



Advanced Network Security

Lecture 2: Introduction to Mobile Networks

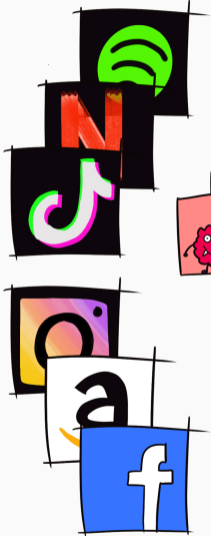
Harald Vranken, Katharina Kohls

September 15, 2022

Open University Nijmegen
Radboud University Nijmegen

Ubiquity of Mobile Devices

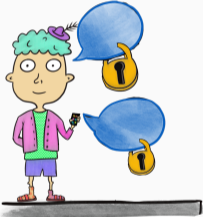
Gaming
...
Shopping
...
Assistants



Media



Weather

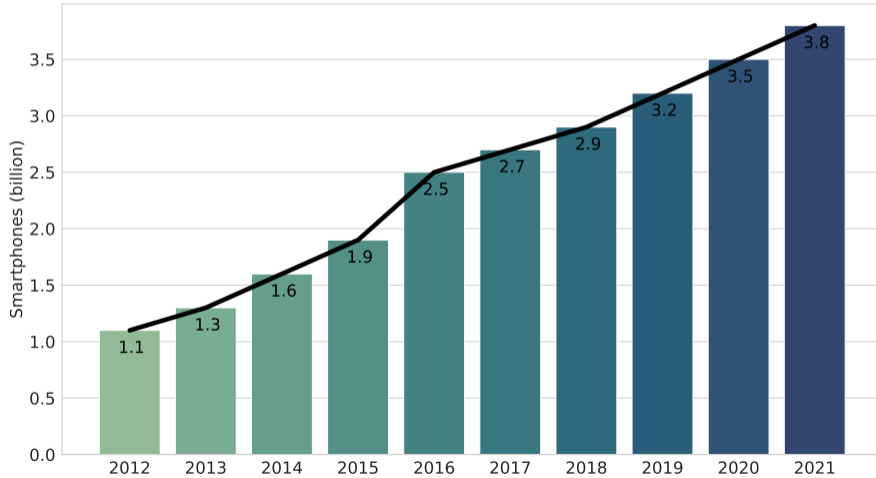


Calling

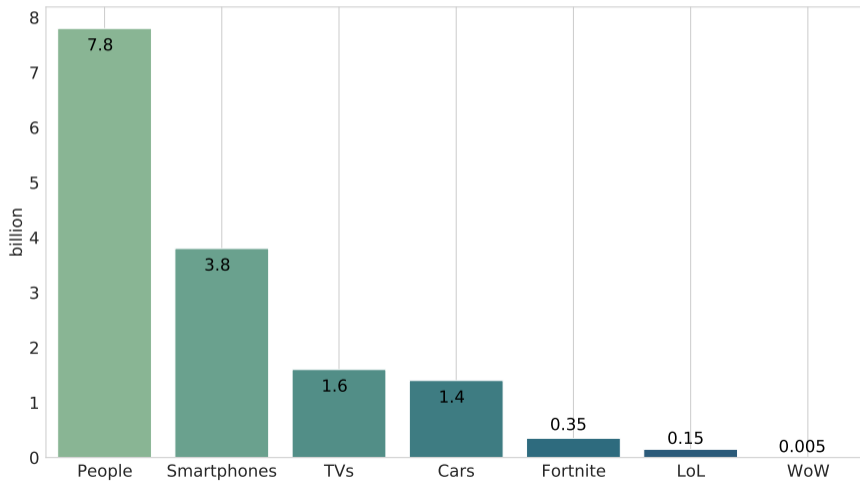


Texting

How present are smartphones?



Let's put this into reference!



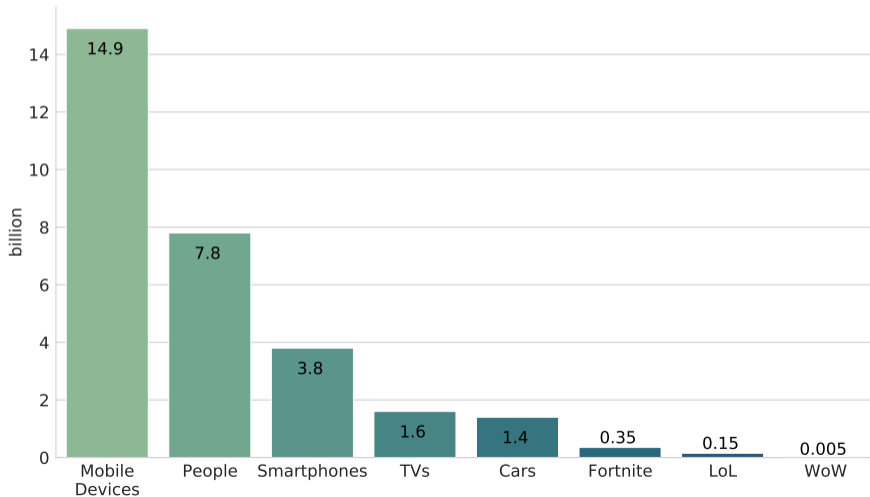
It's not only about smartphones!





How many mobile devices do you have?

Let's get the real reference now!



- ▶ Critical infrastructures and emergency
 - Food and water
 - Public health
 - Transportation systems
 - Security services
- ▶ Industrial contexts
 - Sensors
 - Machines
 - Complex and automated systems



Mobile Devices

- ▶ There are tons of mobile devices
- ▶ Many of them use the cellular network
- ▶ Familiar for us: Casual use cases
- ▶ Not so familiar: Emerging use of mobile networks everywhere else

Our Focus

- ▶ We focus on the **security** of mobile networks
- ▶ Specific attacks and the required technical background

Look out for red slides! They provide a quick summary of a topic block and questions to test your knowledge.

Detailed content overview:

2	Mobile Networks	Introduction to Mobile Networks	Sep 15
3	Attacks	Layer-2 Attacks and Requirements	Sep 22
4	ReVoLTE Attack	Decrypting Phone Calls	Sep 29
5	4G and 5G	Outlook on 5G	Oct 06
6	5G SUCI Catcher	Next-Gen Tracking	Oct 13
7	Presentations 1	Mobile Network Security	Oct 20

Mobile Network Basics

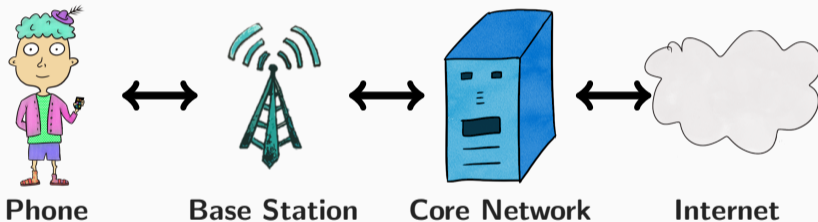
Mobile (Security) Evolution

Mobile Security Goals

Repetitive? A bit. Mobile context? New!





Summary

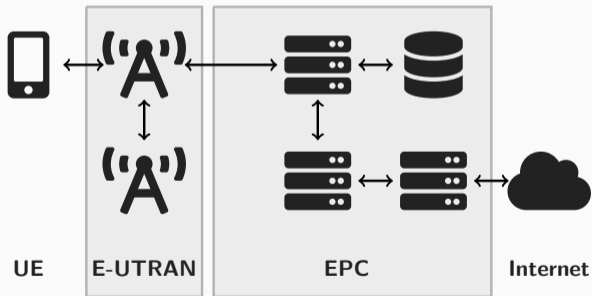
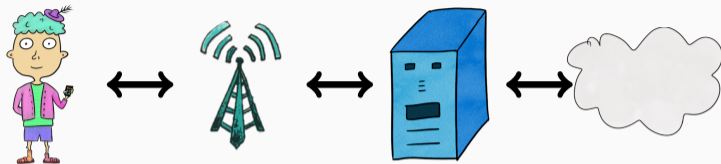
Mobile Network Basics







Generic Components



- ▶ **Phone:** Connects to the network
- ▶ **Base Station:** Provides the *radio connection*
- ▶ **Core Network:** Provides the main management
- ▶ **Internet:** Where you want to go

Component	Icon
Phone	
Base Station	
Core Network	
Internet	



Component	LTE Acronym	LTE Component	Icon
Phone	UE	User Equipment	
Base Station	eNodeB	Evolved Node B	
Core Network	EPC	Evolved Packet Core	
Internet	IP Network	IP Network	

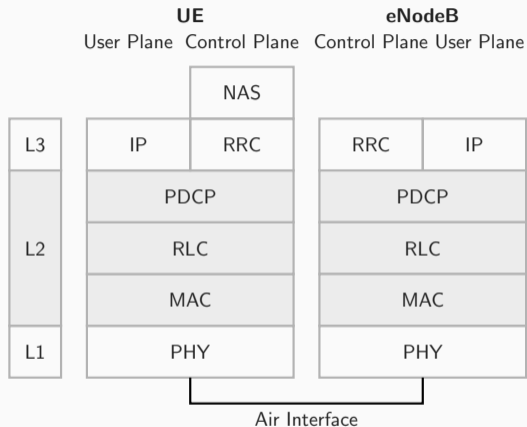
Focusing on the wireless connection:

- ▶ We focus on the **air interface**  ↔ 
- ▶ Another term for this is **radio access network**
- ▶ In LTE, the radio access network is called **E-UTRAN**

So far, we looked at some very basic components of a mobile network and how they are connected.

We now go into detail and take a look at the LTE protocol stack.

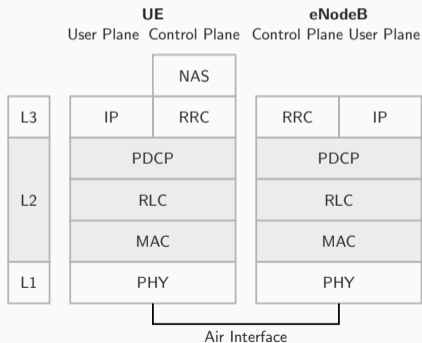
The next part is important 



Get a better understanding: Compare this to the ISO/OSI or the TCP/IP stack

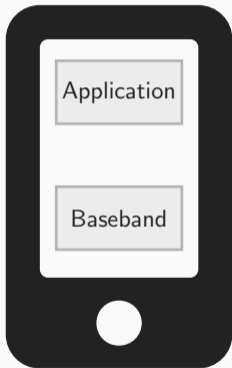
LTE Protocol Stack Layers

- ▶ **User Plane:** *Your* data, for example the website you request.
- ▶ **Control Plane:** *Network* data, what's needed to manage the connection.



- ▶ **NAS:** Non Access Stratum
- ▶ **RRC:** Radio Resource Control
- ▶ **IP:** Internet Protocol
- ▶ **PDCP:** Packet Data Convergence
- ▶ **RLC:** Radio Link Control
- ▶ **MAC:** Medium Access Control
- ▶ **PHY:** Physical Layer

- ▶ **NAS**: Connects the UE *inside* the E-UTRAN with MME *outside* the E-UTRAN. Authentication of UE, security control, paging.
- ▶ **RRC**: Manages the connection between the UE and the eNodeB. Connection establishment/release, radio bearer establishment, reconfiguration, ...
- ▶ **PDCP**: Transport of data with ciphering and integrity protection (RRC) and transport of IP packets (IP).
- ▶ **RLC**: Transport PDCP data in different modes (Acknowledged (AM), Unacknowledged (UM), Transparent (TM)).
- ▶ **MAC**: Logical channels for RLC for multiplexing into the physical transmission. Scheduling of within and between UEs.
- ▶ **PHY**: Transport data over the air interface.



Application Processor

- ▶ The OS implements the network stack
- ▶ Standard Ethernet connection like WiFi

Baseband Processor

- ▶ The Baseband implements the modem
- ▶ Mobile data connection

Website request:

- ▶ Browser sends request
- ▶ Goes down the network stack
- ▶ Data link and physical layer are *Ethernet-specific*

Application Processor



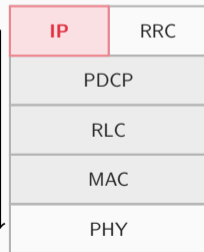
Baseband receives IP packet:

- ▶ Encapsulate in LTE-specific PDCP
- ▶ Hand down further
- ▶ Transmit via *air interface*

Application Processor



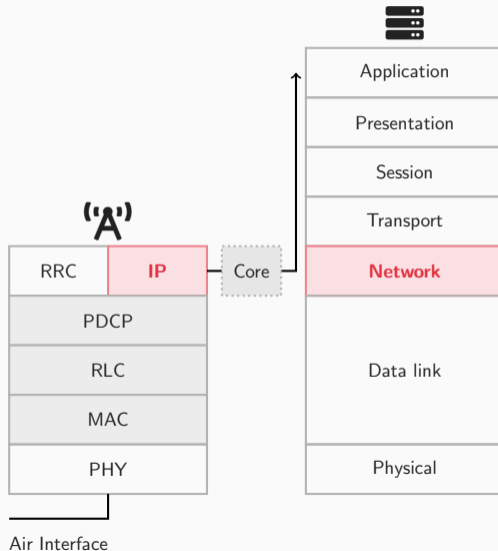
Baseband Processor



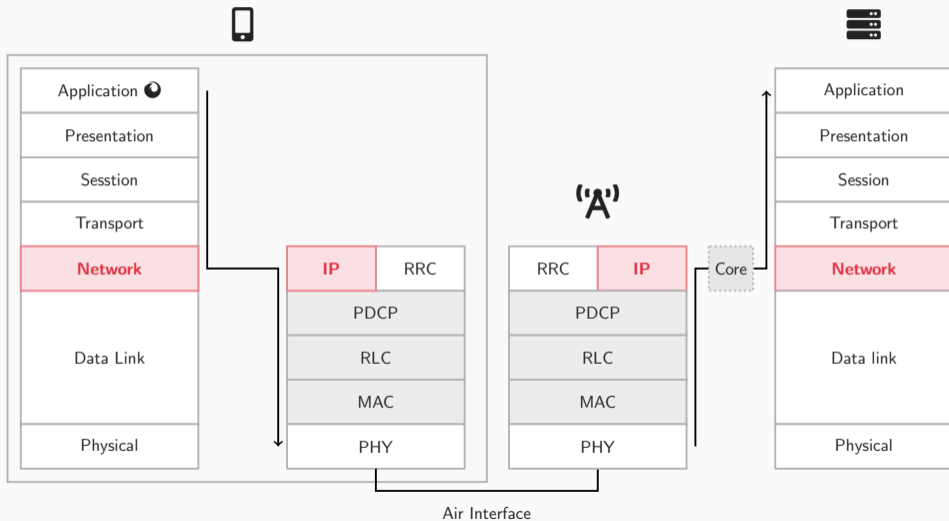
Air Interface

Website Request

- ▶ The eNodeB connects to the core network
- ▶ From there the requests reaches the internet
- ▶ The LTE stack represents the “Data link layer”



Combining Stacks → ('A') →



(1) **Application Processor**

- Browser prepares website request
- Go down the stack
- On the network layer, *Baseband* takes over

(2) **Baseband Processor**

- Receives the IP packet
- Encapsulates it in PDCP
- Hand down, send via air interface

(3) **Base Station**

- Receive request
- Hand up the stack

(4) **Core Network**

- Process packets
- Hand over to Internet

(5) **Internet stack takes over again**

- Go up the stack
- Server receives request

Network Setup

- ▶ A generic network consists of UE ↔ eNodeB ↔ EPC
- ▶ We focus on the air interface E-UTRAN
- ▶ LTE has its own mobile stack, comparable to the data link layer

Next Steps

- ▶ General security goals
- ▶ Security in mobile networks

Exam Preparation

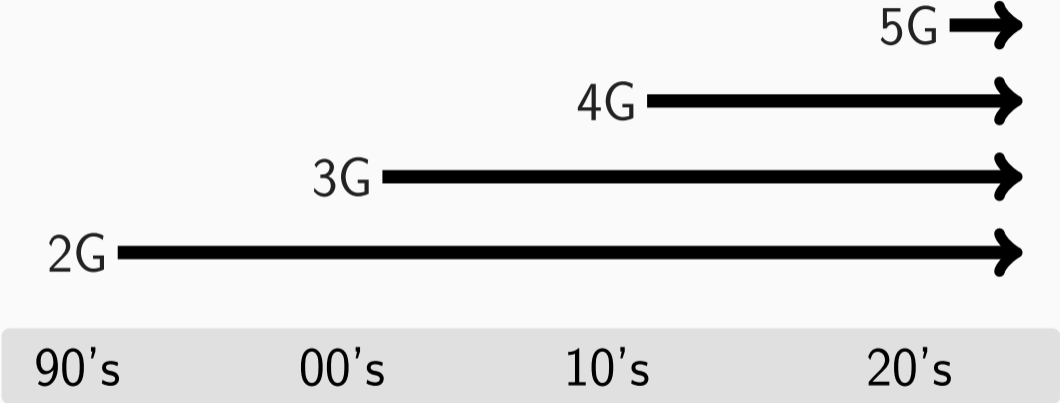
- ▶ You get a cheat sheet with all acronyms.
- ▶ This only helps if you have an idea of what things do.
- ▶ If there are things you *do not* need for the exam, I'll mark them.

Example Questions (test your knowledge, no guarantees)

- ▶ What does the application processor do? What does the baseband processor do?
What is the main difference between both?
- ▶ Sketch the communication between entities when you want to fetch a website with your phone and mobile data plan (ignore the stack for a moment).
- ▶ What is the air interface?
- ▶ Name all four layer-2 protocols of the LTE stack.

Mobile (Security) Evolution

Mobile Generations



90's

00's

10's

20's

2G



- ▶ Weak crypto voice & data A5/1 GEA1
- ▶ Export ciphers GEA1 A5/2 40bit
- ▶ Missing network authentication
- ▶ Inter-core network builds upon trust (SS7)
- ▶ Vulnerabilities exists until 2G disappears

Conclusion

2G/GSM is completely broken!

90's

00's

10's

20's

3G



- ▶ Improved ciphers for voice and data
- ▶ Same GSM (SS7) inter-core network
- ▶ IMSI catchers and downgrade attacks
- ▶ Less research on 3G

Conclusion

3G is still vulnerable to certain attacks

90's

00's

10's

20's

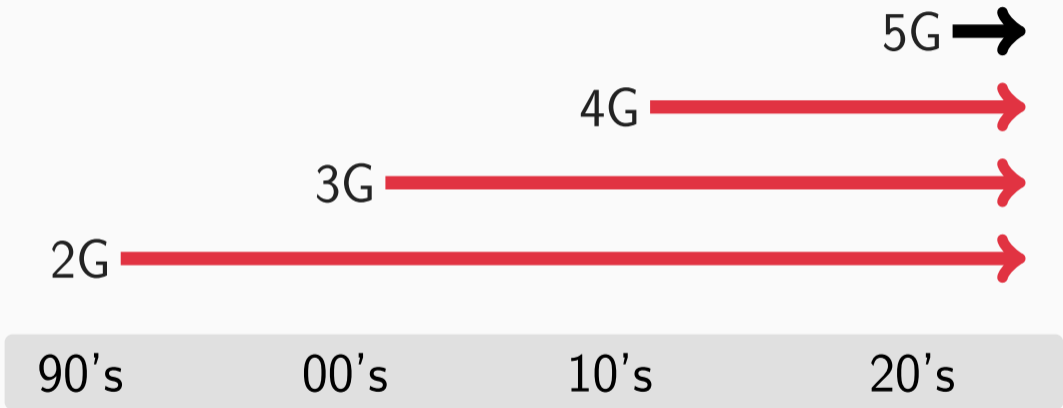
4G 

- ▶ Improved ciphers for voice and data
- ▶ New inter-core network (Diameter) but same attacks
- ▶ IMSI catchers and downgrade attacks
- ▶ Missing user plane integrity protection
- ▶ More sophisticated attacks & capabilities

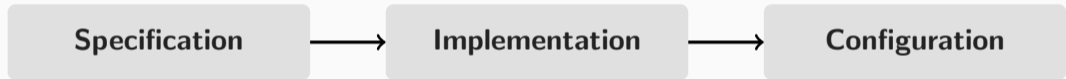
Conclusion

4G improved security but not perfect

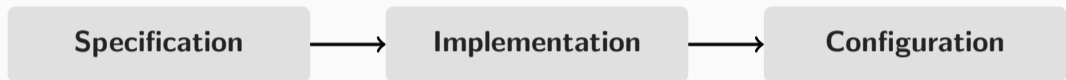
Inherited Weaknesses



How is a new mobile generation being created?



How is a new mobile generation being created?



Define things on paper

Things are flawed by definition.

Update specification 😬

Transform it into code

All devices with this implementation are flawed.

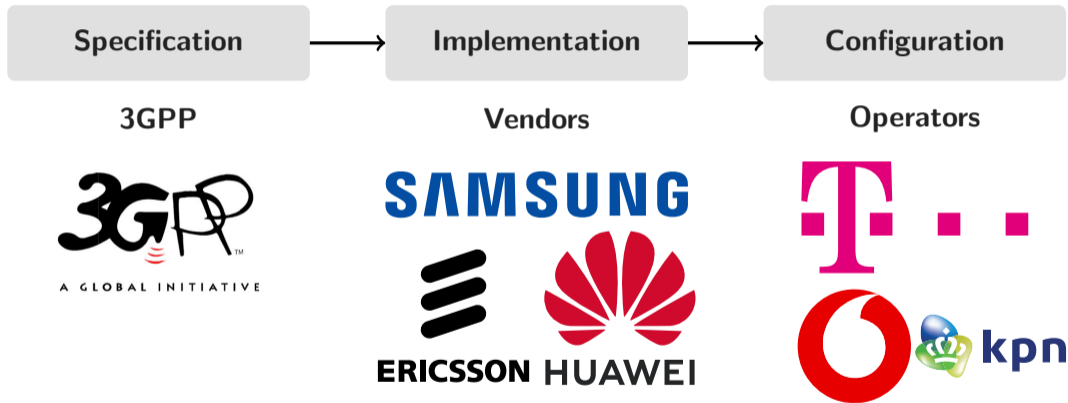
Patch implementation 😬

Fine-tune the live network

Local network has a flawed configuration.

Patch configuration 😊

Who is responsible?



2G, 3G, 4G, 5G

- ▶ Each mobile generation has their own flaws
- ▶ 4G is the current mobile generation
- ▶ Better than 3G, still not perfect
- ▶ 5G is pretty similar

Mobile Lifecycle

- ▶ Specification → Implementation → Configuration
- ▶ Flaws are inherited from one step to the next
- ▶ It's not always possible to patch a flaw
- ▶ 3GPP is responsible of the specification, vendors are responsible of implementations, operators are responsible of configurations.

- ▶ Explain why it is so difficult to remove flaws from the specification.
- ▶ What is the role of vendors? Where do we find their products?
- ▶ What is the current mobile generation?
- ▶ Who is responsible of the configuration of networks?
- ▶ Describe the most important difference between a specification flaw and an implementation flaw.

Mobile Security Goals

Repetitive? A bit. Mobile context? New!

Confidentiality

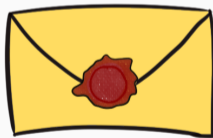
Privacy

Integrity

Availability

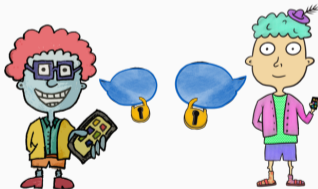
Only authorized access allowed:

- ▶ Protect content from unwanted access
- ▶ Involve only intended communication partners



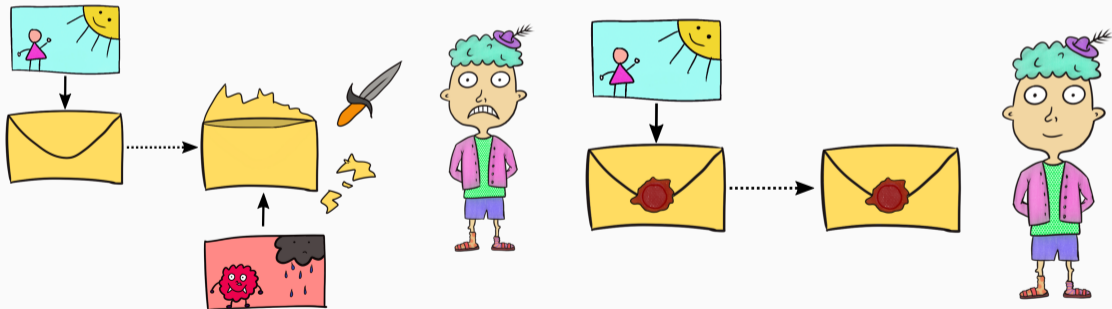
The provider knows this, but an attacker must not:

- ▶ Your geographical location
- ▶ Your temporary or even permanent identity



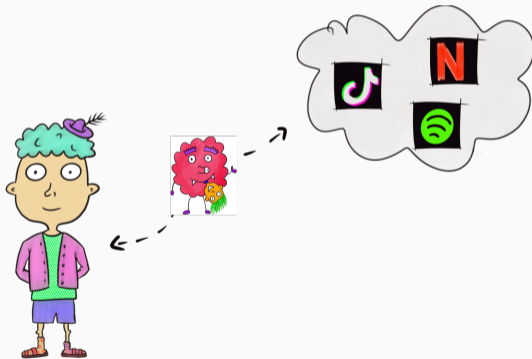
Nobody fiddled with the data:

- ▶ Original message arrives at the recipient
- ▶ Not changed along the way



Being able to reach a service:

- ▶ Service is up and functioning
- ▶ You can reach it when needed



CIA + P

- ▶ Confidentiality, Integrity, Availability, Privacy
- ▶ These are *general* security goals
- ▶ We'll later see what this means in the context of LTE

Exam Examples

- ▶ Remember CIA + P and what this is about
- ▶ More important: Understand this in the context of LTE!

Security Category	Mobile Network Aims
Confidentiality	Confidentiality of User Data Traffic Confidentiality of Voice/Video Calls Confidentiality of text messages (SMS) / RCS
Privacy	Location Privacy Identity Privacy
Integrity	Correct Charging Service Traffic Integrity Mutual Authentication Software and Hardware Integrity
Availability	Undistributed Service

Attack Aims versus Security Goals

Security Category	Mobile Network Aims	AttackAims
Confidentiality	Confidentiality of User Data Traffic	Interception of Internet traffic
	Confidentiality of Voice/Video Calls	Eavesdropping Phone Calls
	Confidentiality of text messages (SMS) / RCS	Interception of text messages / RCS
Privacy	Location Privacy	User tracking
	Identity Privacy	User identification
		User localization
Integrity	Correct Charging Service	Fraud attacks
	Traffic Integrity	Modification of traffic
	Mutual Authentication	Impersonation attack
	Software and Hardware Integrity	Malware and Hardware Trojan
Availability		Downgrade Attacks (stepping stone attack)
	Undistributed Service	DoS of target subscribers
		DoS of infrastructure (ransom)

Confidentiality: Only authorized access allowed

Security Category	Mobile Network Aims	AttackAims
Confidentiality	Confidentiality of User Data Traffic	Interception of Internet traffic
	Confidentiality of Voice/Video Calls	Eavesdropping Phone Calls
	Confidentiality of text messages (SMS) / RCS	Interception of text messages / RCS

Privacy: Provider knows this, attacker must not.

Security Category	Mobile Network Aims	AttackAims
Privacy	Location Privacy Identity Privacy	User tracking User identification User localization

Integrity: Nobody fiddled with the data

Security Category	Mobile Network Aims	AttackAims
Integrity	Correct Charging Service	Fraud attacks
	Traffic Integrity	Modification of traffic
	Mutual Authentication	Impersonation attack
	Software and Hardware Integrity	Malware and Hardware Trojan

Availability: Being able to reach a service

Security Category	Mobile Network Aims	AttackAims
Availability	Undistributed Service	Downgrade Attacks (stepping stone attack) DoS of target subscribers DoS of infrastructure (ransom)

Summary

Basics and Security

- ▶ Radio Access Network: Basic features of mobile networks
- ▶ Mobile Evolution: Inherited problems
- ▶ CIA + P: General security features
- ▶ Discussion: How attack aims contradict security goals

Next Time

- ▶ Three attacks against LTE
- ▶ Website fingerprinting
- ▶ Identity mapping
- ▶ User data redirection
- ▶ ... and the required background

Acronyms

AKA	Authentication and Key Agreement
C-RNTI	Cell Radio Network Temporary Identity
eNodeB	Evolved NodeB
EPC	Evolved Packet Core
E-UTRAN	Evolved Universal Terrestrial Radio Access
EPLMN	Equivalent PLMN
GUTI	Globally Unique Temporary Identifier
HPLMN	Home PLMN
HSS	Home Subscriber Service
IMSI	International Mobile Subscriber Identity
LTE	Long Term Evolution
MAC	Medium Access Control
MCC	Mobile Country Code
MME	Mobility Management Entity
MNC	Mobile Network Code
NAS	Non-Access Stratum
P-GW	PDN Gateway
PDCP	Packet Data Convergence Protocol
PDN	Packet Data Network
PHY	Physical Layer
PLMN	Public Land Mobile Network
RAP	Random Access Preamble
RA-RNTI	Random Access RNTI
RLC	Radio Link Control
RNTI	Radio Network Temporary Identity
RRC	Radio Resource Control
S-GW	Serving Gateway
S1AP	S1 Application Protocol
SCTP	Stream Control Transmission Protocol
VPLMN	Visiting PLMN
SDR	Software Defined Radio
TMSI	Temporary Mobile Subscriber Identity
UE	User Equipment