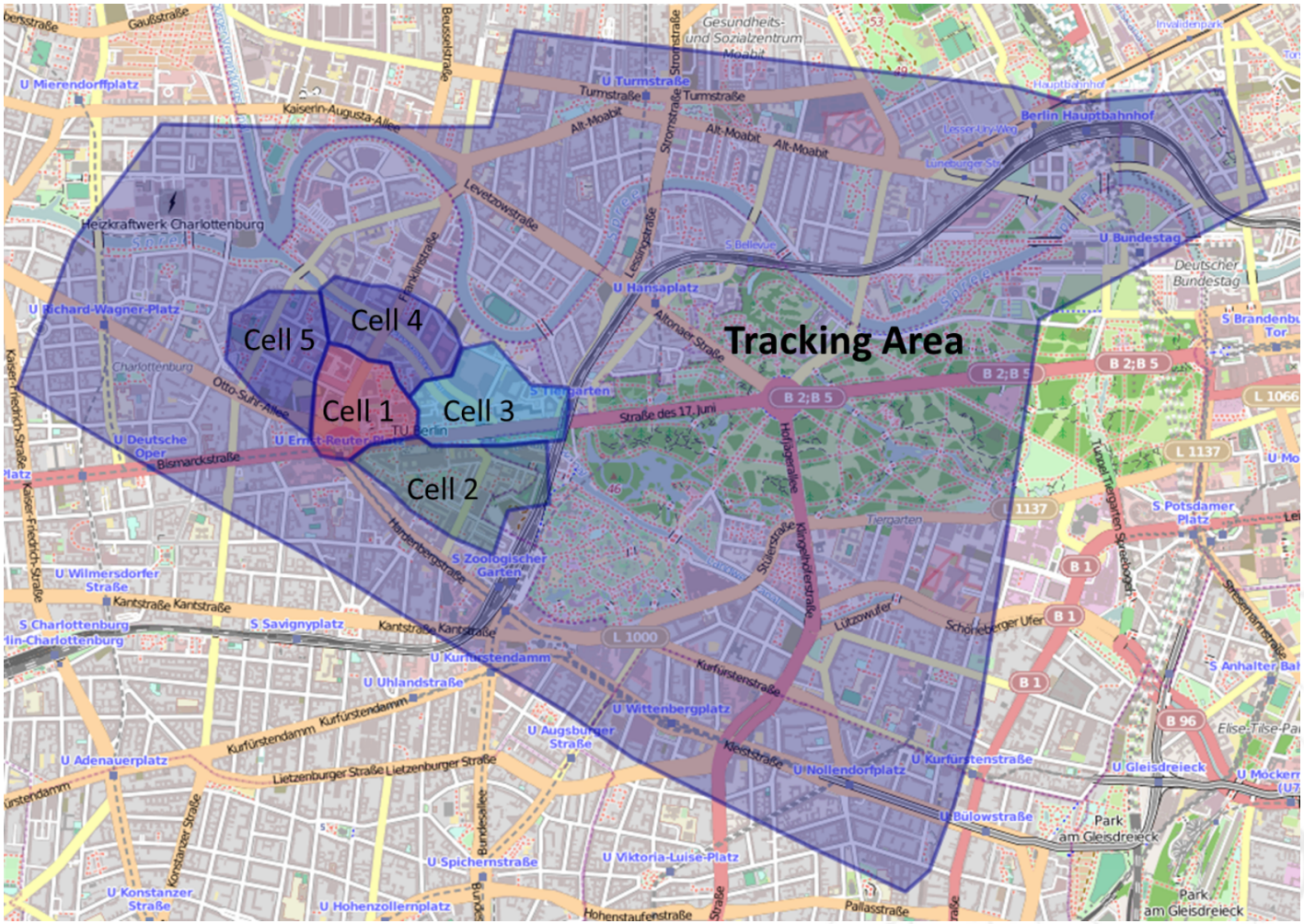
Radio Access Network (RAN)

- Transmits data between the UE and the core network
- (BTS)^{2G}, (nodeB)^{3G}, (enodeB)^{4G}
- For Mobility Management
  - Circuit Switched Services
    - Location Areas (LAs)^{2G,3G}
  - Packet-Switched Services
    - Routing Areas (RAs)^{2G,3G}
    - Tracking Areas (TAs)^{4G}



Background

Tracking Areas in a city



Background

Core Network (CN)

- Delivering the services (e. g., phone calls and Internet connection)
- Manages the connection mobility
  - Several core network elements are utilized
    - $(HLR)^{2G}$, $(HSS)^{3G,4G}$: Its security functionality is often referred as Authentication Center (AuC)
- Security Establishment

Background

Inter Network

Many services require a connection to other communication networks:

- Public Switched Telephone Network (PSTN)
- Internet
- Other Mobile Networks
  - SS7/Diameter:
    - Roaming
    - Text messages
    - Call forwarding

Background

Radio Channels

Three main types of logical channels:

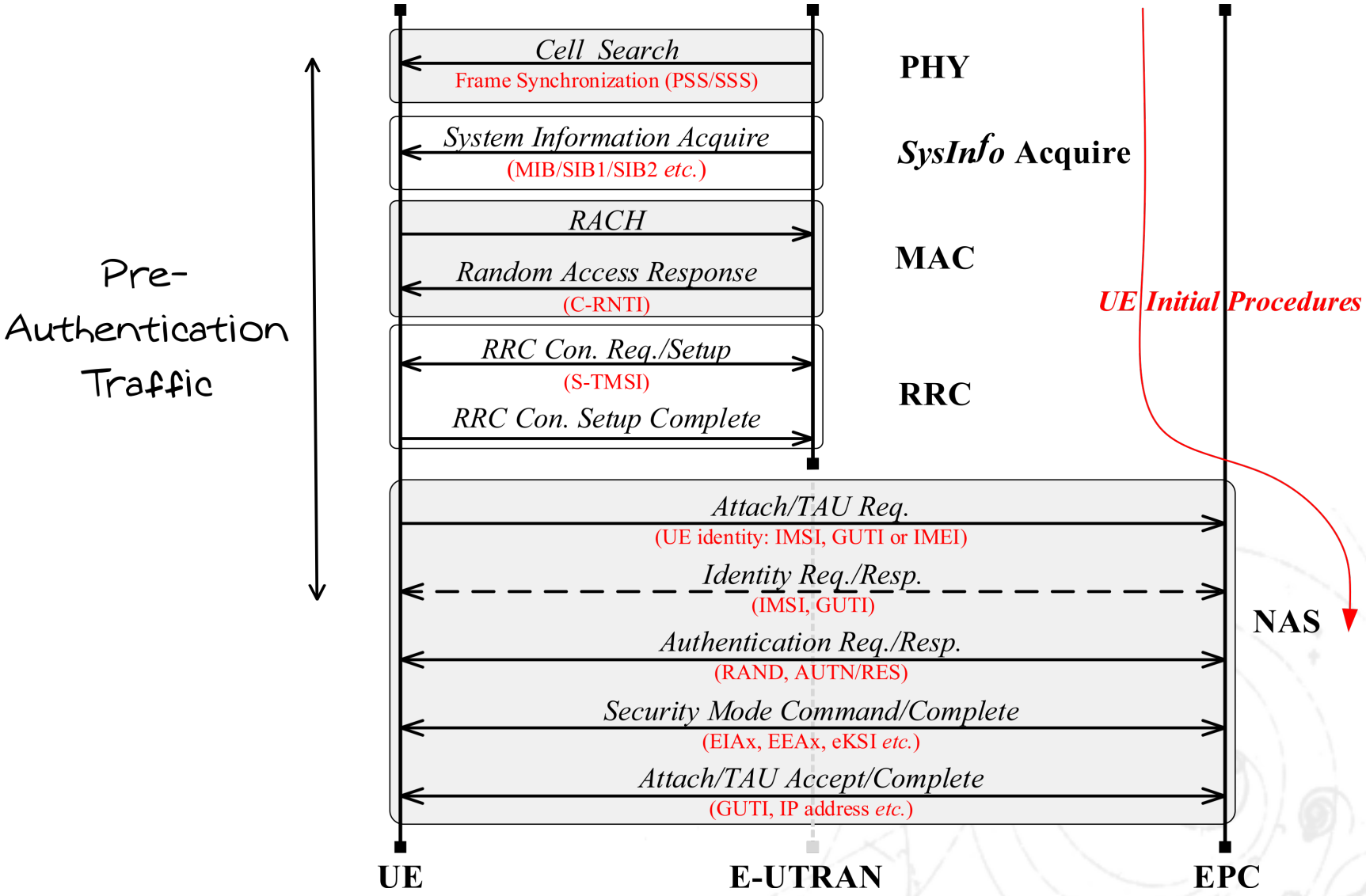
- Broadcast control channels
  - Information about serving Base station
  - Information about Neighbors
  - Information about Network Configuration
- Paging channels
  - Calling out a specific UE for sending traffic to
- Dedicated channels
  - Are used for traffic to and from each single device

Encryption and Integrity

If initiated by the network $\rightarrow$ Only Dedicated Channels

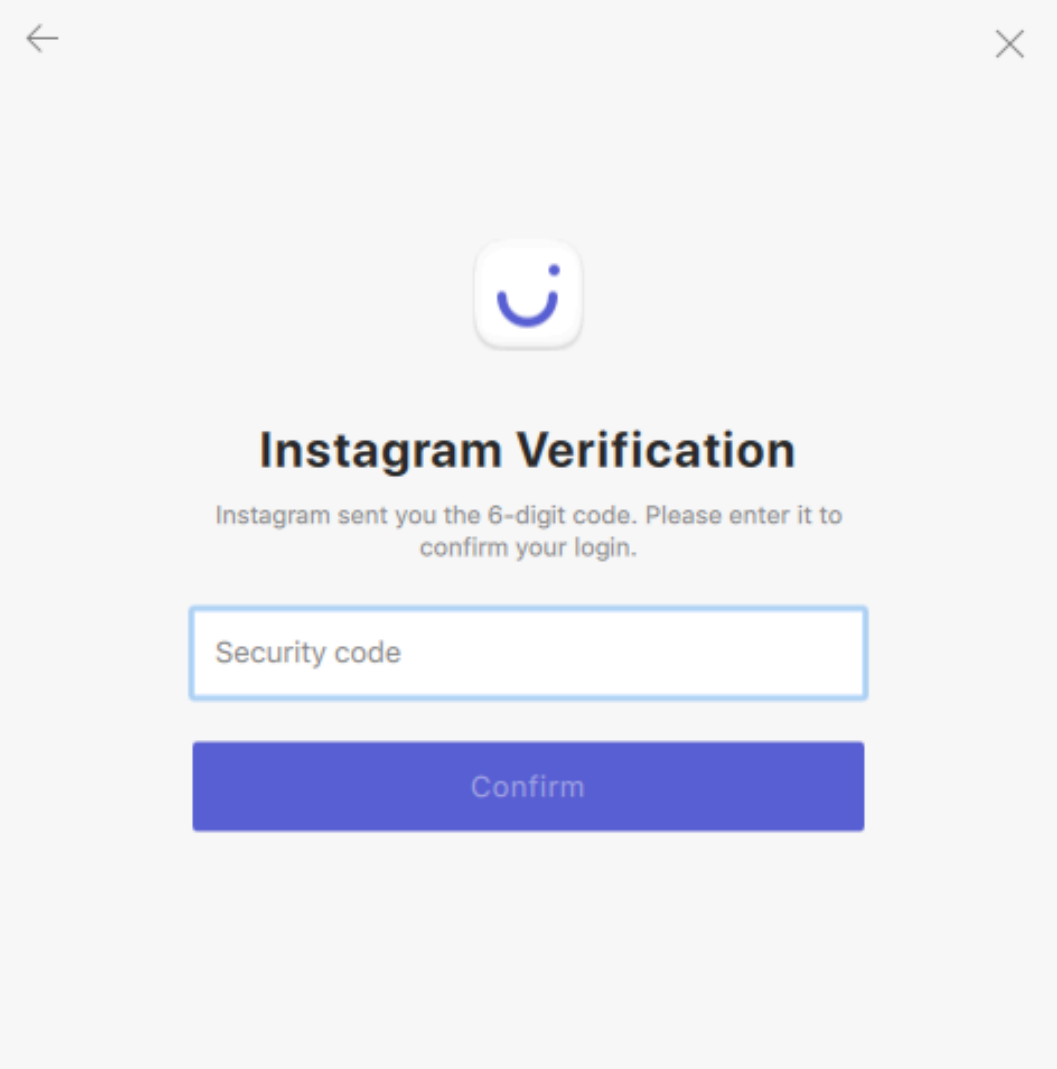
Background

What is Pre-Authentication Traffic?



Background

What is Authentication Traffic?



Background

Pre-Authentication Traffic and Security Establishment

Definition

All traffic that happens before the setup of an authenticated session is defined as pre-authentication traffic.

- Paging, other broadcasts, most of the radio resource allocations, and low-level signaling traffic are always unprotected
- GSM only establishes user authentication
- UMTS, LTE establish mutual authentication

Background

Mobility Management and Paging - Part i

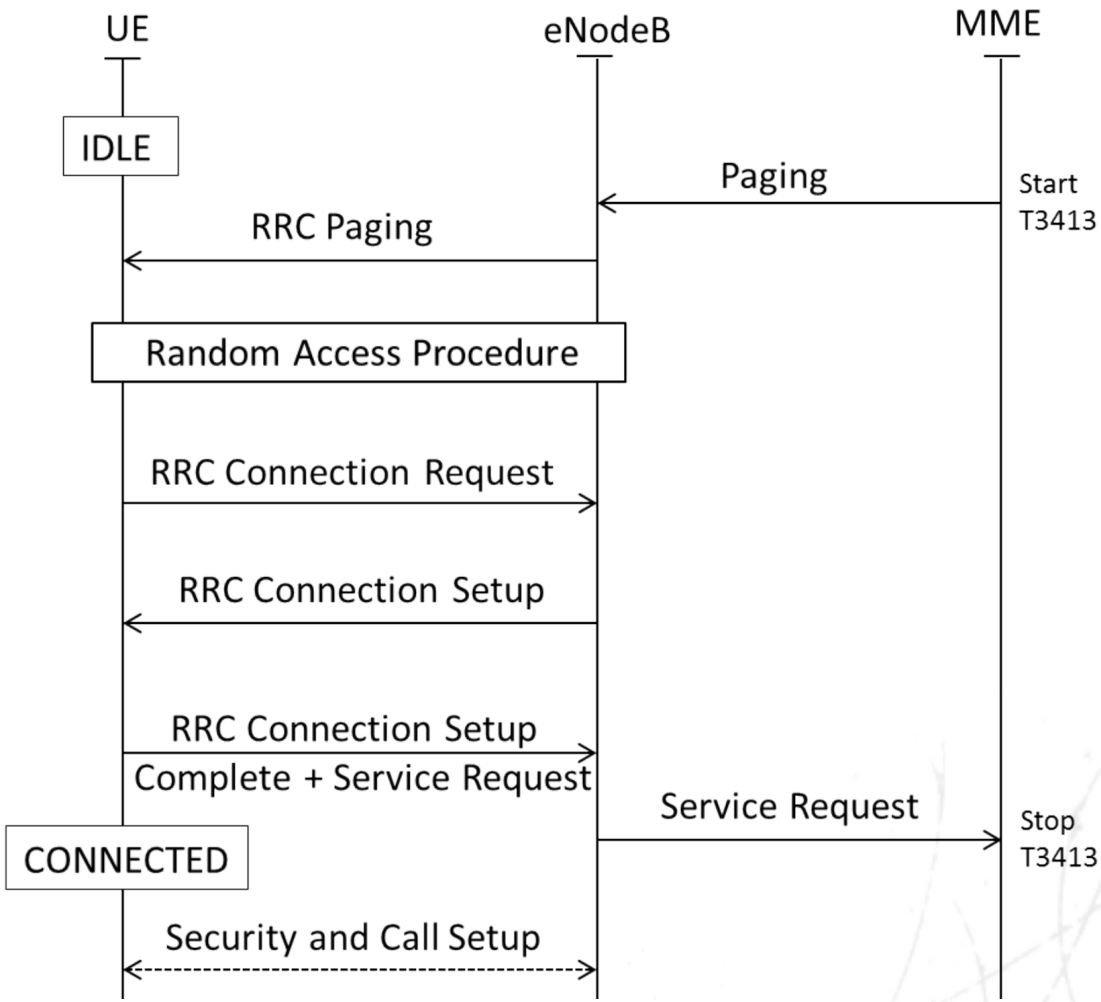
Definition

When no active data transmission or phone call is ongoing, the phone goes into the idle state.

- The network only knows the coarse Location Area
- The phone listens to the paging channel
  - incoming phone call
  - message
  - Typing notifications (WhatsApp, Telegram)!
- Paging message $\rightarrow$ UE contacts Network

Background

Mobility Management and Paging - Part i- example



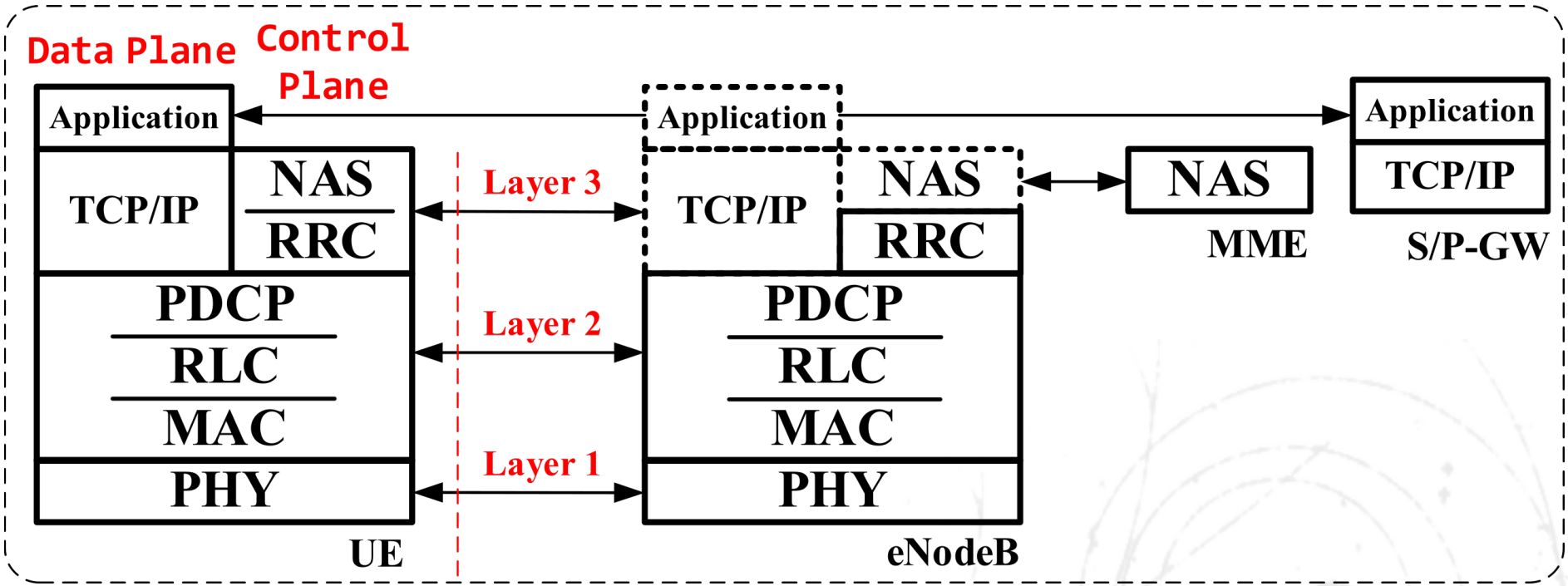
Location Update Request

Inters a different Location Area $\rightarrow$ MS sends a LUR

- Periodic location updates (typically every 24h)
- (Routing Area Update)^{2G,3G}
- (Tracking Area Update)^{4G}

Background

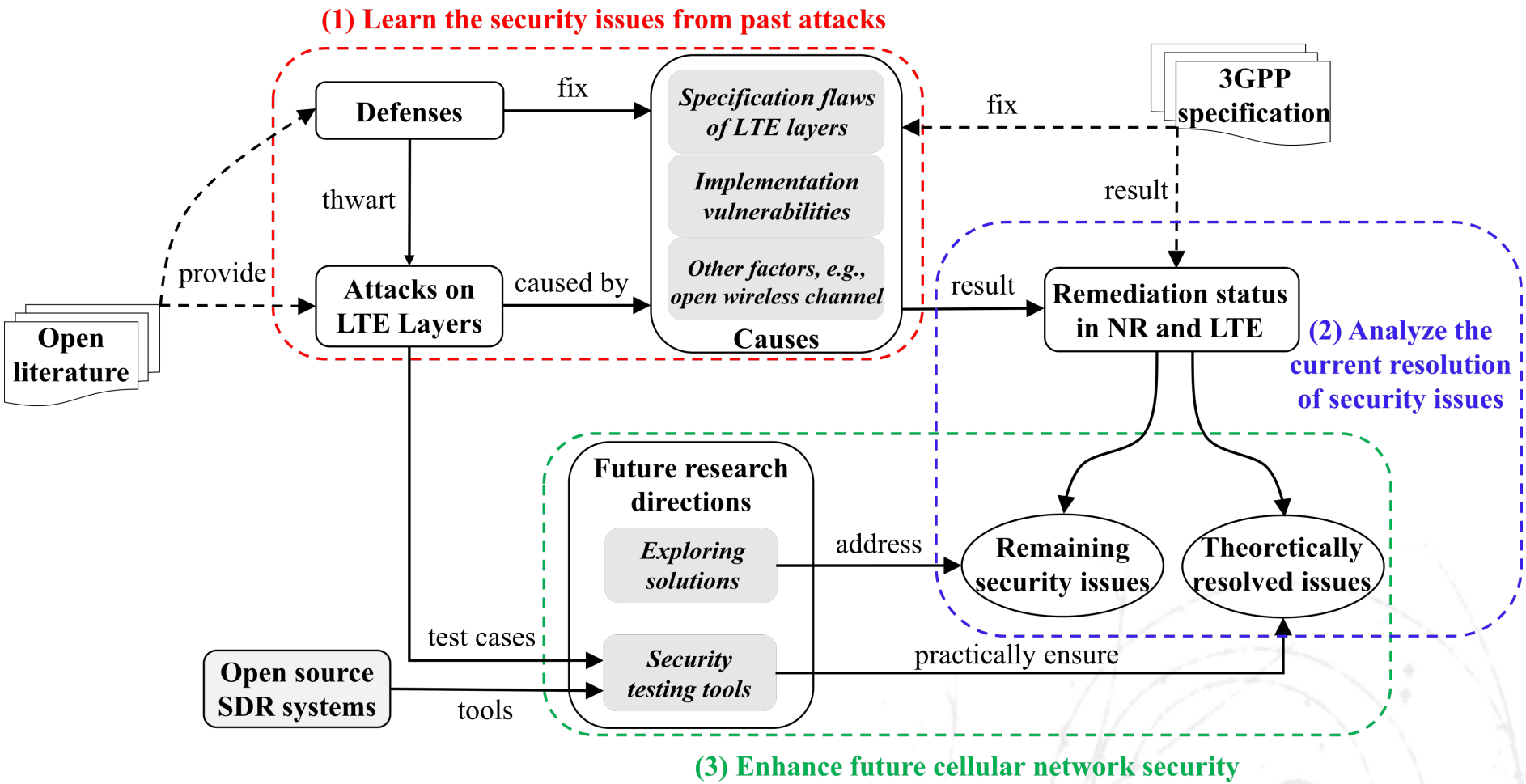
LTE Layers[1]



[1] Yu et al., "Improving 4G/5G air interface security: A survey of existing attacks on different LTE layers".

METHODOLOGY OF SYSTEMATIZATION

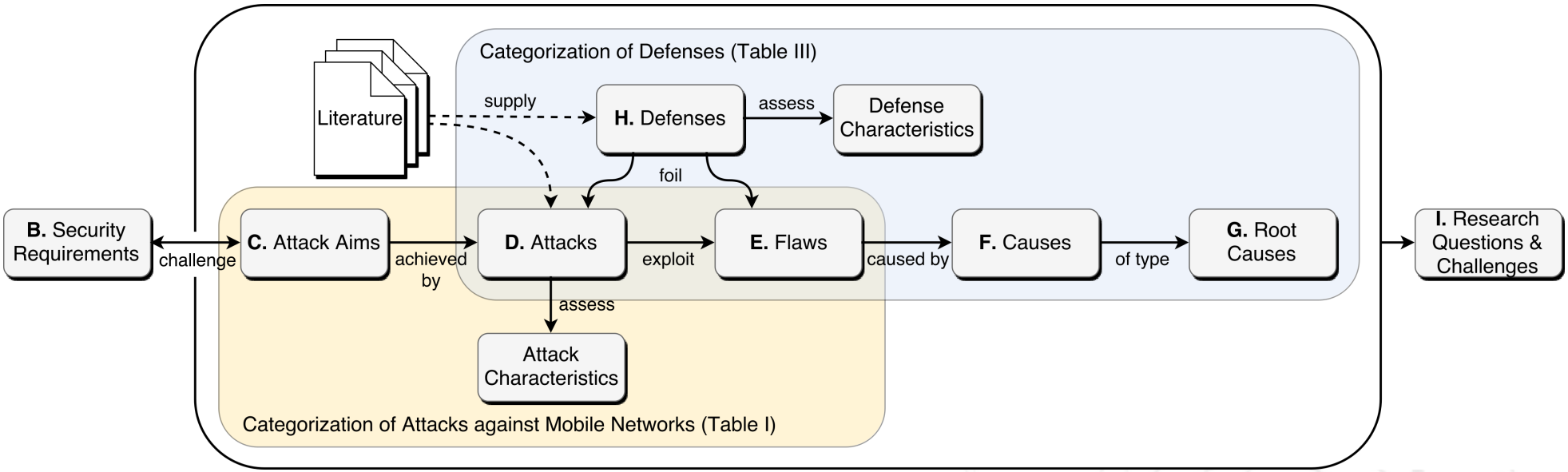
Method i[2]



[2]Yu et al., "Improving 4G/5G air interface security: A survey of existing attacks on different LTE layers".

METHODOLOGY OF SYSTEMATIZATION

Method ii[3]



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

METHODOLOGY OF SYSTEMATIZATION

Method ii- Example

Definition

Radio Measurement Reports can be requested by a base station without authentication

Radio Measurement Report Request Attack

attack can pinponit a victim

- Security Requirement $\rightarrow$ Location Confidentiality
- Attack Aim $\rightarrow$ User's Privacy
- Flaw $\rightarrow$ requests for Radio Measurement Reports are part of the unsecured pre-authentication traffic
- Cause $\rightarrow$ existing of pre-authentication traffic
- Root Cause $\rightarrow$ lies in Specifications

METHODOLOGY OF SYSTEMATIZATION

Method ii- Example - explained

METHODOLOGY OF SYSTEMATIZATION

Method ii- Example Continued ...

How to Defend against this specific attack?

1. This specific request to be authenticated

But ...

Pre-authentication traffic will be insecure

2. Eliminate pre-authenticated traffic completely

Open research question

how to develop a **privacy-preserving** specification while keeping the maintainability of mobile networks?

METHODOLOGY OF SYSTEMATIZATION I

Method ii- Security Requirements

- Confidentiality

Definition

- "Absence of unauthorized disclosure of information"[a]
- "the network shall provide several appropriate levels of user privacy including communication confidentiality, location privacy, and identity protection"[b]

---

[a] Avizienis et al., "Basic concepts and taxonomy of dependable and secure computing".

[b] 3GPP, *TS 22.278*.

METHODOLOGY OF SYSTEMATIZATION II

Method ii- Security Requirements

- Availability

Definition

Availability denotes the readiness and the continuity of correct services[a]

[a] Avizienis et al., "Basic concepts and taxonomy of dependable and secure computing".

- System Integrity (Not data or transmission integrity)
  - system integrity focuses on the hard- and software of the network components

METHODOLOGY OF SYSTEMATIZATION III

Method ii- Security Requirements

Definition

Integrity is defined as the absence of unauthorized system alterations[a]

[a] Avizienis et al., "Basic concepts and taxonomy of dependable and secure computing".

- Unauthorized Service Access and Correct Charging

Definition

The service should only be accessible to authorized parties[a]

[a] 3GPP, *TS 22.278*.

Attack Aims I

Method ii- Attack Aims

Each attack aim challenges one of the security requirements

- Attacks on Privacy:
  - Identity protection
  - Location privacy
- Attacks on Secrecy:
  - Communication confidentiality, e.g., the content of the transmission
- Denial of Service:
  - The availability of services, or parts of them.

Or parts of them ...

- Downgrade Attack
- Disabling Security

- Attacks on Integrity
- Fraud Attacks

Attacks I

Method ii- Attacker Capabilities

Definition

Attacks exploit system flaws under the defined attack aims.

What are building blocks of an attacker?

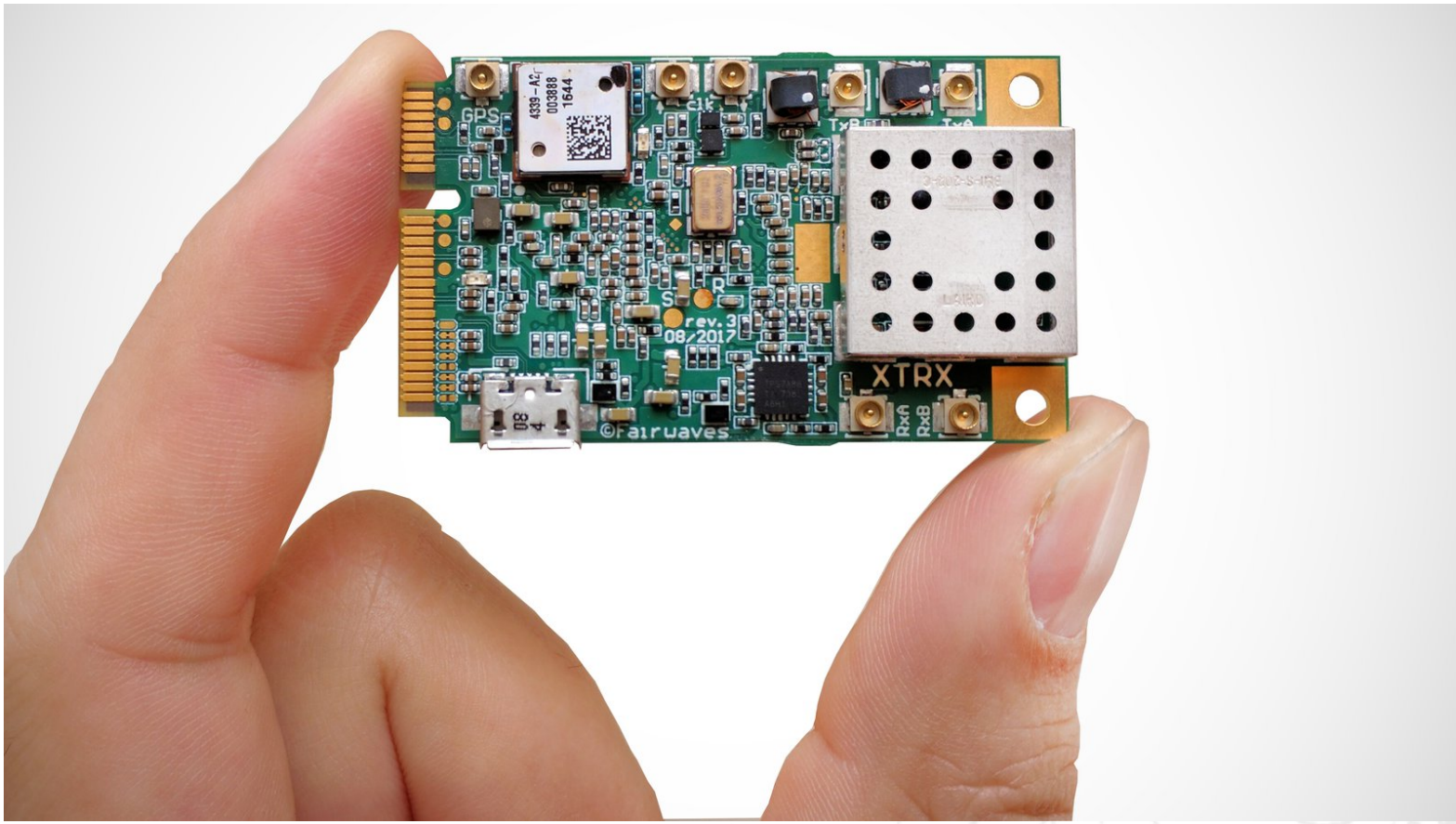
- Passive Radio
  - Can receive
    - Captures Radio Transmission
    - Decodes Signals
    - Reads raw messages
  - Can not Transmit

How's that possible?

Software Defined Radio

Attacks II

Method ii- Attacker Capabilities

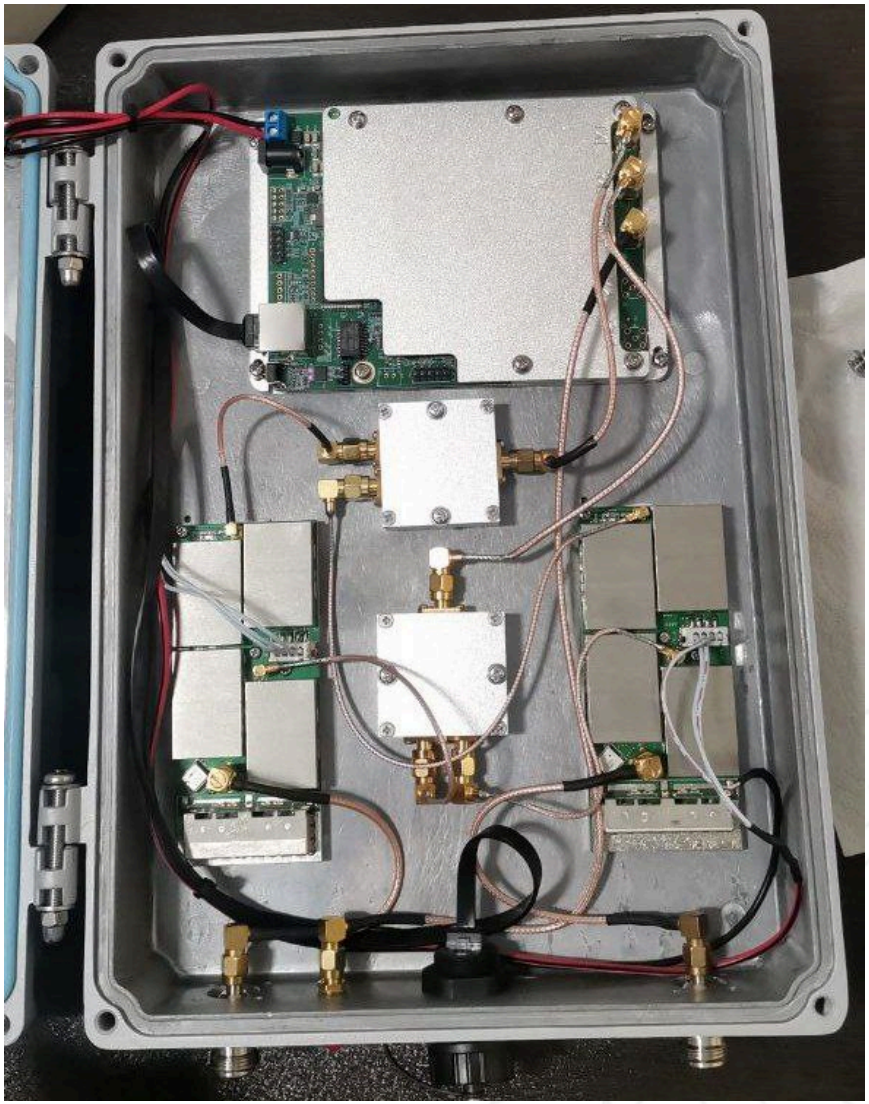


Attacks III

Method ii- Attacker Capabilities

Attacks IV

Method ii- Attacker Capabilities



Attacks V

Method ii- Attacker Capabilities

Attacks VI

Method ii- Attacker Capabilities

- Active Radio
  - Control over radio transmissions
    - Can Transmit
    - Can Receive
- User Traffic
- SS7/Diameter Interface
  - Can send SS7 messages to other networks
  - Some network providers send SS7 access!
- Nondestructive Physical

Definition

A nondestructive-physical attacker temporarily has physical access to the victim's device, but neither destroys nor modifies hardware or software

- PSTN Interface
- Internet Traffic

Attacks I

Method ii- Limitations, Target, Technology, Range

- Limitations of Attacker Capabilities

Betray

Trusted People

- Target
  - who is harmed by the attack?
- Technology

Definition

This category maps the applicability of an attack to the three major access technology generations and assesses if there has been a security development

- Range: indirect indicator of impact and cost

Systematization

Overview

TABLE I
ROOT CAUSES RELATED TO CAUSES

Root Cause	Cause
Specification Issue	Unsecured Pre-Authentication Traffic
	Non-Existing Mutual Authentication
	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

Root Cause: Specification Issue

Definition

Specifications ensure the interoperability between implementations by specifying protocols, state machines, and interfaces.

However

Issues in the specification $\rightarrow$ Flaws $\rightarrow$ Attack

Root Cause: Specification Issue

Attacks

TABLE II
CATEGORIZATION OF DEFENSES

Attacks	Cause	Root Cause
Fake Base Station SMS Spam Encryption Downgrade MitM IMSI Catcher AKA Protocol Linkability Attack IMSI Paging Attack Location/Tracking Area not Allowed (Downgrade)	Non-Existing Mutual Authentication	TS Issues
Measurement Reports Localization TMSI Deanonymization (Paging Attack) Unauthenticated IMEI Request Unauthenticated IMSI Request (IMSI Catcher) GPS Receiver Denial of Service Paging Response Race DoS	Unsecured Pre-Authentication Traffic	
OTA SIM Card Update Key Reconstruction Inter eNodeB User Plane Key Desynchronization Attack Key Reusage Across Cipher and Network Generations Passive Over-the-Air Decryption of A5/1 and A5/2 SIM Key Extraction via COMP128v1 Cryptoanalysis Weak Key due to Inter-Technology Handover	Weak Cryptography	

Cause: Unsecured Pre-Authentication Traffic

What about pre-authentication traffic?

The signaling traffic prior the security establishment with the AKA protocol is unprotected

- Not encrypted
- Not integrity-protected

Hmmm ...

The phone fully obeys the network, even if the latter is not genuine

Cause: Unsecured Pre-Authentication Traffic

IMSI CATCHER - Examples

Cause: Unsecured Pre-Authentication Traffic I

IMSI CATCHER - Examples

Cause: Unsecured Pre-Authentication Traffic II

IMSI CATCHER - Examples

Cause: Unsecured Pre-Authentication Traffic

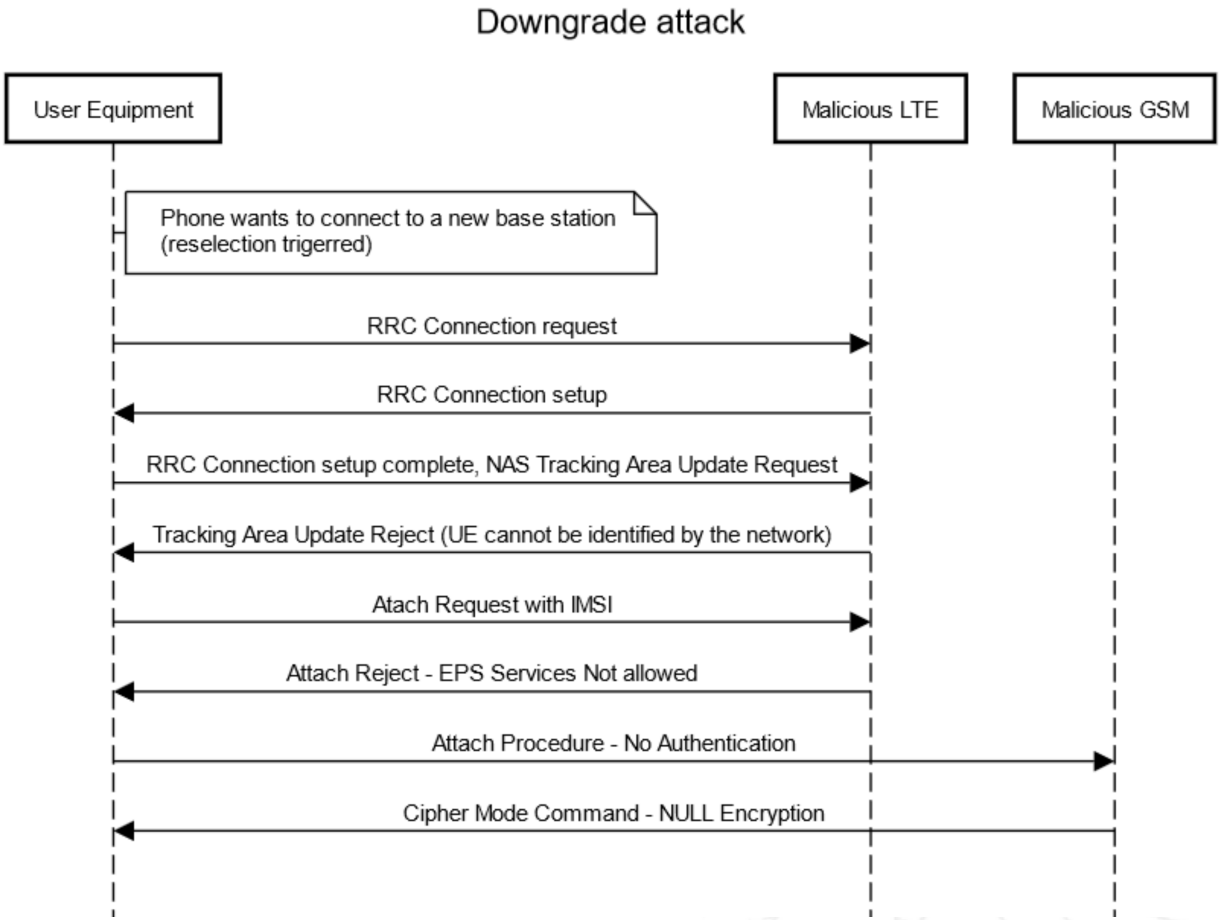
IMSI CATCHER - What is it?

- Active Attack
- Attacker simulates a genuine base station to the phone by broadcasting genuine network identifiers
- Attacker can ask for IMSI, IMEI $\rightarrow$ Challenges User's Privacy (Identity and Location)
- Obtaining User's Location
  - roughly $\rightarrow$ Paging the user
  - almost exact $\rightarrow$ Requesting Measurement Reports

Cause: Unsecured Pre-Authentication Traffic

IMSI CATCHER - Downgrade Attack

(pre-authentication traffic)^{4G} $\rightarrow$ tracking are update reject $\rightarrow$ Denying service on LTE $\rightarrow$ phone camps on a 2G/3G cell



Cause: Unsecured Pre-Authentication Traffic

IMSI CATCHER - Assessment

- An active radio attacker is limited to his/her radio vicinity
- Most of these attacks undermine the victim's data or location privacy
- Many commercially available products exploit unsecured pre-authentication traffic

Cause: Non-Existing Mutual Authentication

Fake Base Station

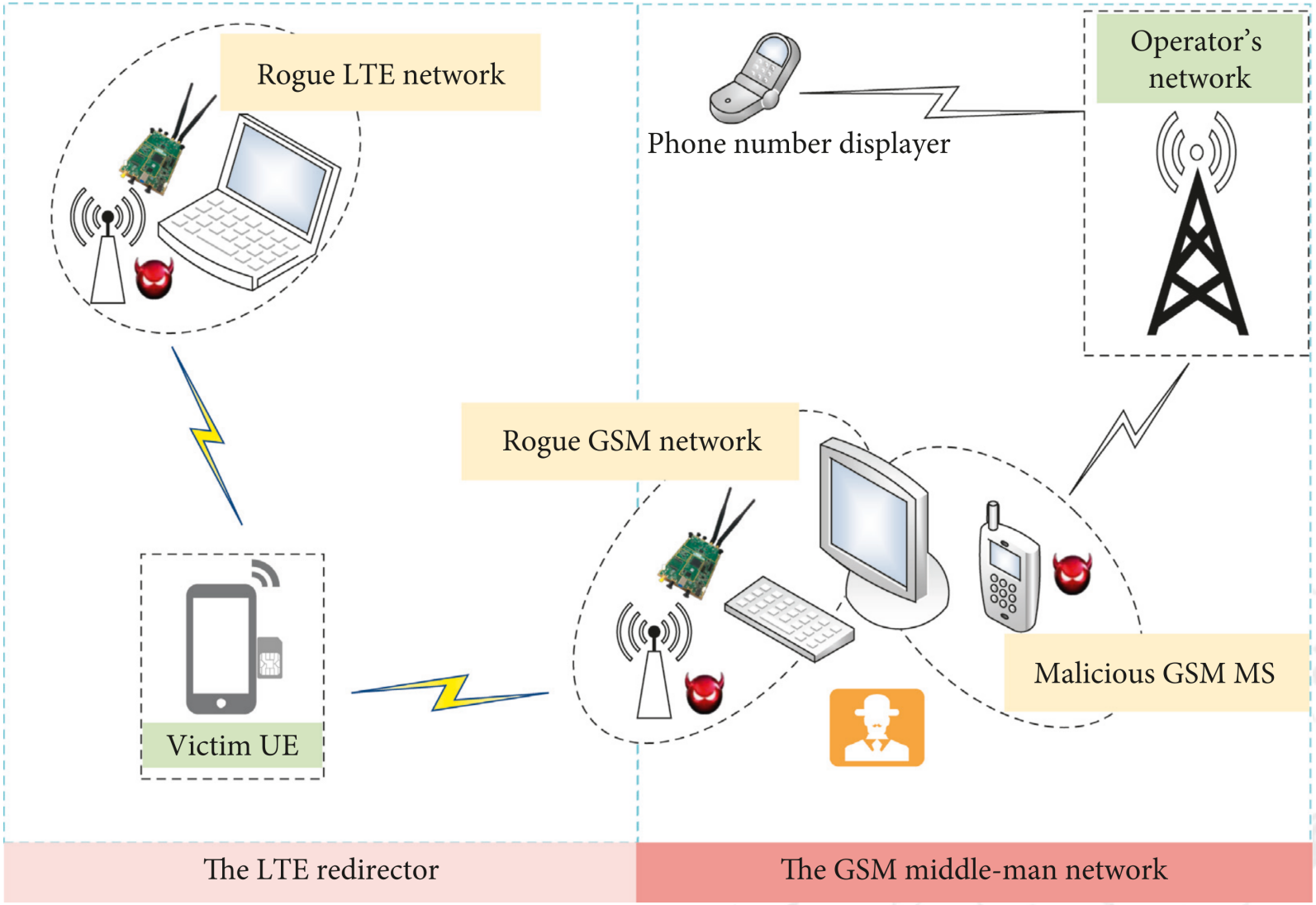
- GSM does not include network authentication → No mutual authentication → MS trusts any network → **MitM is possible**
- GSM include MS authentication

Thank god we have UMTS/LTE

pre-uthenticated traffic → Downgrade to 2G → **MitM** !!!!!

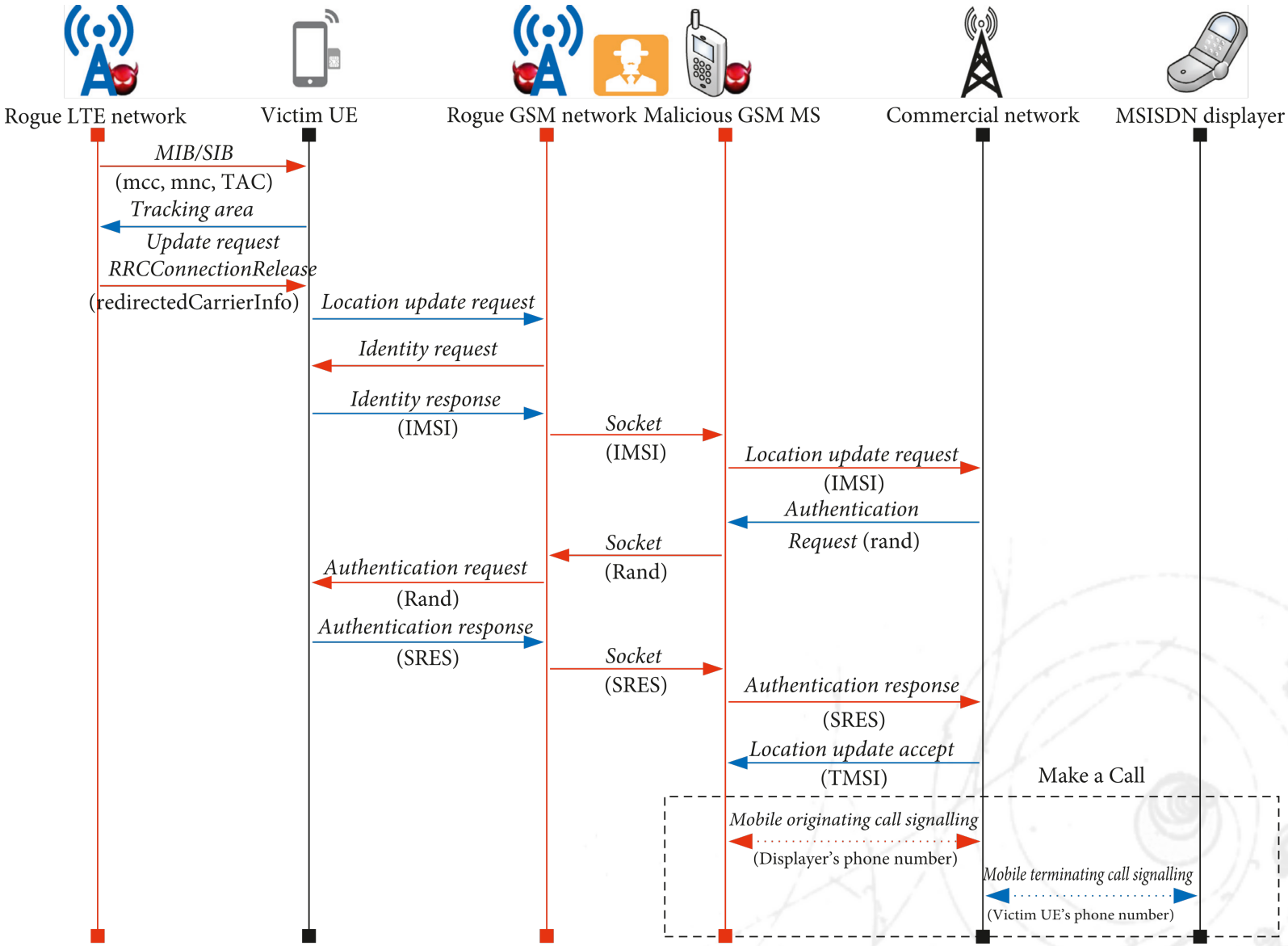
Cause: Non-Existing Mutual Authentication

LTE Phone number Catcher



Cause: Non-Existing Mutual Authentication

LTE Phone number Catcher - Algorithm

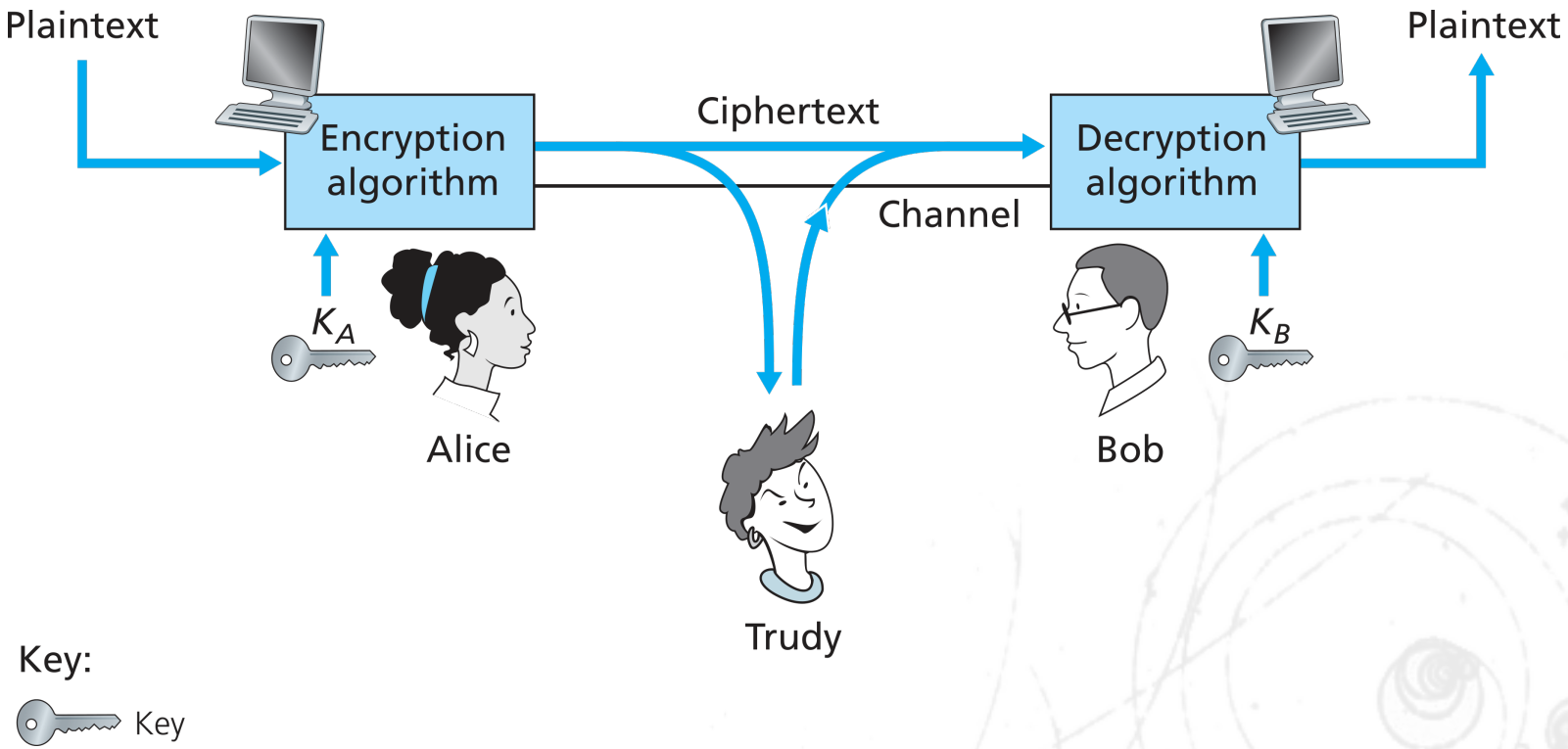


Cause: Weak Cryptography

Introduction

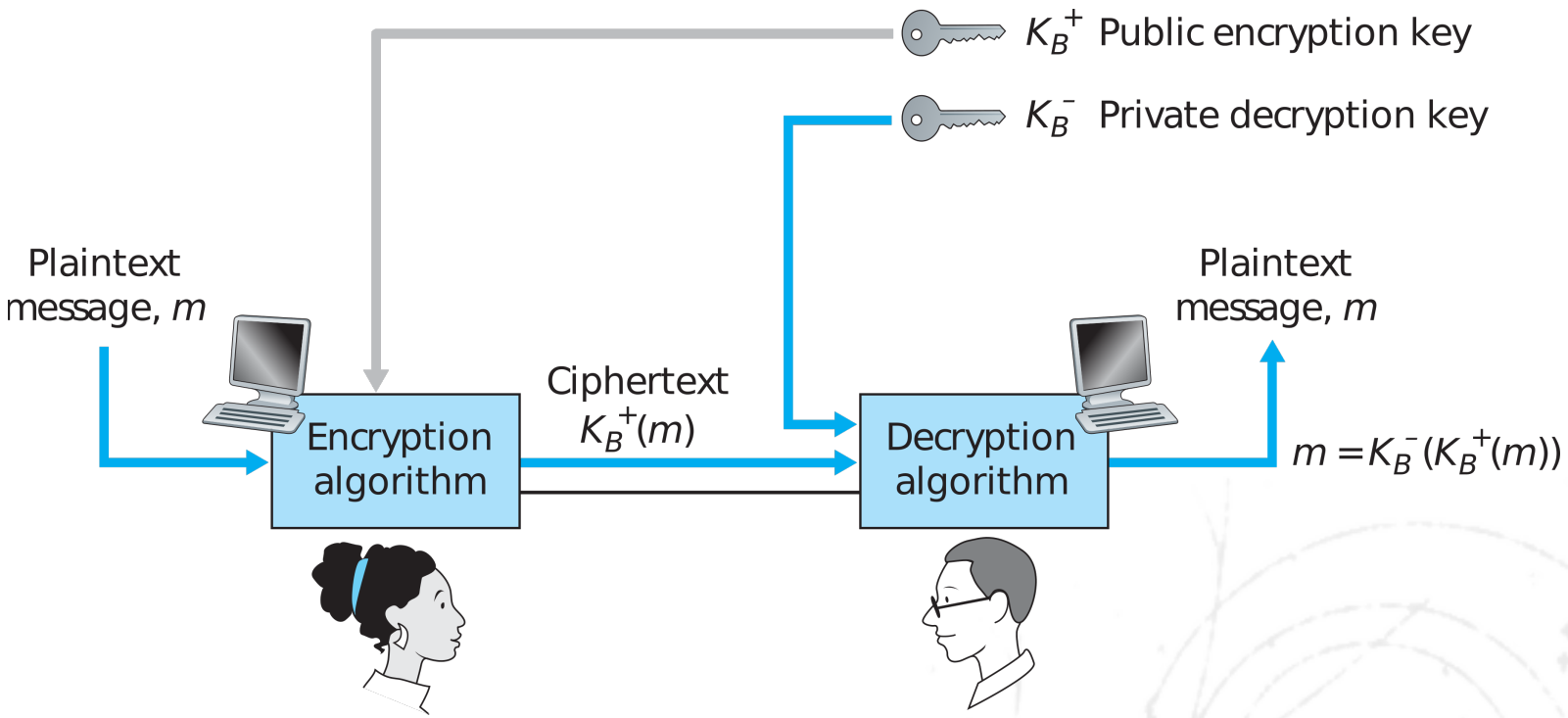
Definition

Cryptography provides the means to achieve data confidentiality



Cause: Weak Cryptography

Public Key



Cause: Weak Cryptography

Attacks

TABLE III
CIPHER OVERVIEW

	Cipher	Type	Effective (nom.) key length	Attackable
2G	A5/0	Null Cipher	–	●
	A5/1 + Comp128v1/2	LFSR-based	54 (64) bits	●
	A5/1 + Comp128v3	LFSR-based	64 bits	●
	A5/2	LFSR-based	40 (64) bits	●
	A5/3	KASUMI	64 bits	◐
	A5/4	KASUMI	128 bits	○
	GEA1	LFSR-based	64 bits	●
	GEA2	LFSR-based	64 bits	●
	GEA3	KASUMI	64 bits	◐
	GEA4	KASUMI	128 bits	○
3G	UEA0	Null Cipher	–	●
	UEA1	KASUMI	128 bits	○
	UEA2	SNOW 3G	128 bits	○
4G	EEA0	Null Cipher	–	●
	EEA1	SNOW 3G	128 bits	○
	EEA2	AES	128 bits	○
	EEA3	ZUC	128 bits	○

○ not attackable ● attacks with commodity hardware known
◐ attacks known, but not practicable or not demonstrated

Take Aways

Hold it tight

- When you see the E,G sign $\rightarrow$ don't call your lawyer!
- If you're an important person $\rightarrow$ You're not safe!
- If you're Person of Interest $\rightarrow$ Get rid of the battery!

References I

- 3GPP. *Service requirements for the Evolved Packet System (EPS)*. publisher: 3rd Generation Partnership Project (3GPP). URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=641 (visited on 12/11/2022).
- Avizienis, A. et al. "Basic concepts and taxonomy of dependable and secure computing". In: *IEEE Transactions on Dependable and Secure Computing* 1.1 (2004), pp. 11–33. DOI: 10.1109/TDSC.2004.2.
- Rupprecht, David et al. "On Security Research Towards Future Mobile Network Generations". In: *IEEE Communications Surveys Tutorials* 20.3 (2018), pp. 2518–2542. DOI: 10.1109/COMST.2018.2820728.

References II

Yu, Chuan et al. “Improving 4G/5G air interface security: A survey of existing attacks on different LTE layers”. In: *Computer Networks* 201 (2021), p. 108532. ISSN: 1389-1286. DOI: https://doi.org/10.1016/j.comnet.2021.108532. URL: https://www.sciencedirect.com/science/article/pii/S1389128621004576.