



Network security

Introduction

Lecture 1

Security and Applied Logic Master

Adela Georgescu
Facultatea de Matematica – Informatica
Universitatea Bucuresti

Logistics

- People



Course

Adela Georgescu

adela@fmi.unibuc.ro

adela.georgescu@unibuc.ro

Lab

Adela Georgescu

Logistics

1. Lectures
 - » 2h course weekly – Tuesday 8.10 - 10
 - » 2h lab/every 2 weeks – Tuesday 10-12
 2. Grading
 - 1,5 p lab
 - 1,5 p lab project
 - 2p course project
 - 5p exam
 - +1p bonus – for activity during lectures
 3. Passing criteria
 - $\geq 4.5p$ at the final exam
 - $\geq 4.5p$ in total
- **Moodle** – all info and materials for course and lab



Security domains

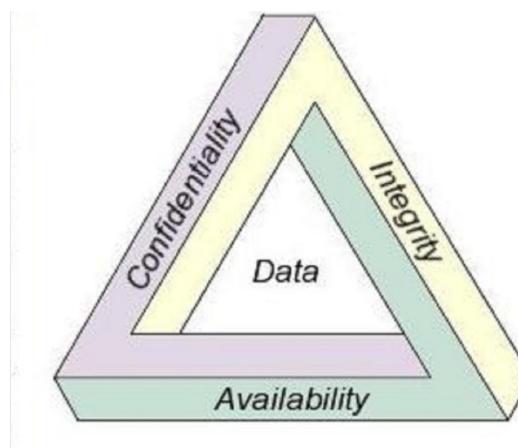
- **Computer Security** - protects data and resources (usually refers to computer systems)
 - Security policies, access control, malware etc.
- **Network Security** - protects data during transmission and communication
- **Web Security** - protection against a web attacker
- **Software Security** - protects the software used in a computer system

What's in this course?

- General security principles (today)
- Wi-Fi – security: WEP, WPA, WPA2 – protocols
- Mobile security: GSM, LTE, 5G
- Internet protocol security: TLS, IPSec

Security objectives

- C-I-A: confidentiality, integrity, availability
- **Confidentiality** – protected goods can only be seen by authorized persons
- **Integrity** - protected goods can only be modified by authorized persons
- **Availability** - protected goods can only be used by authorized persons



Security principles

- Criptographic
 - ✓ Kerkoff (open design): secret key, public algorithms and design
 - ✓ Key separation principle: use different keys for different goals (confidentiality, integrity, authentication)
 - ✓ Principle of diversity: use different types of cryptographic algorithms (avoid the same attack against all)

Security principles

- Other principles
 - Principle of simplicity: keep it simple
 - Security by default: keep the default configuration as secure as possible

Security principles

- Other principles
 - Principle of minimal trust: minimize the number of trusted entities
 - Principle of the weakest link: the security of a system is given by its weakest point
 - Principle of least privilege: grant the **exact** privilege required to perform an activity

Security principles

- Principle of modularization: keep everything modular – makes changes easier
- Defence in depth – security at different layers



Network security

- Lecture 2.1 -

Introduction (Wireless Security)

Adela Georgescu*

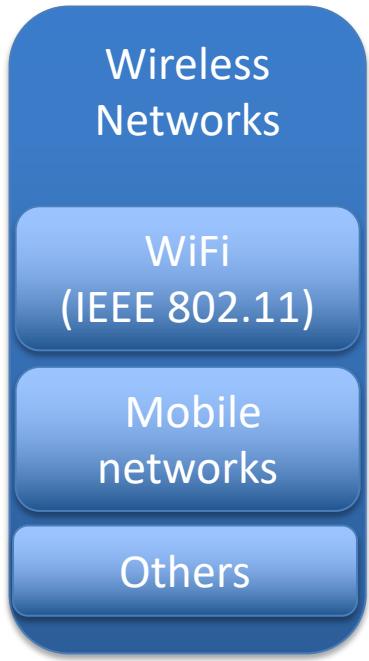
Faculty of Mathematics and Computer Science
University of Bucharest

*slides belonging to Ruxandra Olimid

Contents

1. What do we learn about wireless security?
2. Why?
3. What is the difference between wireless and wired networks?

About



- Security technologies, methods, protocols
- Models, design principles
- Vulnerabilities and attacks

Ethical
aspects!

IEEE 802.11 Wireless LAN / Wi-Fi

Security Requirements

Security Principles

Security Architecture



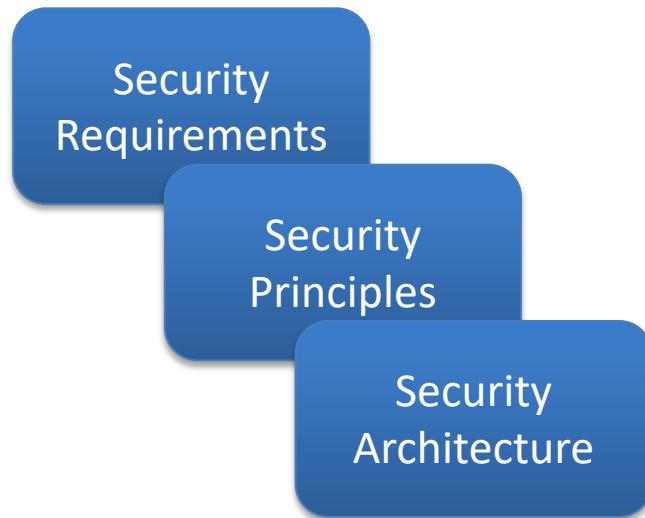
Cryptography

Vulnerabilities

Attacks

Security aspects only! No pure networking!

Mobile networks

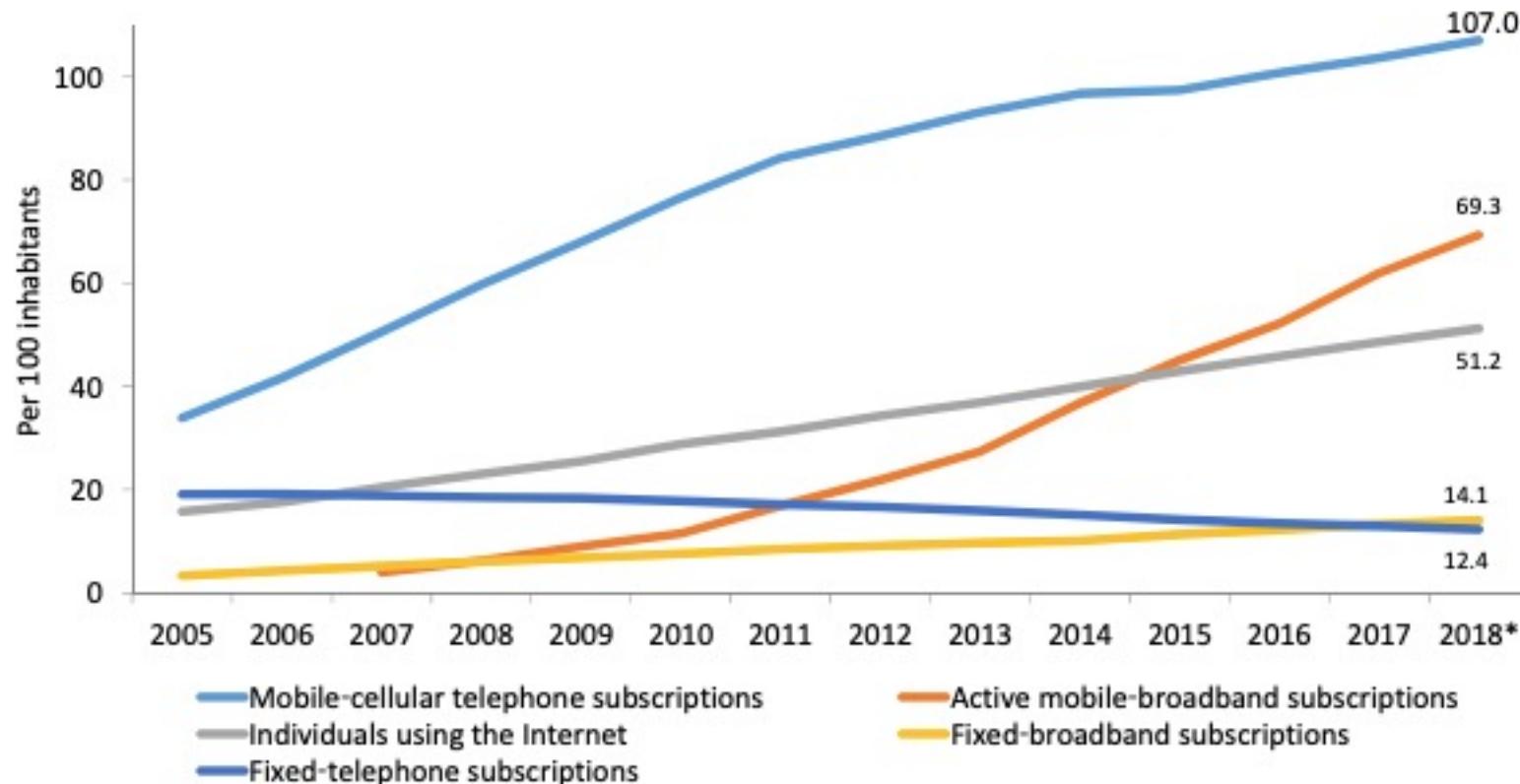


Security aspects only! No pure telecom!

Motivation

ITU: Measuring the Information Society Report 2018

Chart 1.1: Global ICT developments, 2005–2018*



<https://www.itu.int/en/ITU-D/Statistics/Pages/publications/misr2018.aspx>

<https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2018/MISR-2018-Vol-1-E.pdf>

Motivation

Romania

Romania has a competitive mobile market, with very affordable prices and high penetration rates. The country's accession to the European Union in 2007 spurred competition and prompted regulatory reforms in line with the European Union acquis. Competition in the fixed-broadband market is infrastructure-based and optical fibre is the most popular choice, making Romania one the European countries with the highest average broadband speeds.

Mobile services: Four mobile network operators are serving the market. Three of them are pan-European providers (Orange Romania S.A., Vodafone Romania S.A. and Telekom RMC S.A.) and one is a regional operator (RCS & RDS S.A.). There are also a number of MVNOs active in the market, but their share remains very small (ANCOM, 2015). Mobile-cellular and mobile-broadband penetration are high and close to the European average, and prices for both services are very affordable. All MNOs offer LTE services and LTE coverage is being extended, while 3G has already reached nearly full population coverage.

Fixed services: Fixed-broadband penetration in Romania is relatively low compared with the European average and neighbouring countries. Romania's national broadband plan identifies several reasons for this: the late market liberalization (2003) and launch of DSL services (2005), limited use of personal computers, high mobile-broadband take-up and low incomes, especially in rural areas.³⁷⁰ The market is evolving, however, both in terms of subscription numbers

Key Indicators for Romania (2017)	Europe	World
Fixed-telephone sub. per 100 inhab.	19.8	35.8
Mobile-cellular sub. per 100 inhab.	114.6	120.4
Active mobile-broadband sub. per 100 inhab.	82.9	85.9
3G coverage (% of population)	100.0	98.3
LTE/WiMAX coverage (% of population)	83.2	89.6
Individuals using the Internet (%)	63.7	77.2
Households with a computer (%)	73.0	78.6
Households with Internet access (%)	76.5	80.6
International bandwidth per Internet user (kbit/s)	49.8	117.5
Fixed-broadband sub. per 100 inhab.	24.3	30.4
Fixed-broadband sub. by speed tiers, % distribution		
-256 kbit/s to 2 Mbit/s	0.5	0.6
-2 to 10 Mbit/s	8.0	12.4
-equal to or above 10 Mbit/s	91.4	87.0

Note: Data in italics are ITU estimates. Source: ITU (as of June 2018).

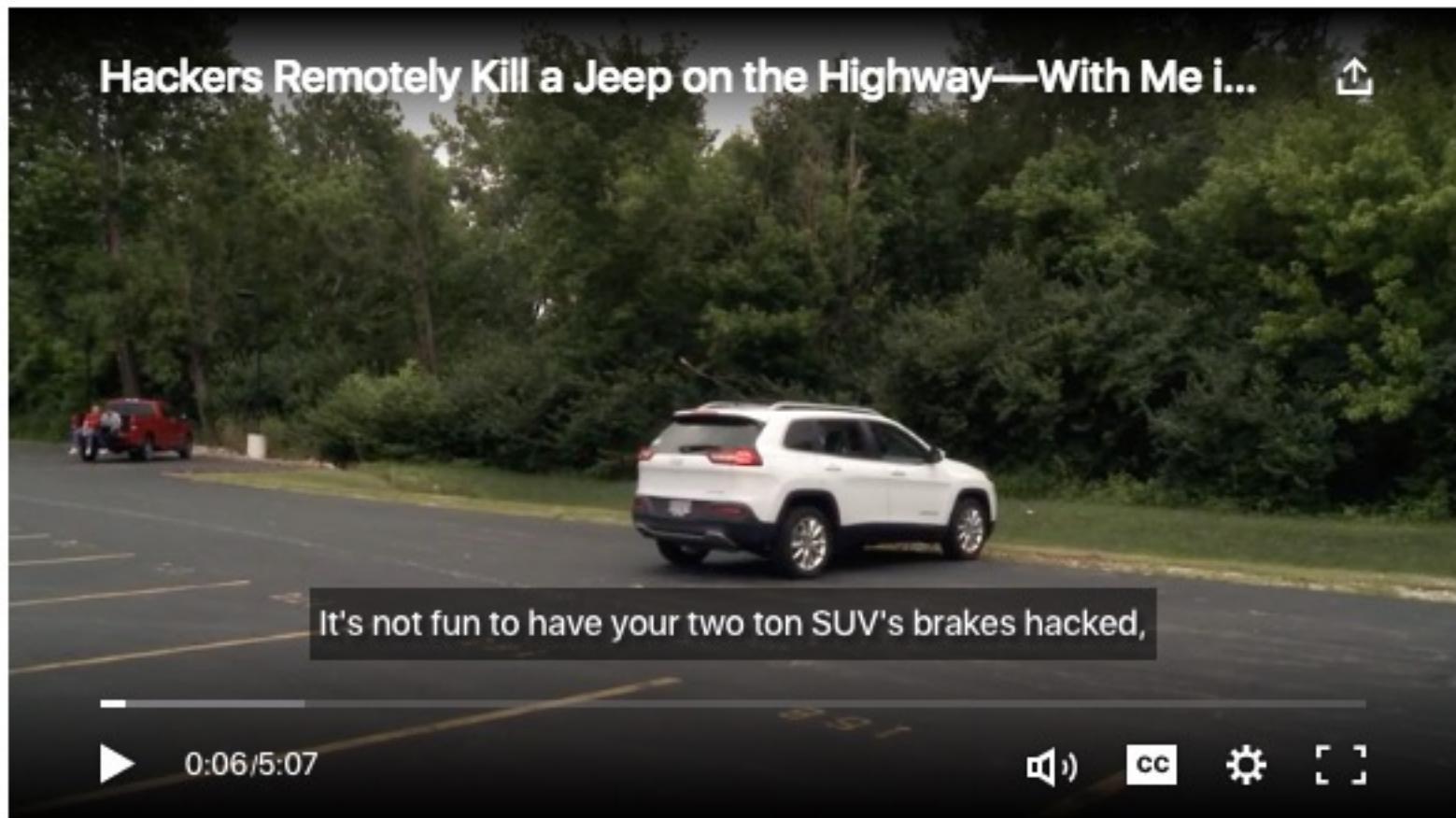
focus of the Government in recent years is on digitalization and broadband development. The National Strategy for the Romanian Digital Agenda 2020 illustrates the Government's efforts in this regard. In line with European targets, Romania aims at achieving 100 per cent of households with fixed-broadband coverage by 2020, 80 per cent of households with over 30 Mbit/s broadband coverage and 45 per cent of households with over 100 Mbit/s coverage. Special emphasis is placed on broadband development in rural and disadvantaged areas. Stimulating competition and promoting mobile-broadband access were also identified as main drivers of growth.³⁷² Ro-NET, a project to build broadband infrastructure in disadvantaged areas, was launched by the Ministry of Communications and Information Society in 2015. The Ministry will remain the owner of the fibre-optic backhaul infrastructure that is to cover over 3 000 km throughout Romania.³⁷³

<https://www.itu.int/en/ITU-D/Statistics/Pages/publications/misr2018.aspx>

<https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2018/MISR-2018-Vol-2-E.pdf>

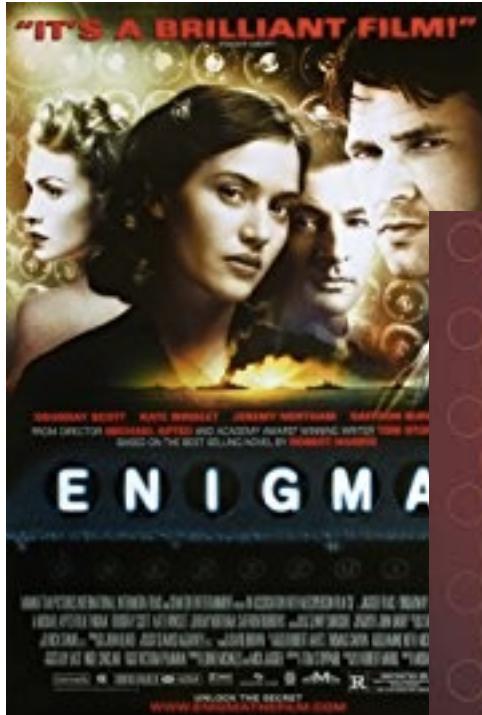
Motivation

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT



<https://www.wired.com/2015/07/hackers-remotely-kill-jEEP-highway/>

Motivation



Motivation

Experimental Assessment of Private Information Disclosure in LTE Mobile Networks

Stig F. Mjølsnes and Ruxandra F. Olimid
Department of Information Security and Communication Technology,
NTNU - Norwegian University of Science and Technology

Tools

- Hardware: Hack RF One [1]
- Software: LTE Cell Scanner and Tracker [2]

Figure 2. HackRF One [1]

Results

We sniffed the radio interface and intercepted parameters of a commercial mobile network in the Trondheim NTNU campus area:

- Figure 3 shows an example of cell search on a given frequency, listing cells that correspond to commercial eNodeBs in the area.

Figure 3. Commercial LTE Cells

Abstract

Open source software running on SDR (Software Defined Radio) devices now allow building a full-fledged mobile network at low cost. These novel tools open up for exciting possibilities to analyse and verify by experiments the behaviour of existing and emerging mobile networks in new lab environments, for instance at universities. We use SDR equipment and open source software to analyse the feasibility of disclosing private information that is sent over the LTE access network. We verify by experiments that identity information can be obtained both passively, by listening on the radio link, and actively, by running considerable low detectable rogue base stations to impersonate the commercial network. Moreover, we implement a downgrade attack (to non-LTE networks) with minimal changes to the open source software.

Motivation & Contribution

- Disclosure of sensitive information in mobile networks has important consequences for both the privacy of sub-

Tools

- Hardware: USRP B200 mini [3]
- Software: Open Air Interface (OAI) [4]

Figure 6. B200mini [3]

Results

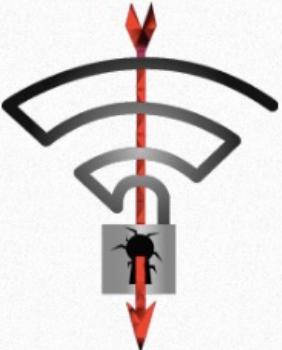
We built an IMSI Catcher that collects subscribers' identifiers (IMSI) in the area of NTNU and then makes the phone reconnect to the commercial network in 2 ways:

- Figure 7 exemplifies an Identity Response message (displayed in Wireshark) that contains the IMSI as a response of an Identity Request (based on our previous results in [5])

Figure 7. Identity Response message (Wireshark)

http://ruxandraolimid.weebly.com/uploads/2/0/1/0/20109229/final_Lte.pdf

Motivation



Key Reinstallation Attacks

Breaking WPA2 by forcing nonce reuse

Discovered by [Mathy Vanhoef](#) of [imec-DistriNet](#), KU Leuven

[INTRO](#) [DEMO](#) [DETAILS](#) [PAPER](#) [TOOLS](#) [Q&A](#)

INTRODUCTION

We discovered serious weaknesses in WPA2, a protocol that secures all modern protected Wi-Fi networks. An attacker within range of a victim can exploit these weaknesses using key reinstallation attacks (KRACKs). Concretely, attackers can use this novel attack technique to read information that was previously assumed to be safely encrypted. This can be abused to steal sensitive information such as credit card numbers, passwords, chat messages, emails, photos, and so on. **The attack works against all modern protected Wi-Fi networks.** Depending on the network configuration, it is also possible to inject and manipulate data. For example, an attacker might be able to inject ransomware or other malware into websites.

<https://www.krackattacks.com/>

Video: <https://youtu.be/Oh4WURZoR98>

Paper: <https://papers.mathyvanhoef.com/ccs2017.pdf>

Why is wireless security different?

- In theory: not much different from the security of wired networks
- In practice:
 - Direct access to the transmission medium
 - Hard to detect passive attacks
 - Broadcast communication
 - Dynamicity (roaming, mobility, etc.)
 - Constraint devices (computing power, energy consumption, etc.)
 - Men-in-the-Middle (MitM), radio jamming
 - ...



Network Security

- Lecture 2.2 -

IEEE 802.11 Wireless LAN / Wi-Fi Intro

Adela Georgescu*

Faculty of Mathematics and Computer Science
University of Bucharest

*slides belonging to Ruxandra Olimid

Contents

1. IEEE 802.11 / Wi-Fi, history, evolution
2. IEEE 802.11 Wireless LAN Architecture

About

- IEEE 802.11: technical standard (Physical layer and MAC sublayer) for implementing Wireless LAN (WLAN) networks



- Wi-Fi: (products / equipment of) wireless network(s) implementing the IEEE 802.11 standard; a technology based on IEEE 802.11; trademark of the Wi-Fi Alliance



WiFi evolution



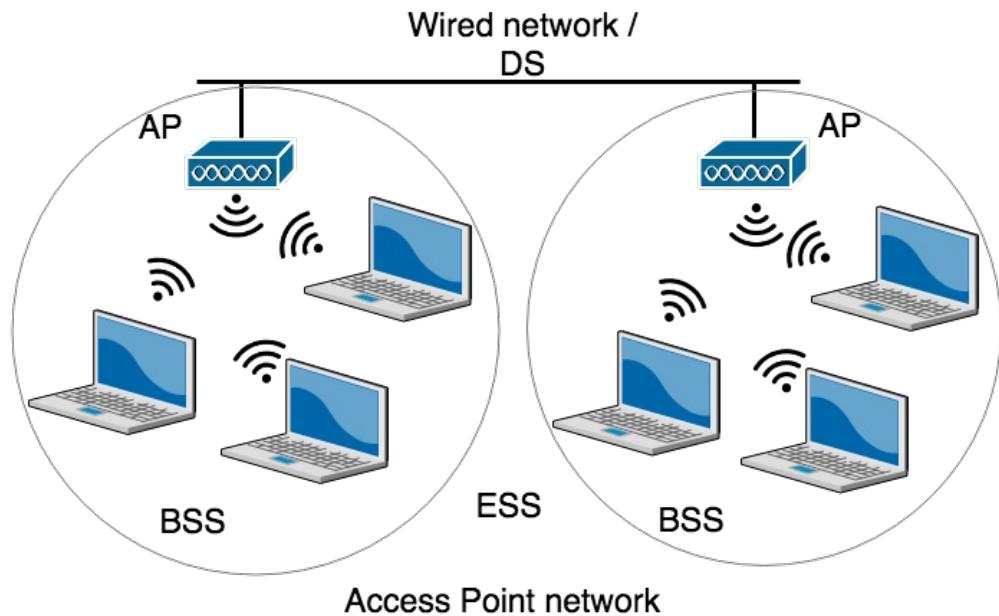
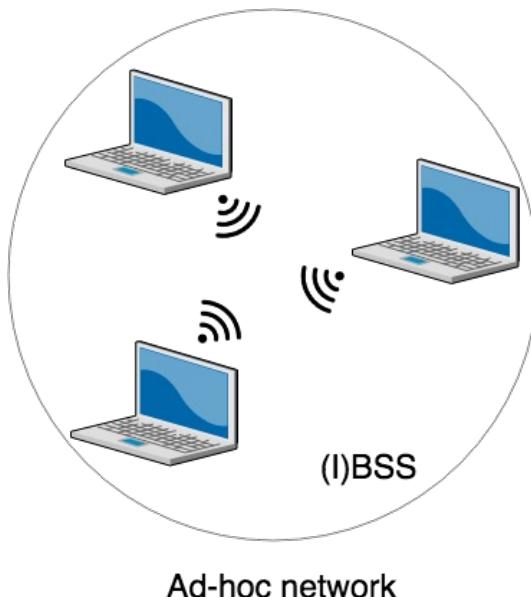
www.wi-fi.org



Celebrating 20 Years of WiFi

[Source: <https://www.wi-fi.org/who-we-are/history>]

IEEE 802.11 Wireless LAN - Arhitecture



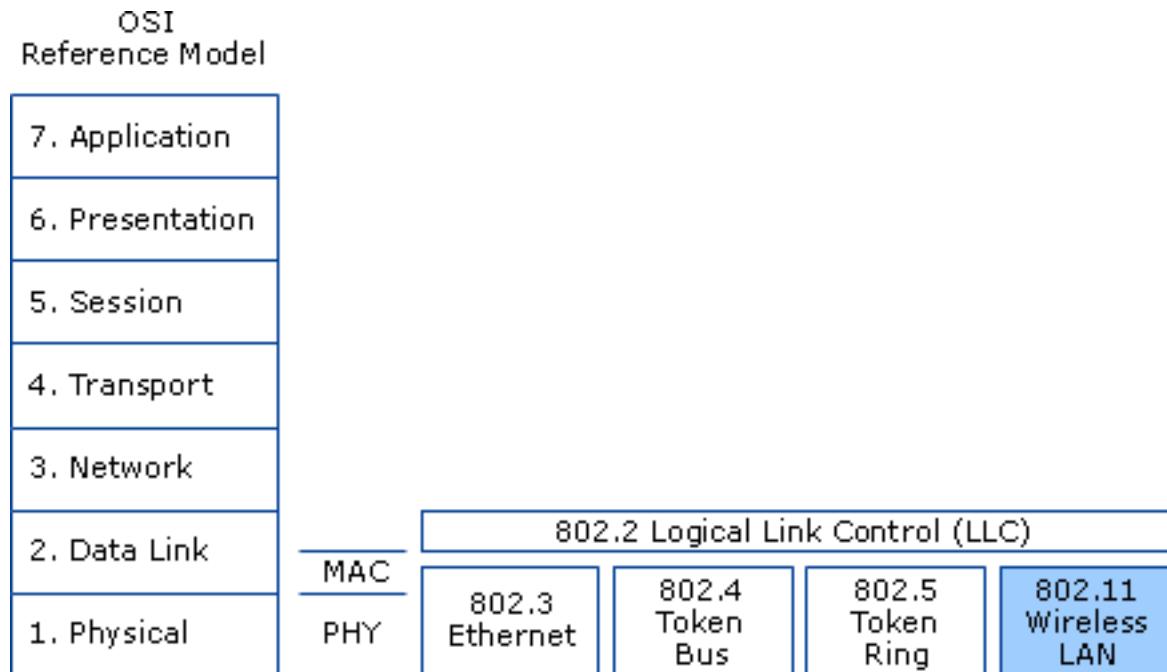
STA: Station
AP: Access Point
BSS: Basic Service Set
IBSS: Independent BSS
ESS: Extended Service Set
DS: Distribution System

- Network types:
- Ad-hoc
 - infrastructure (with AP)

IEEE 802.11 Wireless LAN - Architecture

- STA (Stations):
 - Laptops, Tablets, Smartphones...
- AP (Access Point):
 - A device that acts as a communication hub
- BSS (Basic Service Set):
 - Identified by Service Set ID (SSID)
 - Either several STAs directly connected to any other(ad-hoc - IBSS), either several STAs connected by an AP
- ESS (Extended Service Set):
 - Identified by Extended SSID (ESSID)
 - Several APs connected to the same wired network

IEEE 802.11 Wireless LAN vs. OSI

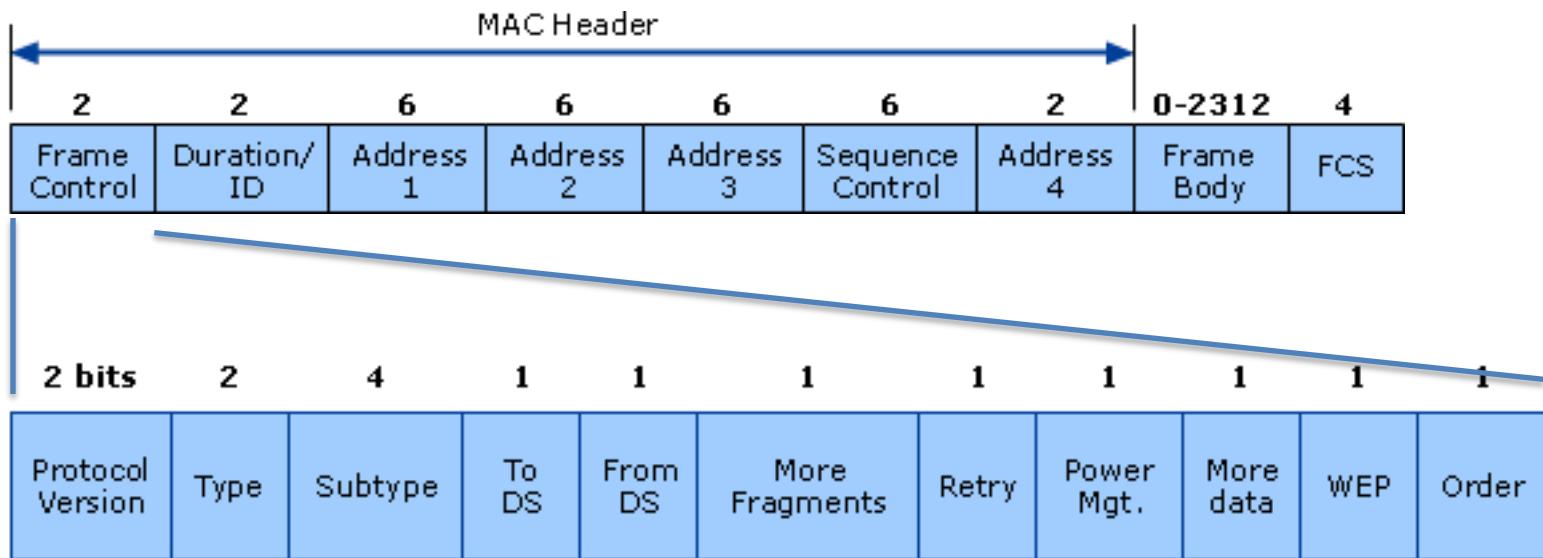


[Source: [https://technet.microsoft.com/pt-pt/library/cc757419\(v=ws.10\).aspx](https://technet.microsoft.com/pt-pt/library/cc757419(v=ws.10).aspx)]

Defines in OSI :

- Physical layer
- Media Access Control (MAC) sublayer of Data Link layer (data is grouped in frames, error detection – FCS/CRC)

IEEE 802.11 MAC Frame Format



[Source: [https://technet.microsoft.com/pt-pt/library/cc757419\(v=ws.10\).aspx](https://technet.microsoft.com/pt-pt/library/cc757419(v=ws.10).aspx)]

FCS: Frame Check Sequence

DS: Distribution System

WEP: Wired Equivalent Privacy

IEEE 802.11 MAC Frame Format

- **Frame control:** frame type (**control** - indicates start/stop/retransmit, **management** - negotiation between AP and STA, or **data**), control information
 - **Duration/connection ID:** channel allocation time
 - **Addresses:** source, destination and AP MAC addresses
 - **Sequence control:** numbering and reassembly
 - **Frame body:** MAC Service Data Unit (**MSDU**) or fragment of MSDU, data
 - **Frame Check Sequence (FCS):** 32-bit **Cyclic Redundancy Check (CRC)**
-
- **Protocol version:** 802.11 version
 - **Type:** control, management, or data
 - **Subtype:** identifies function of frame
 - **To DS:** 1 if destined for DS
 - **From DS:** 1 if leaving DS
 - **More fragments:** 1 if fragments follow
 - **Retry:** 1 if retransmission of previous frame
 - **Power management:** 1 if transmitting station is in sleep mode
 - **More data:** Indicates that station has more data to send
 - **WEP:** 1 if Wired Equivalent Privacy is implemented
 - **Order:** 1 if any data frame is sent using the strictly ordered service

IEEE 802.11 Wireless LAN / Wi-Fi

Security Requirements

Security Principles

Security Architecture



Cryptography

Vulnerabilities

Attacks

Security aspects only! No pure networking!

IEEE 802.11 Security

Improved security

- By default OFF
- Authorization to AP based on MAC address
- IEEE 802.11: Wired Equivalent Privacy (WEP)
Bad designed
- IEEE 802.11i-draft: WPA (Wi-Fi Protected Access)
WEP + TKIP (Wi-Fi industry fix)
- IEEE 802.11i: Robust Security Network (RSN) /WPA2



Network Security

- Lecture 2.3 -

Wired Equivalent Privacy (WEP)

Adela Georgescu*

Faculty of Mathematics and Computer Science

University of Bucharest

*slides belonging to Ruxandra Olimid

Contents

1. Protocol description
2. Vulnerabilities and attacks
3. Lessons to learn

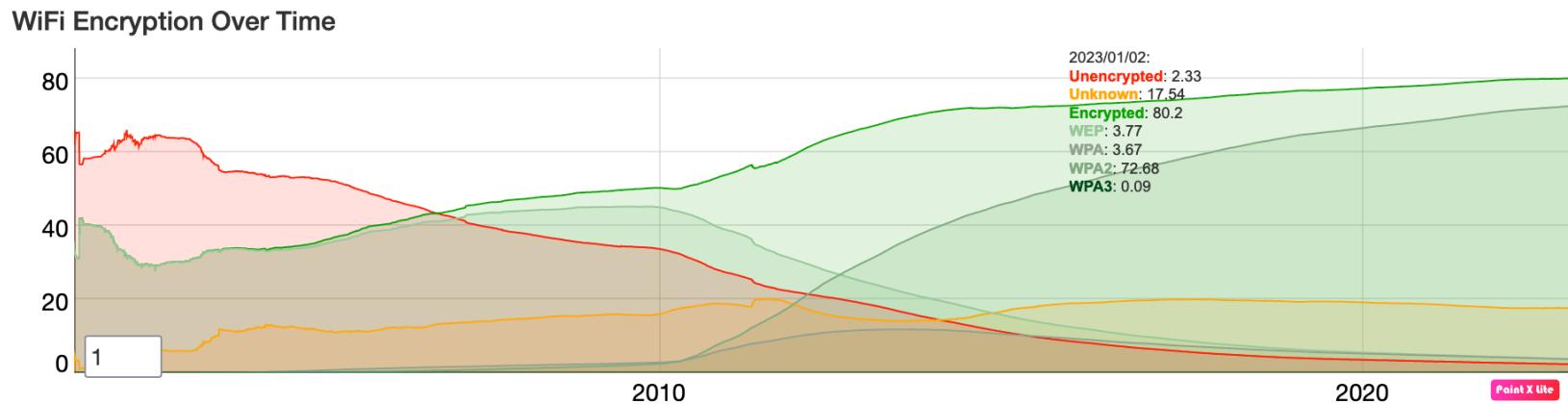
IEEE 802.11 Security

Improved security

- By default OFF
- Authorization to AP based on MAC address
- IEEE 802.11: Wired Equivalent Privacy (WEP)
Bad designed
- IEEE 802.11i-draft: WPA (Wi-Fi Protected Access)
WEP + TKIP (Wi-Fi industry fix)
- IEEE 802.11i: Robust Security Network (RSN) /WPA2

Wired Equivalent Privacy (WEP)

- Original security mechanism IEEE 802.11 (1999)
- Deprecated since 2008, but still in use
- Interesting to study as a negative example 😊



[Source: <https://wigle.net/stats>]

Security goals

- **Data confidentiality:**
 - Ensures protection against eavesdropping (on the radio channel)
- **Data integrity:**
 - Protects against message insertion and modification
- **Network access control:**
 - Protects the use of WLAN resources
- **Others:**
 - Exportable
 - Hardware and software efficient

How WEP works?

Design idea

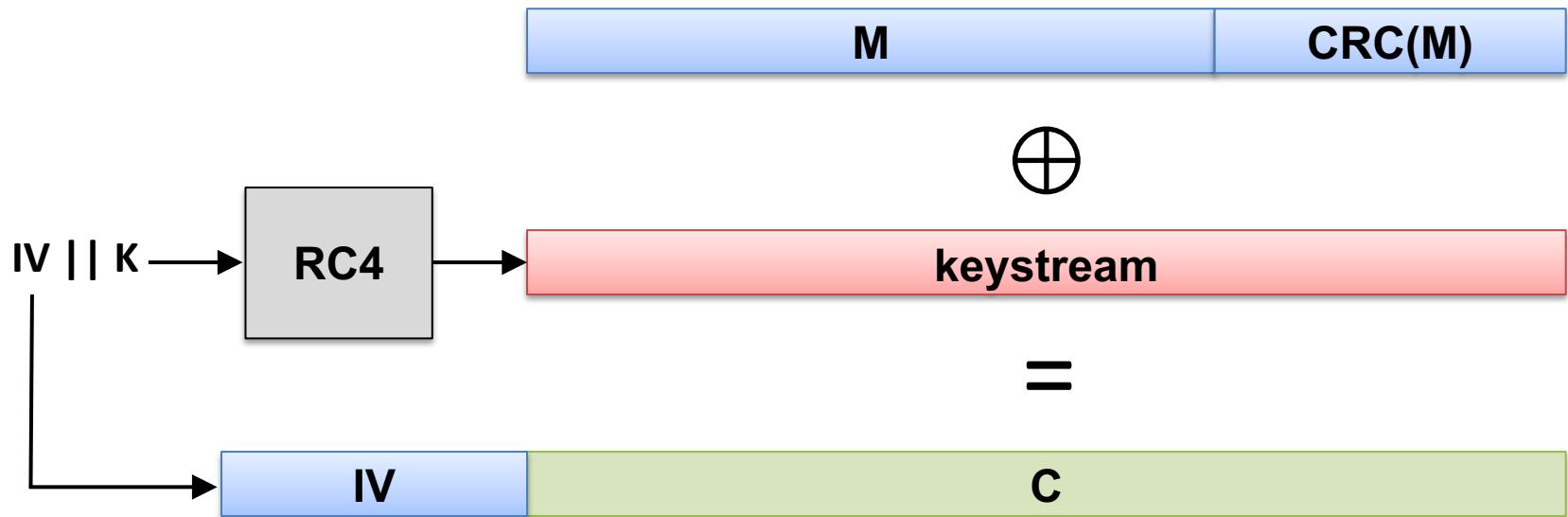
- Key management:
 - A single key for all devices in a BSS
 - Export: 40-bit keys
- Data confidentiality:
 - Encryption of data frames transmitted over the wireless communication medium using the cryptographic key
- Data integrity:
 - Use of Cyclic Redundancy Check (CRC)

WEP authentication



- **Auth Challenge:**
 - AP sends a random challenge on 128 bits
- **Auth Response:**
 - The STA encrypts the challenge with the secret key using WEP and sends the encrypted text to the AP
- **Auth Success:**
 - AP decrypts and compares the plaintext with the challenge; if they are equal, authentication is successful

WEP Encryption (in theory)

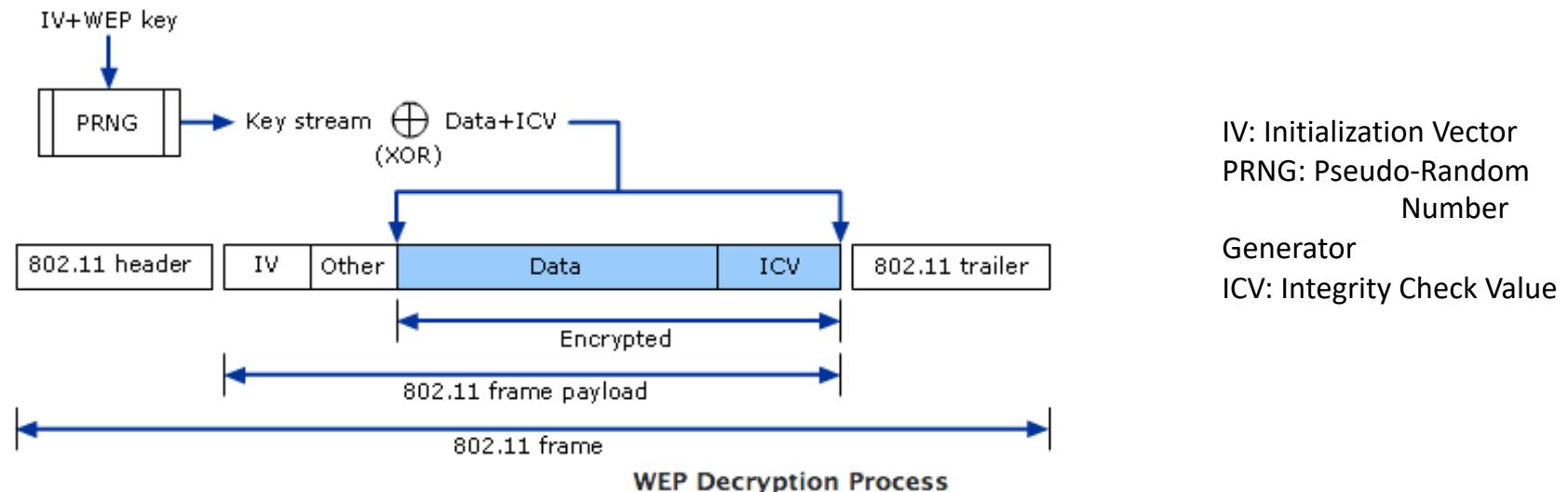


- Uses **RC4**
- IV: 24 bits, K: 104 bits (40 bits)
- IV is used in counter mode (0, 1, 2, ...)

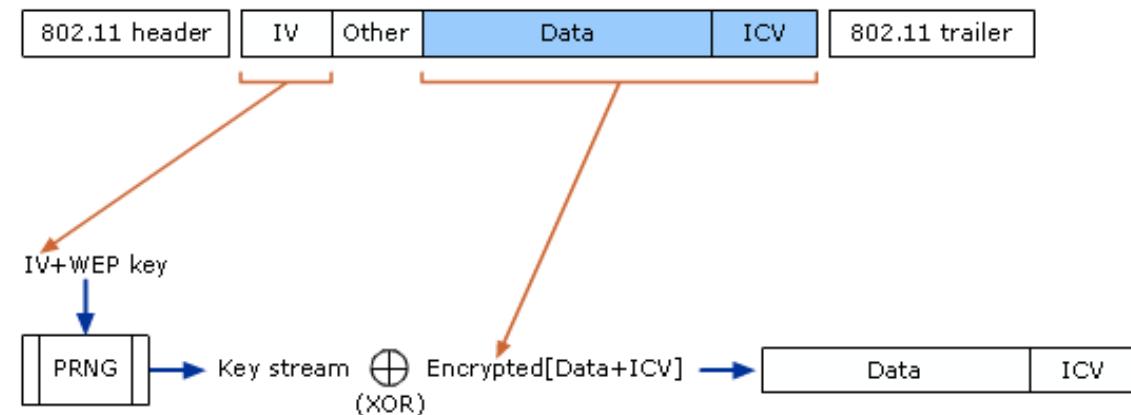
IV: Initialization Vector
K: Cryptographic Key
RC4: Rivest Code 4
CRC: Cyclic Redundancy Check

WEP Encryption (in practice)

WEP Encryption Process



WEP Decryption Process



[Source: [https://technet.microsoft.com/pt-pt/library/cc757419\(v=ws.10\).aspx](https://technet.microsoft.com/pt-pt/library/cc757419(v=ws.10).aspx)]

Security issues?

Problem 1 - Authentication

Question: What can the adversary learn through a passive attack?

Answer: A **passive adversary** eavesdrops on the plaintext (the challenge) și ciphertext-ul and finds out the *keystream* for a given IV:

$$c \oplus m = m \oplus \text{keystream} \oplus m = \text{keystream}$$

Question: Is authentication secure (it can be forged)?

Answer: No, it is not secure! The adversary knows the keystream for a given IV. He reuses the IV, XORs the challenge with the keystream found as before and returns a valid ciphertext to the AP.

Problem 1 - Authentication

Question: Is this mutual authentication?

Answer: No! The AP is not authenticated to STA.

Question: Why is this a problem?

Answer: In general, the absence of mutual authentication enables the emergence of rogue APs (a false AP that sends challenges and receives answers)

Problem 2 - Linearity

Question: If there is no CRC, can the adversary change certain bits in the clear message as desired?

Answer: Yes!

- intercept c ; change c to $c' = c \oplus m'$ and send c' instead of c
- at destination:

$$c' \oplus \text{keystream} = c \oplus m' \oplus \text{keystream} = m \oplus k \oplus m' \oplus k = m \oplus m'$$

CRC is linear: for any m_1, m_2 , $\text{CRC}(m_1 \oplus m_2) = \text{CRC}(m_1) \oplus F(m_2)$

This allows an adversary to modify the ciphertext (by xor-ing with some desired value) and, due to linearity, modify the CRC accordingly

CRC provides **no integrity** (against [intended attacks](#)), it is only an error correction-mechanism ([unintended attacks](#))!

Problem 3 – Re-use of the same IV

Question: What happens when using the same IV for a fixed key K?

Answer: we get the same *keystream* (since RC4 is deterministic!)

Question: Can we say that WEP is secure?

Answer: No!

$$\begin{aligned}c_1 &= m_1 \parallel CRC(m_1) \oplus keystream \\c_2 &= m_2 \parallel CRC(m_2) \oplus keystream \\ \Rightarrow c_1 \oplus c_2 &= m_1 \parallel CRC(m_1) \oplus m_2 \parallel CRC(m_2)\end{aligned}$$

This reveals information about m_1 and m_2

Question: How many possible values can IV take?

Answer: Only 2^{24} !

(IV will repeat every few hours; moreover, IV is reset to 0 at every power cycle)

Other problems...

- RC4 is not a secure PRG! Weak keys, attacks, ...
- Replay attacks (there is no protection mechanism) ...
- Message injection (if *keystream is known* for a given IV)
- **Man-in-the-Middle (MitM)**: directly, by recovering the key, or by using rogue AP (open auth. mode)

Recovering the key

Smashing WEP in A Passive Attack

Pouyan Sepehrdad¹, Petr Sušil² *, Serge Vaudenay², and Martin Vuagnoux

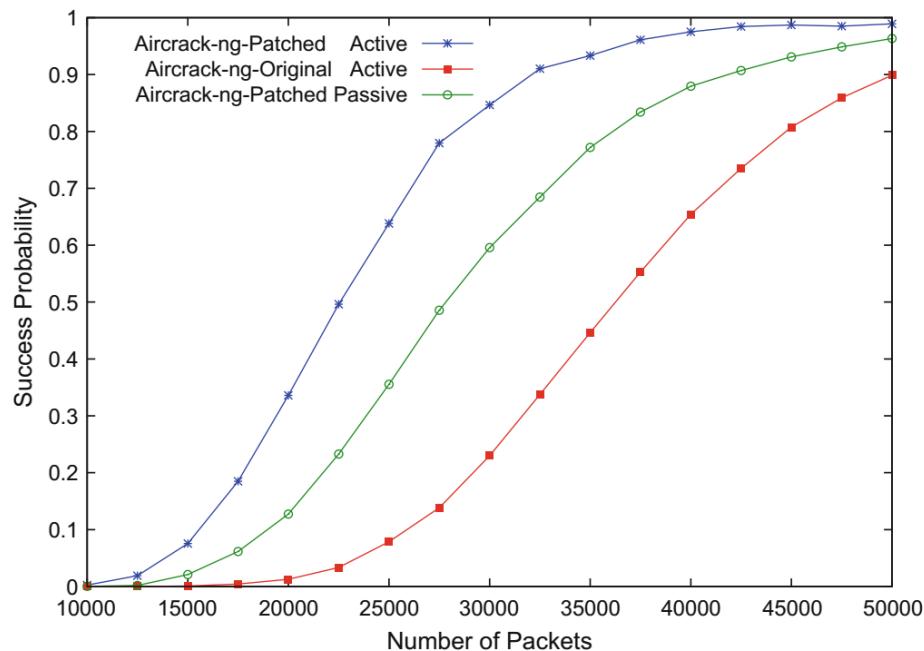
¹ Intel CRI-SC at TU-Darmstadt, Darmstadt, Germany

² EPFL, Lausanne, Switzerland

pouyan.sepehrdad@trust.cased.de,

r.susil, serge.vaudenay}@epfl.ch,

martin@vuagnoux.com



- 5-10 seconds for finding the key on 104 bits

• ...

Fig. 5. Our attacks success probability (both active and passive attacks) with respect to the number of packets compared to Aircrack-ng in active attack mode.

[Video: <https://www.youtube.com/watch?v=JDG9ZAmfIBs>]

Design WEP...

- Clear design goals 
- Open standard 
- Use of well-known and studied cryptographic primitives 
- Public review / analysis / competition 

Lessons to learn...

- Difficult to design a secure protocol
- Use well-known and analysed cryptographic primitives
- Make the protocol public ([Kerckhoffs's principle](#)); public security analysis is important
- Use clear definitions and security proofs



Network Security

- Lecture 3 -

Wi-Fi Protected Access (WPA)

Adela Georgescu*

Faculty of Mathematics and Computer Science
University of Bucharest

*slides belonging to Ruxandra Olimid

Contents

1. Improvements on WEP
2. Description

IEEE 802.11 Security

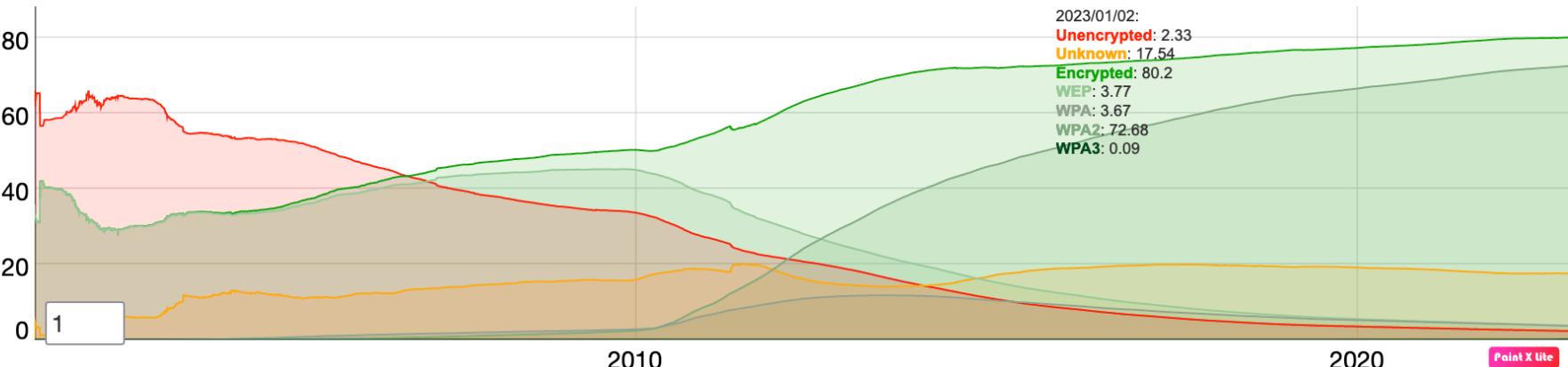
Improved security

- By default OFF
- Authorization to AP based on MAC address
- IEEE 802.11: Wired Equivalent Privacy (WEP)
Bad designed
- IEEE 802.11i-draft: WPA (Wi-Fi Protected Access)
WEP + TKIP (Wi-Fi industry fix)
- IEEE 802.11i: Robust Security Network (RSN) /WPA2
- WPA3

Wi-Fi Protected Access (WPA)

- *Wi-Fi industry fix* of Wi-Fi Alliance (802.11i-draft) – easy to adopt solution
- WEP + Temporal Key Integrity Protocol (TKIP)
- Deprecated since 2014, but still in use

WiFi Encryption Over Time



[Source: <https://wigle.net/stats>]

Recall WEP

- No **confidentiality**:
 - short IV \Rightarrow reuse of keystream RC4
 - Key recovery (< 60 seconds)
- No **integrity**:
 - CRC is not a MAC!
- No protection against **replay attack**
- No **key management**:
 - Unique key (104 bit) for encrypting messages
 - Unique key used by all WLAN users

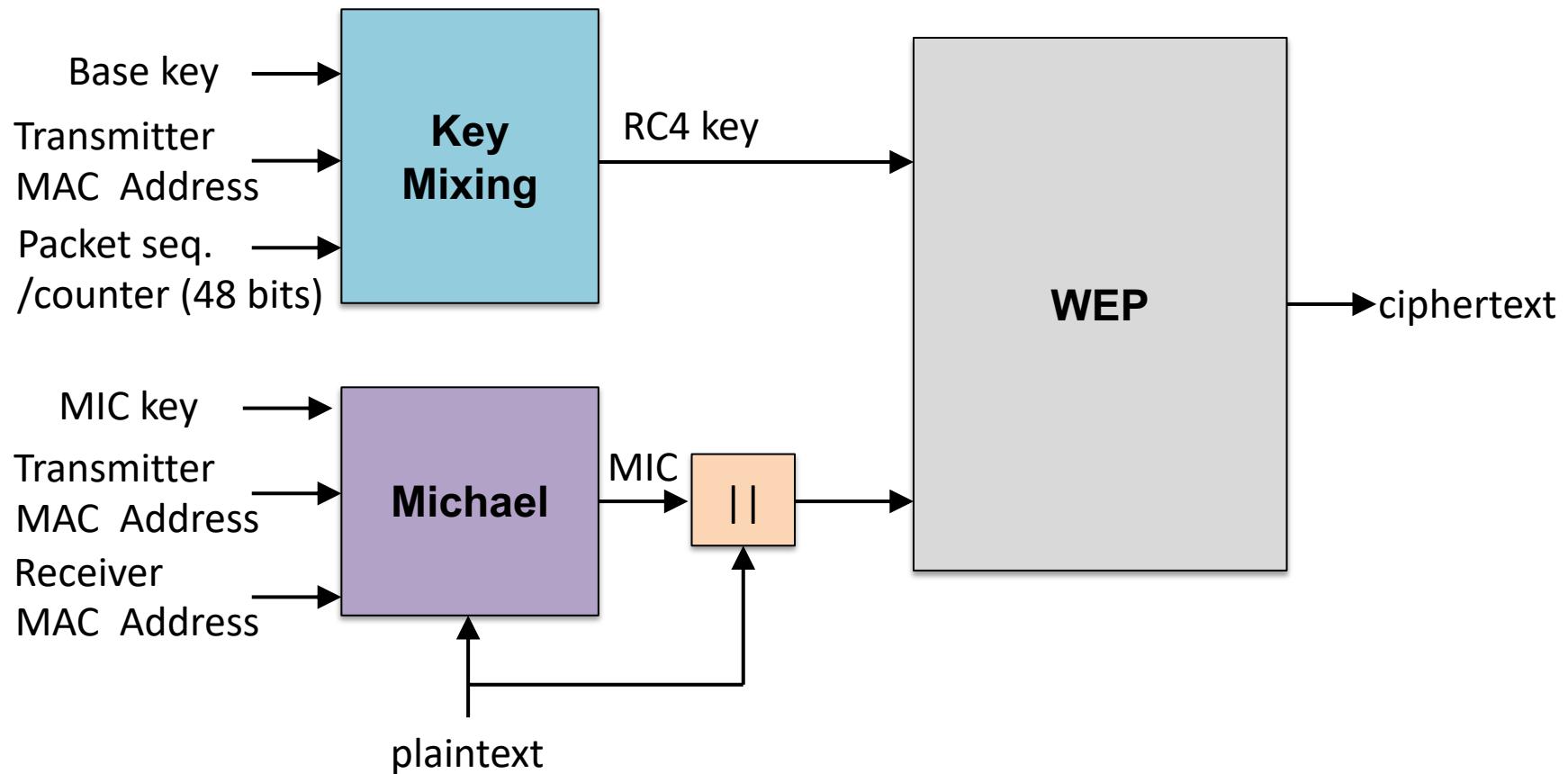
Improvements on WEP

- **Encryption:**
 - TKIP to improve WEP encryption (e.g., a new key for every packet/frame)
 - Possibility to use AES (optional, not all the devices could handle AES)
- **Integrity:**
 - Michael, a new algorithm
- **Authentication:**
 - 802.1X (initially defined for Ethernet networks, later adopted for 802.11 WLAN)
 - 802.11 - optional 802.1X authentication, WPA – mandatory 802.1X authentication
- **Key generation and distribution:**
 - 802.1X

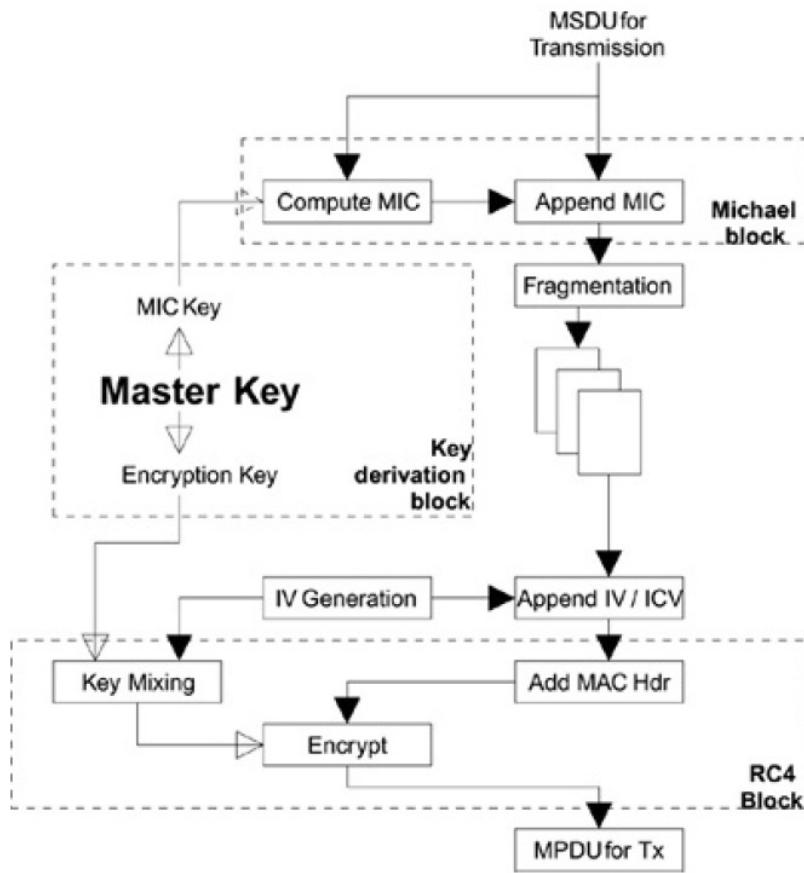
TKIP

(Temporary Key Integrity Protocol)

TKIP (Temporary Key Integrity Protocol)

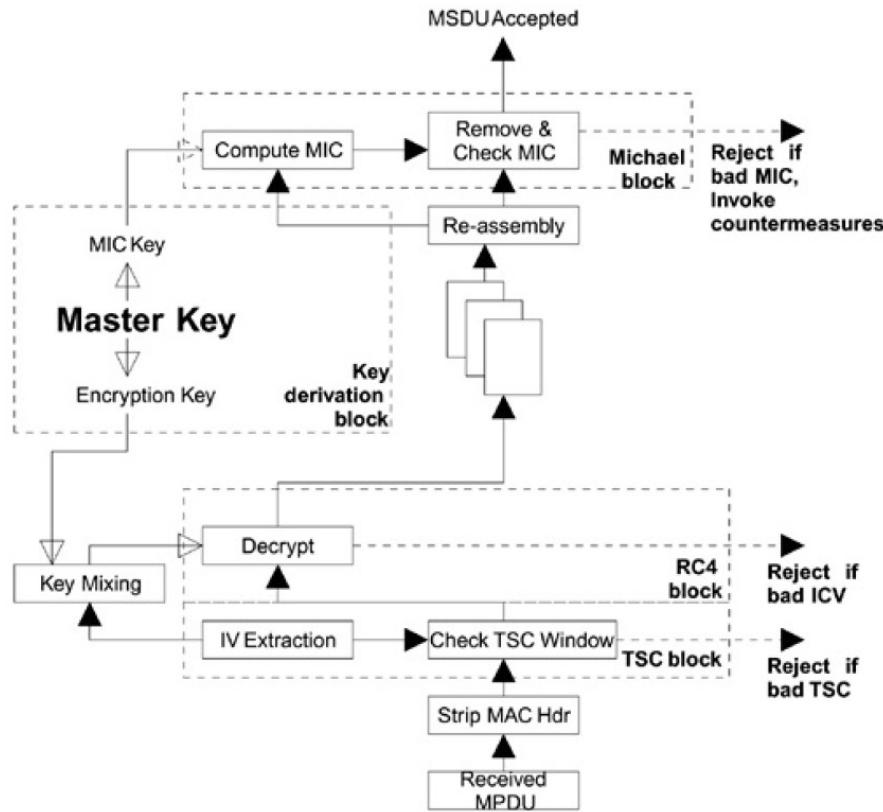


TKIP for transmission



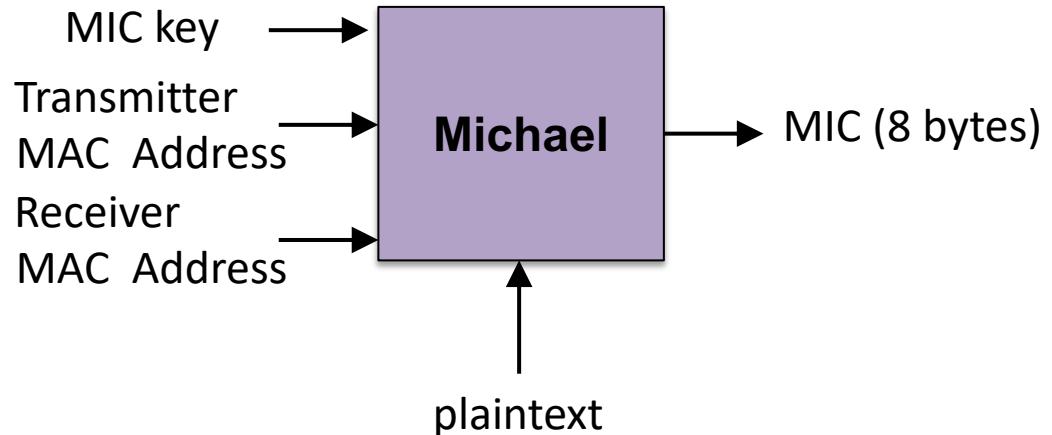
[Source: Course book, Edney & Arbaugh, Chapter 11]

TKIP for reception



[Source: Course book, Edney & Arbaugh, Chapter 11]

Michael



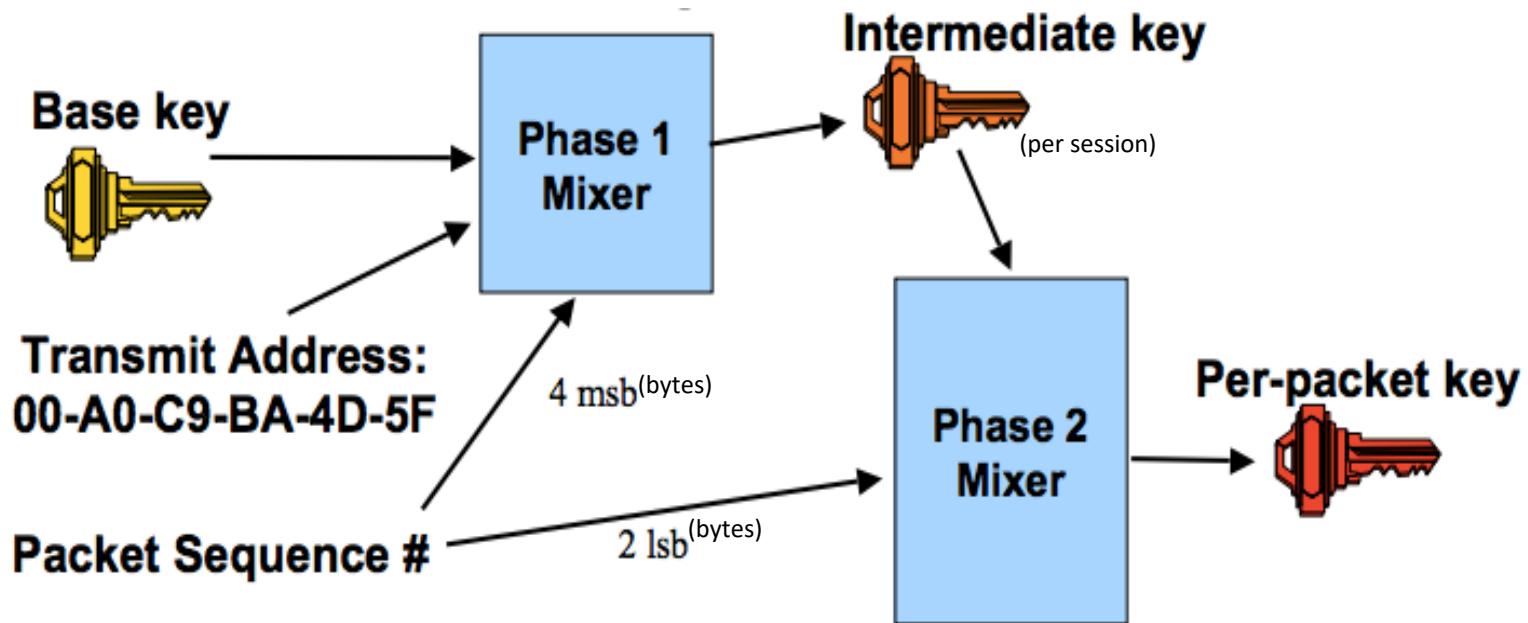
- **MIC key:** 64 bits
 - **Output:** 64 bits (8 bytes)
-
- **Problem:** 20 bits security level;

Question: Why is this a problem?

Answer: Adversary can try random MIC with probability one in a million to guess a valid one ($2^{20} = 1048576$).

Solution? Limitation of MIC verification by the adversary (delay of 1 min. when detecting attacks). A new problem arises : **DoS!**

TKIP – Key Mixing

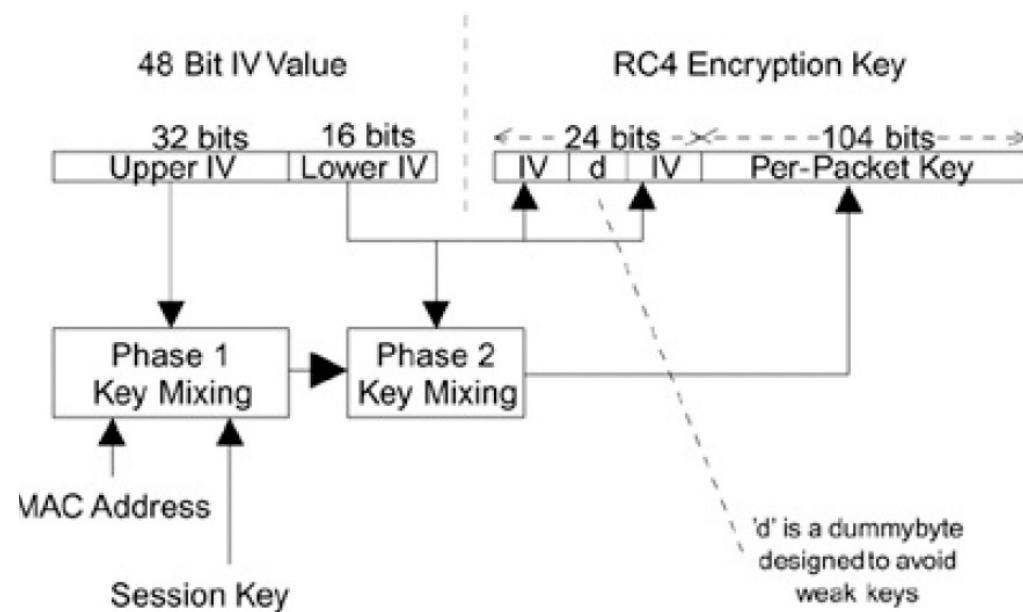


[Source: IEEE 802.11i Overview http://ieee802.org/16/liaison/docs/80211-05_0123r1.pdf]

TKIP (Temporary Key Integrity Protocol)

- **Temporary keys:**
 - 2 mixing stages
 - Equipment dependent, via transmitter MAC address
 - Dependent on packet sequence (48 bits, not 24 as IV had in WEP)
- **Goal:**
 - Avoid keystream reuse (keys become temporary) / collision attacks are avoided
 - Avoid packet retransmission on IV reuse (possible space now becomes 2^{48}) / **replay attacks**

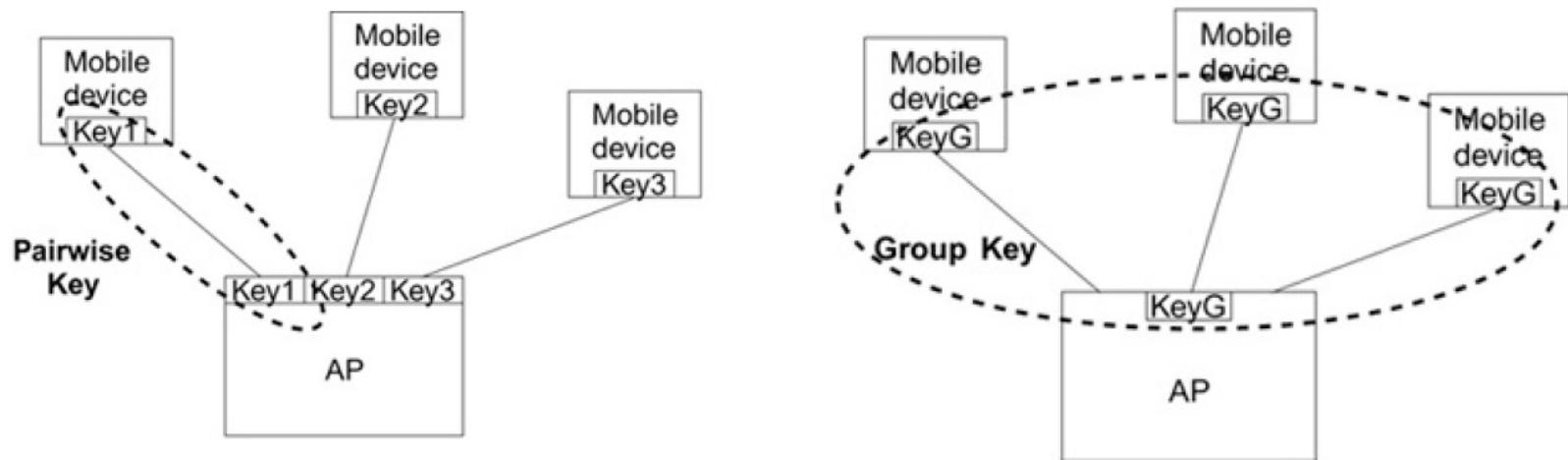
TKIP (Temporary Key Integrity Protocol) – key mixing



[Source: Course book, Edney & Arbaugh, Chapter 11]

TKIP (Temporary Key Integrity Protocol) – key generation

- Pairwise keys – communication between STA and AP
- Group keys – for broadcast messages



[Source: Course book, Edney & Arbaugh, Chapter 10]

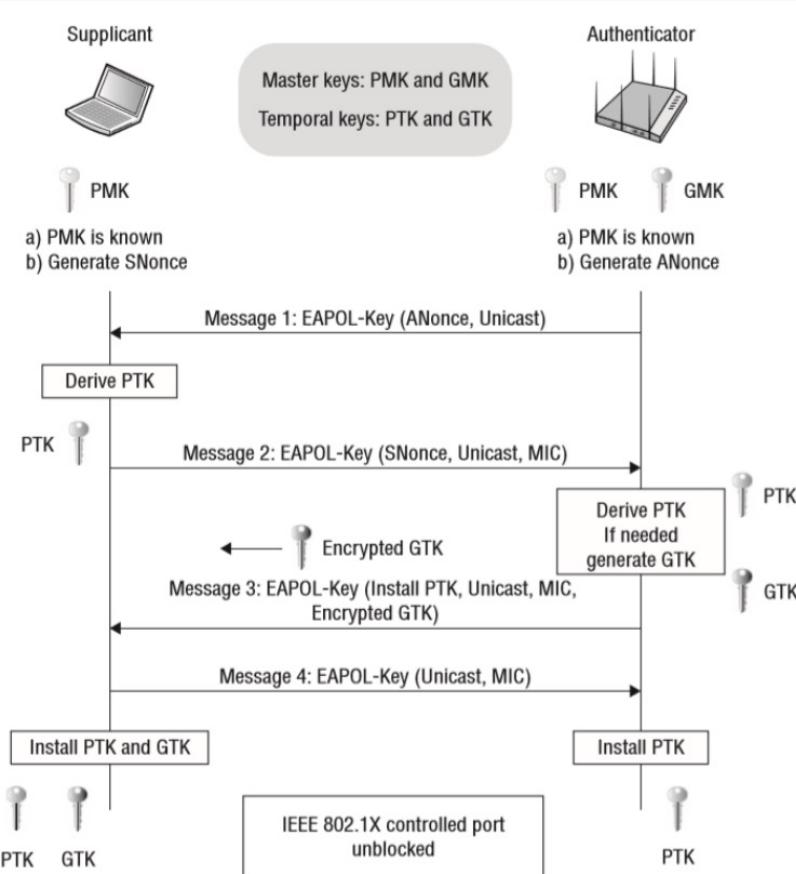
- Preshared keys – pre-installed on STA and AP
- Server-based keys – derived in upper-layer authentication

TKIP (Temporary Key Integrity Protocol) – key generation

- PMK (Pairwise Master Key) / 2 variants:
 - pre-shared key, 256 bits
 - 802.1X PMK is unique for every STA, sent by the authentication server to the AP (upper layer authentication)
- Base key / PTK (Pairwise Transient Key) – computed by STA and AP:

$$PTK = f(PMK, \text{Nonce}_{AP}, \text{Nonce}_{STA}, MAC_{AP}, MAC_{STA})$$

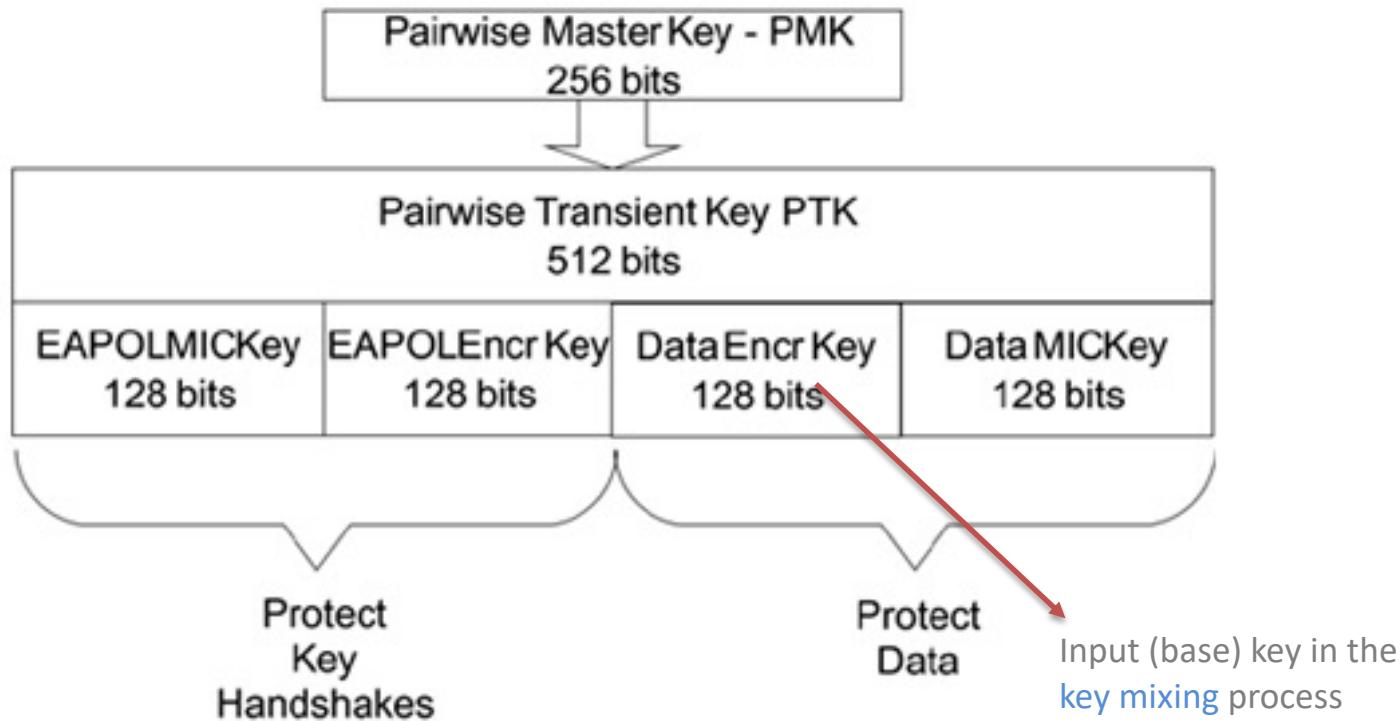
TKIP (Temporary Key Integrity Protocol) – 4-way handshake



- allows STA and AP to exchange nonces for computing temporal keys

[Source: <https://www.wifi-professionals.com/2019/01/4-way-handshake>]

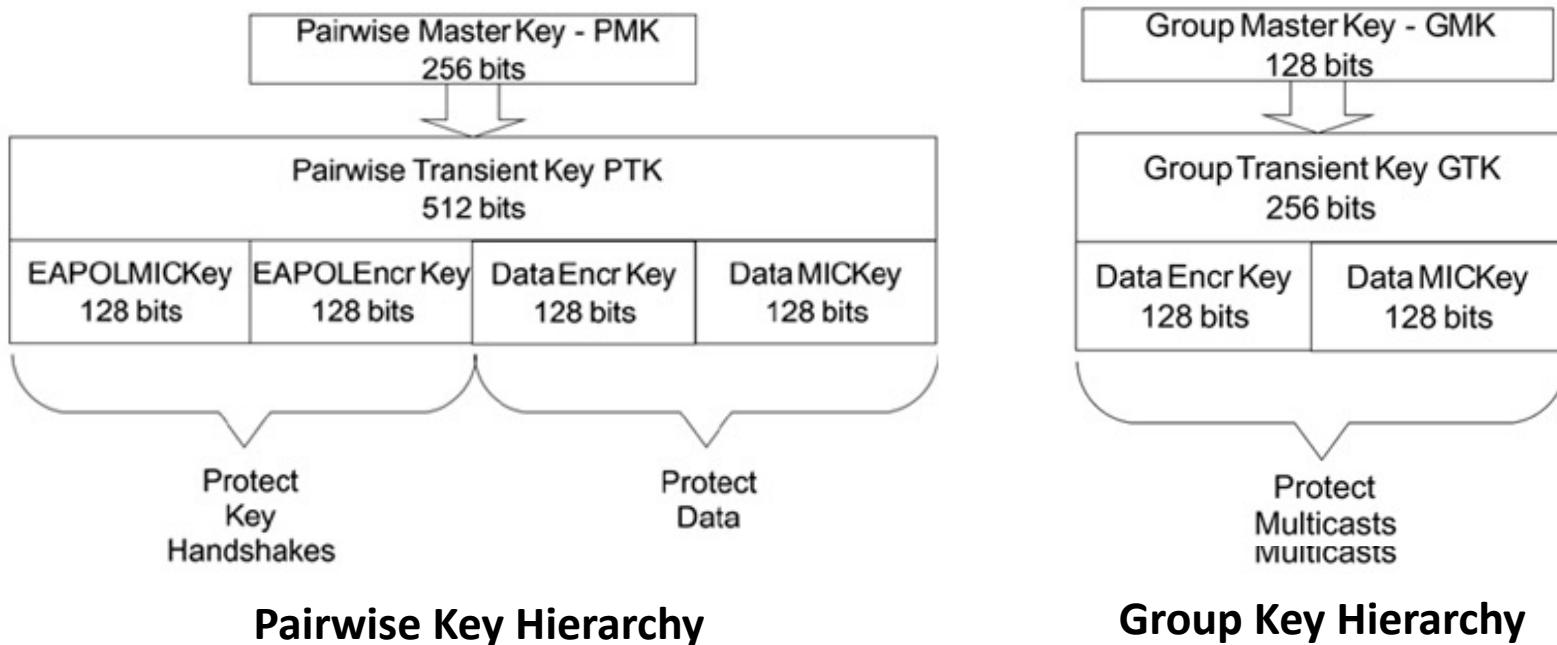
TKIP Pairwise Key Hierarchy



[Source: Course book, Edney & Arbaugh, Chapter 10]

TKIP Key Hierarchy

$$PTK = f(PMK, \text{Nonce}_{AP}, \text{Nonce}_{STA}, MAC_{AP}, MAC_{STA}) \quad GTK = f(GMK, \text{Nonce}_{AP}, MAC_{AP})$$



[Source: Course book, Edney & Arbaugh, Chapter 10]

*Group Key Hierarchy: folosit la broadcast communication

WPA design

- It tries to address all WEP issues
- Limited by device capabilities (software upgrade)
- Compatible with 802.11i (WPA as draft 802.11i)



Network Security

- Lecture 4.1 -

802.1X & EAPOL

Adela Georgescu*

Faculty of Mathematics and Computer Science
University of Bucharest

*slides belonging to Ruxandra Olimid

Outline

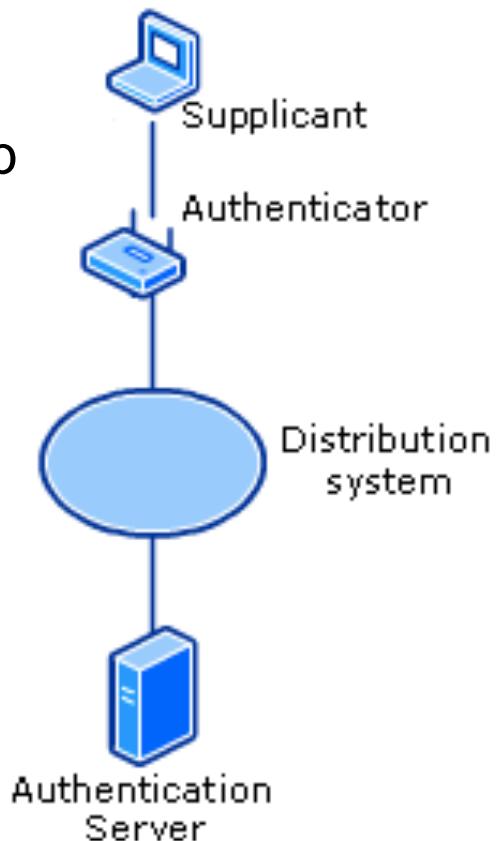
1. 802.1X architecture
2. EAPOL authentication

802.1X

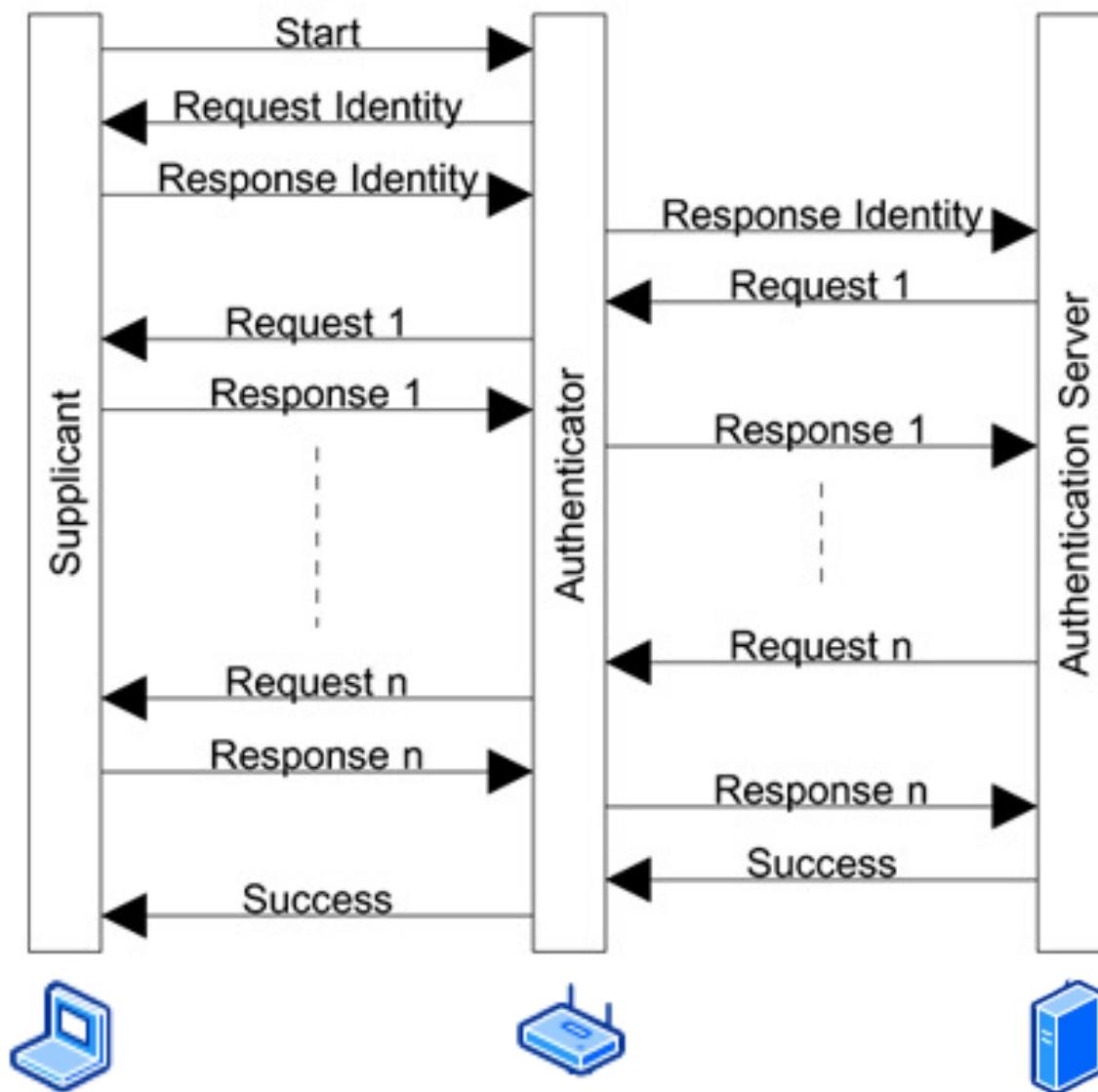
- Standard initially defined for Ethernet networks, later on adopted for 802.11 WLAN
- Defines access control in the network (port-based), but also offers authenticated access in the network
- Extensible Authentication Protocol (EAP) over LAN (EAPOL) is an authentication mechanism Point to Point Protocol (PPP) adopted for LAN.
- 802.1X uses EAPOL for transmitting messages between entities.

IEEE 802.1X architecture

- **Supplicant:**
 - An entity who requests the services (wants to join the network); e.g.: a laptop
- **Authenticator:**
 - An entity who controls access before granting access to services; e.g.: an AP
- **Authentication Server:**
 - Makes authorization decisions e.g.: sometimes inside AP but more often through **RADIUS** (Remote Authentication Dial-In User Service)



EAPOL Authentication Sequence

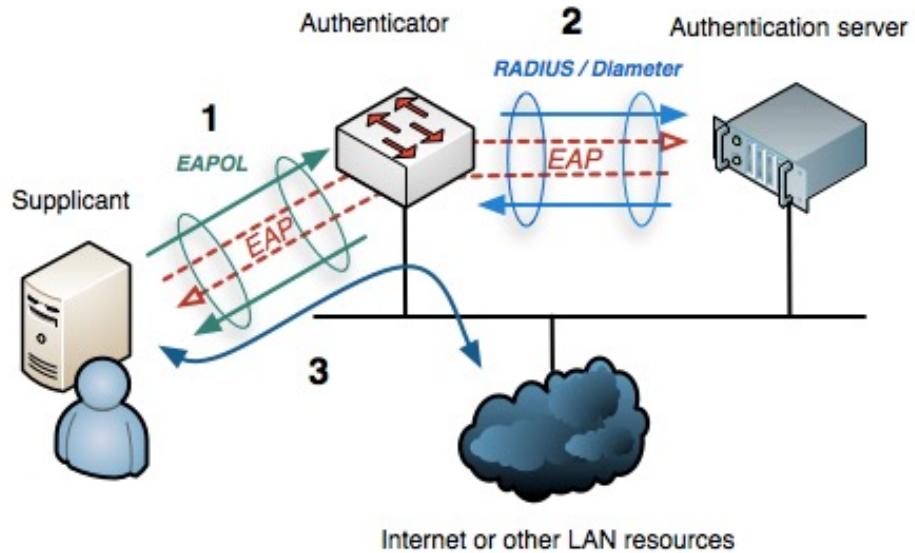
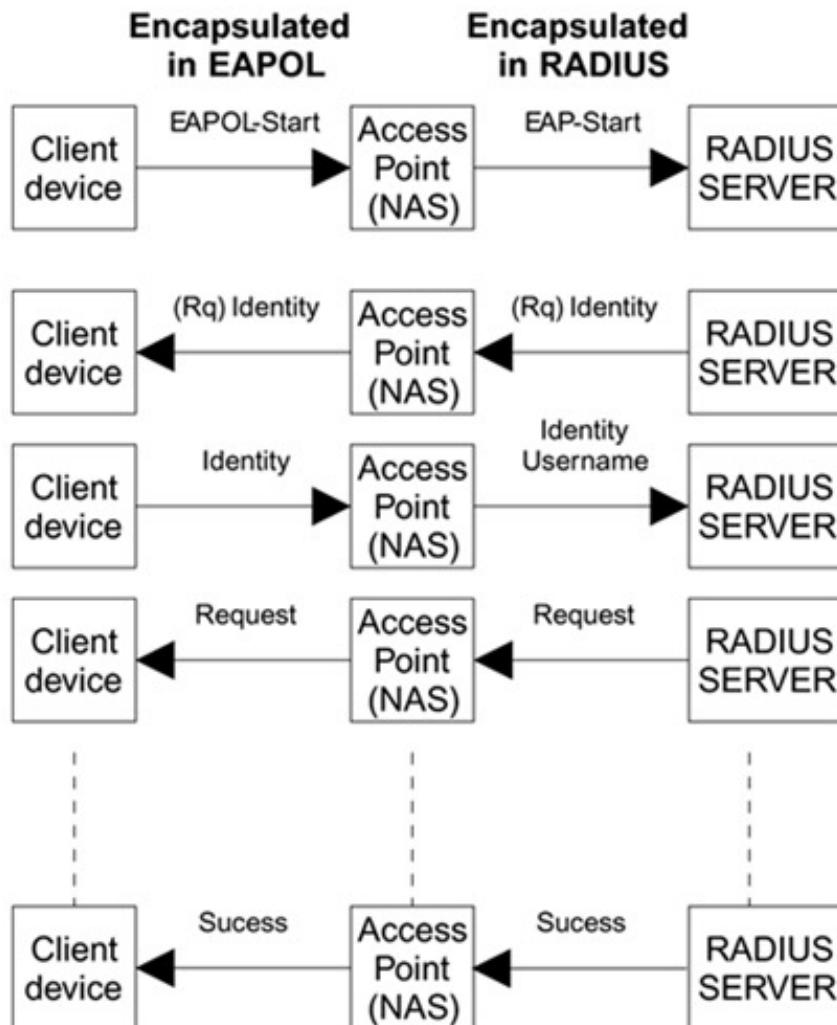


[Source: Course book, Edney &Arbaugh, Chapter 8]

EAPOL Authentication

- Generic framework for authentication
- Encapsulates specific protocols (e.g., TLS, AKA)
- **Goal:** prove that both entities know the same secret
- 4 specific messages: *Request*, *Response*, *Success*, *Failure*

EAPOL Encapsulation



[Source: https://en.wikipedia.org/wiki/IEEE_802.1X]

RADIUS

- Remote Authentication Dial In User Service (RADIUS)
- Defines:
 - A set of functionalities common across authentication servers
 - A protocol that allows accessing these functionalities
- Specified by IETF
- EAP over RADIUS extension (RFC2869)
- Challenge-response mechanism



Network Security

- Lecture 4.2 -

IEEE 802.11i RSN / WPA2

Adela Georgescu*

Faculty of Mathematics and Computer Science
University of Bucharest

*slides belonging to Ruxandra Olimid

Outline

- RNS
- CCMP
- Key Hierarchy
- Security / Attacks

IEEE 802.11 Security

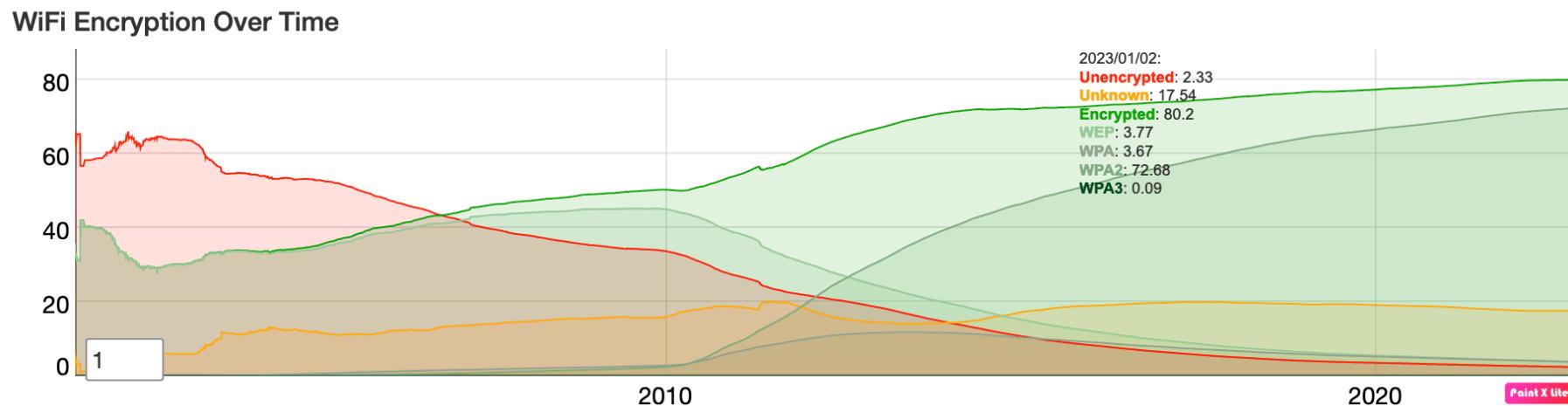
- By default **OFF**
- Authorization to AP based on **MAC address**
- IEEE 802.11: **Wired Equivalent Privacy (WEP)**

Bad designed
- IEEE 802.11i-draft: **WPA (Wi-Fi Protected Access)**

WEP + TKIP (Wi-Fi industry fix)
- IEEE 802.11i: **Robust Security Network (RSN) /WPA2**
- WPA3

Wi-Fi Protected Access II (WPA2)

- Introduced by the Wi-Fi Alliance in 2004 as a long-term solution to replace WEP
- Known as 802.11i
- Used until the introduction of WPA3 (although key reinstallation attacks were published in 2017)

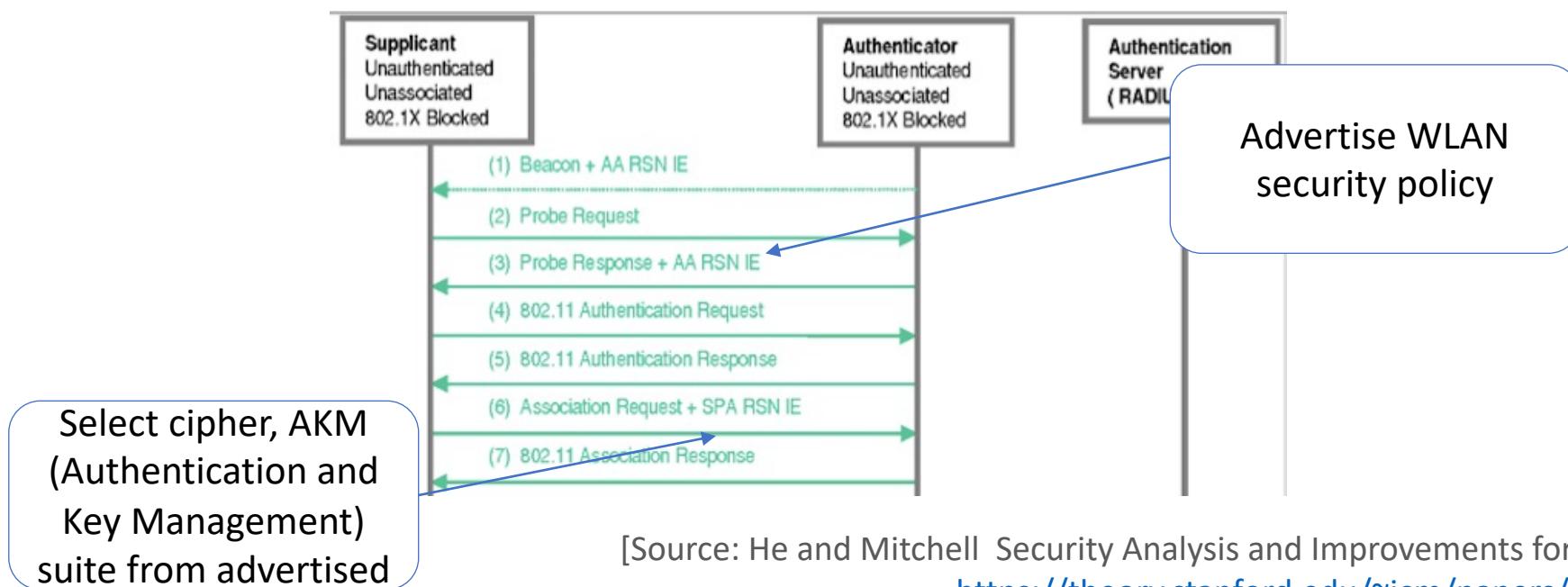


[Source: <https://wigle.net/stats>]

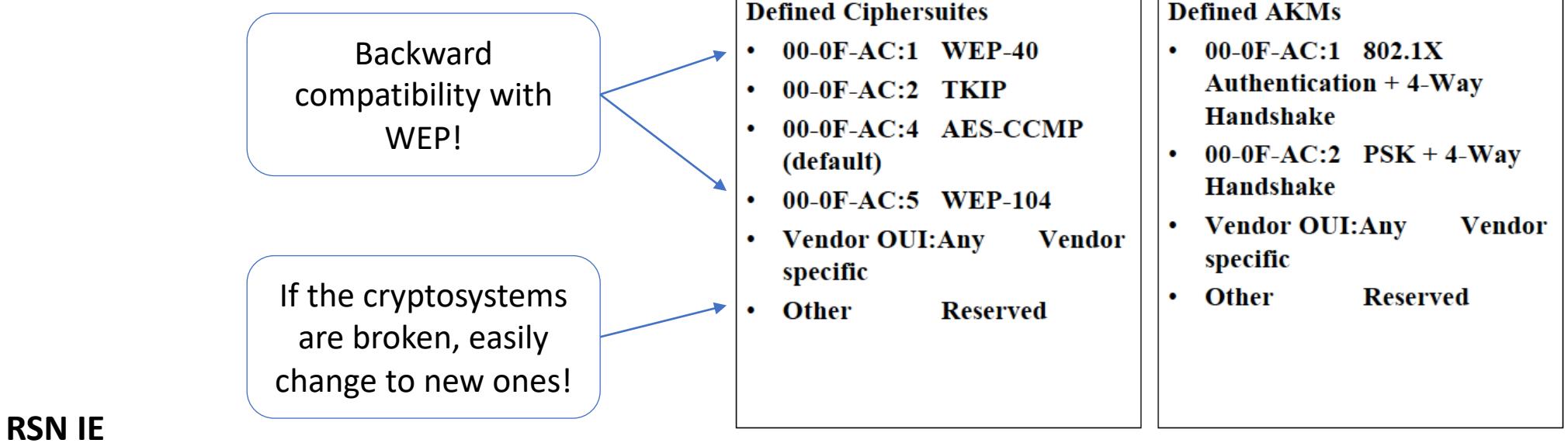
Robust Security Network (RSN)

RSN: a protocol for establishing a secure communication over 802.11 wireless networks

RSN Information Element (IE): data structure for advertising and negotiating security capabilities



Robust Security Network (RSN)



Element ID	Length	Version
Group Key Ciphersuite Selector		
Pairwise Ciphersuite Count	Pairwise Ciphersuite List	
Pairwise Ciphersuite List	AKM Count	
AKM List		
Capabilities	PMK ID Count	
PMK ID List		

[Source: 802.11i Overview doc.: IEEE 802.11-04/0123r1]

Security Goals

Tries to address all known WEP Problems

- Reply detection

Packet Number (PN), replay counter

- Key management protocols

Similar to WPA, discussed in more details

- Access control

Uses **802.1X architecture**

Security Goals

Tries to address all known WEP Problems

- Confidentiality

Uses **Advanced Encryption Standard (AES)**, instead of RC4

- Message integrity and authentication

Uses 128 bits **Counter Mode with CBC-MAC Protocol (CCMP)**

Authenticated encryption using CTR mode and CBC-MAC assumes 128-bit blocks and a single crypto key



[Source: IEEE 802.11i Overview http://ieee802.org/16/liaison/docs/80211-05_0123r1.pdf]

CCM Mode

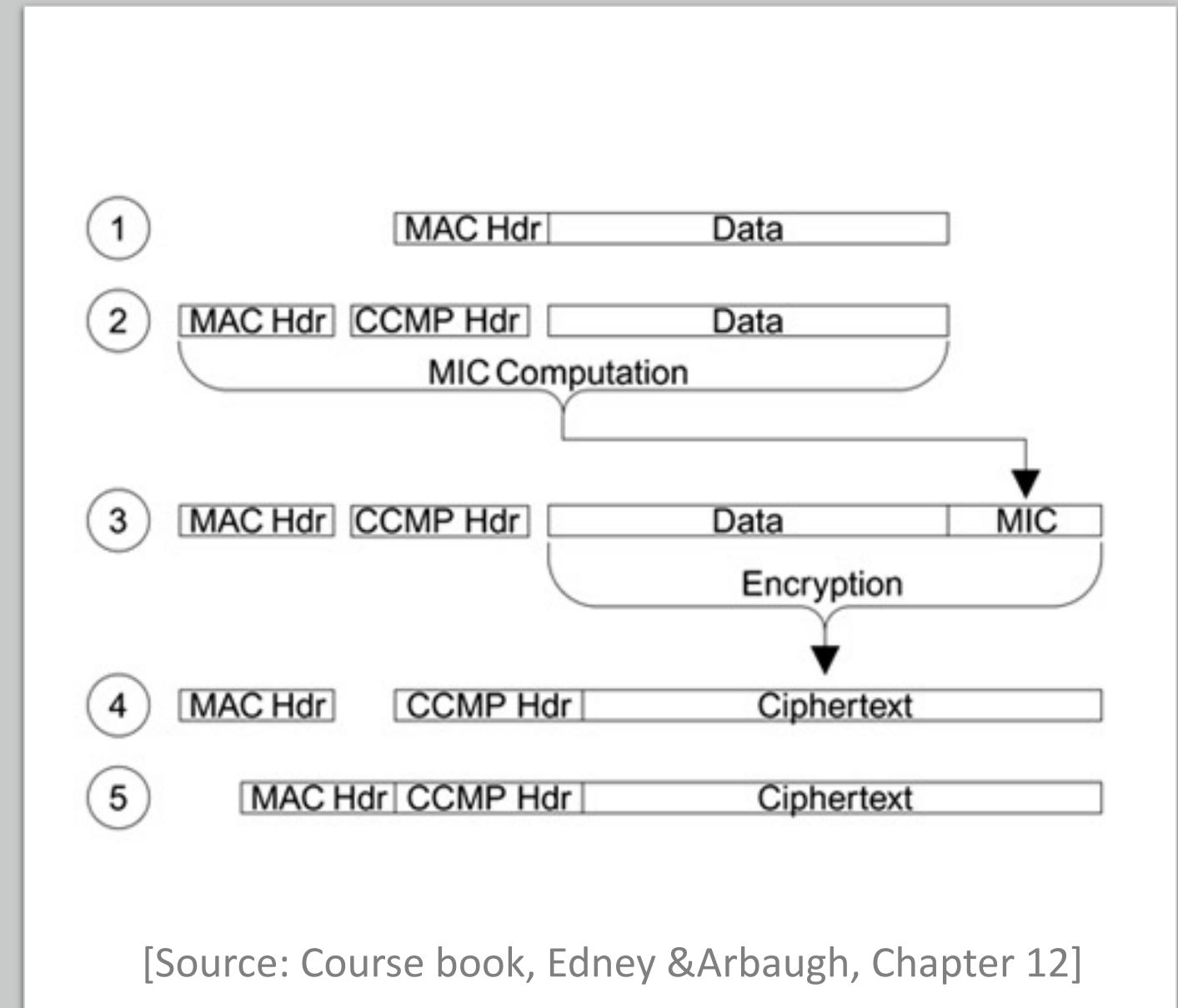
- Authenticated encryption (with associated data) combining CTR mode and CBC-MAC:
 - appends a CBC-MAC on the header, length of the header and plaintext
 - encrypts in CTR mode (plaintext blocks with 1,2,3... and MIC with counter value 0)
- Uses a single crypto key (temporal key shared by STA and AP) and assumes 128-bit blocks



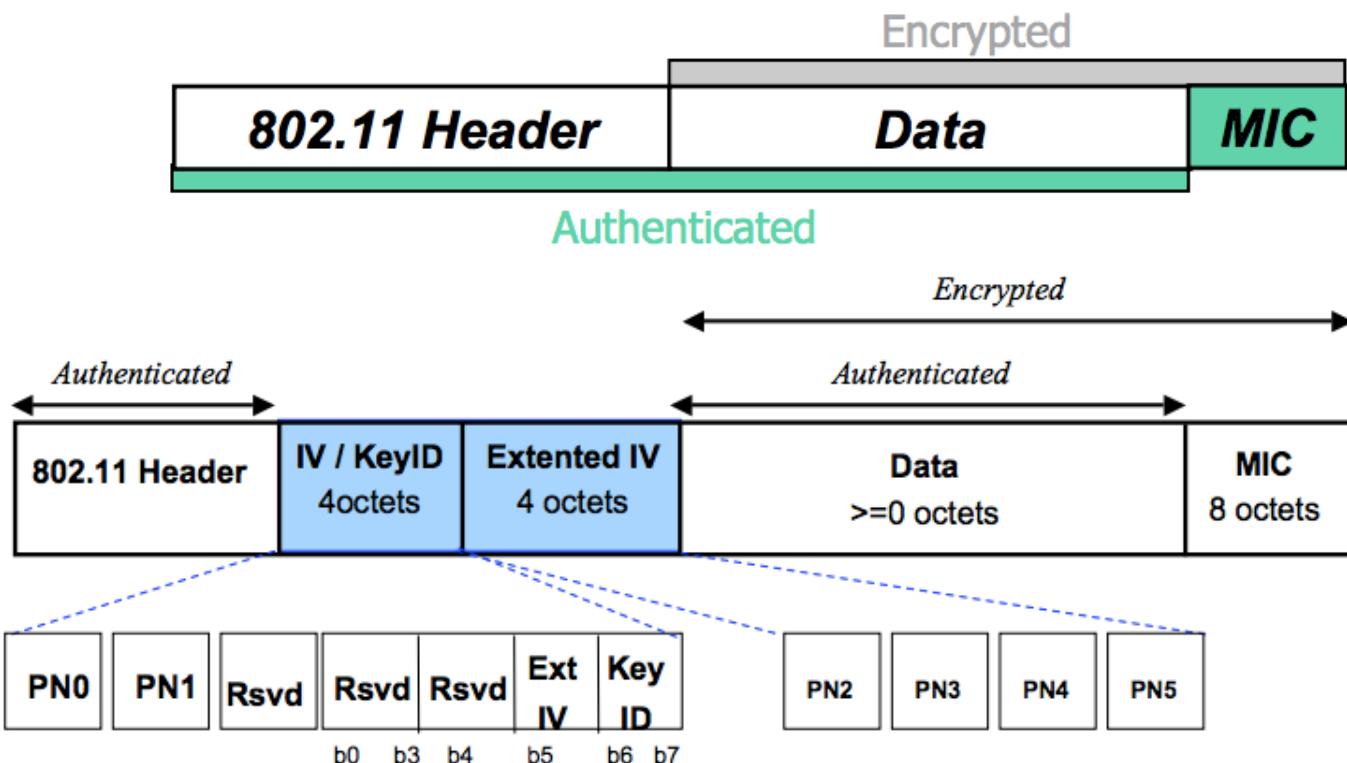
[Source: IEEE 802.11i Overview http://ieee802.org/16/liaison/docs/80211-05_0123r1.pdf]

CCM Mode

- 1) Unencrypted MPDU; MAC header contains source and destination addresses;
- 2) CCMP header (32 bits) is constructed
- 3) MIC is computed to protect fields from the MAC header, the CCMP header and the data
- 4) Data and MIC are encrypted; CCMP header is pre-appended
- 5) MAC header is pre-appended



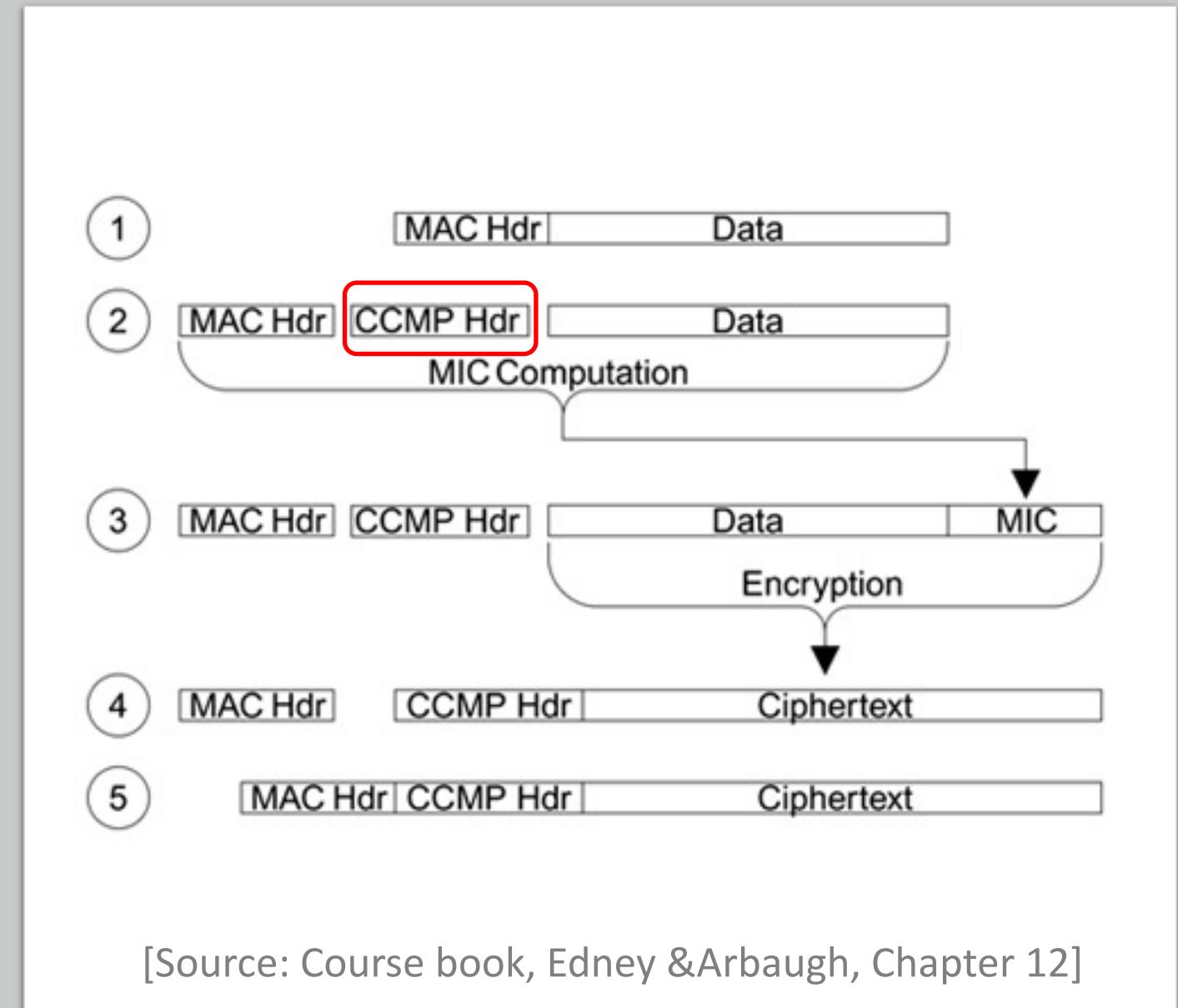
CCMP MPDU Format



[Source: IEEE 802.11i Overview http://ieee802.org/16/liaison/docs/80211-05_0123r1.pdf]

CCM Mode

- 1) Unencrypted MPDU; MAC header contains source and destination addresses;
- 2) CCMP header (32 bits) is constructed
- 3) MIC is computed to protect fields from the MAC header, the CCMP header and the data
- 4) Data and MIC are encrypted; CCMP header is pre-appended
- 5) MAC header is pre-appended

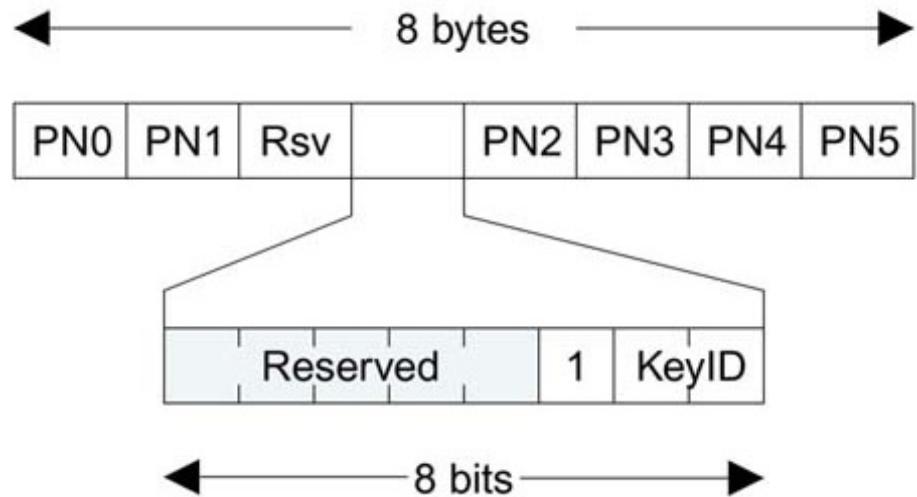


CCMP Header

Purposes:

- Provides the **Packet Number (PN)** that provides replay protection and gives to the receiver the nonce required for decryption
- In case of multicast, it gives to the receiver the group key used for encryption

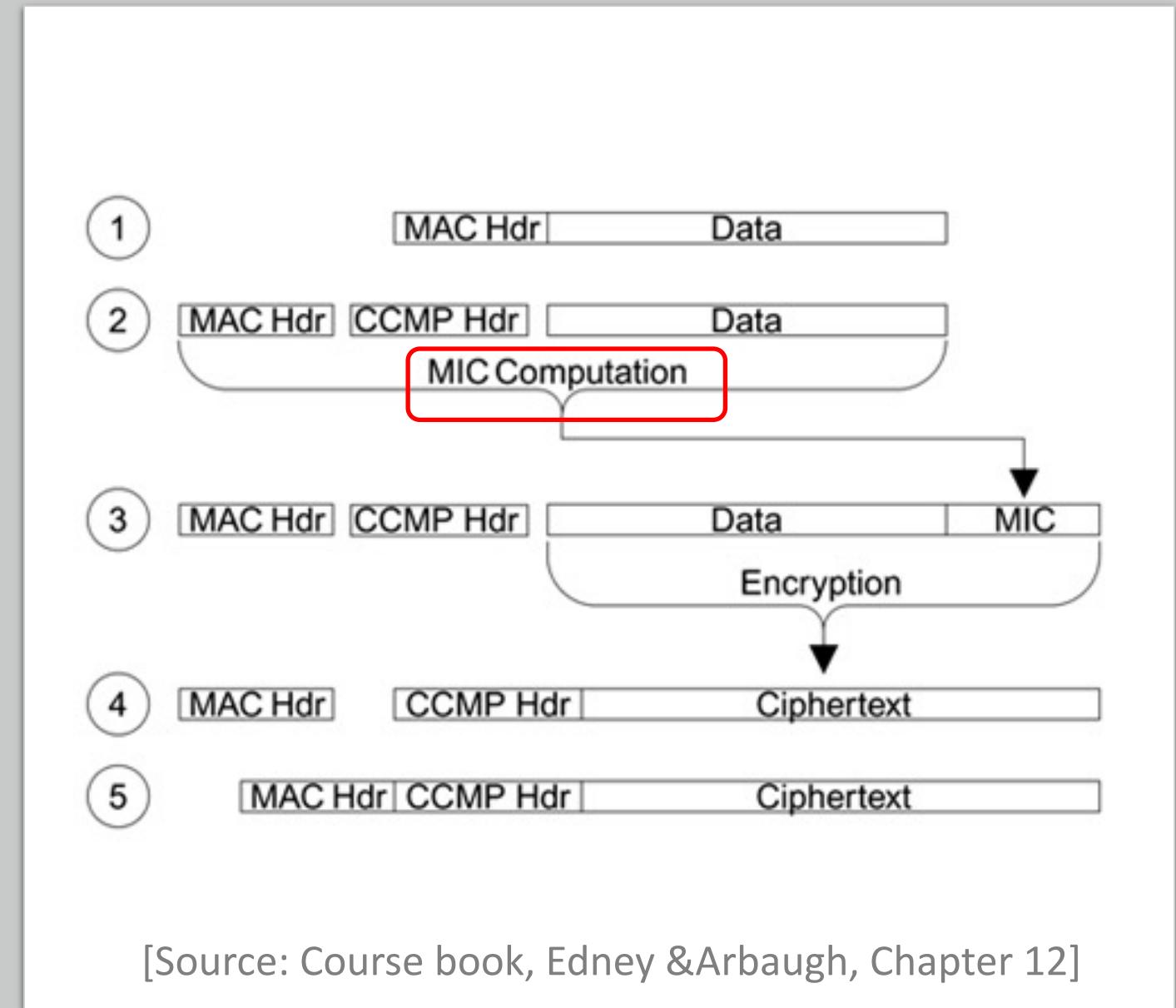
- Packet Number (PN): 48 bits (6 bytes)
- 1: indicates RSN
- KeyID: to select the group key id (from max.4 provisioned)



[Source: Course book, Edney & Arbaugh, Chapter 12]

CCM Mode

- 1) Unencrypted MPDU; MAC header contains source and destination addresses;
- 2) CCMP header (32 bits) is constructed
- 3) MIC is computed to protect fields from the MAC header, the CCMP header and the data
- 4) Data and MIC are encrypted; CCMP header is pre-appended
- 5) MAC header is pre-appended

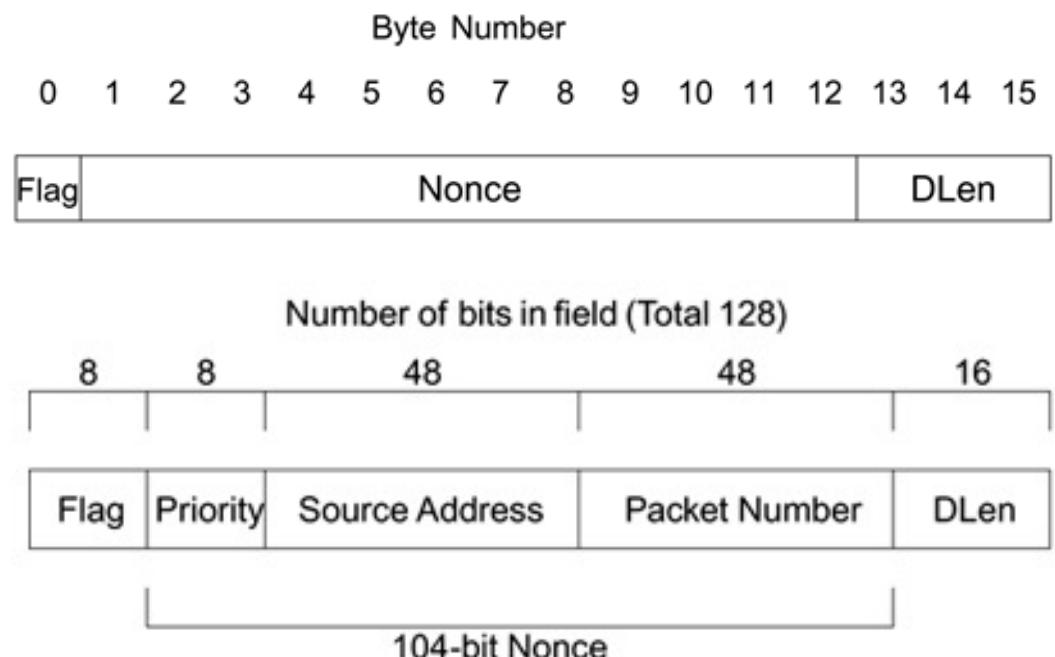


MIC Computation

- Uses **CBC-MAC**, with a starting block – see CCMP Encapsulation slide
- 64-bit (8 bytes) MIC, so last 64 bits are discarded

Starting block (IV) is formed in a special way:

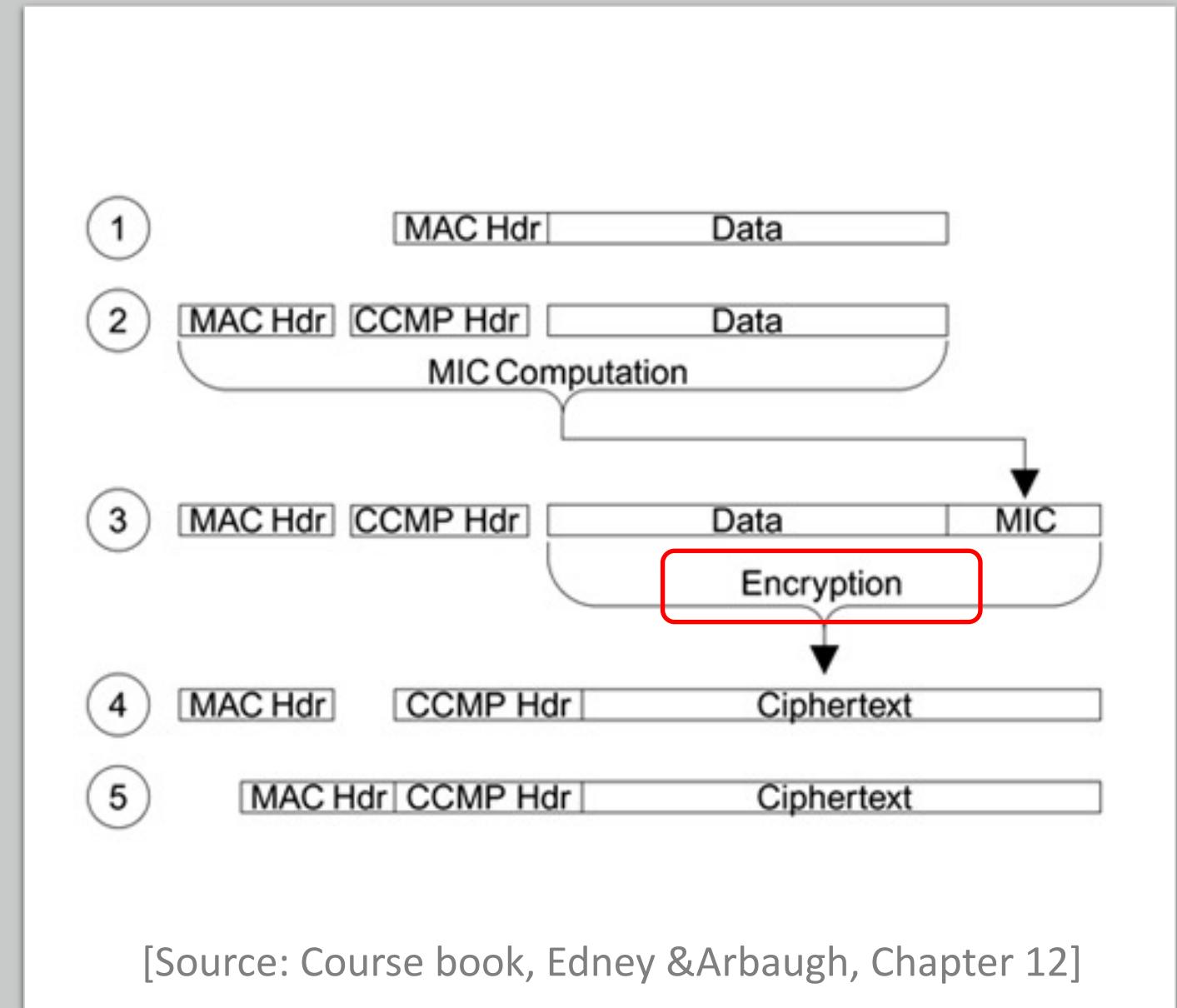
- **Flag:** 01011001 (fixed)
- **Nonce:** contains both the PN and the source address to assure uniqueness (the PN could have been already used by one of the two communicating parties in another conversation); priority might refer to different streams (audio, video, etc.);
- **DLen:** length of the data



[Source: Course book, Edney &Arbaugh, Chapter 12]

CCM Mode

- 1) Unencrypted MPDU; MAC header contains source and destination addresses;
- 2) CCMP header (32 bits) is constructed
- 3) MIC is computed to protect fields from the MAC header, the CCMP header and the data
- 4) Data and MIC are encrypted; CCMP header is pre-appended
- 5) MAC header is pre-appended

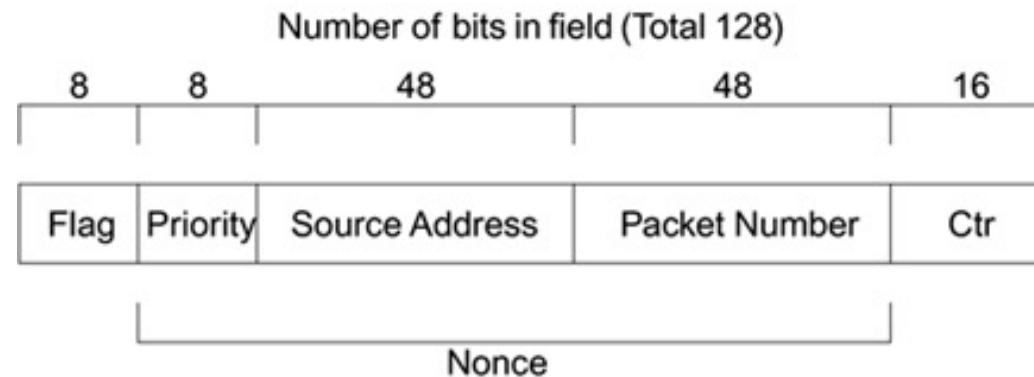


Encryption

- Uses **CTR-AES**

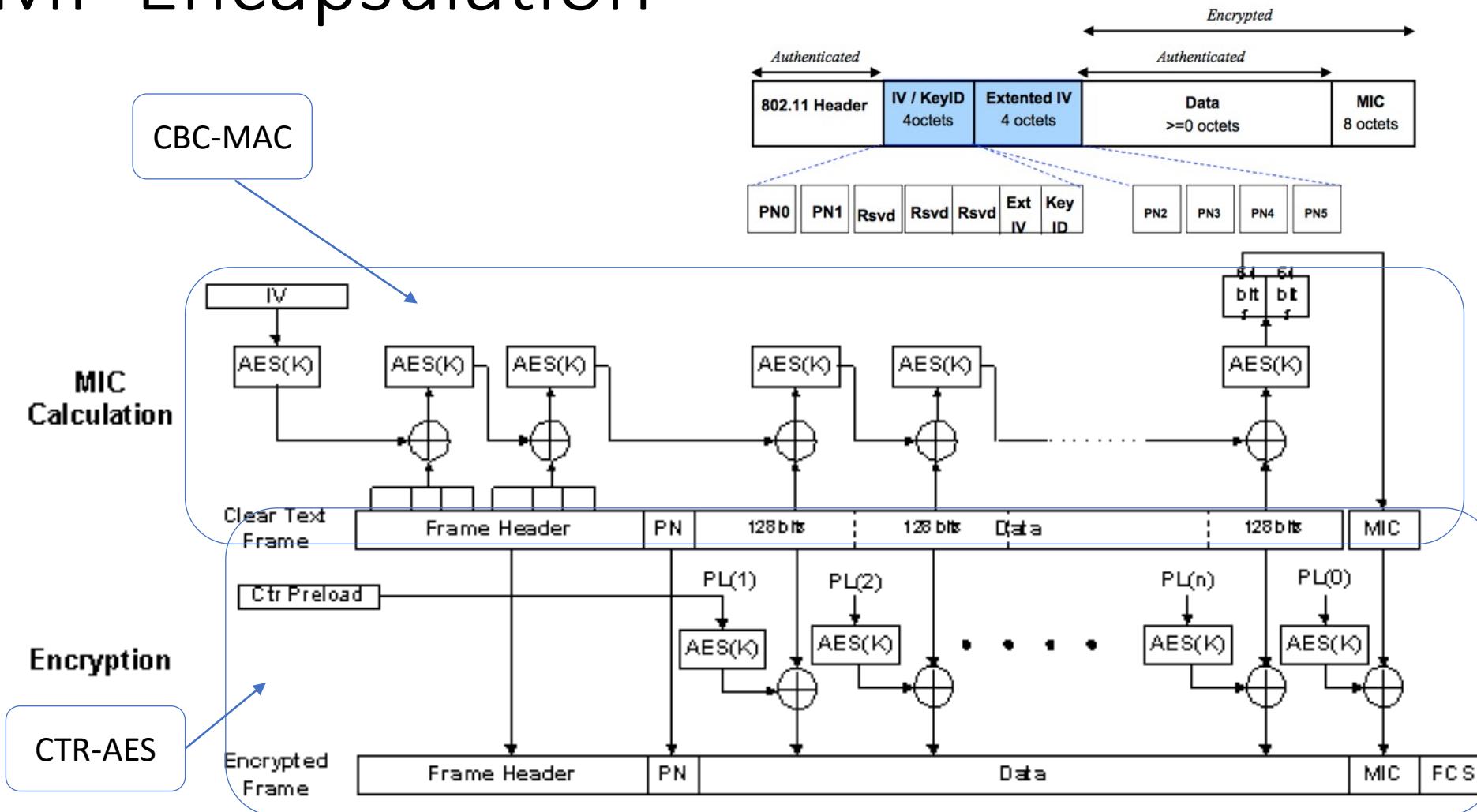
Counter block (PL0,PL1...):

- **Flag:** 01011001 (fixed)
- **Nonce:** contains both the PN and the source address to assure uniqueness (the PN could have been already used by one of the two communicating parties in another conversation); priority might refer to different streams (audio, video, etc.);
- **Ctr:** starts at 1 and increases



[Source: Course book, Edney & Arbaugh, Chapter 12]

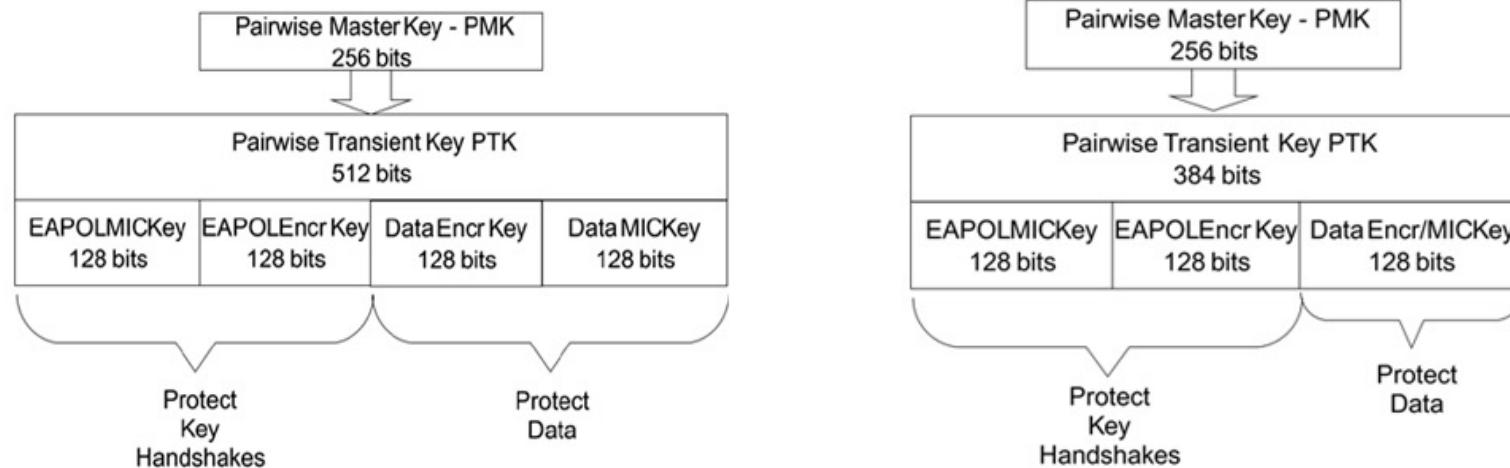
CCMP Encapsulation



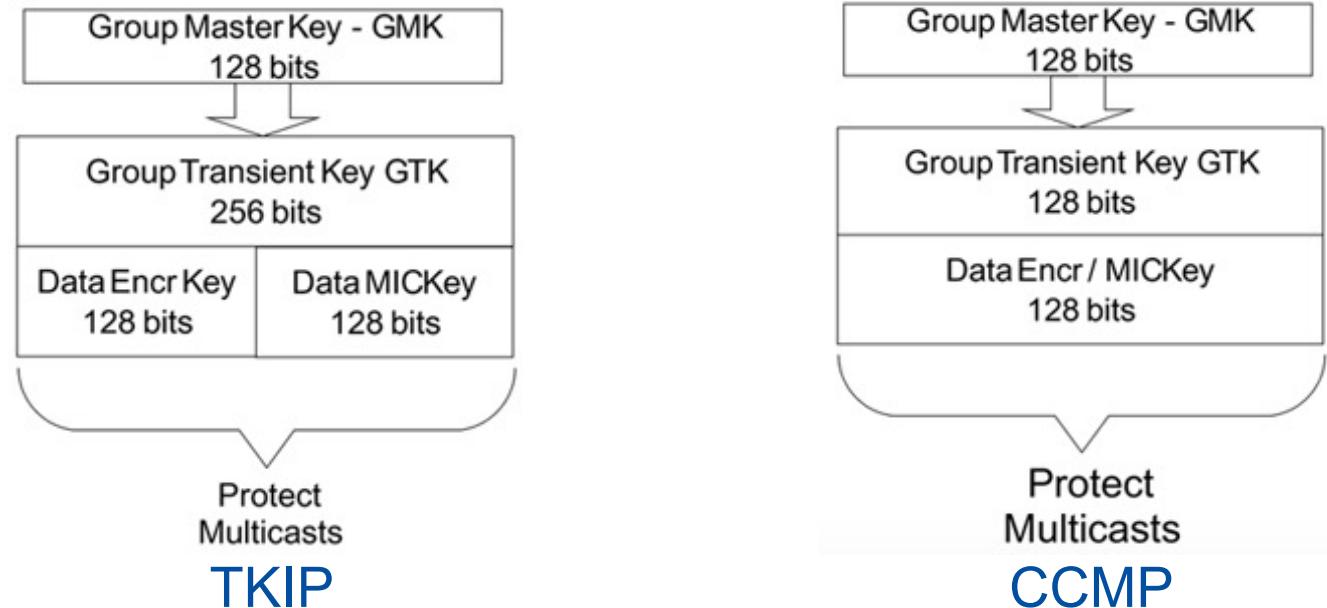
More details in the course book – Edney & Arbaugh, Chapter 12

Key hierarchy (TKIP vs CCMP)

Pairwise



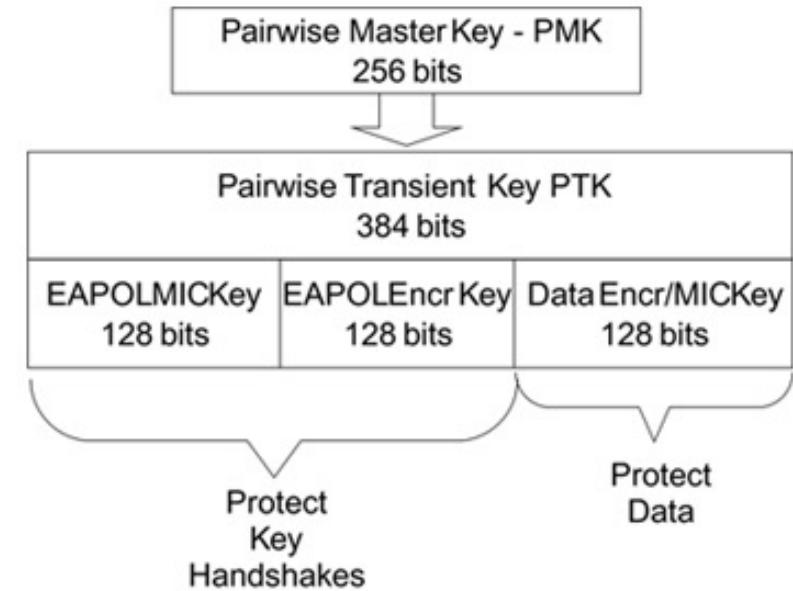
Group



[Source: Course book, Edney & Arbaugh, Chapter 10]

Pairwise CCMP Key Hierarchy

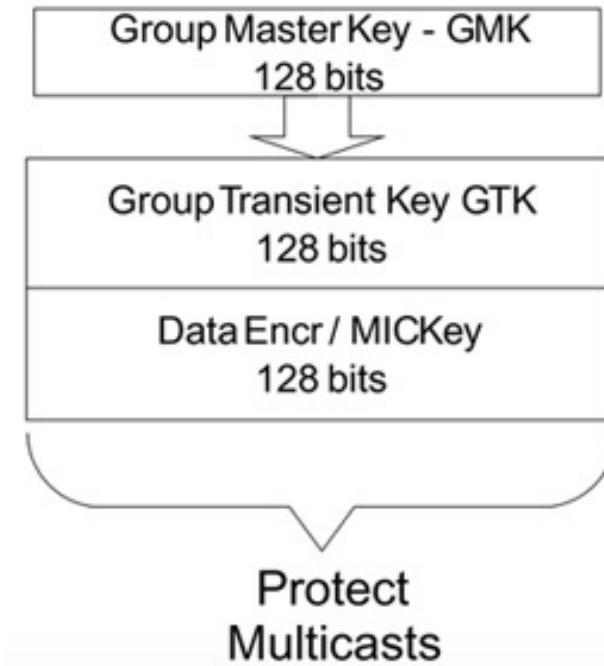
- **Pairwise Master Key (PMK):**
 - 256 bits, symmetric key
 - Preshared or server supplied by upper layers (e.g.: authentication server sends to AP)
- **Pairwise Transient Key (PTK):**
$$PTK = f(PMK, NonceA, NonceB, A, B)$$
- **Temporal Keys:**
 - Up to 3 keys (128 bits):
 - EAPOL-keys: encryption key, integrity key
 - Data encryption and data integrity key (**a single key!**)



[Source: Course book, Edney & Arbaugh, Chapter 10]

Group CCMP Key Hierarchy

- Used for multi- and broadcast communication
- **Group Master Key (GMK):**
 - 256 bits, symmetric key
 - Generated by the AP
- **Group Transient Keys (GTK):**
$$GTK = f(GMK, Nonce, AP)$$
- **Temporal Key:**
 - Encryption and integrity key 128 bits
(a single key!)



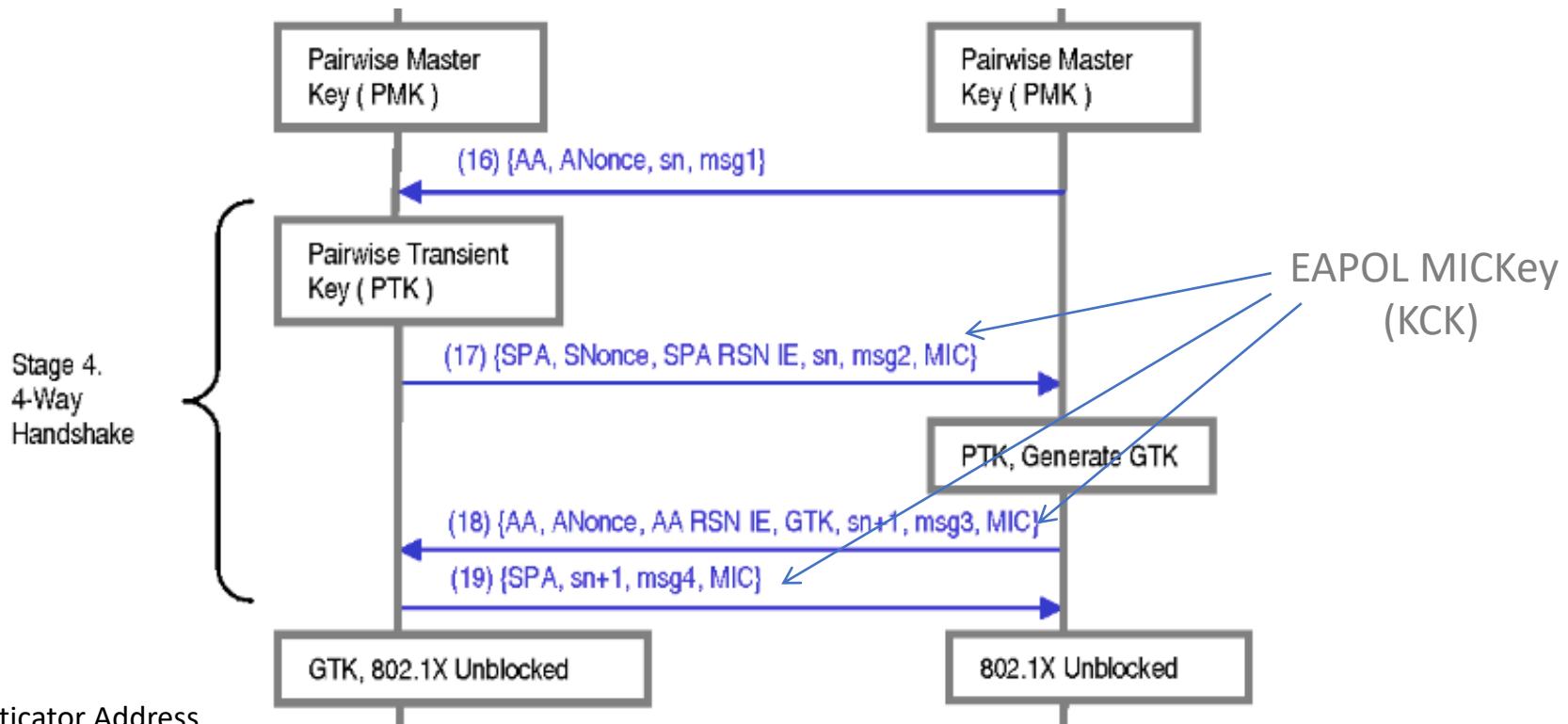
[Source: Course book, Edney & Arbaugh, Chapter 10]

802.11 Key Derivation Function (KDF)

$$\text{PTK} \leftarrow \text{KDF}(\text{PMK}, \min\{\text{Addr}_{AP}, \text{Addr}_{STA}\} \parallel \max\{\text{Addr}_{AP}, \text{Addr}_{STA}\}, \max\{N_{AP}, N_{STA}\})$$

- KDF is based on **HMAC-SHA-1**

4-Way Handshake protocol



AA: Authenticator Address

SPA: Supplicant Address

ANonce: nonce generated by the Authenticator (AP)

SNonce: nonce generated by the Supplicant (STA)

sn: sequence number

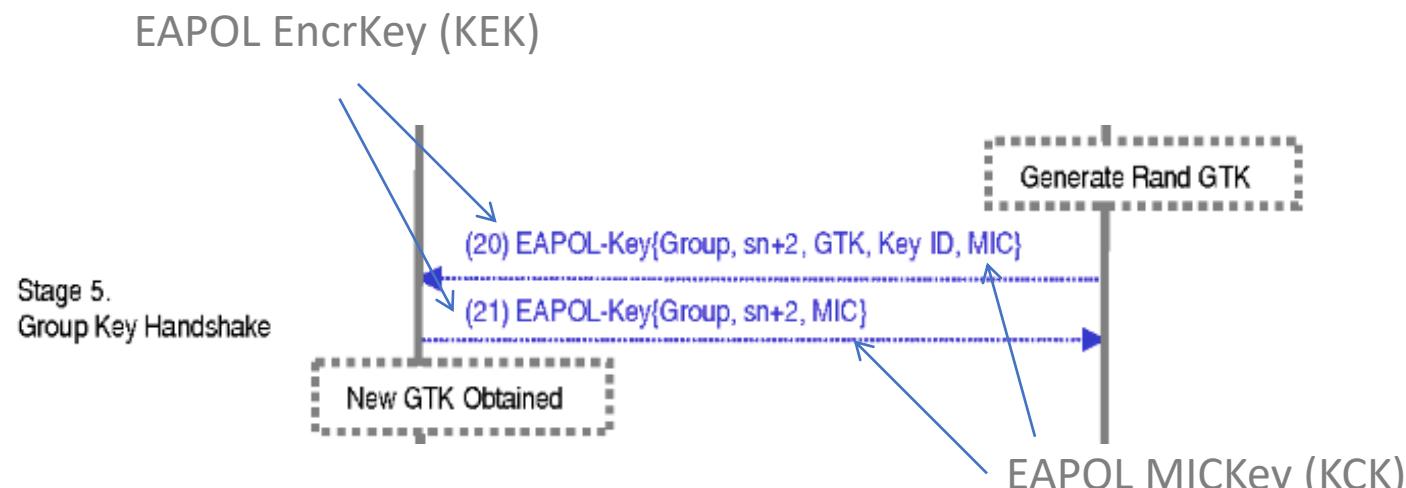
Encrypted data communication follows

[Source: He and Mitchell Security Analysis and Improvements for IEEE 802.11i
<https://theory.stanford.edu/~jcm/papers/NDSS05.pdf>]

4WHS properties

- No **forward secrecy**
 - PMK + MACs + Nonces enough to derive PTK
 - Can decrypt old recorded communication sessions
- Vulnerable to dictionary attacks
 - If PMK derived from weak password
 - Capture MACs + Nonces → guess password → derive PMK

Group Key Generation and Distribution



Encryption data communication follows

AA: Authenticator Address

SA: Suplicant Address

ANonce: nonce generated by
the Authenticator (AP)

SNonce: nonce generated by
the Suplicant (STA)

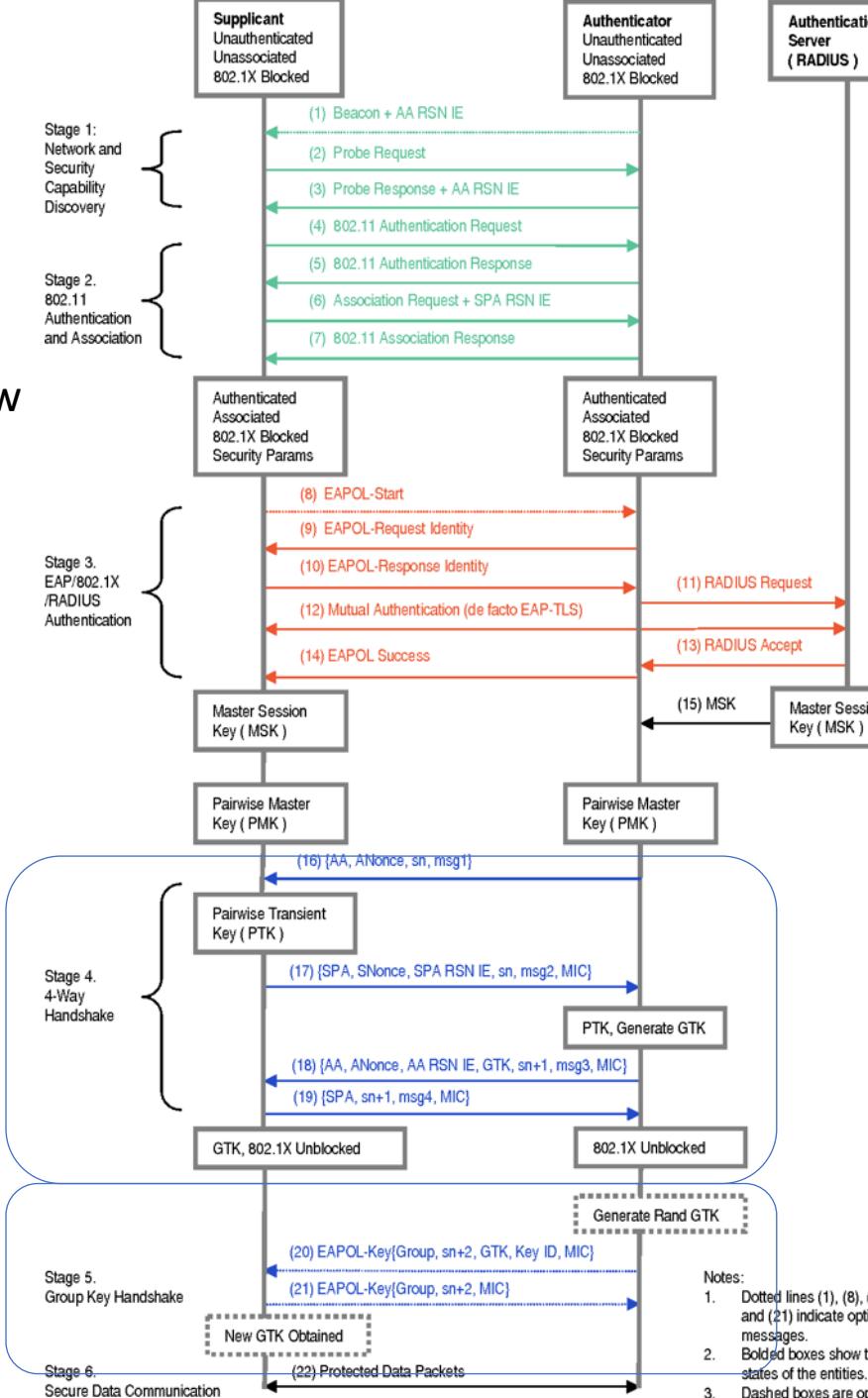
sn: sequence number

[Source: He and Mitchell Security Analysis and Improvements for IEEE 802.11i
<https://theory.stanford.edu/~jcm/papers/NDSS05.pdf>]

RSN/WPA2

Association Overview

RSN IE: RSN Identification Element (set of capabilities)
 AA: Authenticator Address
 SA: Supplicant Address
 ANonce: nonce generated by the Authenticator (AP)
 SNonce: nonce generated by the Supplicant (STA)

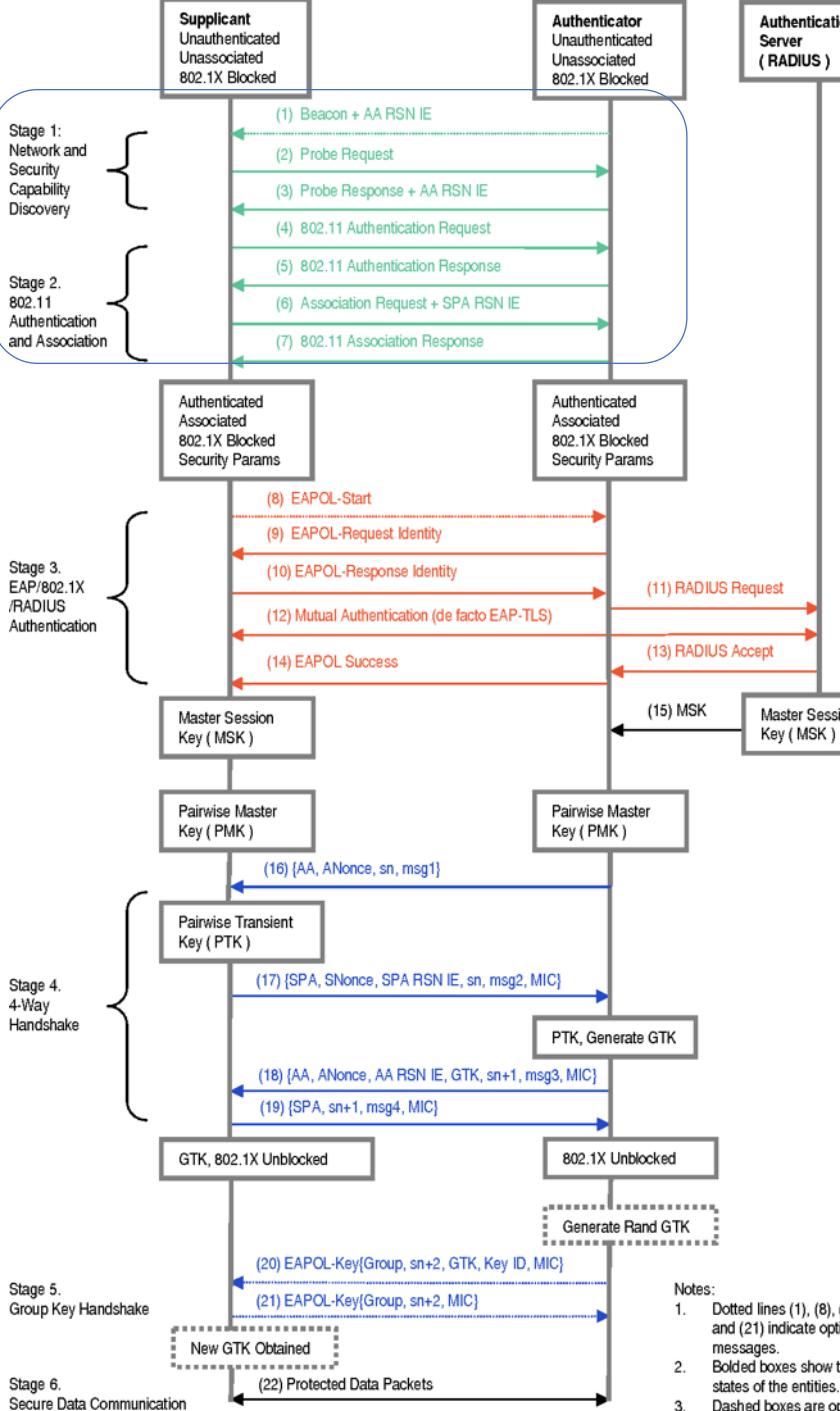


[Source: He and Mitchell Security Analysis and Improvements for IEEE 802.11i
<https://theory.stanford.edu/~jcm/papers/NDSS05.pdf>]

RSN/WPA2

Association Overview

RSN IE: RSN Identification Element (set of capabilities)
 AA: Authenticator Address
 SA: Supplicant Address
 ANonce: nonce generated by the Authenticator (AP)
 SNonce: nonce generated by the Supplicant (STA)



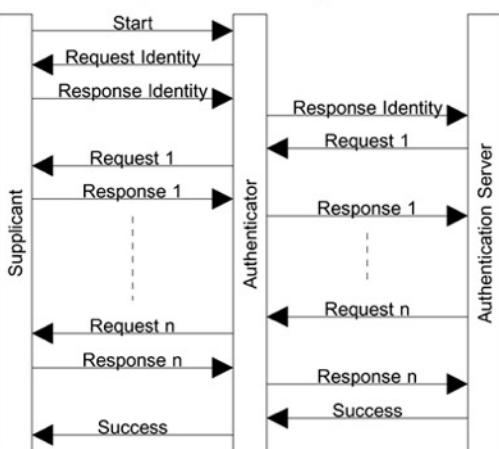
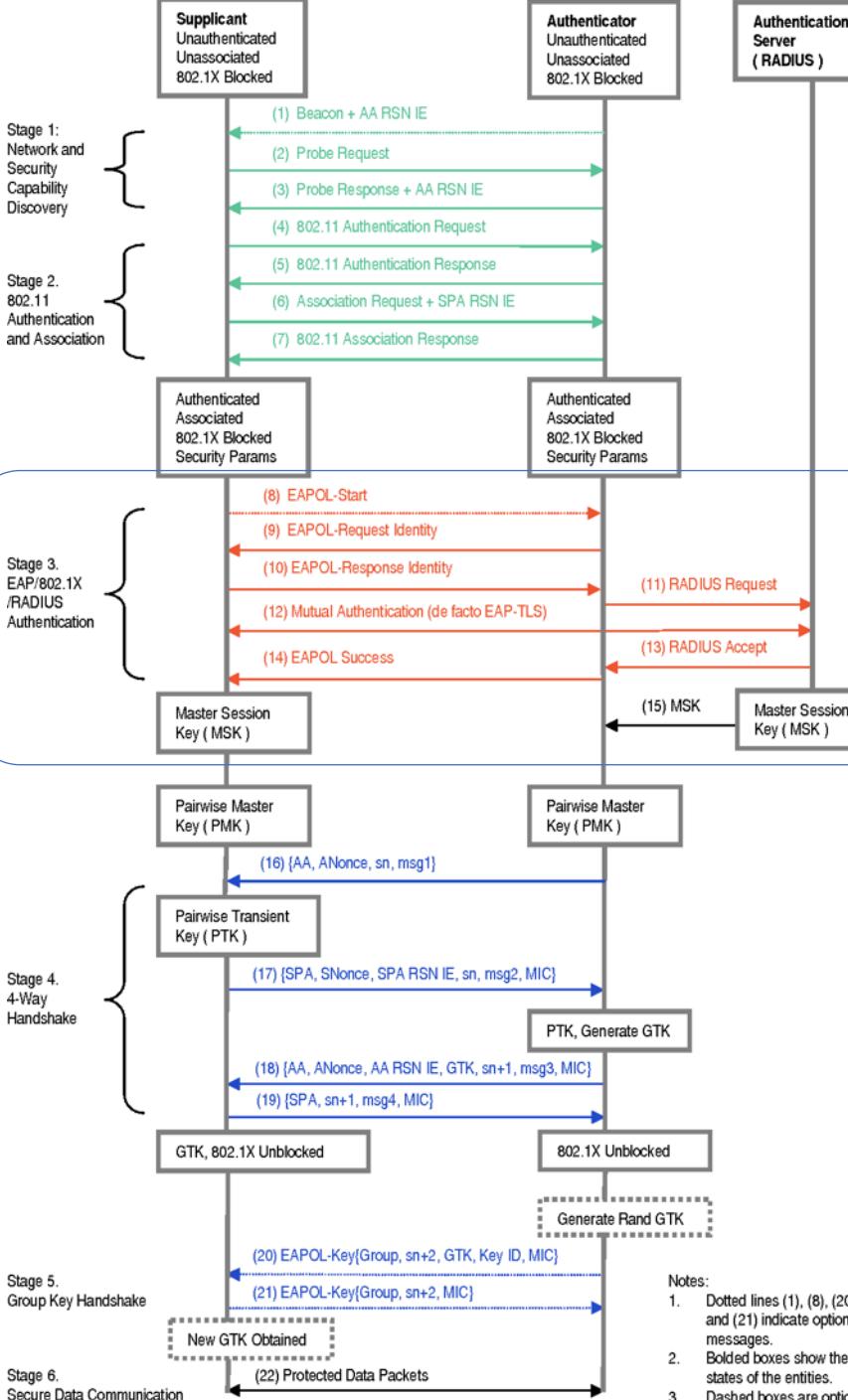
[Source: He and Mitchell Security Analysis and Improvements for IEEE 802.11i
<https://theory.stanford.edu/~jcm/papers/NDSS05.pdf>]

RSN/WPA2

Association Overview

Both parties prove to know the same MSK

RSN IE: RSN Identification Element (set of capabilities)
 AA: Authenticator Address
 SA: Suplicant Address
 ANonce: nonce generated by the Authenticator (AP)
 SNonce: nonce generated by the Suplicant (STA)

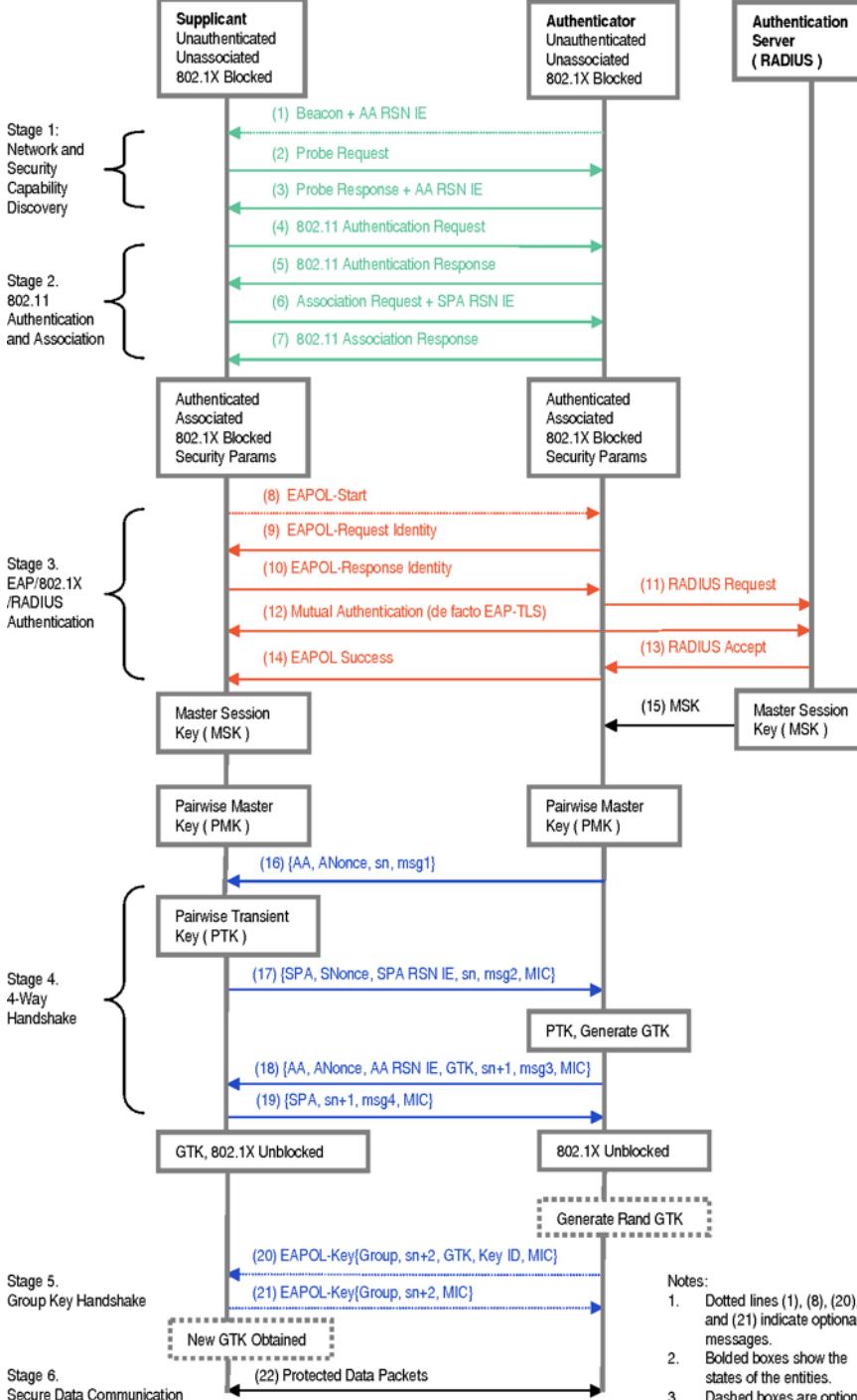


Remember 802.1x
 [Source: Course book, Edney &Arbaugh, Chapter 8]

RSN/WPA2

Association Overview

RSN IE: RSN Identification Element (set of capabilities)
 AA: Authenticator Address
 SA: Suplicant Address
 ANonce: nonce generated by the Authenticator (AP)
 SNonce: nonce generated by the Suplicant (STA)



[Source: He and Mitchell Security Analysis and Improvements for IEEE 802.11i
<https://theory.stanford.edu/~jcm/papers/NDSS05.pdf>]

Security / Attacks

- CCM Mode: theoretical security proof

[Jonsson, J. (2003, January). On the security of CTR+ CBC-MAC. In SelectedAreas in Cryptography(pp. 76-93). Springer Berlin Heidelberg]

- In practice: does the security proof model applies to the protocol?



The screenshot shows the homepage of the KRACK attacks website. At the top left is a graphic of a Wi-Fi signal with a red arrow pointing through it, and a padlock with a red arrow pointing towards it. To the right of the graphic, the title "Key Reinstallation Attacks" is displayed in large bold letters, followed by the subtitle "Breaking WPA2 by forcing nonce reuse". Below the title, a note states "Discovered by [Mathy Vanhoef](#) of [imec-DistriNet](#), KU Leuven". A navigation bar at the bottom includes links for "INTRO", "DEMO", "DETAILS", "PAPER", "TOOLS", and "Q&A". The main content area is titled "INTRODUCTION" in blue capital letters. The text describes the discovery of serious weaknesses in WPA2, noting that an attacker can exploit these using "key reinstallation attacks (KRACKs)". It explains that attackers can read previously assumed-to-be-secure encrypted information, steal sensitive data like credit card numbers and passwords, and inject or manipulate data. The attack is said to work against all modern protected Wi-Fi networks.

<https://www.krackattacks.com/>

Paper: <https://papers.mathyvanhoef.com/ccs2017.pdf>

Video: <https://youtu.be/Oh4WURZoR98>

WPA2

- We will look into WPA3 next time



Network Security

- Lecture 5 -

WPA3

Adela Georgescu*

Faculty of Mathematics and Computer Science
University of Bucharest

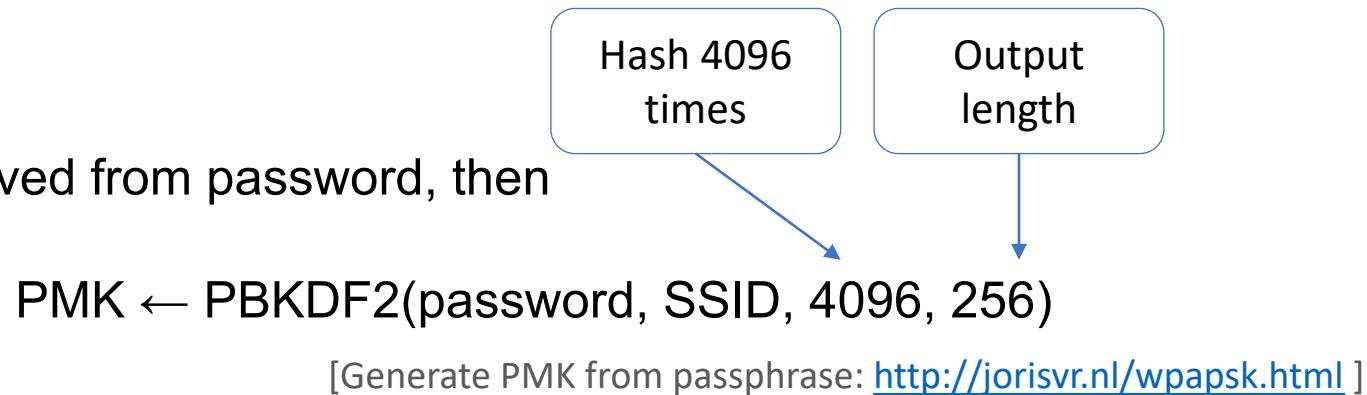
*slides belonging to Ruxandra Olimid

Outline

- WPA2 security issues
- Introduce WPA3
- SAE
- Dragonfly Handshake
- Attacks / Vulnerabilities

WPA2-PSK: Problem 1 – Scalability, Dynamicity

- The same value PSK (=PMK) for all entities in WLAN



- If PMK is derived from password, then

$$\text{PMK} \leftarrow \text{PBKDF2}(\text{password}, \text{SSID}, 4096, 256)$$

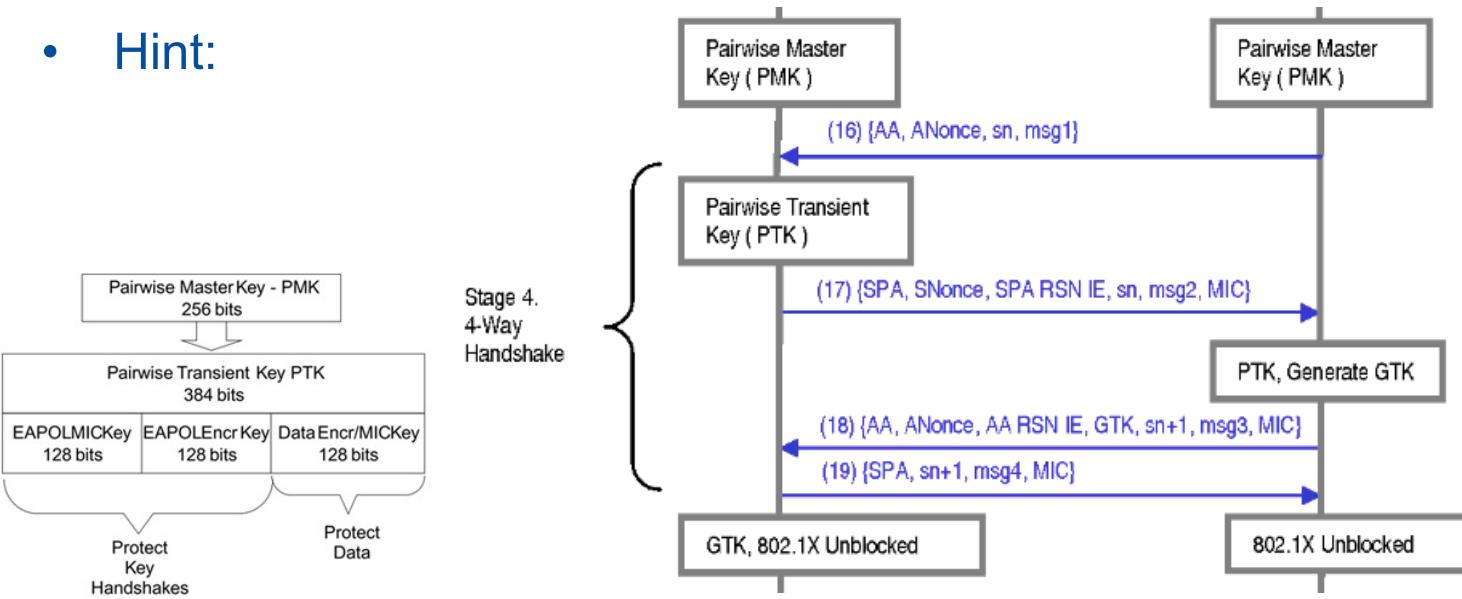
[Generate PMK from passphrase: <http://jorisvr.nl/wpapsk.html>]

- **Question:** What are the problems here?
- **Answer:**
 - PSK has to be manually installed on APs and STAs, so it is not scalable
 - When changing the password, all equipment must be updated
 - If one piece of equipment is compromised, all are compromised

WPA2-PSK: Problem 2 - Insider Attack

- **Question:** Why WPA2-PSK is vulnerable to *insider attack*?

- **Hint:**



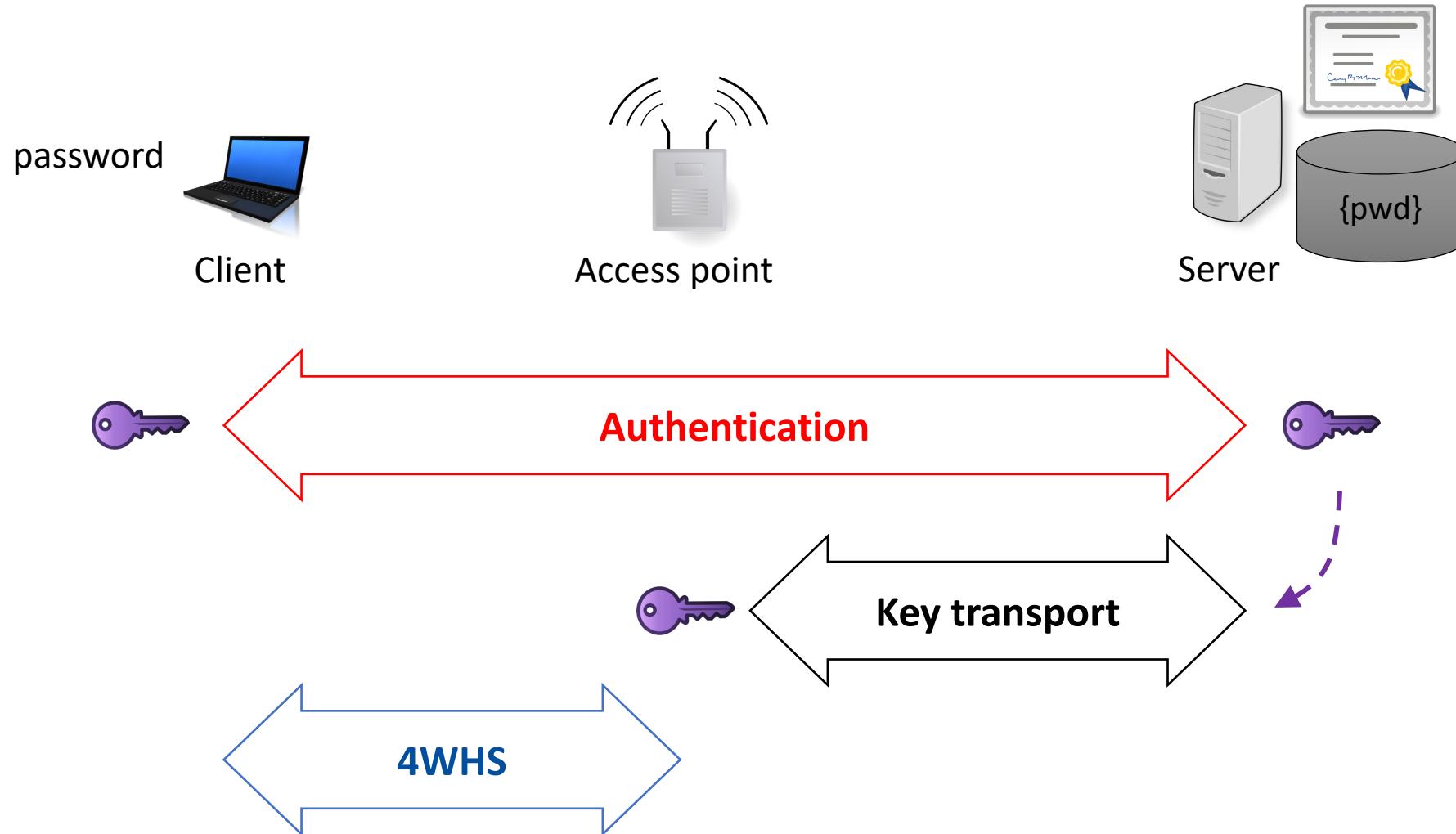
- **Answer:** An insider can eavesdrop on the nonce values and determine the CCMP key, so both confidentiality and integrity are compromised

[Source: He and Mitchell Security Analysis and Improvements for IEEE 802.11i
<https://theory.stanford.edu/~jcm/papers/NDSS05.pdf>]

WPA2-PSK: Problem 3 - Outsider Attack

- **Question:** Why is WPA2-PSK vulnerable (outsider attack) if PSK is a weak password?
- **Answer:** It is vulnerable to *dictionary attack*

WPA2-Enterprise

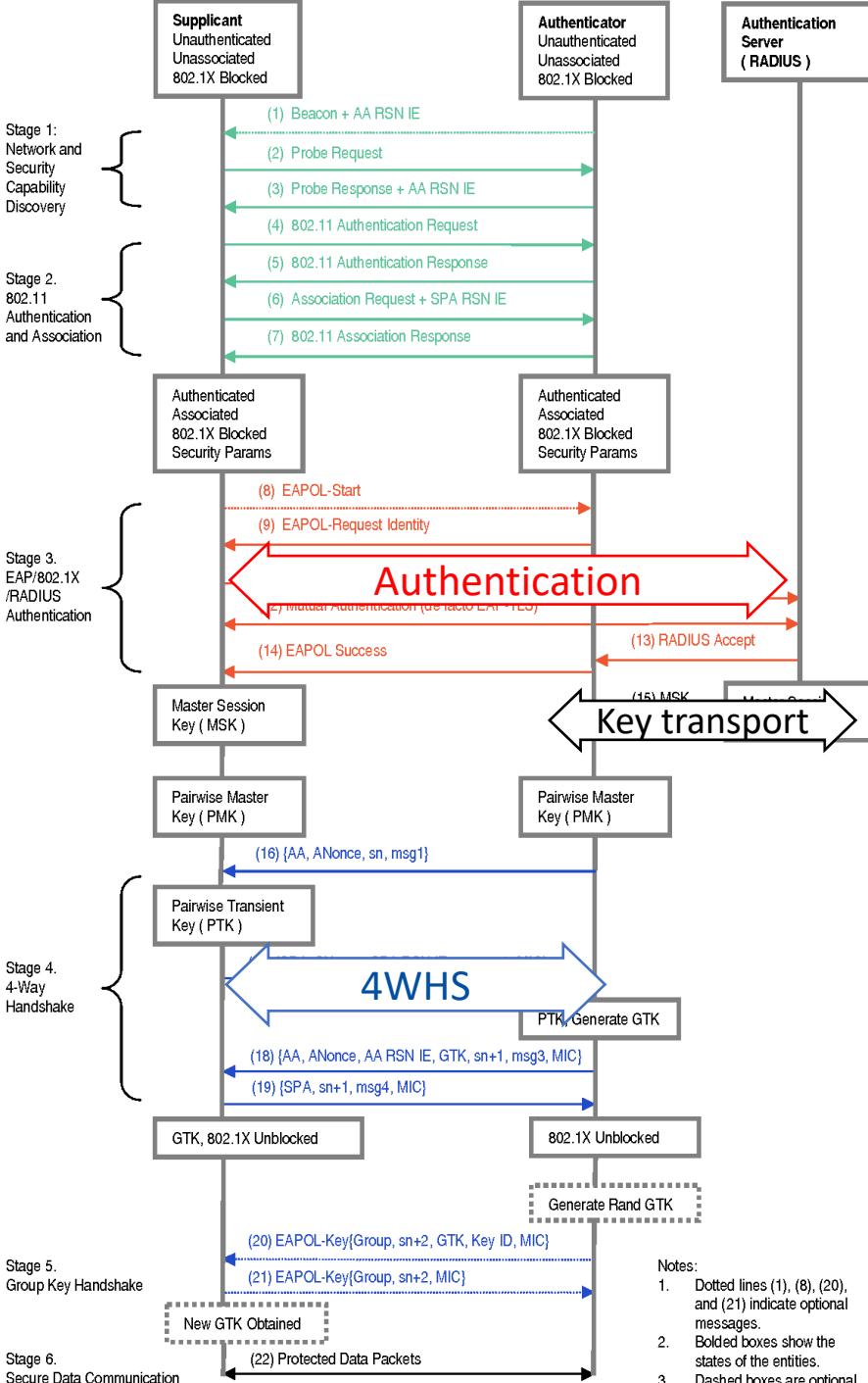


[Slide ack: Håkon Jacobsen]

RSN/ WPA2

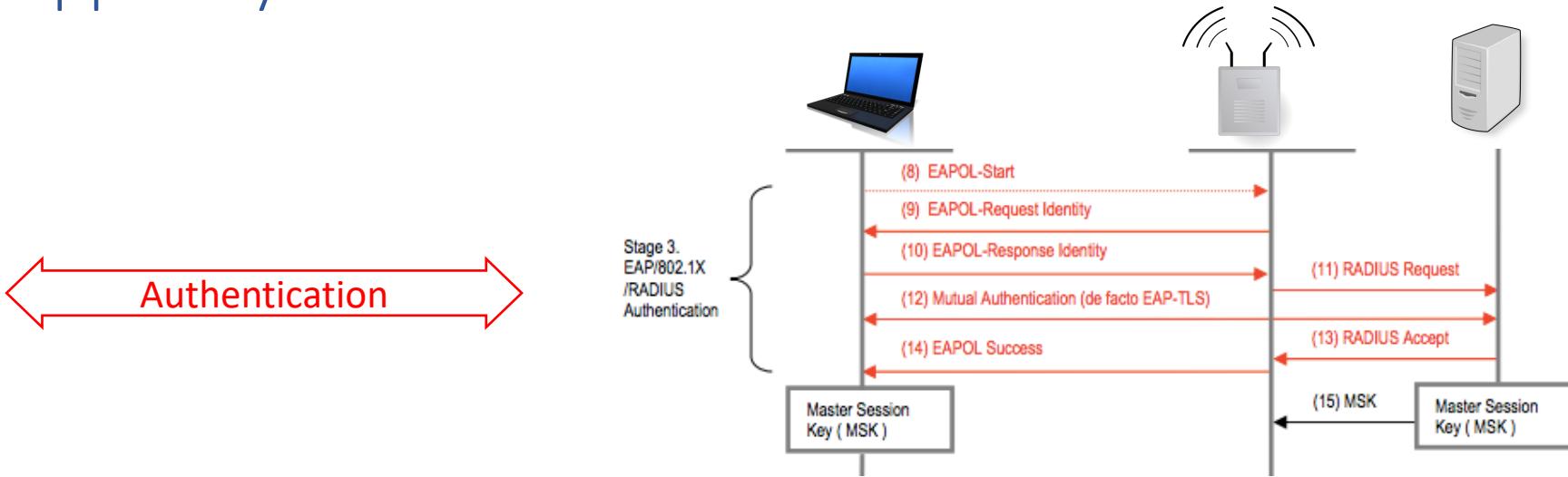
Association Overview

RSN IE: RSN Identification Element (set of capabilities)
 AA: Authenticator Address
 SA: Supplicant Address
 ANonce: nonce generated by the Authenticator (AP)
 SNonce: nonce generated by the Supplicant (STA)



[Source: He and Mitchell Security Analysis and Improvements for IEEE 802.11i
<https://theory.stanford.edu/~jcm/papers/NDSS05.pdf>]

Upper-layer Authentication



- Methods that can be used for authentication in RSN:
 - Protected EAP (PEAP)
 - Transport Layer Security (TLS) – default for WPA
 - GSM-SIM
 - ... (many others)

WPA3 - Changes

- WPA3 Personal and WPA3 Enterprise
- Introduces **Simultaneous Authentication of Equals (SAE)** to replace the pre-shared key exchange
- SAE is a variant of the **Dragonfly Handshake**
- Enterprise: must offer at least 192 bits of security (e.g., 384-bit EC)
- Enforces **802.11w** – security of **management frames** (e.g., radio management, QoS)

The Dragonfly Handshake

- Is a Password Authenticated Key Exchange (PAKE)
- Starts with a password and generates a higher entropy key
- Supports Elliptic Curve Cryptography (ECC)
- Has 2 phases:
 - *Commit*
 - *Confirm*

WPA3 – SAE Handshake

[Source: Vanhoef, M. and Ronen, E., 2020, May. Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd. In 2020 IEEE Symposium on Security and Privacy (SP) (pp. 517-533). IEEE.]

P: Password

k : the final / negotiated key

(k is further used in the 4WH, as in WPA2; i.e. k is like the PMK)

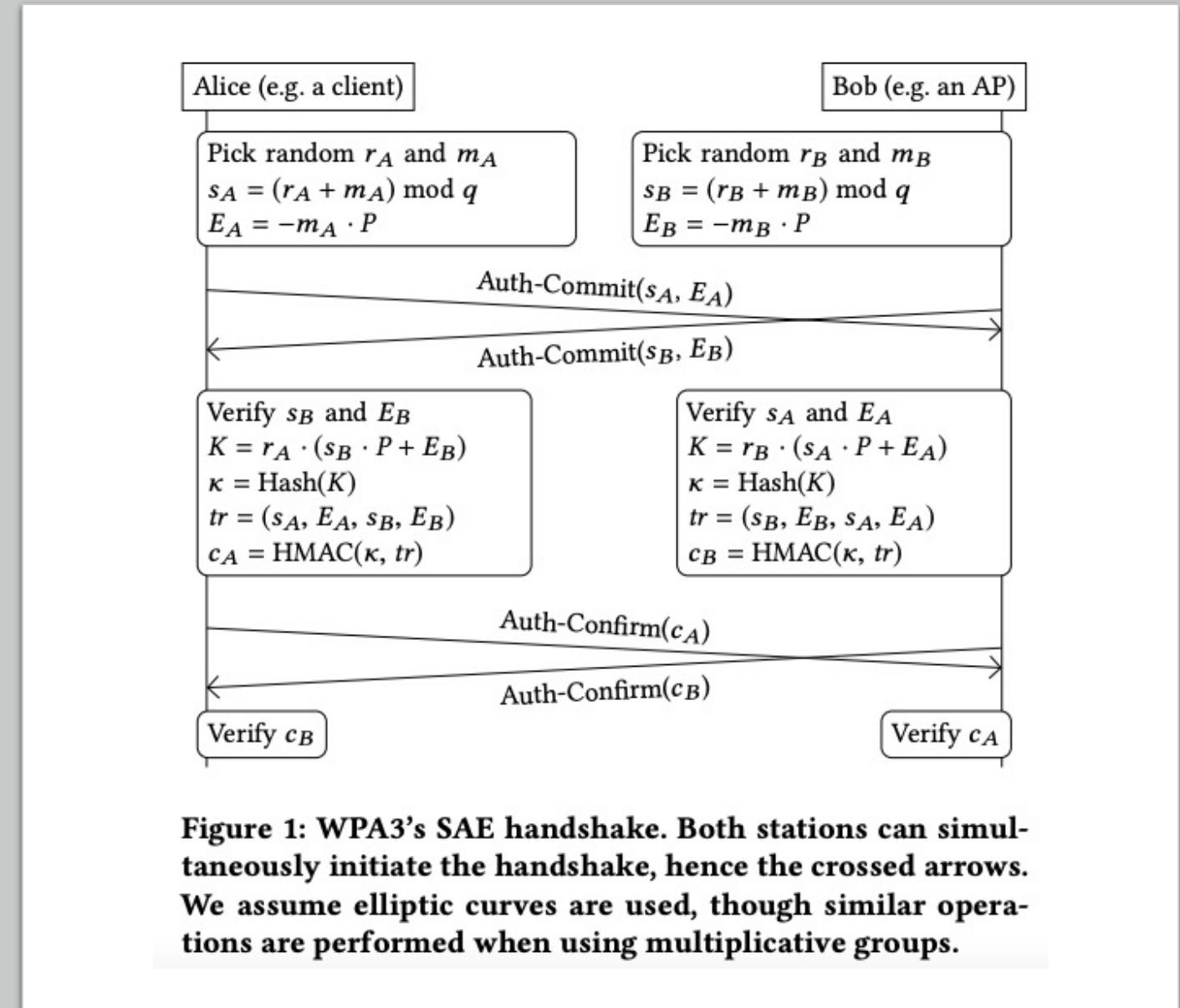


Figure 1: WPA3's SAE handshake. Both stations can simultaneously initiate the handshake, hence the crossed arrows. We assume elliptic curves are used, though similar operations are performed when using multiplicative groups.

WPA3 – Security against a dictionary attack

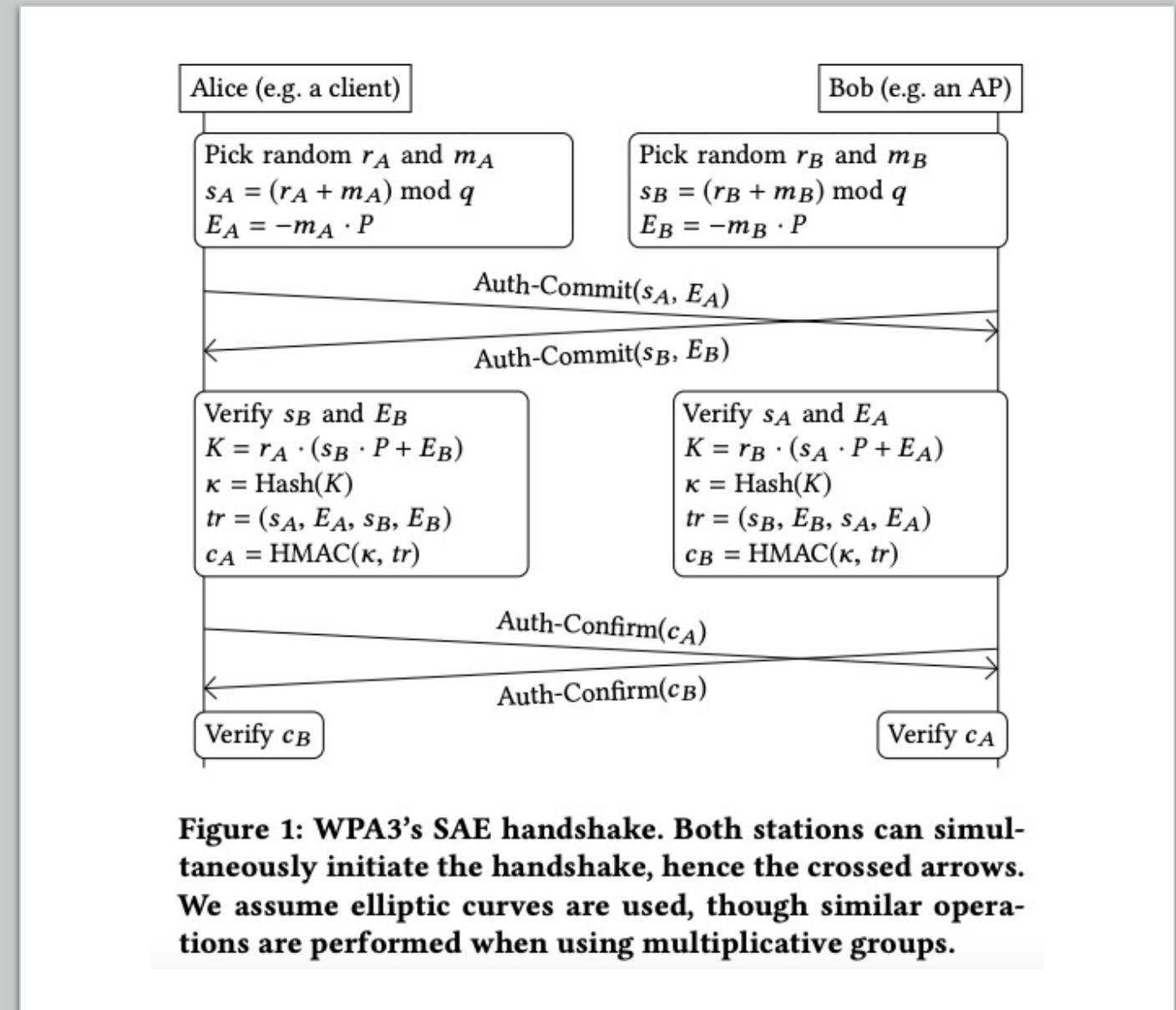
[Source: Vanhoef, M. and Ronen, E., 2020, May. Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd. In 2020 IEEE Symposium on Security and Privacy (SP) (pp. 517-533). IEEE.]

P: Password

k: the final / negotiated key

Remember: WPA2 was vulnerable to a dictionary attack by capturing a handshake.

WPA3 offers protection, why?



Backward compatibility

- Scenario: both WPA2 and WPA3 are supported, and the same password is used
- WPA3 has some detection of **downgrade to WPA2** (at changing the AP capabilities in the RSN IE), but this does not help (until detection, a handshake capture already makes the password vulnerable to a dictionary attack in WPA2).

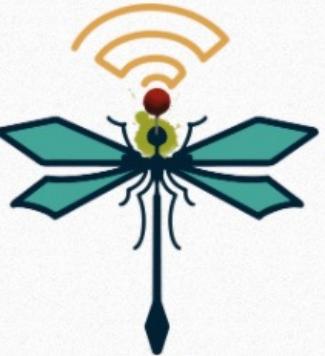
[Source: Vanhoef, M. and Ronen, E., 2020, May. Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd. In *2020 IEEE Symposium on Security and Privacy (SP)* (pp. 517-533). IEEE.]

Other problems

- **DoS**: spoof commit frames to the AP (the AP will have to do too many verifications)
- **Timing attacks, side-channels attacks** (mostly caused by how the pre-shared password is encoded into a group element in the Dragonfly handshake)

[Source: Vanhoef, M. and Ronen, E., 2020, May. Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd. In *2020 IEEE Symposium on Security and Privacy (SP)* (pp. 517-533). IEEE.]

Dragonblood (2020)



DRAGONBLOOD

Analysing WPA3's Dragonfly Handshake

By [Mathy Vanhoef](#) (NYUAD) and [Eyal Ronen](#) (Tel Aviv University & KU Leuven)

INTRO NEW DETAILS PAPER TOOLS Q&A

INTRODUCTION

April 2019 — Modern Wi-Fi networks use WPA2 to protect transmitted data. However, because WPA2 is more than 14 years old, the Wi-Fi Alliance [recently announced](#) the new and more secure WPA3 protocol. One of the supposed advantages of WPA3 is that, thanks to its underlying Dragonfly handshake, it's near impossible to [crack](#) the password of a network. Unfortunately, we found that **even with WPA3, an attacker within range of a victim can still recover the password**. If the victim uses no extra protection such as [HTTPS](#), this allows an attacker to steal sensitive information such as passwords and emails. We hope our disclosure motivates vendors to mitigate our attacks before WPA3 becomes widespread.

<https://wpa3.mathyvanhoef.com/>

WiFi Networks

- We have now finished studying WiFi security



Network Security

- Lecture 6 -

TLS

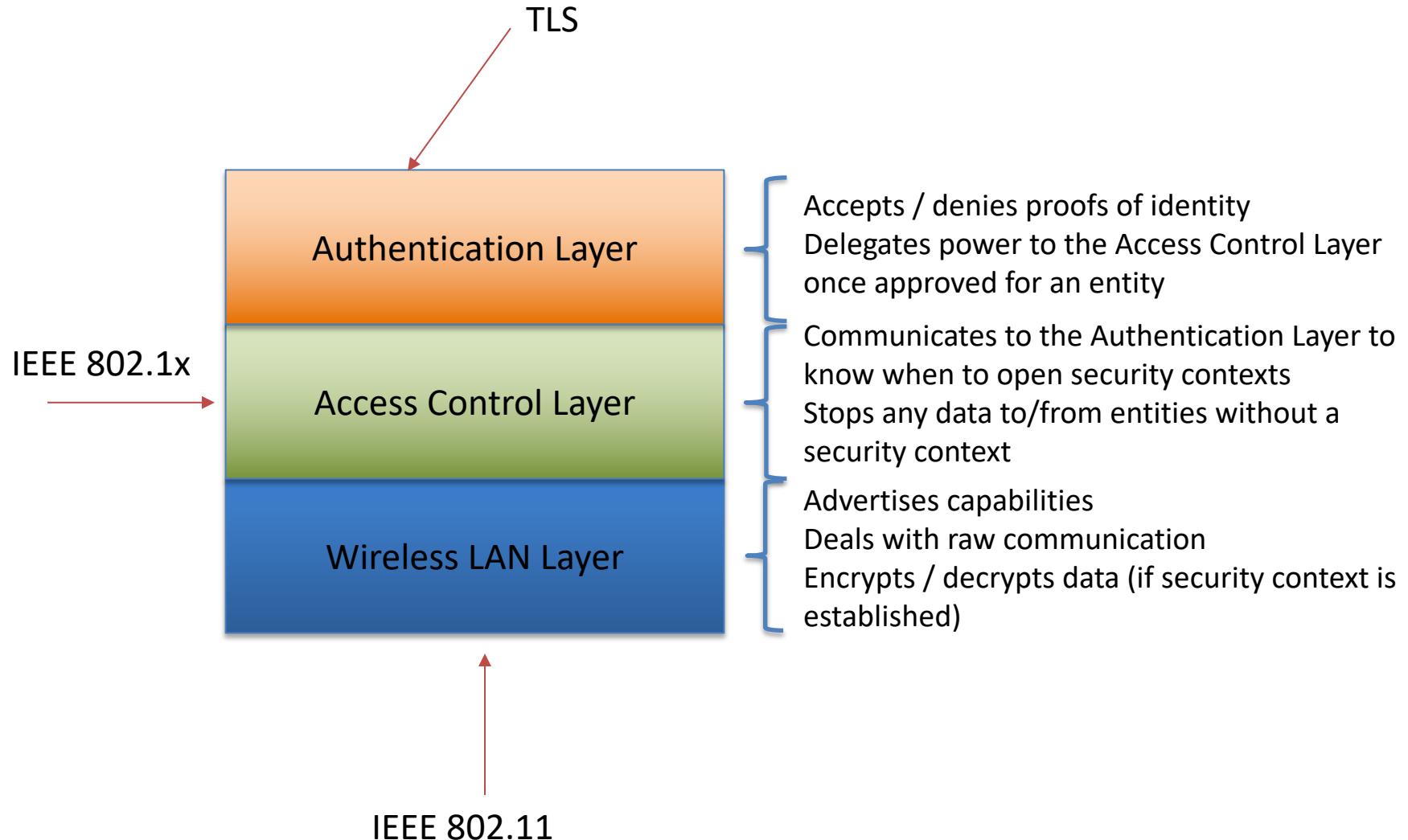
Adela Georgescu

Faculty of Mathematics and Computer Science
University of Bucharest

Outline

1. Security levels
2. TLS

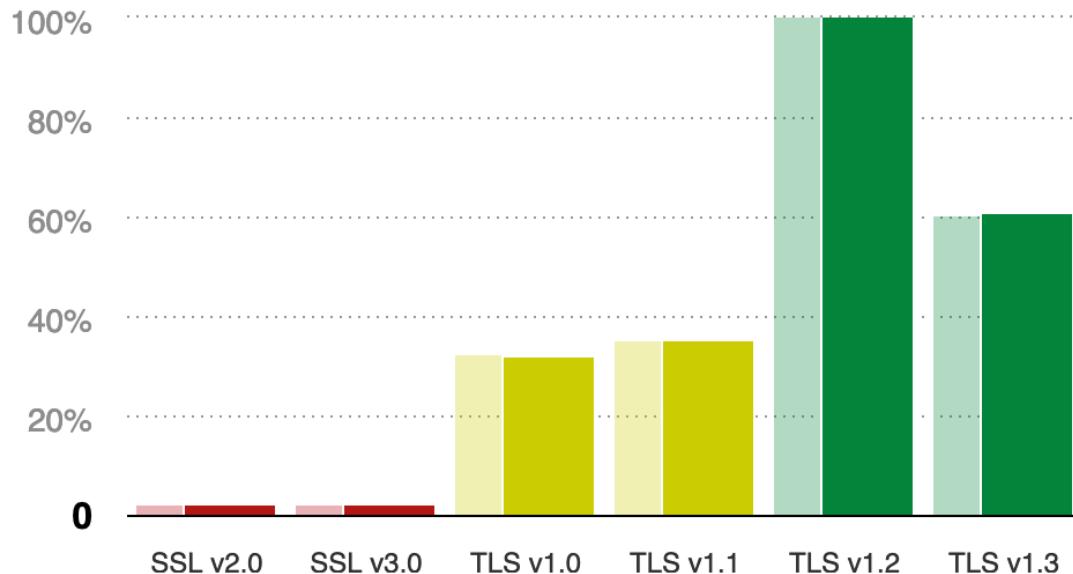
Security levels



TLS

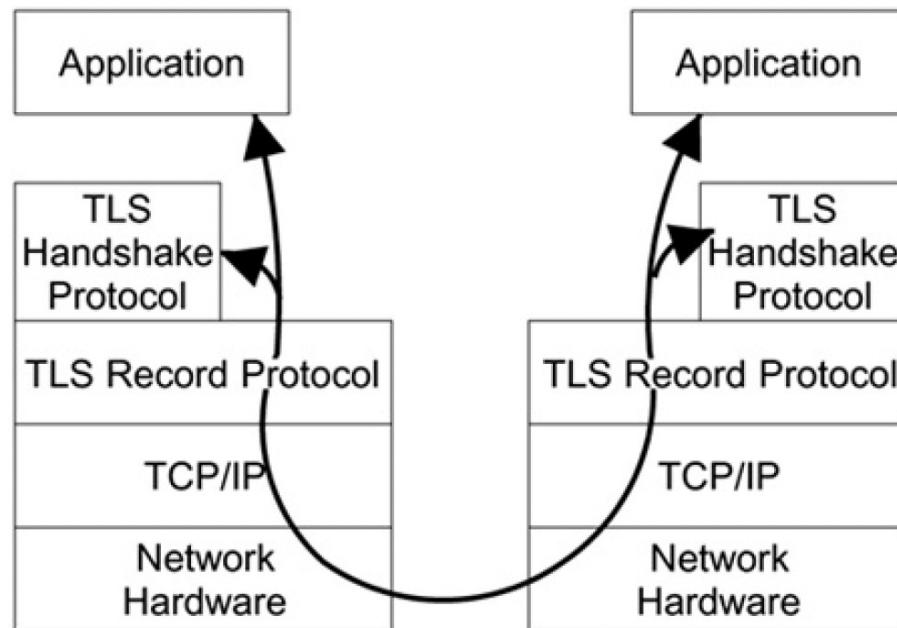
- First versions: SSL – Netscape (1995) – SSL 3.0 most well-known
- TLS 1.0 – 1999; TLS 1.1 – 2006; TLS 1.2 – 2008; TLS 1.3 - 2018

Protocol Support



TLS

- Provides authentication, encryption and data compression
- 2 layers: **handshake protocol** and **record protocol**



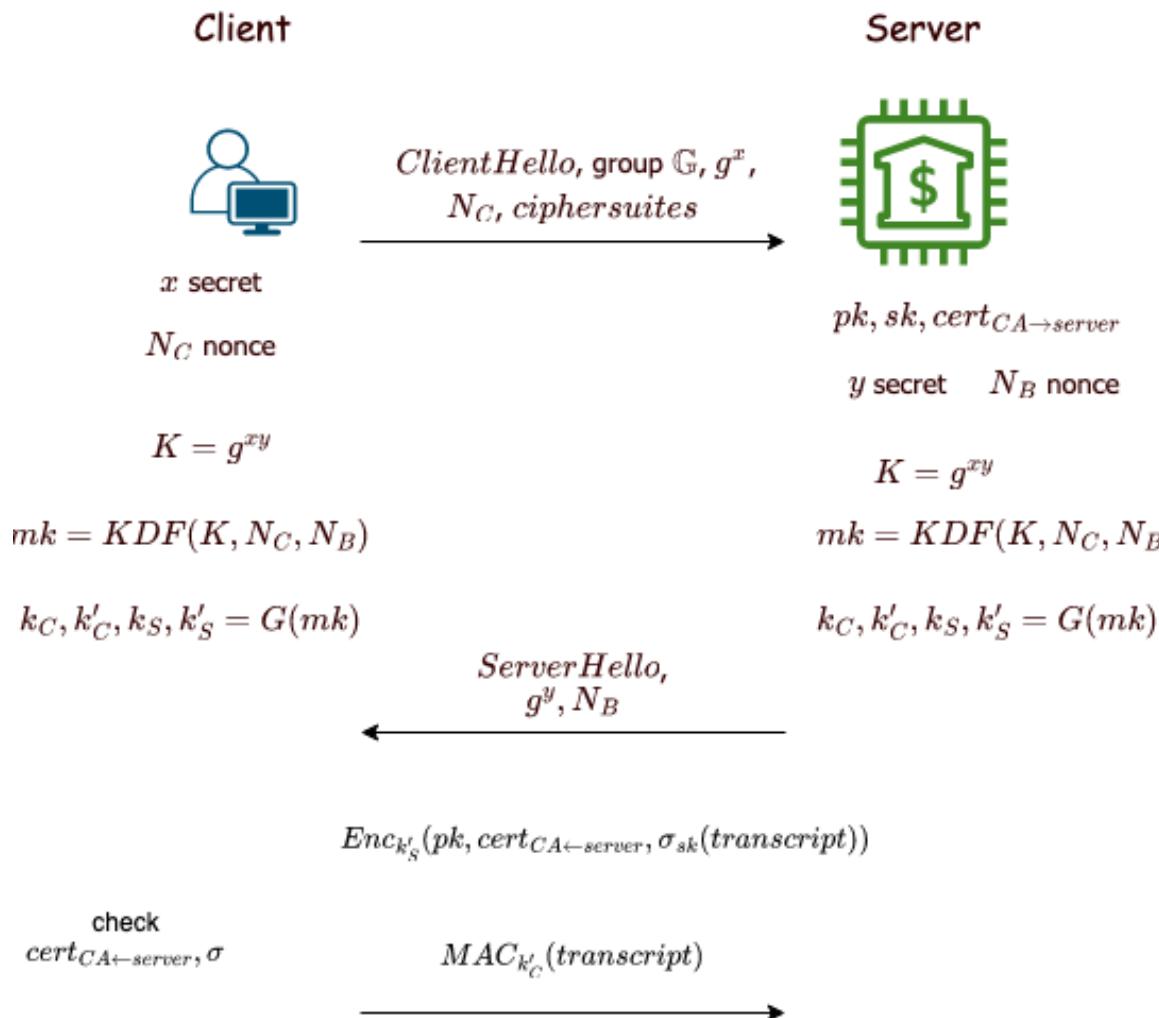
[Source: Course book, Edney &Arbaugh, Chapter 9]

TLS 1.3 handshake



[Source: <https://www.thesslstore.com/blog/tls-1-3-handshake-tls-1-2/>]

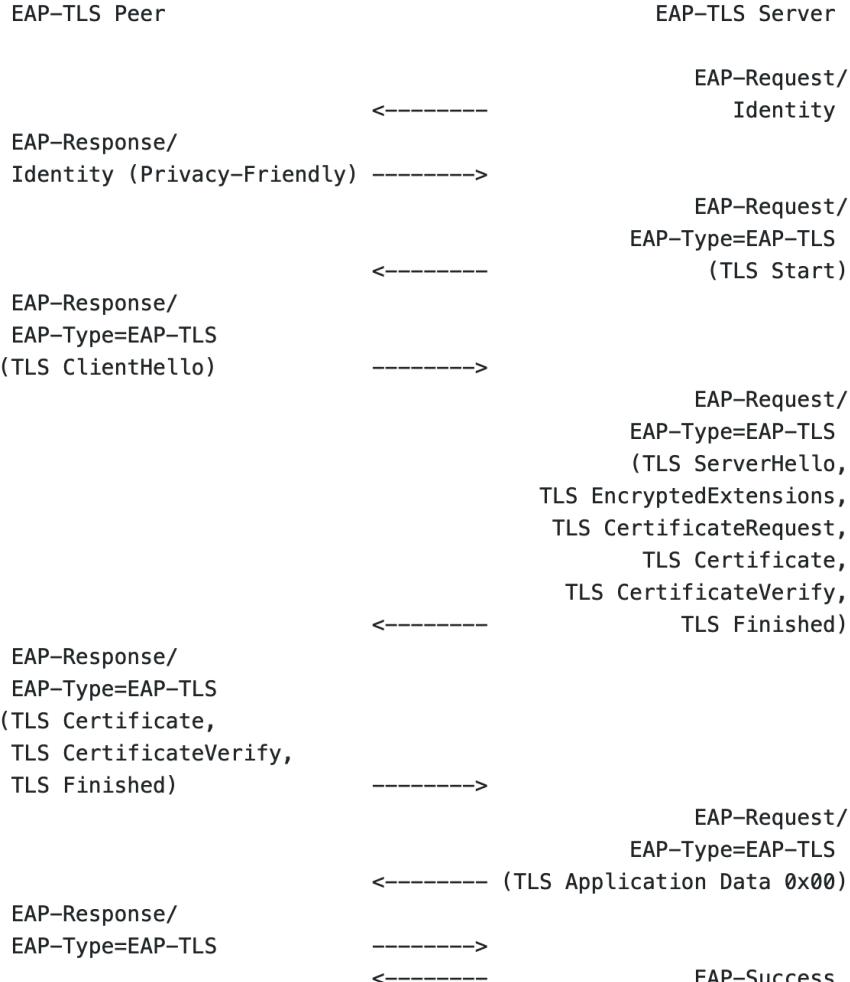
TLS 1.3 handshake



TLS 1.3 handshake

- Supported ciphersuites
 - TLS_AES_128_GCM_SHA256
 - TLS AES 256 GCM SHA384
 - TLS CHACHA20 POLY1305 SHA256
 - TLS AES 128 CCM SHA256
 - TLS AES 128 CCM 8 SHA256
- Transcript – all messages sent in the protocol until the current moment
- keys k'_S and k'_C only used during handshake

EAP-TLS



[Source: RFC 9190]



Network Security

- Lecture 7 -

Mobile Security

Adela Georgescu

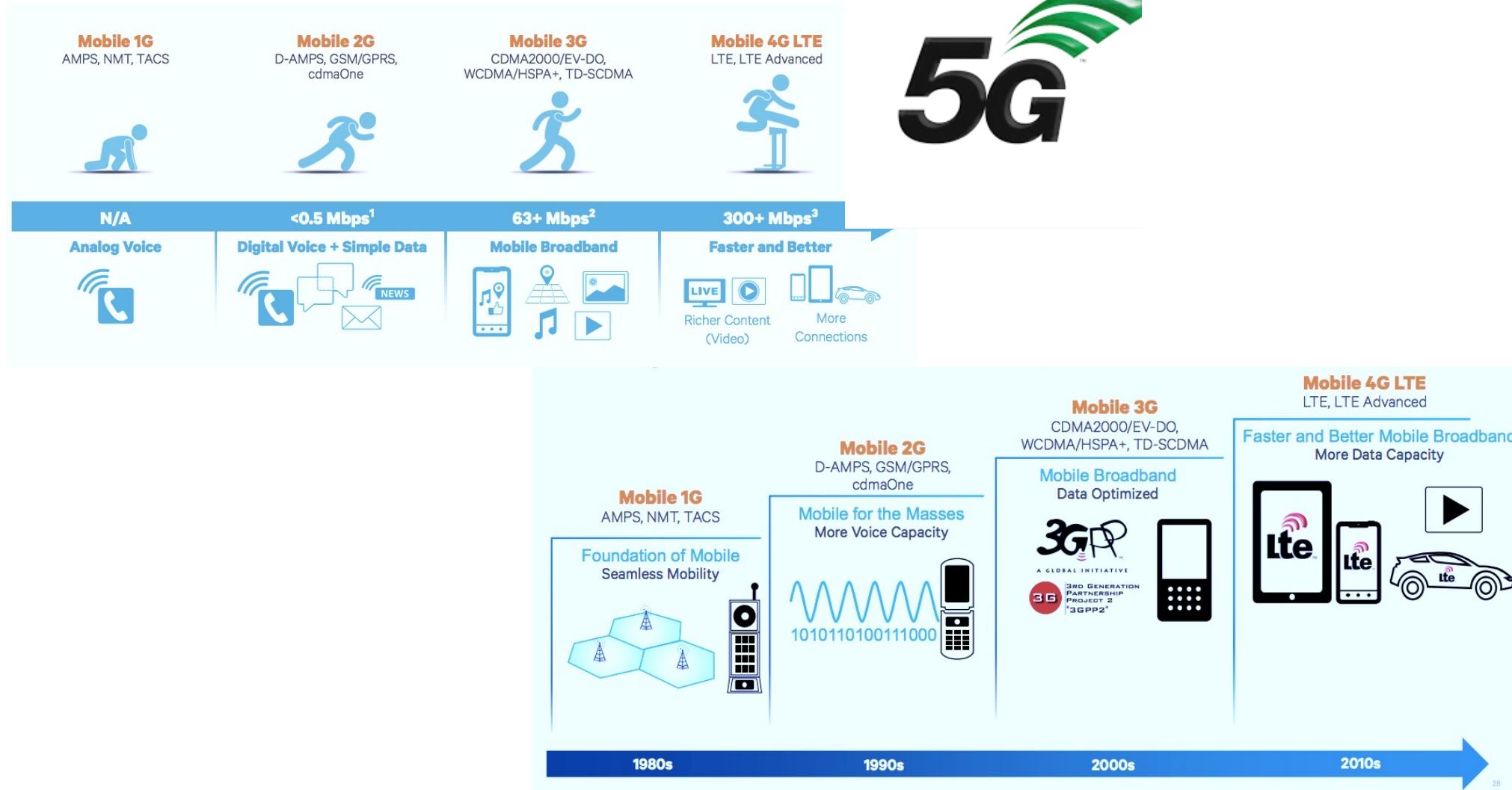
Faculty of Mathematics and Computer Science
University of Bucharest

*slides belonging to Ruxandra Olimid

Outline

- Intro to Mobile Security
- GSM Architecture
- GSM Security Requirements / Principles
- Vulnerabilities and Attacks

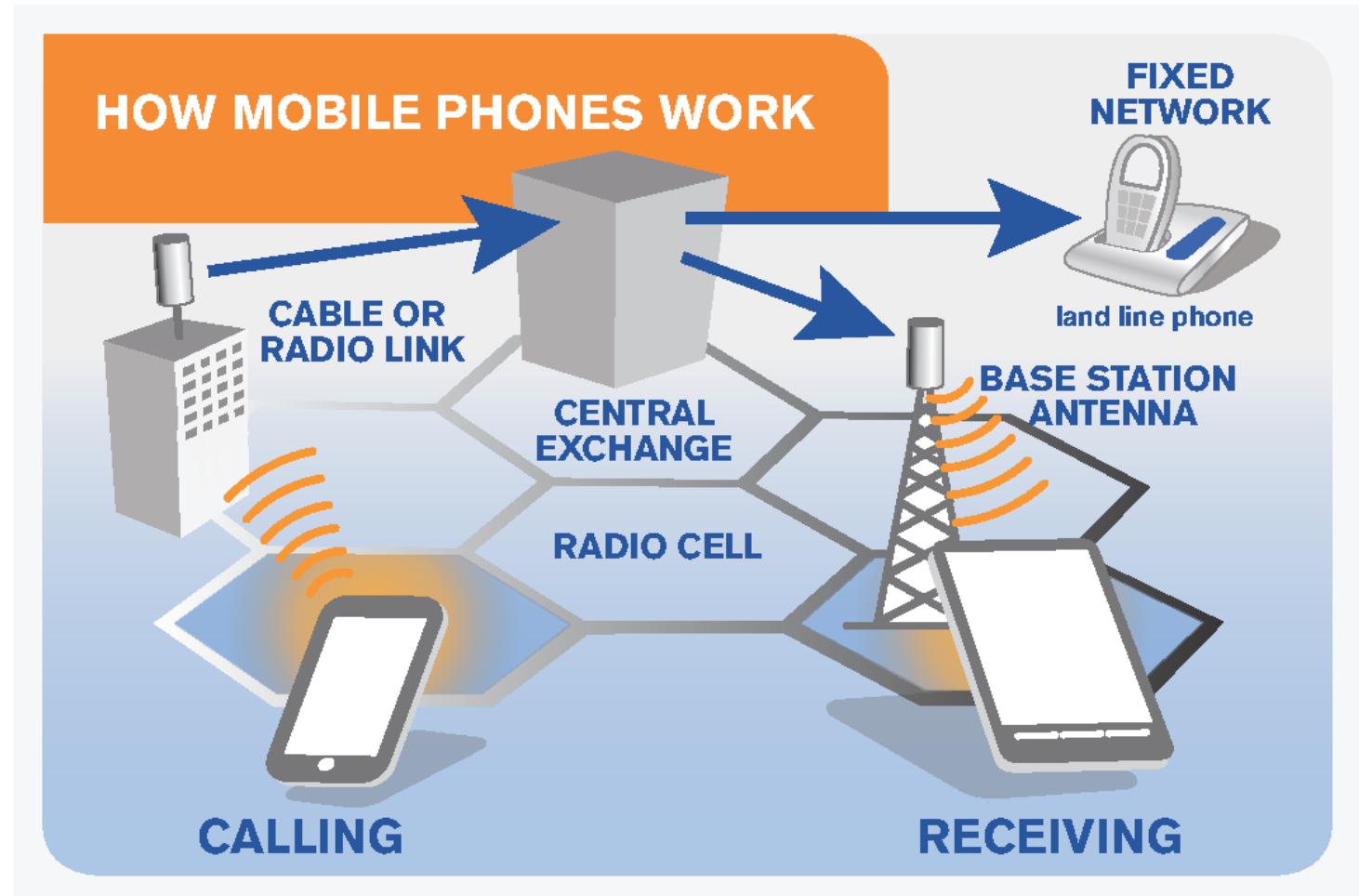
Evolution



[Source: Qualcomm – The Evolution of Mobile Technologies, '14]

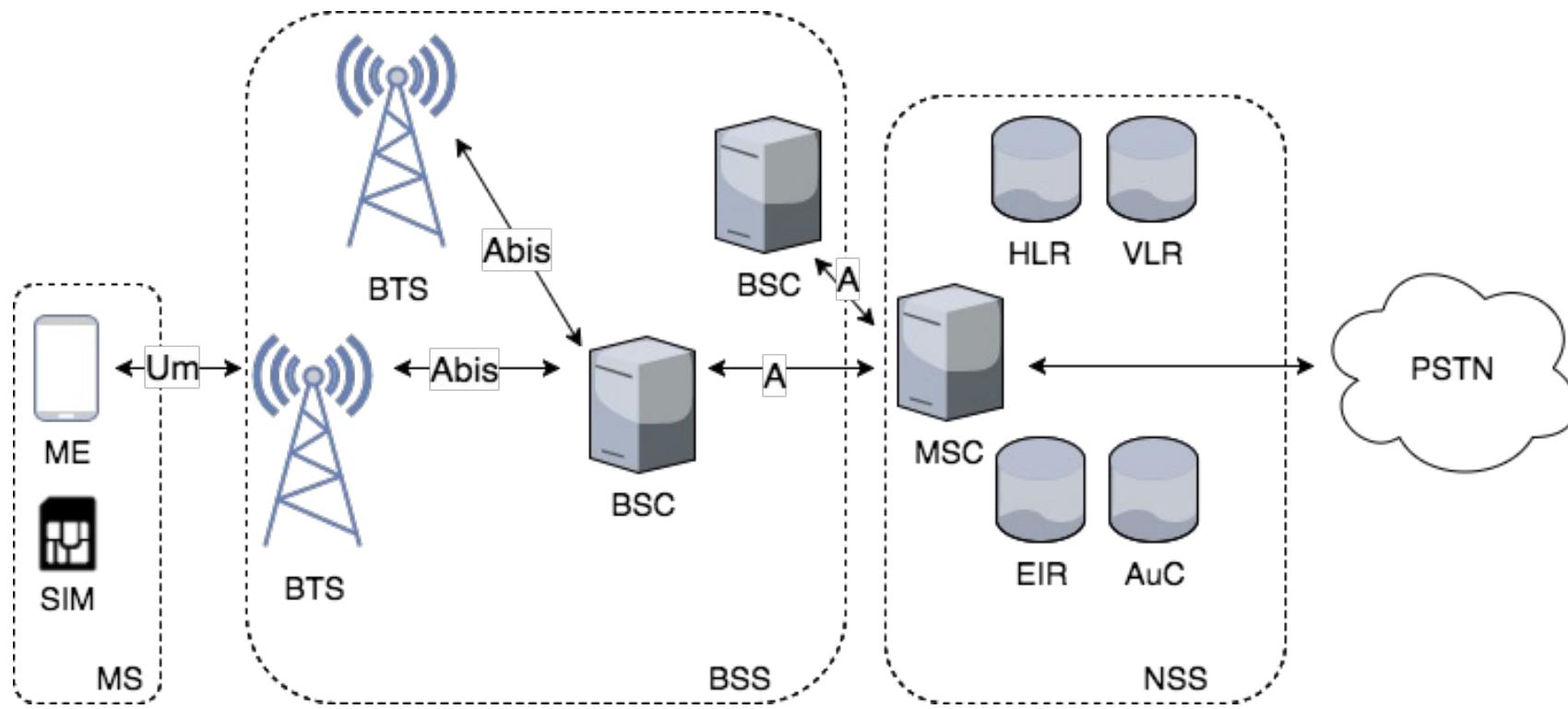
Overview

- User device
- Access network
 - Radio link
- Core network



[Source: ITU EMF Guide <http://emfguide.itu.int/emfguide.html>]

GSM - Architecture



MS: Mobile Station

ME: Mobile Equipment

SIM: Subscriber Identity Module

BSS: Base Station Subsystem

BTS: Base Transceiver Station

BSC: Base Station Controller

NSS: Network Subsystem

MSC: Mobile Services Switching Center

HLR: Home Location Register

VLR: Visitor Location Register

EIR: Equipment Identity Register

AuC: Authentication Center

PSTN: Public Switched Telephone Network

GSM - Arhitecture

- **MS (Mobile Station):**
 - Consists in a Mobile Equipment (ME) and the Subscriber's Identity Module (SIM)
- **BSS (Base Station Subsystem):**
 - Consists in several BTSs and BSCs
 - The BSC is a central element that controls the radio network, maintaining radio connectivity with several BTSs and providing connection to the NSS
 - BTS is the element to which the MS connects to in the GSM network via radio link; its functions include signal processing, signaling, ciphering
- **NSS (Network SubSystem):**
 - MSC is the main element of the NSS with respect to call functions, being responsible for call control, BSS control, and interconnecting to the external networks (PSTN)

GSM - Arhitecture

- **VLR (Visitor Location Register):**
 - Stores information about subscribers that are served by the MSC (it maintains copies of the data from HLR, increasing efficiency: decreases the number of messages that are exchanged between the MSC and the HLR)
 - Usually is not independent hardware, but a software component of the MSC
- **HLR (Home Location Register):**
 - It is the main database in GSM
 - Maintains information for each subscriber: IMSI, phone no. - MSISDN (Mobile Station International Subscriber Directory Number), available services for the subscriber, location, etc.
- **AuC (Authentication Center):**
 - For each subscriber, stores the permanent key K_i that is also stored in the SIM
 - Generates the authentication vectors (RAND, SRES, K_C) in the authentication phase

GSM - Arhitecture

- **EIR (Equipment Identity Register):**
 - Keeps inventory of the devices in the mobile network, which are identified by their IMEI
 - Keeps up to date 3 lists:
 -  • White list: contains the equipment that are compliant to the operator and can access the mobile network without any restriction
 -  • Black list: contains the equipment that have been reported as stolen or that have been proved to affect the network functionality, and that are restricted to access the mobile network
 -  • Gray list: contains the equipment that are not fully compliant to the operator, and are allowed to access the network but there are under surveillance

GSM – Security Principles

Goal: GSM should be as secure as the wired network (PSTN) ...
...but, security mechanisms should not have a negative impact on the
usability of the system

- Security requirements in GSM:
- *Access control to the MS:* provide authenticated user access to the mobile station
- *Anonymity of subscribers (privacy):* keep the identity of the subscribers (and their location, possibility of linking calls, etc.) hidden to external parties
- *Authentication of subscribers:* subscribers must prove their identity and their right to access mobile services
- *Confidentiality:* maintain the confidentiality on the radio link

GSM – Security Principles

Weaknesses in GSM security:

- No specification about the *integrity of the data*
- *Breaking Kerckhoffs' principle*: cryptographic algorithms were kept confidential (e.g.: A5/1, A5/2), and their strength was not publicly tested
- *Limited encryption*: data is encrypted on the radio link only
- *Short keys*; cryptosystems are vulnerable to *exhaustive search attack*
- *Unilateral authentication*: The mobile station does not authenticate the network (only the network authenticates the mobile station)
- *Active attacks are possible*; e.g.: IMSI Catchers, when an adversary masquerades a legitimate BTS

Mobile Equipment (ME)



- Identification:
 - **IMEI** (International Mobile Equipment Identity), a number used to identify the mobile phone; it is printed on the device, and it can be displayed by dialing *#06#
 - **IMEISV** (IMEI Software Version) discards the check digit from the IMEI and adds 2 digits SVN (Software Version Number)
- Access control:
 - IMEI can be used to deny connectivity to the network for stolen phones based on a blacklist stored by the operator
 - Biometric authentication; e.g.: fingerprint recognition, voice recognition
 - Screen unlock mechanisms; e.g.: codes, patterns

SIM Card



Identification:

- **IMSI** (International Mobile Subscriber Identity), a global unique identifier for the subscriber ($\cong 15$ digits)
- **ICCID** (Integrated Circuit Card ID) it is the identifier of the SIM itself and printed on the SIM card

Access control:

- **PIN** (Personal Identification Number), a sequence of numbers required to unlock the SIM card
- **PUK** (Personal Unlocking Key), a code required when the PIN has been introduced incorrectly several times

IMSI (International Mobile Subscriber Identity)

MCC (Mobile Country Code) - 3 digits -	MNC (Mobile Network Code) - 2 digits (EU) / 3 digits (US) -	MSIN (Mobile Subscriber Identification Number)
242 (Norway)	01 (Telenor) / 02 (Telia)	XXXXXXXXXXXX
226 (Romania)	01 (Vodafone) / 10 (Orange)	XXXXXXXXXXXX

SIM Card



Authentication and Confidentiality:

- **IMSI** (International Mobile Subscriber Identity)
- **TMSI** (Temporary Mobile Subscriber Identity), a temporary identity used to restrict the sending of IMSI over the air and mitigate eavesdrop attacks
- **K_i**, a 128-bits permanent key
- Cryptographic mechanisms: a *challenge-response mechanism* that uses the permanent key for the authentication of the subscriber and a *key generation mechanism* for confidentiality of communication

SIM cards must be tamper-resistant (i.e. an adversary should not be able to read / modify the security information stored on the SIM card). Otherwise, SIM cards become vulnerable to cloning attacks, for which the attacker creates copies of the SIM card to use in different purposes (eavesdropping on the victim, making calls on the victim behalf, etc.)

*Terminology: Initially, the card itself was also called a SIM, later the card itself was called UICC (Universal Integrated Circuit Card) and the SIM was considered the application running on the card

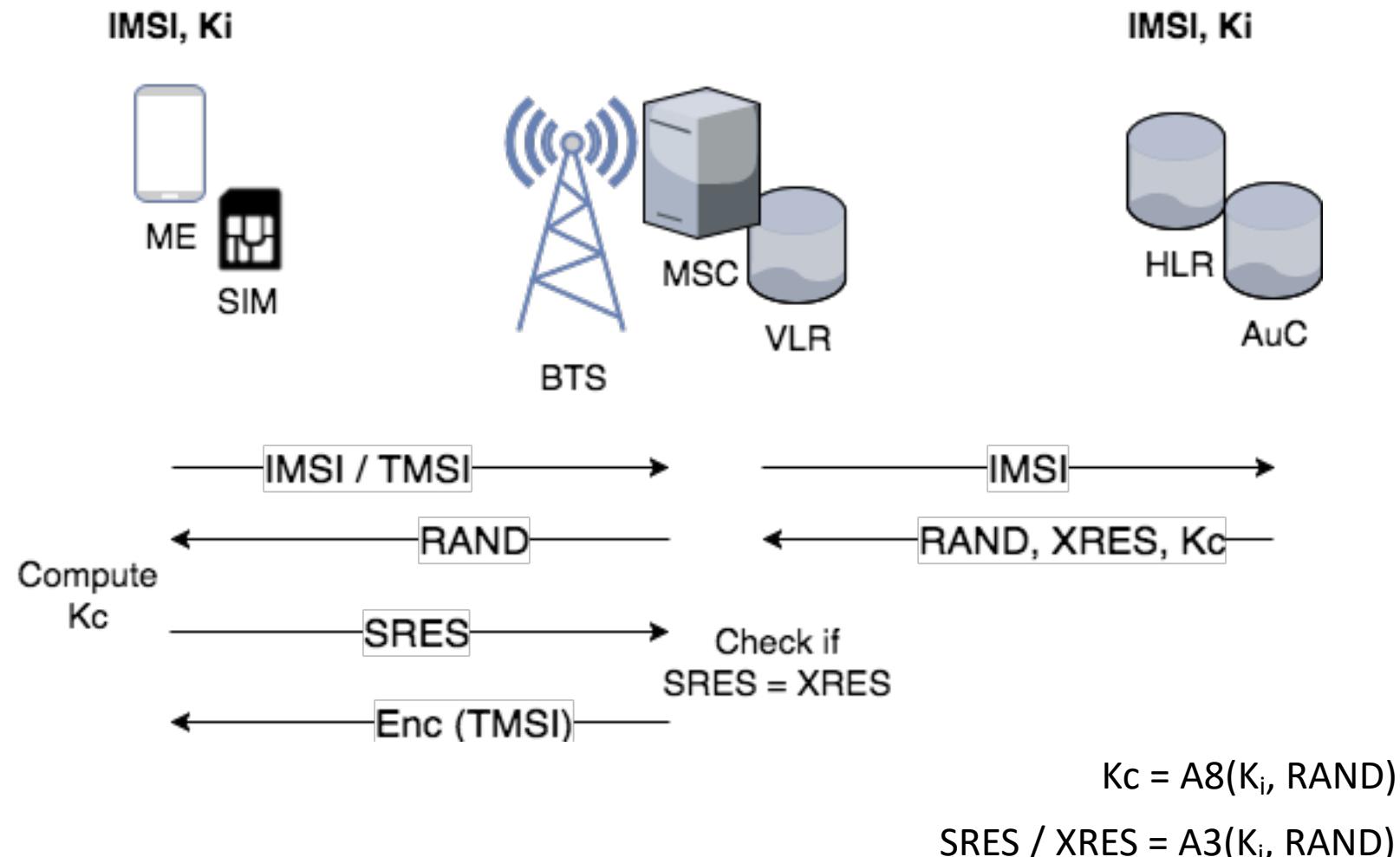
Anonymity of Subscribers

- **Goal:** Keep the identity (presence/absence in an area, location, etc.) of the subscriber private to unauthorized parties
- A subscriber can identify itself by one of the following identifiers:
 - **IMSI** - permanent identity
 - **TMSI** - temporary identity
- **Principles:**
 - Introduce the TMSI as a way to avoid IMSI exposure on the radio interface
 - e.g.: IMSI uniquely identifies a subscriber, and if it is intercepted it suffices to prove the presence of the subscriber in a location
 - TMSI is assigned to the MS when it authenticates to the network, and it is local in the visiting network (VLR keeps the IMSI – TMSI correspondence); the MS stores the TMSI in the SIM to use it even after rebooting
 - TMSI must be renewed at specific intervals (tradeoff with efficiency); a TMSI that is not changed often enough can break privacy too

Authentication of Subscribers

- **Goal:** Prove the identity of the subscriber to the mobile network, and avoid unauthorized parties to access the mobile services
- The authentication mechanism uses:
 - The permanent key K_i , unique for each subscriber, that is stored:
 - in the SIM card (**subscriber's side**)
 - in the AuC (**network operator's side**)
 - Cryptographic algorithms: **A3** (subscriber authentication), **A8** (key generation)
- **Principles:**
 - K_i does never leave the 2 locations (SIM, AuC);
 - Authentication consists in checking if the subscriber knows the correct key K_i by using a *challenge-response mechanism*
 - The serving network does not have access to the key K_i , so it cannot perform authentication without help from the home network
 - During authentication phase, is derived a key K_c that will be later used for encryption

Authentication of Subscribers



Authentication Triplets

- **Goal:** Allow the visiting network to authenticate the MS without knowing K_i and improve efficiency by using batches of triplets
- A triplet used for authentication is

$$(\text{RAND}, \text{XRES}, K_c)$$

where $\text{XRES} = A3(K_i, \text{RAND})$ and $Kc = A8(K_i, \text{RAND})$

- **Operation:**
 - AuC produces batches of triplets for each MS, each with a different RAND and sends them to the HLR
 - For a single request, the VLR receives a batch of triplets from the HLR (to avoid often communication between the VLR and the HLR)
 - If the network runs out of triplets, it should request more from the HLR, but if not it is allowed to reuse triples

Encryption

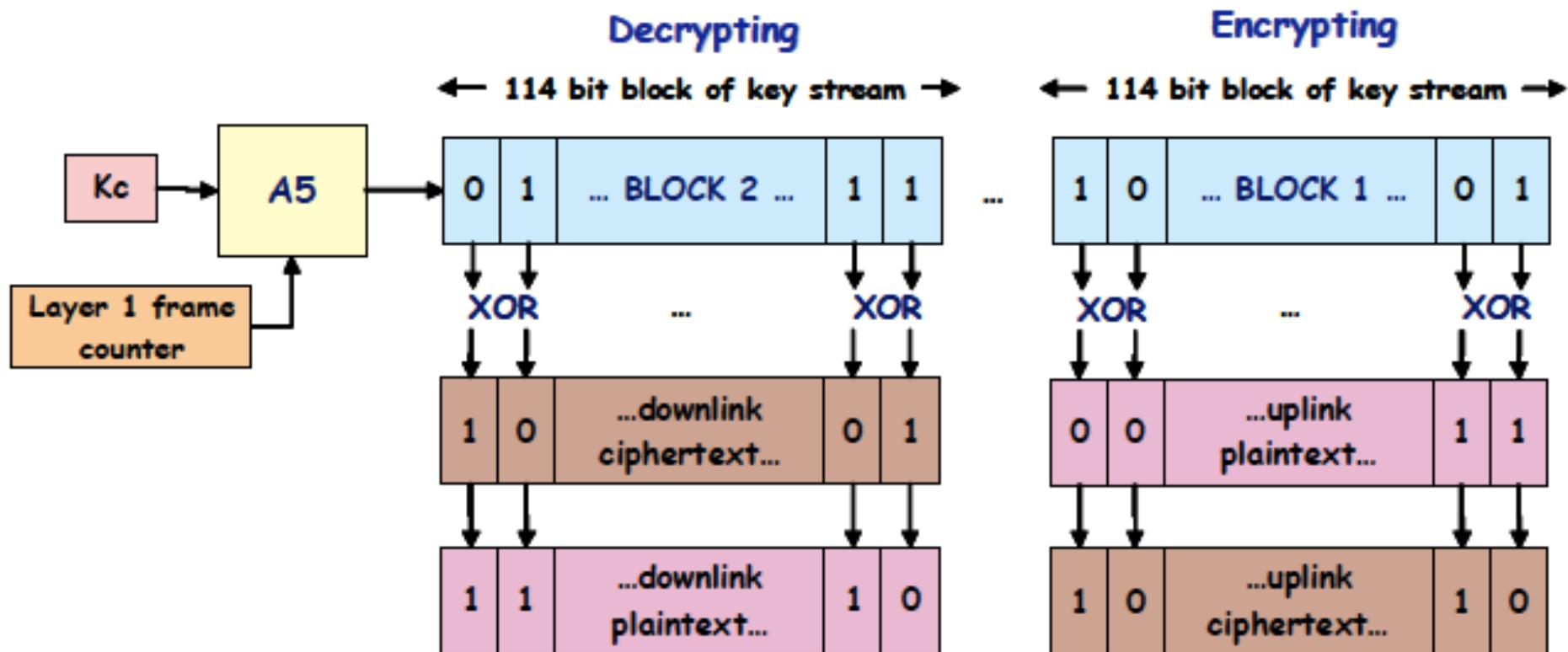
- **Goal:** Encrypt all communication between the mobile station and the BTS (both phone calls and sensitive signaling information such as TMSI, MSISDN, etc.)
- The GSM encryption uses:
 - The key K_c , derived in the authentication mechanism
 - Encryption algorithm: **A5** (radio encryption)
- **Principles:**
 - Encryption is only performed on the radio link (!)
 - The encryption algorithm uses as input the session key K_c derived from the authentication phase
- **Operation:**
 - The key K_c is used as the encryption key for a stream cipher (LFSR-based):

$$\text{Ciphertext} = \text{A5}(K_c, \text{Plaintext})$$

Encryption

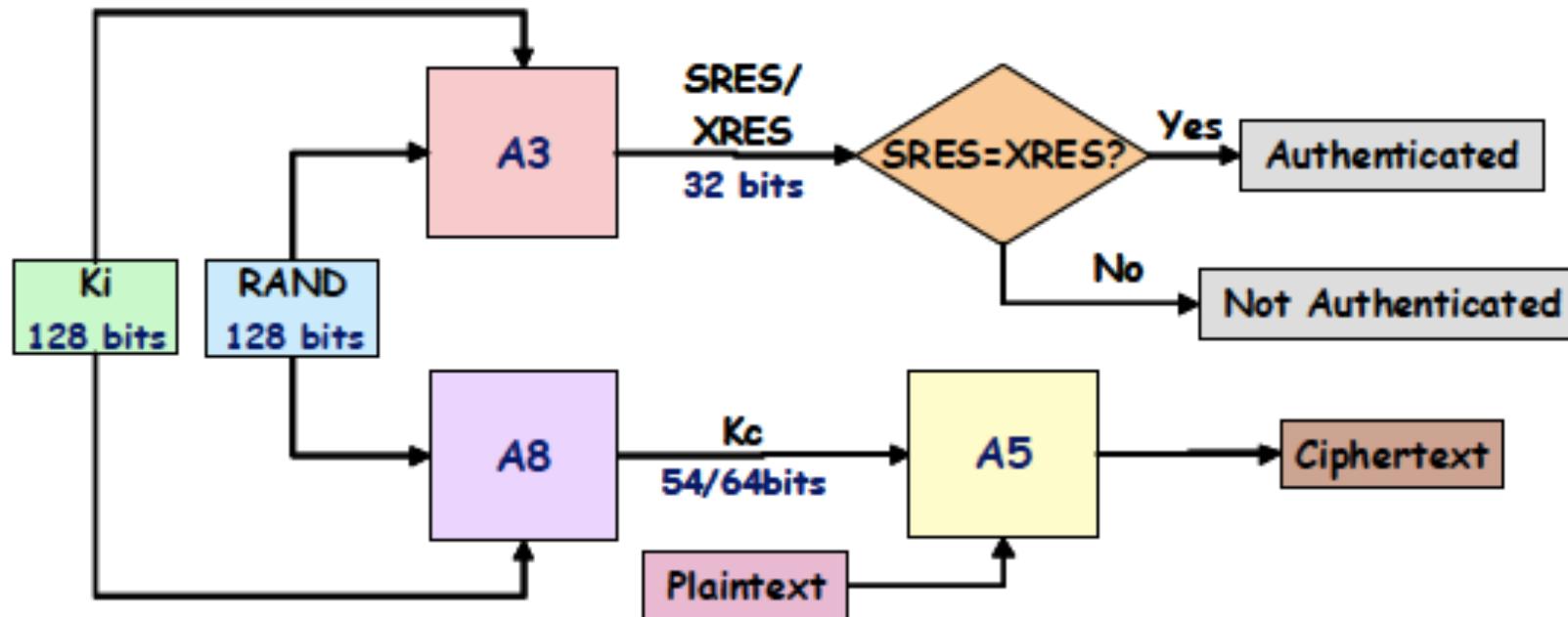
- Both A5/1 and A5/2 were not public, breaking *Kerckhoffs' principle*
- Encryption operates at the physical layer (Layer 1), which brings some advantages:
 - Maximum amount of data is encrypted (both user and signaling data)
 - The encryption algorithm can be implemented in hardware
- A5 algorithms are **stream ciphers**, so encryption is performed bit-by-bit
- A *frame counter* (22 bits) is used as an additional input together with the key K_c
- **Vulnerability!** The frame counter repeats every 2^{22} frames (approx. every 3.5 hours), so the key stream repeats if the K_c is not renewed meanwhile
- GSM is *full duplex*: for each frame, first 114-bit block (Block1) is used for encryption of data that is being transmitted, and the second 114-bit block (Block2) is used for decryption of data that is being received

Encryption



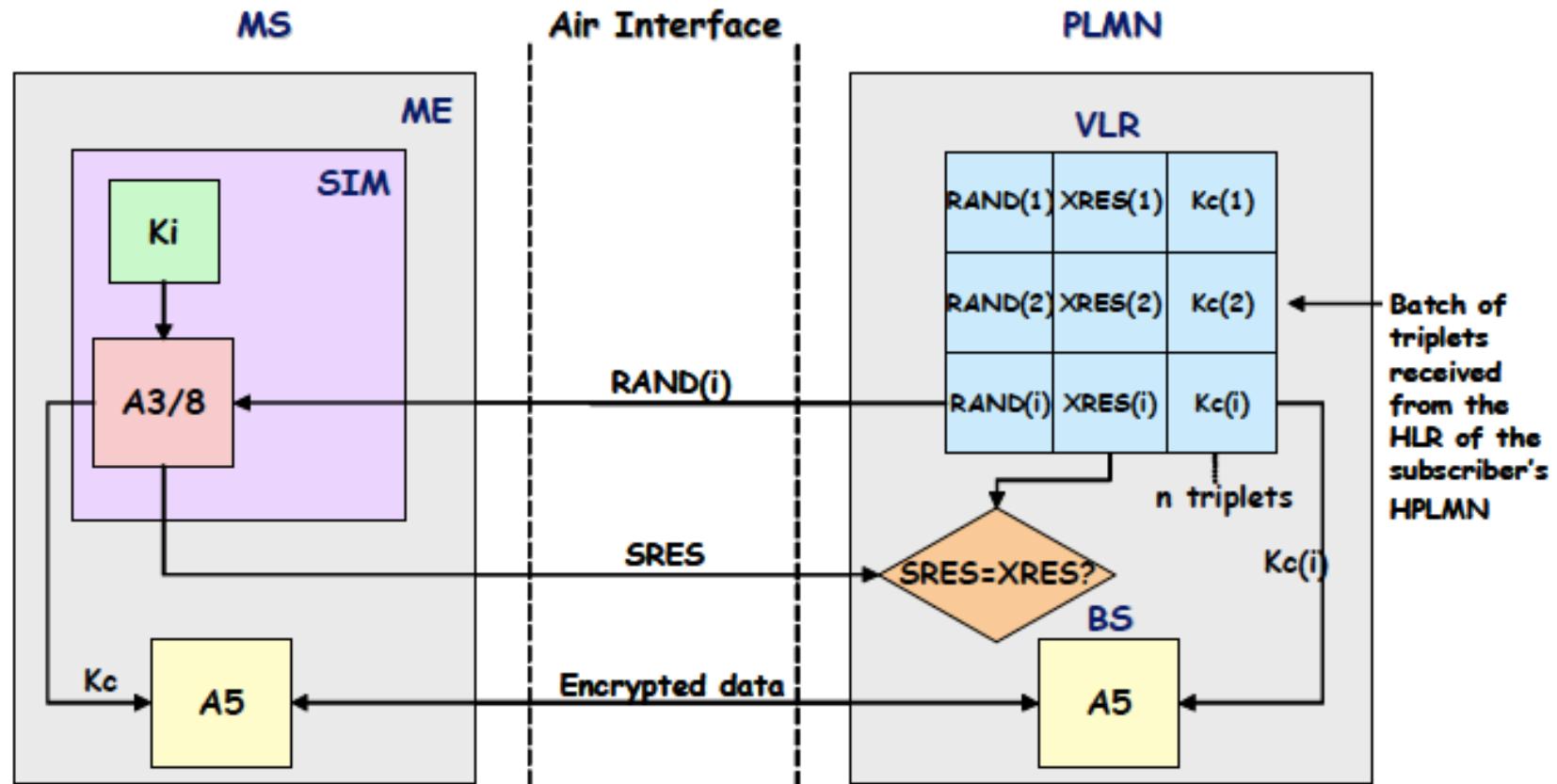
[Source: P.S.Pagliusi – A Contemporany Foreword on GSM Security, InfraSec '02]

Overview



[Source: P.S.Pagliusi – A Contemporany Foreword on GSM Security, InfraSec '02]

Overview



[Source: P.S.Pagliusi – A Contemporary Foreword on GSM Security, InfraSec '02]

Crypto

Key	Length / Input + Output	Info
K_i	128 bits	Key shared between the subscriber and the network operator, stored in the SIM and AuC
K_c	54/64 bits	Secret session key, that will be used for encryption $K_c = A8(K_i, RAND)$
RAND	128 bits	Random challenge
SRES / XRES (Signed Response / Expected Response)	32 bits	Response to the challenge request / Expected response to the challenge request $SRES / XRES = A3(K_i, RAND)$
A3, resp. A8	Input: K_i , RAND Output: SRES, resp. K_c	Generic algorithms for authentication, resp. key generation (no specific algorithms) e.g.: COMP128 combines A3 and A5 and generates XRES (32 bits) and K_c (54 random bits concatenated to 10 bits of 0) Stored in the SIM
A5	Input: K_c , plaintext Output: ciphertext	Class of standardized encryption algorithms: A5/0 (no encryption), A5/1 (CEPT + USA), A5/2 (Asia), A5/3 (Kasumi, UMTS) Stored in the mobile equipment (not SIM!)



Network Security

- Lecture 8 -

Mobile Security

GSM II

Adela Georgescu

Faculty of Mathematics and Computer Science
University of Bucharest

*slides belonging to Ruxandra Olimid

Security Principles

- **Modularity:**
 - GSM is modular in the sense that the cryptographic algorithms can be replaced with others, as long as maintain the same input-output structure
 - A5 refers to a family of algorithms; e.g.: A5/1, A5/2, A5/3 (64 bits key K_c); A5/0 (no encryption), A5/4 (128 bits key K_c) – some used for UMTS (e.g.: A5/3)
- **Standardization:**
 - A5 must be standardized (e.g.: MS must communicate to BTS in roaming)
 - A3, A8 must not necessary be standardized, because both parties involved (the SIM and the AuC) belong to the same network operator; however, 3GPP gave an example algorithm set TS55.205

Security Principles

- Use the SIM as a security module:
 - Authentication and confidentiality are performed based on a shared secret (K_i)
 - The SIM stores secret information of the subscriber (K_i , IMSI) and cryptographic algorithms (A3, A8)
 - Should be tamper-resistant
- Security in the visiting network:
 - The key K_i must not be shared to the visitor network
 - Authentication triplets allow authentication in visitor networks
- Algorithms' requirements:
 - Statistically impossible to guess SRES
 - Statistically impossible to find K_i , K_c from the eavesdropped data
 - ... (assumptions that exclude trivial attacks)

Vulnerabilities and Attacks

- **Passive attacks:**
 - The adversary eavesdrops on the radio link and gets the IMSI
 - The attack is possible because the IMSI is sent in clear over the radio link when the MS possesses no TMSI or it cannot be identified by using the TMSI
- **Active attacks:**
 - The adversary requests the IMSI from the MS
 - **IMSI Catcher:** the adversary masquerades a legitimate BTS and asks the MS for the IMSI
 - The attack is possible because the MS does not authenticate the network - and cell reselection criteria is signal strength
 - We will learn more on IMSI Catchers when we will study LTE

Vulnerabilities and Attacks

- Cryptanalysis:
 - Key length
 - the key length of K_c (54/64 bits) is too small to provide security
 - Exhaustive search (brute force) can break the key in a few hours
 - **COMP128** was cracked in 1998 (by Wagner and Goldberg, but apparently known before by some operators)
 - Chosen plaintext attack: K_i is found when about 160 000 pairs RAND-SRES are collected
 - Possible ways to collect RAND-SRES pairs:
 - Steal the SIM and connect to a phone emulator (2 to 10 hours, dependent on the phone)
 - Use a false BTS (longer in time, but does not require physical access to the SIM)

Vulnerabilities and Attacks

- Cryptanalysis:
 - **A5/1** was broken in 1999 (by Biryukov, Shamir, later the attack was improved together with Wagner)
 - Time-memory trade-off:
 - *Pre-processing phase:* Compute a large database of states and related keys of the stream system
 - *Attack phase:* search subsequences of the key stream in the database; if a match is found, the state is the one in the database (with high probability)
 - 2s of known plaintext (both uplink and downlink) to succeed
 - **A5/2** was cryptanalysed in 1999 (Goldberg, Wagner, Green), 2003 (Barkan, Biham, Keller), etc.

Vulnerabilities and Attacks

- **Radio links:**
 - BTS to BSC link is sometimes not wired, making it easily susceptible to eavesdropping
 - Possible because GSM security does NOT consider encryption beyond the BTS-BSC link (but only on the MS – BTS radio link)
- **Engineering attacks:**
 - Attacks against the chip card, side-channel attacks
 - Software attacks
- **Optionality:**
 - Encryption was introduced as an optional feature
 - Very few terminals inform the user if encryption is taking place or not



Network Security

- Lecture 8 -

Universal Mobile Telecommunication System (UMTS) – 3G

Adela Georgescu

Faculty of Mathematics and Computer Science
University of Bucharest

*slides belonging to Ruxandra Olimid

Outline

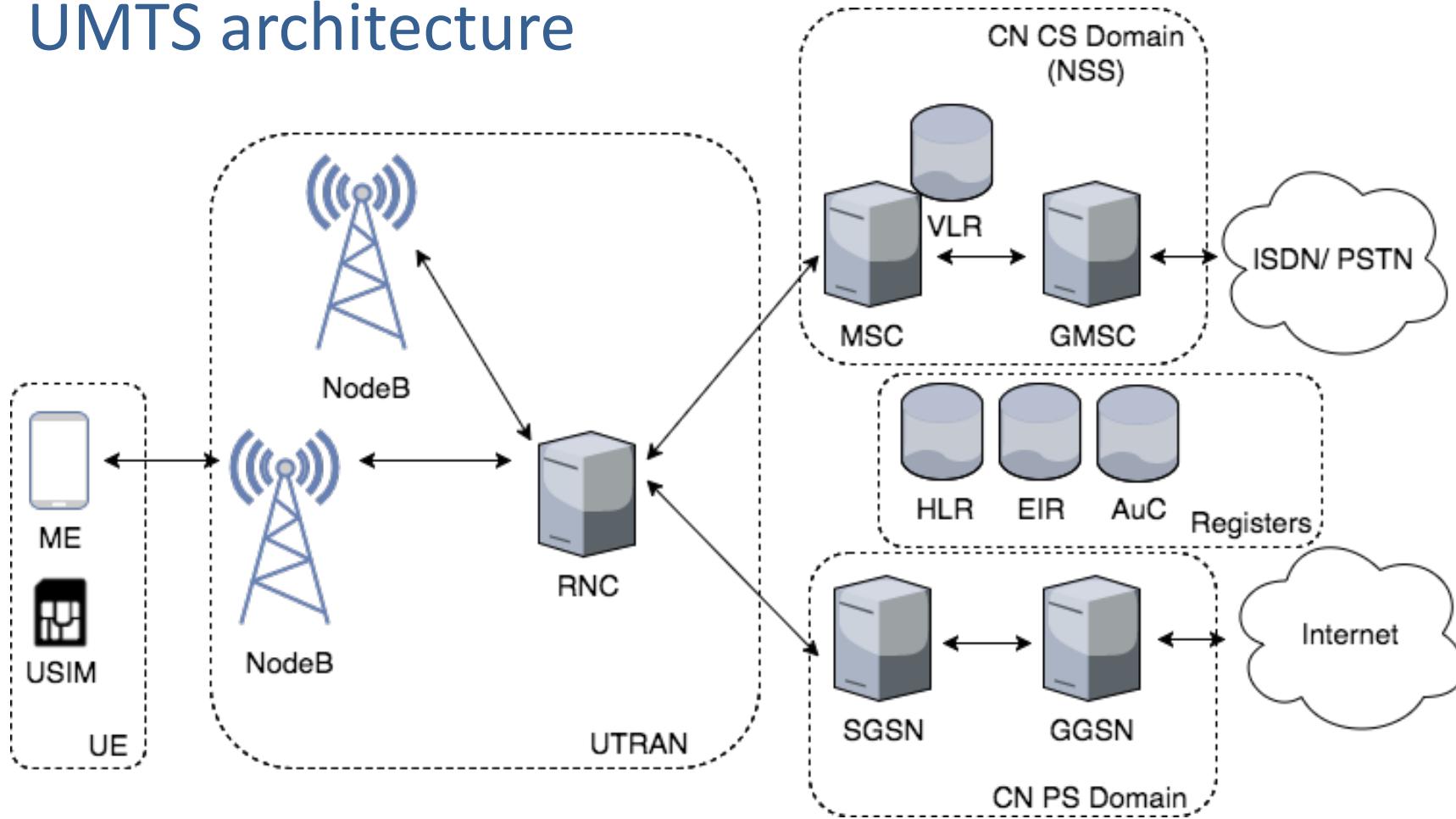
1. UMTS architecture
2. Security principles and implementation
3. Man-in-the-Middle Attack



A GLOBAL INITIATIVE

[Source: <http://www.3gpp.org/>]

UMTS architecture



UE: User Equipment

ME: Mobile Equipment

USIM: Universal SIM

ISDN: Integrated Services Digital Network

PSTN: Public Switched Telephone Network

UTRAN: UMTS Terrestrial Radio

Access Network

RNC: Radio Network Controller

CN CS : Core Network Circuit Switched

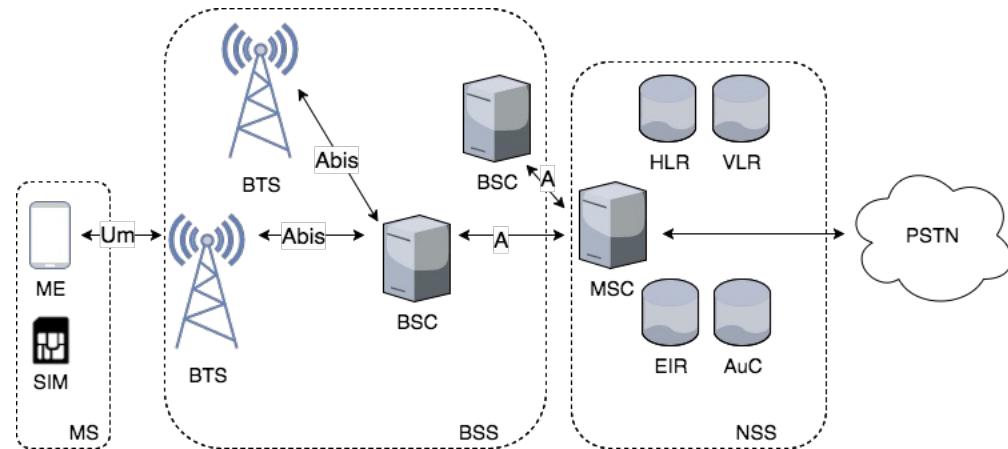
GMSC: Gateway MSC

CN PS : Core Network Packet Switched

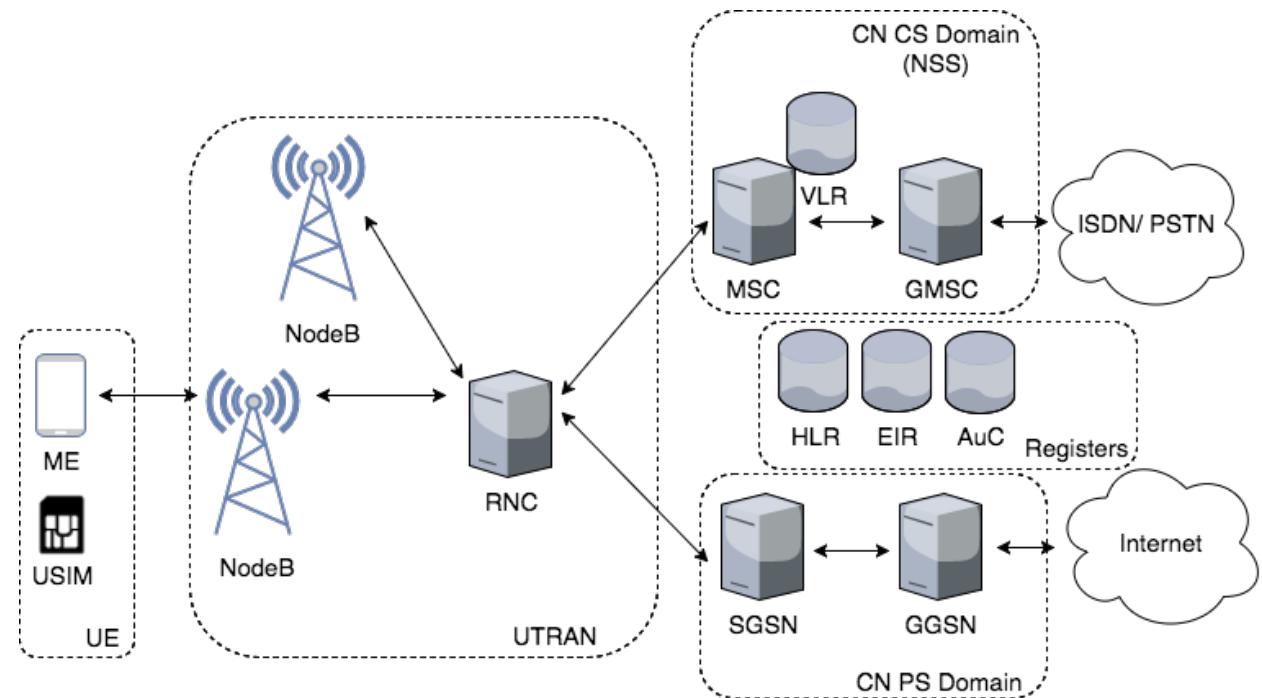
SGSN: Serving GPRS Support Node

GGSN: Gateway GPRS Support Node

UMTS architecture (vs.GSM)



UMTS architecture



UMTS architecture (vs.GSM)

- **UE (User Equipment):**
 - Consists in a Mobile Equipment (ME) and a Universal Subscriber's Identity Module (USIM)
 - Notice the name change: MS vs. UE, SIM vs USIM
- **UTRAN (UMTS Terrestrial Radio Access Network):**
 - NodeB is the base station UMTS (corresponds to BTS in GSM)
 - RNC (Radio Network Controller) is the controller in UMTS (corresponds to BSC in GSM)
- **Authentication:**
 - The same elements as in GSM: VLR, HLR, EIR, AuC

UMTS architecture (vs.GSM)

- The core part is now divided according to the technology used:
packet switched and *circuit switched*
- **CN CS Domain (Core Network Circuit Switched Domain):**
 - Corresponds to NSS in GSM
 - Realises connectivity with ISDN / PSTN
- **CN PS Domain (Core Network Packet Switched Domain):**
 - It is new to UMTS, being responsible for switching and subscriber control for packet switching technology
 - Achieves internet connectivity

UMTS – Security principles

- Taken from GSM:
 - Subscriber authentication, use of (U)SIM
 - Radio interface encryption (for *confidentiality*)
 - Use of temporary identities (for *privacy of subscribers*)
 - Use of registers: HLR, VLR, AuC
- Designed to withstand GSM attacks

GSM – short recap

Weaknesses in GSM security:

- No specification about the *integrity of the data*
- *Breaking Kerckhoffs' principle*: cryptographic algorithms were kept confidential (e.g.: A5/1, A5/2), and their strength was not publicly tested
- *Limited encryption*: data is encrypted on the radio link only
- *Short keys*; cryptosystems are vulnerable to *exhaustive search attack*
- *Unilateral authentication*: The mobile station does not authenticate the network (only the network authenticates the mobile station)
- *Active attacks are possible*; e.g.: IMSI Catchers, when an adversary masquerades a legitimate BTS

UMTS – Security principles

Weaknesses in GSM security:

Addressed in UMTS!

- *Kerckhoffs' principle*: cryptographic algorithms were kept confidential
 - Cryptographic algorithms are public
- *Short cryptographic keys*: *brute force* vulnerable
 - Longer cryptographic keys (128 bits)
- *Limited encryption*: data is encrypted only from MS to BTS
 - Data encryption up to RNC
- *Unilateral authentication*: MS does not authenticate the network, only the network authenticates MS
 - *Mutual authentication (UE and network authenticate each other)*
- No *integrity of data*
 - Use of Message Authentication Code (MAC)

UMTS – Security principles

- New security principles, as an improvement over GSM :
 - ... (previous slide)
 - KASUMI encryption algorithm is exported worldwide
 - The UE and the network negotiate to agree on the encryption and integrity algorithms used
 - Enter SQN (SeQuence Number) in authentication triplets (in AUTN) to avoid *replay attacks* and to ensure *key freshness*

UMTS – Security principles

Weaknesses in UMTS:

- *Active attacks are possible; e.g.: IMSI Catchers, when an adversary impersonates a NodeB*
- *Users are not (generally) aware of the security level*
- *End-to-end (UE-to-UE) security is not considered*
- *Weaknesses in authentication process (no use of PKI)*

We will meet them again in
LTE!

Man-in-the-Middle Attack

UMTS – Man-in-the-Middle Attack

- **Goal:** mount a MitM (Man-in-the-Middle) attack against UMTS - all traffic initiated by the mobile station (UE) is transmitted through the adversary, which has access to the information
- **Main idea:**
 - The adversary obtains an authentication token from any real network, and uses this token to impersonate a GSM base station to the UMTS user
- **The attack is possible due to:**
 - Inter-operability GSM / UMTS
 - GSM does not support integrity protection, so the adversary can fool the UE not to use encryption
- The attack was introduced by **Meyer** and **Wetzel** in 2004

[U.Meyer, S.Wetzel - A Man-in-the-Middle Attack on UMTS, WiSe'04]

UMTS – Man-in-the-Middle Attack

- MitM is known to be easy in **GSM**:
 - Because there is no authentication of the *serving network* to the user, so that an adversary can impersonate a BTS
 - An adversary can impersonate the MS to BTS by simply forwarding authentication traffic
- The attacker can eavesdrop on the communication by fooling both parties into not using encryption (i.e., use A5/0)
- If the attack is possible in GSM, then **UMTS subscribers which use GSM are vulnerable**
- ... but UMTS subscribers are vulnerable even though they roam in UMTS and UMTS authentication is applied
- **Roll-back attack:** *An attack which exploits weaknesses of old versions defined to ensure backward compatibility*

UMTS – Man-in-the-Middle Attack

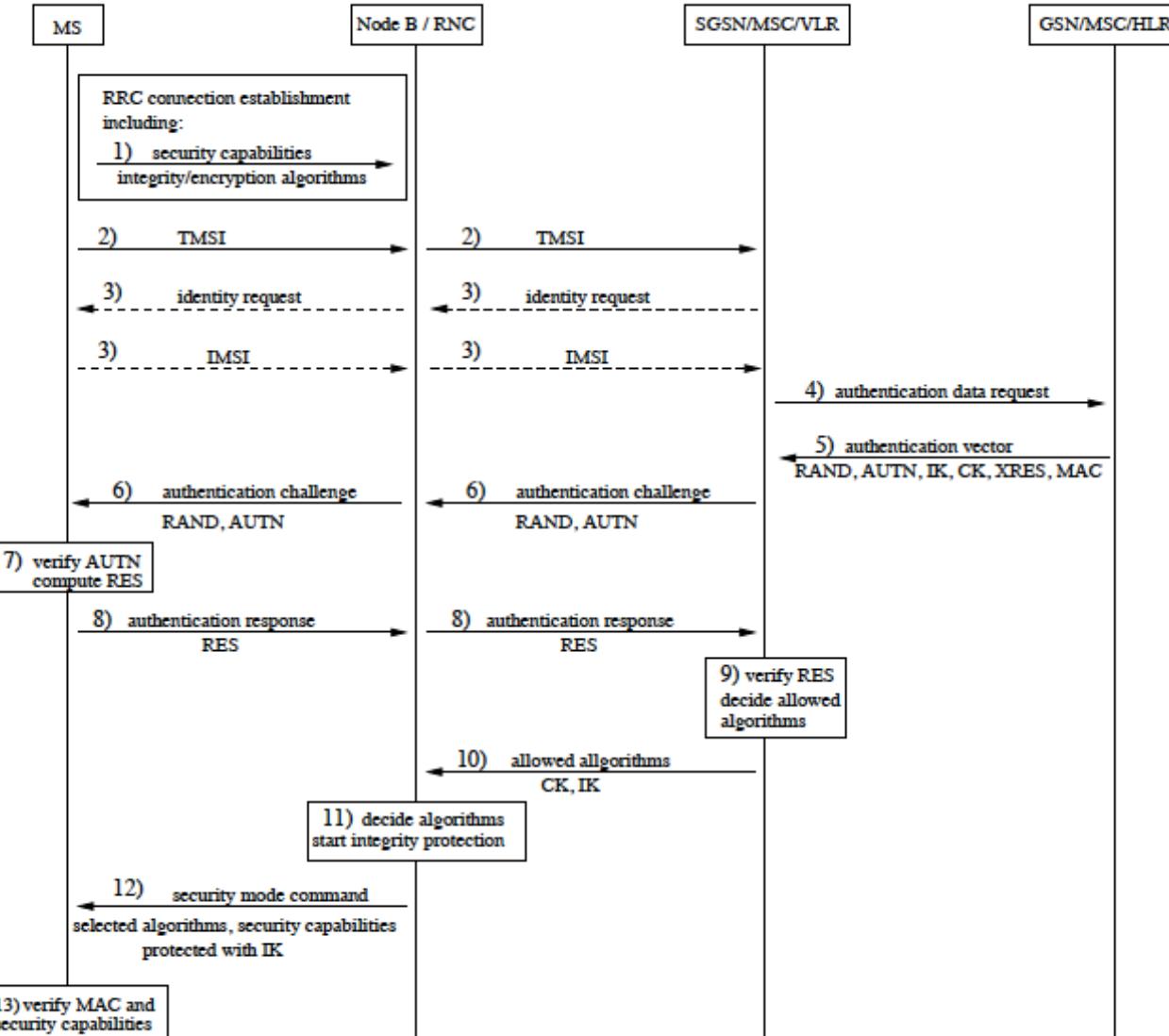
- 2 types of authentication are of interest for the attack:
 - **UE (UMTS) – NodeB (UMTS)**: UMTS subscriber connects to UMTS network by means of NodeB
 - **UE (UMTS) - BTS (GSM)**: UMTS subscriber with UE that allows connecting to GSM, connects to the *serving network* by means of BTS

AKA: UE (UMTS) – NodeB (UMTS)

RRC: Radio Resource Control
 GSN: GPRS Support Node

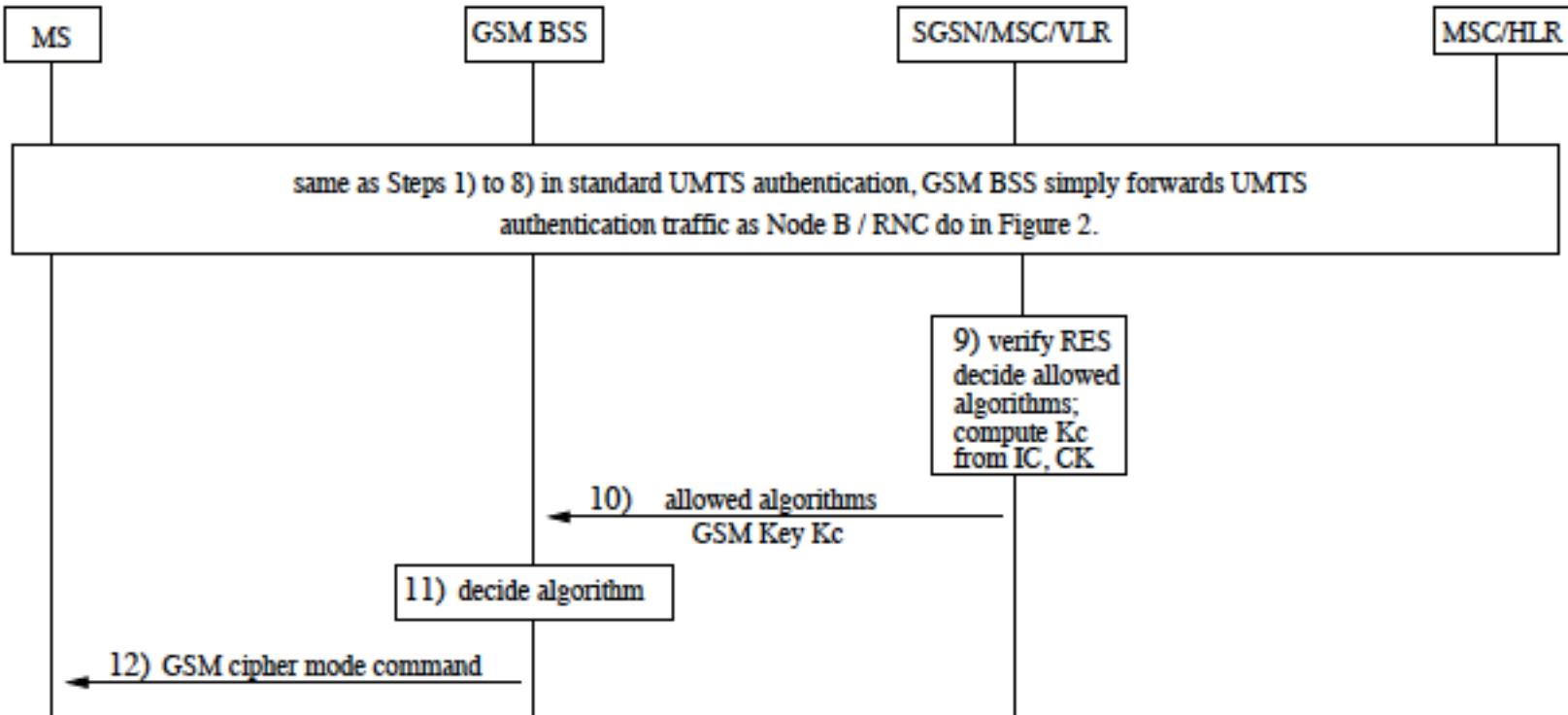
Authentication Data

RAND: random challenge
 AUTN: authentication token
 IK: integrity Key
 CK: encryption key
 XRES: authentication expected response
 MAC: Message Authentication Code, used to provide integrity of the authentication data



[Source: U.Meyer, S.Wetzel - A Man-in-the-Middle Attack on UMTS, WiSe'04]

AKA: UE (UMTS) – BTS (GSM)



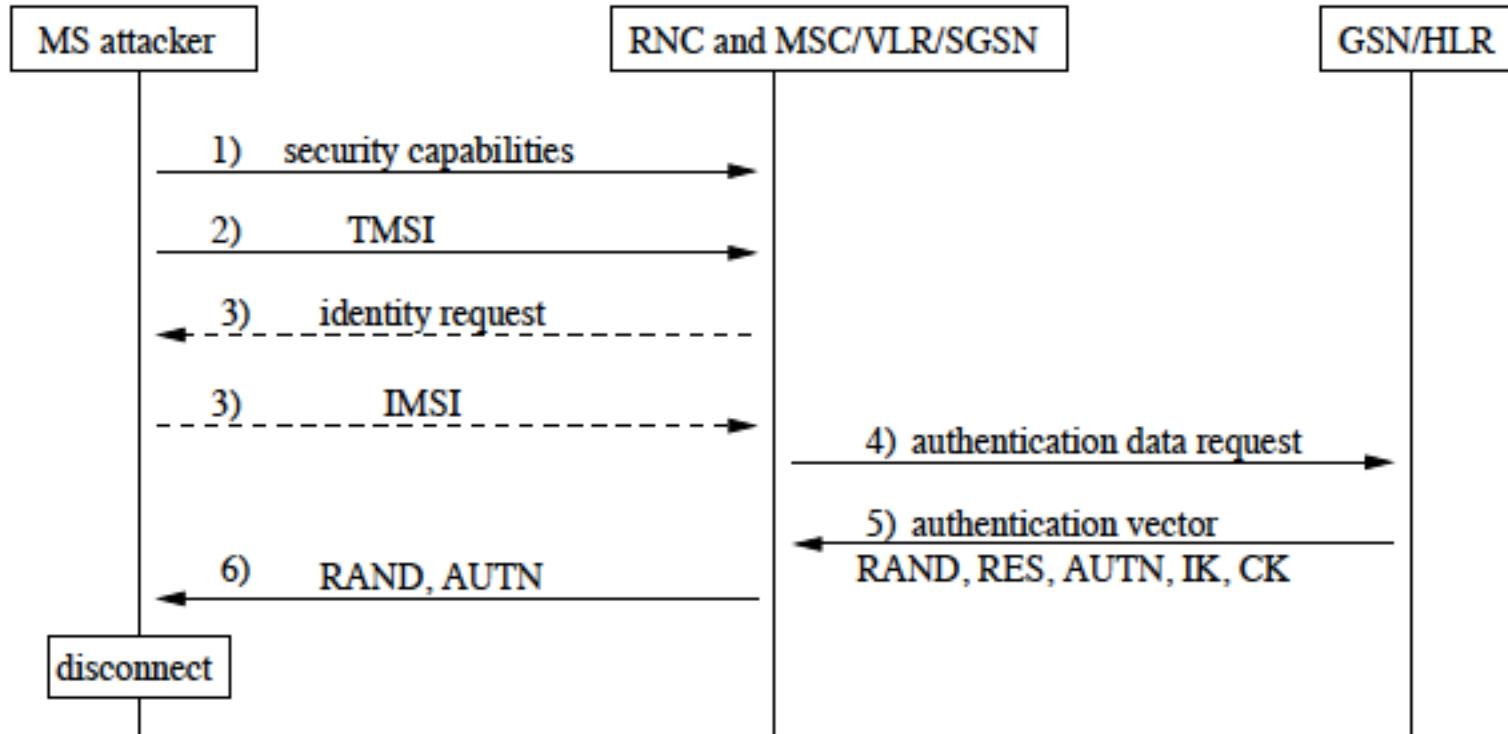
[Source: U.Meyer, S.Wetzel - A Man-in-the-Middle Attack on UMTS, WiSe'04]

Message in step12 can be modified by the adversary because it is not integrity protected (GSM does not support integrity protection)

UMTS – Man-in-the-Middle Attack

- The attacks consists of 2 phases (+1):
 - **Phase 0:** the adversary finds the IMSI of the victim (and its cryptographic capabilities)
 - It is feasible, by initiating an authentication procedure before the attack (IMSI Catcher)
 - **Phase 1:** The adversary acts on behalf of the victim to get a valid authentication token AUTN (from the network)
 - **Phase 2:** The adversary impersonates a BTS (GSM) to determine the victim connect to this fake BTS

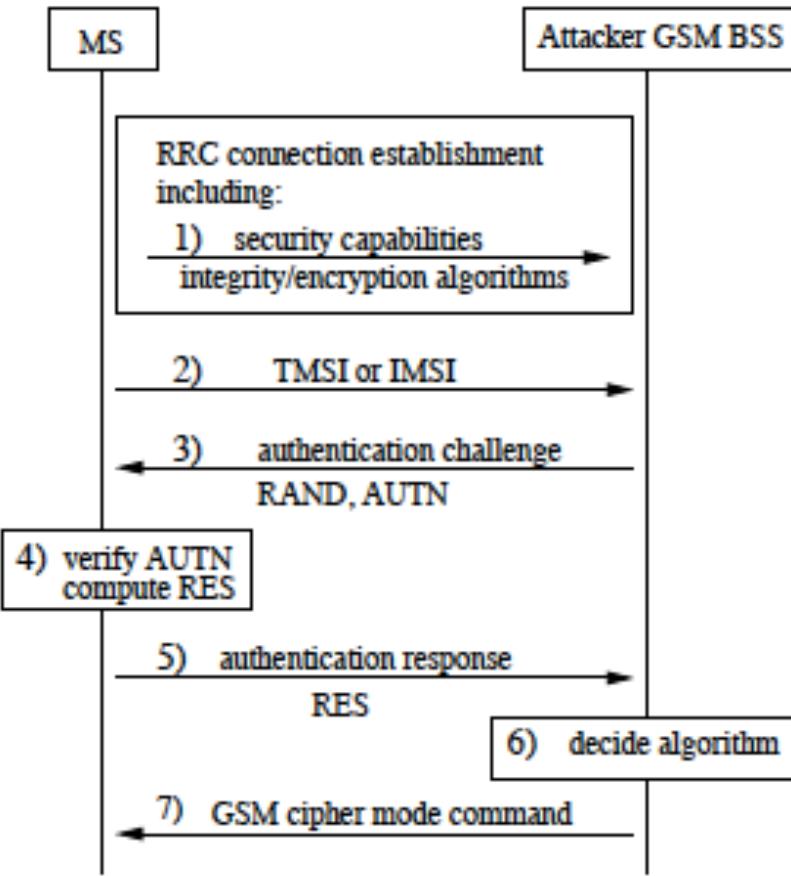
Phase 1



[Source: U.Meyer, S.Wetzel - A Man-in-the-Middle Attack on UMTS, WiSe'04]

Phase 1: The adversary acts on behalf of the victim to get a valid authentication token AUTN (from the network)

Faza 2



[Source: U.Meyer, S.Wetzel - A Man-in-the-Middle Attack on UMTS, WiSe'04]

- **Phase 2:** The adversary impersonates a BTS (GSM) to determine the victim connect to this fake BTS

UMTS – Man-in-the-Middle Attack

- The adversary can decide to use A5/0 (no encryption), if this is accepted by the MS/UE (in phase 1, *security capabilities*)
- The attack does not work if there is another authentication between Phase 1 and Phase 2, otherwise out of *range SQN*
- The attack does not allow impersonating both MS/UE and BTS/NodeB in the same time



Network Security

- Lecture 8 -

Long term evolution
(LTE) – 4G

Adela Georgescu

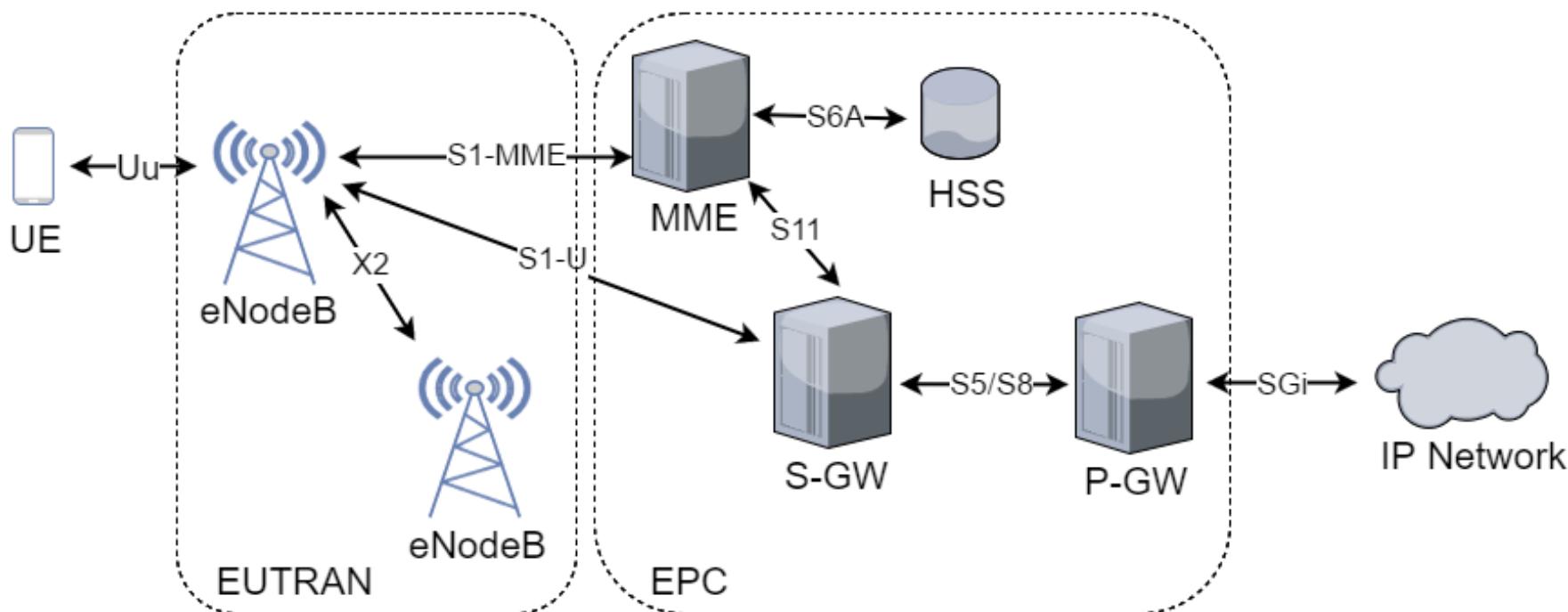
Faculty of Mathematics and Computer Science
University of Bucharest

*slides belonging to Ruxandra Olimid

Outline

- LTE (Security) Architecture
- Security Requirements / Principles
- Vulnerabilities and Attacks

LTE - Architecture



UE: User Equipment

ME: Mobile Equipment

USIM: Universal SIM

EUTRAN: Evolved UTRAN

eNodeB: Evolved NodeB

EPC: Evolved Packet Core

MME: Mobility Management Entity

S-GW: Serving Gateway

P-GW: PDN (Packet Data Network) Gateway

HSS: Home Subscriber Server

LTE - Architecture

- **UE (User Equipment):**
 - Same as in UMTS: consists of the Mobile Equipment (ME) and the Universal Subscriber's Identity Module (USIM)
- **EUTRAN (Evolved UTRAN):**
 - Consists in several eNodeBs
 - A difference from UMTS is that the eNodeBs can communicate directly between themselves
- **EPC (Evolved Packet Core):**
 - UE is authenticated by the MME is responsible for selecting the SGSN at 2G/3G handovers, authentication and resources allocation to UEs. It manages the mobility of UEs in the network when eNodeBs cannot
 - S-GW is an interconnection point between EUTRAN and EPC, is responsible for packet routing and forwarding, buffering download packets, being a mobility anchor for inter-3GPP mobility
 - P-GW is a routing point to provide connectivity to the external PDN

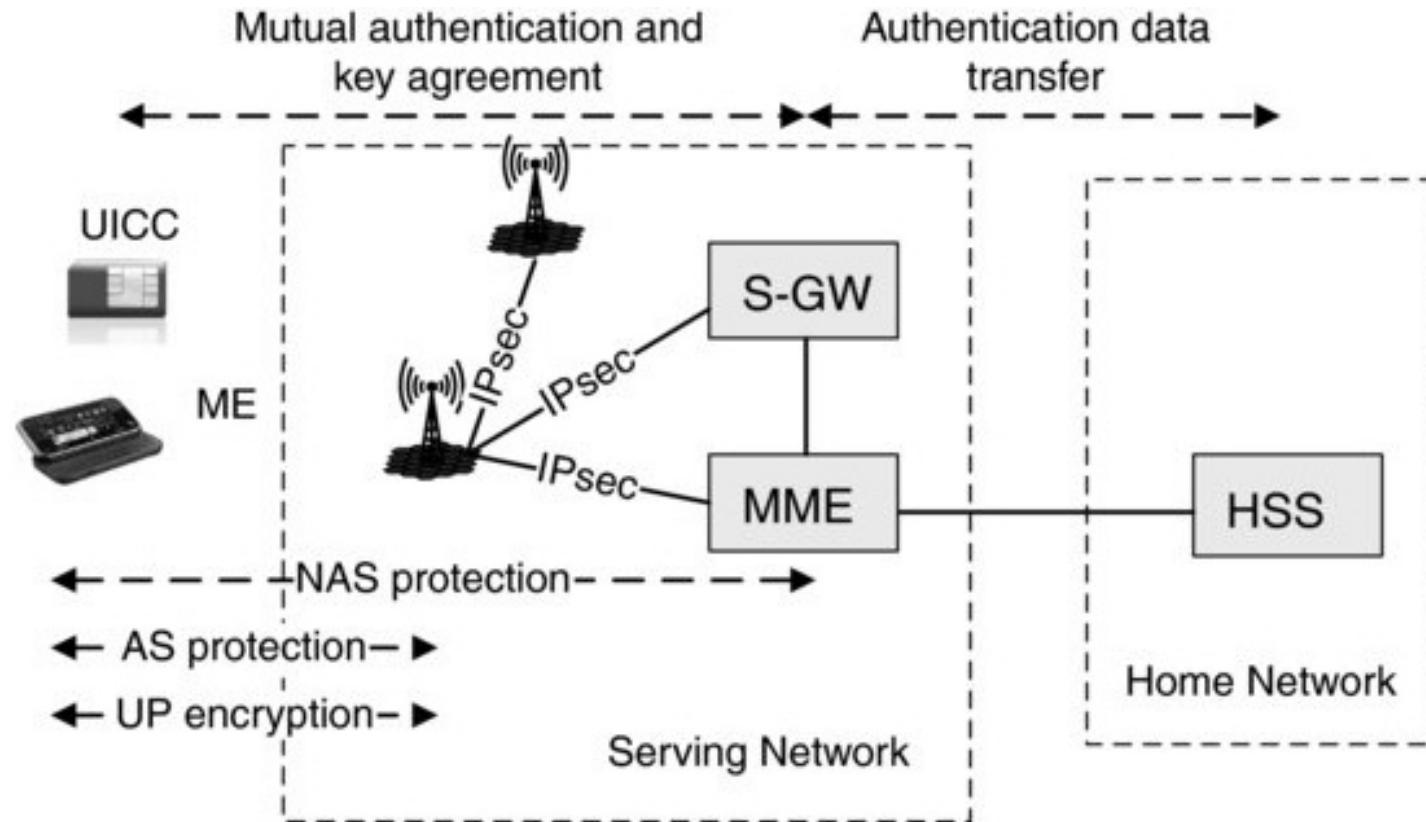
Terminology

- **LTE (Long Term Evolution):**
 - The new radio technology
- **SAE/LTE (System Architecture Evolution / LTE):**
 - Stands for the entire system: LTE technology with access to previous technologies such as GSM and 3G
 - LTE includes the EUTRAN, while SAE includes the EPC
- **EPS (Evolved Packet System):**
 - The technical term for SAE/LTE, but the brand name of the new system has been chosen to be **LTE**

EPS Security Architecture

- GSM and UMTS security mechanisms are used as a basis, but adapted to the EPS architecture
- Protection is performed in both planes:
 - *Signalling plane*
 - *User plane*
- There exists both confidentiality and integrity protection mechanisms:
 - **Confidentiality:** **both signalling and user planes**
 - **Integrity:** **just signalling plane**

EPS Security Architecture



NAS: Non-Access Stratum

AS: Access Stratum

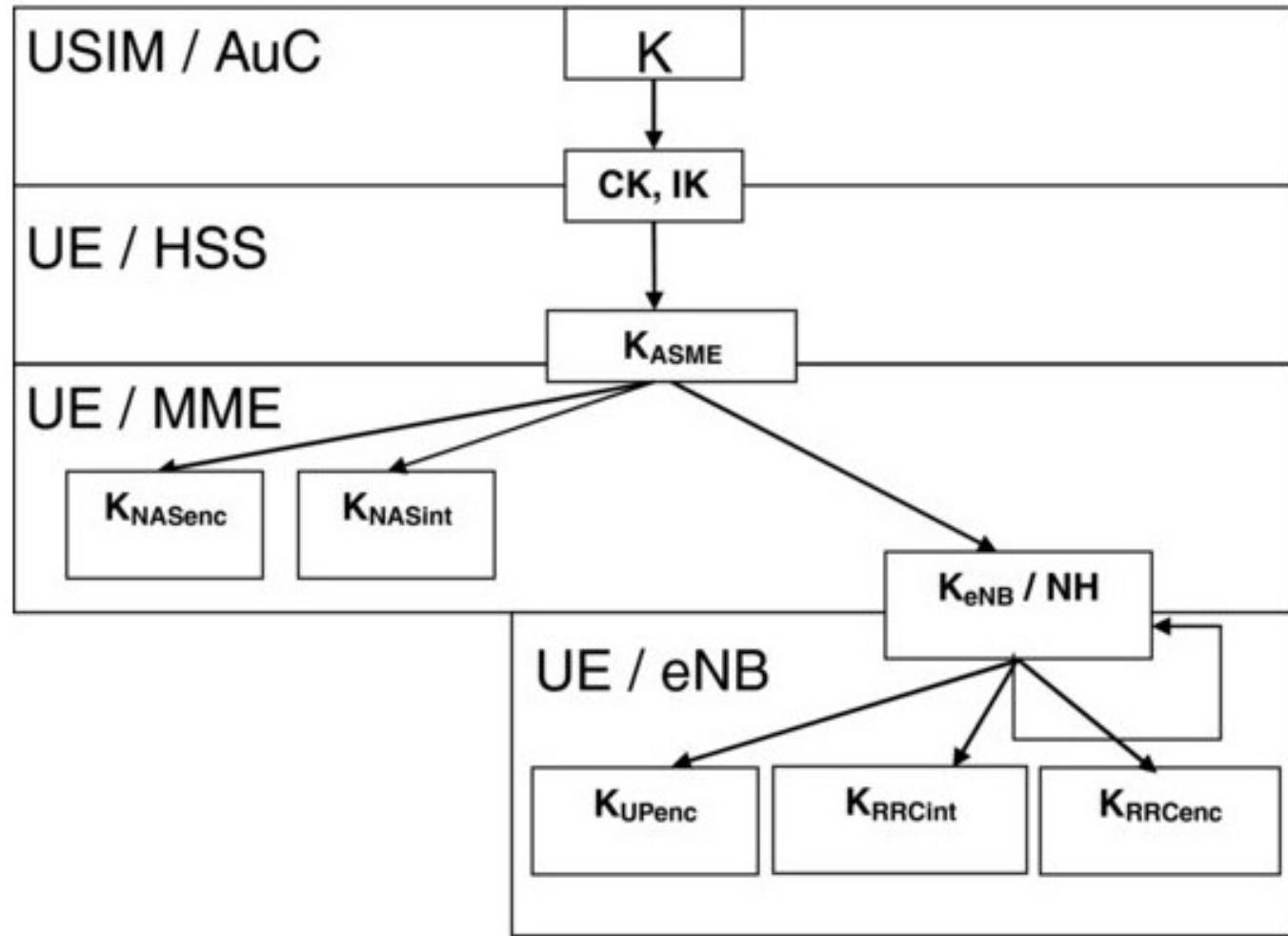
UP: User Plane

[Source: D.Forsberg et al. – LTE Security, Wiley 2012]

EPS Security Architecture

- MME fetches authentication data from the HSS
- MME triggers the authentication and key agreement protocol with the UE, resulting a key K_{ASME}
- 2 derived keys are used for confidentiality (K_{NASenc}) and integrity (K_{NASint}) protection of the signalling data between the MME and the UE - **NAS protection**
- One key is transported to the eNodeB (K_{eNB}), from which 3 other keys are derived:
 - 2 derived keys are used for confidentiality (K_{RRCenc}) and integrity (K_{RRCint}) protection of the signalling data between the eNodeB and the UE - **AS protection**
 - 1 derived key (K_{UPenc}) is used for confidentiality protection of the user plane data between the eNodeB and the UE

Key Hierarchy

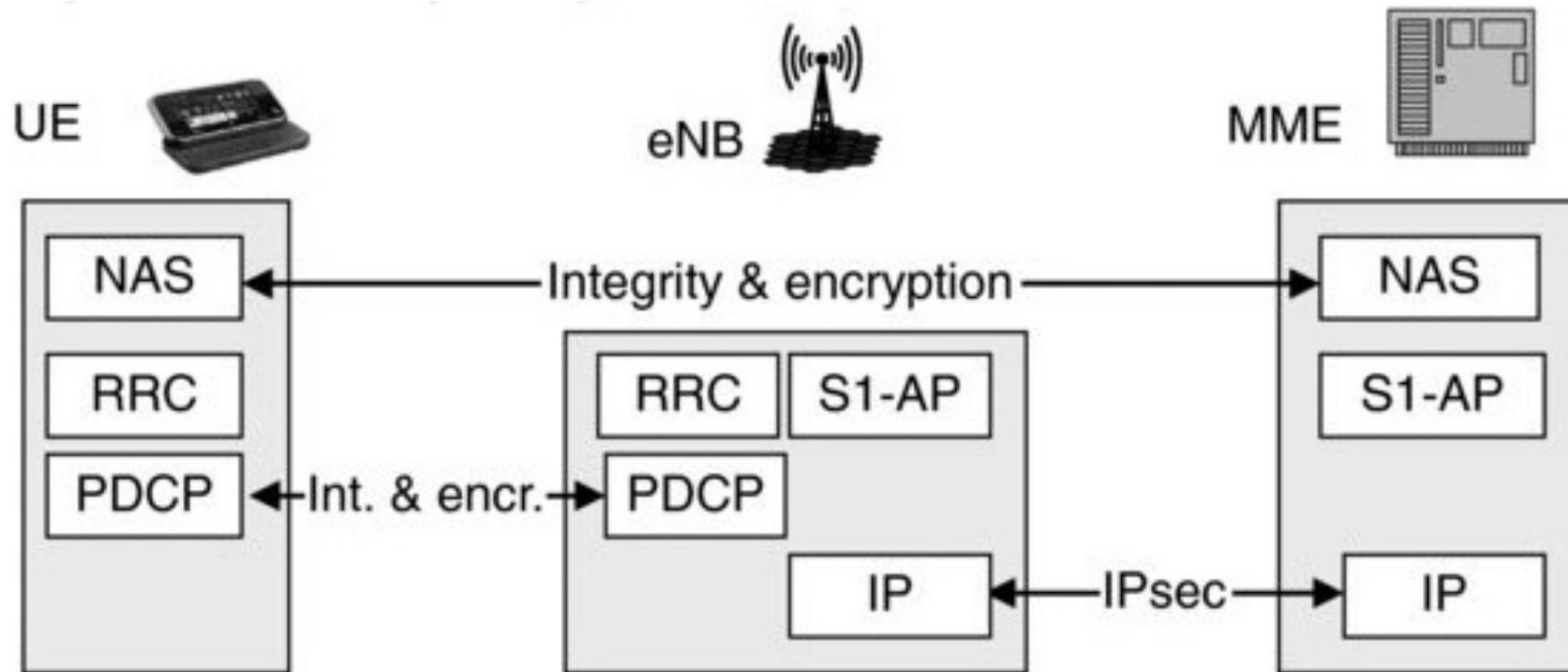


[Source: D.Forsberg et al. – LTE Security, Wiley 2012]

Key Hierarchy

Key	Length	Info
K	128 bits	Key shared between the subscriber and the network operator, stored in the USIM and AuC; permanent key of the subscriber
CK, IK	128 bits	Ciphering key CK and integrity key IK are for UMTS interconnection
K_{ASME}	256 bits	A local master key of the subscriber from which all other keys will be derived; Shared between the UE and the MME
K_{NASenc}, K_{NASint}	128 / 256 bits	Ciphering key K_{NASenc} and integrity key K_{NASint} for NAS protection
K_{eNB} / NH	256 bits	Intermediate key stored in the eNodeB NH (Next Hop) is used in handover
K_{RRCenc}, K_{RRCint}	128 / 256 bits	Ciphering key K_{RRCenc} and integrity key K_{RRCint} for AS protection
K_{UPenc}	128 / 256 bits	Ciphering key K_{UPenc} for user data

EPS Signalling Plane Protection



NAS: Non-Access Stratum

RRC: Radio Resource Control

PDCP: Packet Data Convergence Protocol

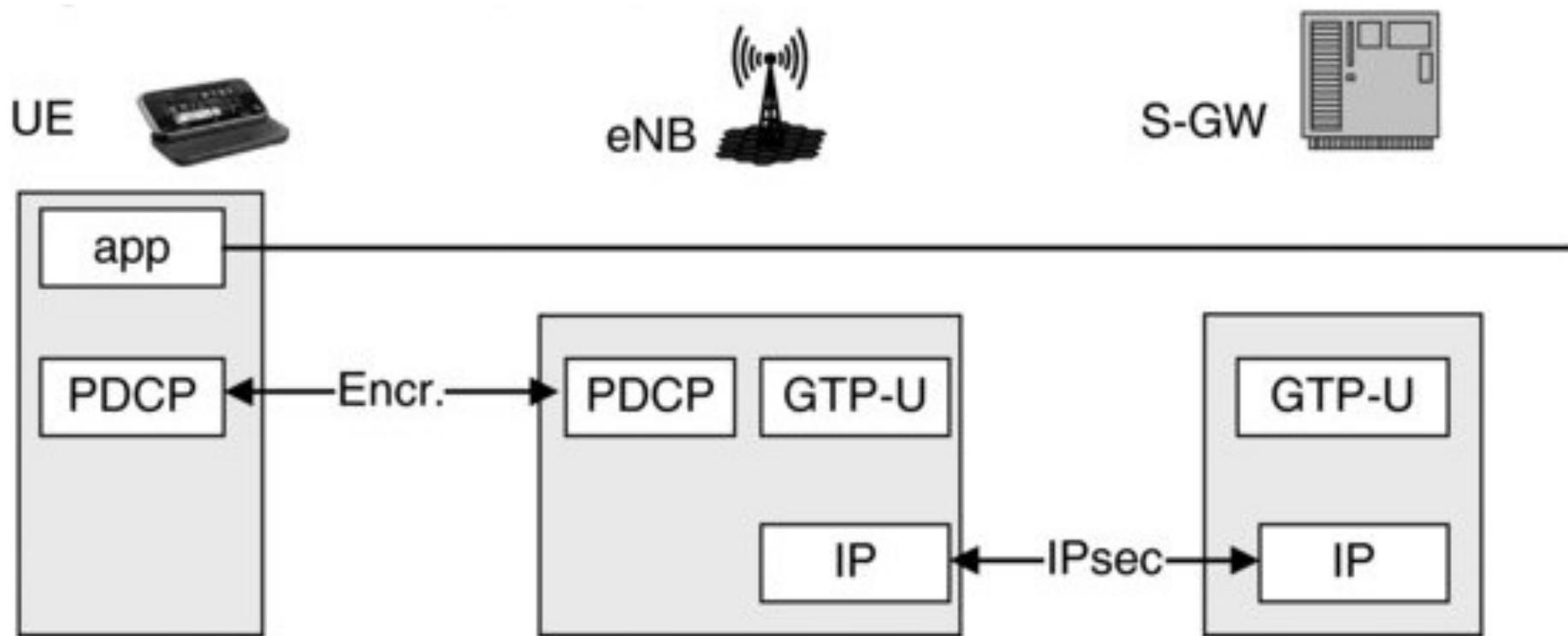
IP: Internet Protocol

[Source: D.Forsberg et al. – LTE Security, Wiley 2012]

EPS Signalling Plane Protection

- **NAS (Non-Access Stratum)**: network layer communication between the UE and the core network
- **RRC (Radio Resource Control)**: layer 3 protocol in the AS (Access Stratum) protocol stack that provides communication between the UE and the eNodeB (the AS level signalling protocol)
- **PDCP (Packet Data Convergence Protocol)**: both RRC signalling and user data are carried by the PDCP, and here is where security is implemented
- **S1-AP**: signalling service between the E-UTRAN and the EPC

EPS User Plane Protection



PDCP: Packet Data Convergence Protocol

GTP: GPRS Tunneling Protocol

[Source: D.Forsberg et al. – LTE Security, Wiley 2012]

EPS User Plane Protection

- PDCP (Packet Data Convergence Protocol): if for signalling data both confidentiality and integrity are supported, user plane protection does not consider integrity
- GTP-U: is used for carrying data from the access network to the core network

Confidentiality is optional for both signalling and user plane!

EPS Security Requirements

- High level and service-related security requirements:
 - EPS should provide authenticity of information between the terminal and the network
 - EPS shall ensure that unauthorized users cannot establish communication through the system
 - EPS shall allow the network to hide its internal structure from the terminal
 - Security policies should be under home operator control
 - EPS shall provide support for lawful interception
 - EPS shall support emergency calls
 - Rel-99 or newer USIM is required for authentication

EPS Security Requirements

- Privacy related security requirements:
 - *EPS shall provide several appropriate levels of user privacy for communication, location and identity*
 - *Communication content, origin and destination shall be protected against disclosure to unauthorized parties*
 - *EPS shall be able to hide user identities from unauthorized parties*
 - *EPS shall be able to hide user location from unauthorized parties*

EPS Security Features

- Features that are carried over from GSM and UMTS:
 - Subscriber authentication, usage of USIM (IMEI stored in the ME and IMSI stored in the UICC)
 - Mutual authentication (from UMTS)
 - Encryption on the radio interface (for *confidentiality*), which remains optional to the network operator
 - Usage of temporary identities (for *privacy of subscribers*)
 - Visibility and configurability of security at the UE (e.g. ciphering indicator) is optional
 - Lawful interception

EPS Security Features

- New features in EPS to overcome the shortcomings in GSM/UMTS:
 - The endpoint for encryption in the network side remains the eNodeB, but physical security requirements are introduced for eNodeB (in UMTS is the RNC, but in GSM is the BTS)
 - No integrity mechanism for the user data (reason: risk to tamper the user data is considered too low to introduce significant overhead by integrity protection, especially for voice)
 - New key hierarchy, more elaborated
 - Improvements on crypto algorithms and protocols

EPS Security Standards



- **TS 33.401:** *3GPP System Architecture Evolution (SAE); Security architecture* / ETSI 133 401
 - EPS security architecture
 - EPS security features, procedures, mechanisms
 - Main reference
- **TS 33.402:** *Security aspects of non-3GPP accesses* / ETSI 133.402
- **TS 33.320:** *Security of Home evolved Node B (HeNB)* / ETSI 133.320
- **TS 36.331:** *Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification* / ETSI 136 331
- **TS 24.301:** *Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS)* / ETSI 124 301
- ...

3GPP: The 3rd Generation Partnership Project
ETSI: European Telecommunications Standards Institute

To remember!

1. LTE (security) architecture
2. Security mechanisms on both the signalling and the user plane
3. Security features (build on previous generations' features)



Network Security

- Lecture 11 -
LTE (cont.)

Adela Georgescu

Faculty of Mathematics and Computer Science
University of Bucharest

*slides belonging to Ruxandra Olimid

Outline

- UE Identification
- EPS AKA
- Key hierarchy (again)
- Cryptographical aspects
- AS / NAS Protection

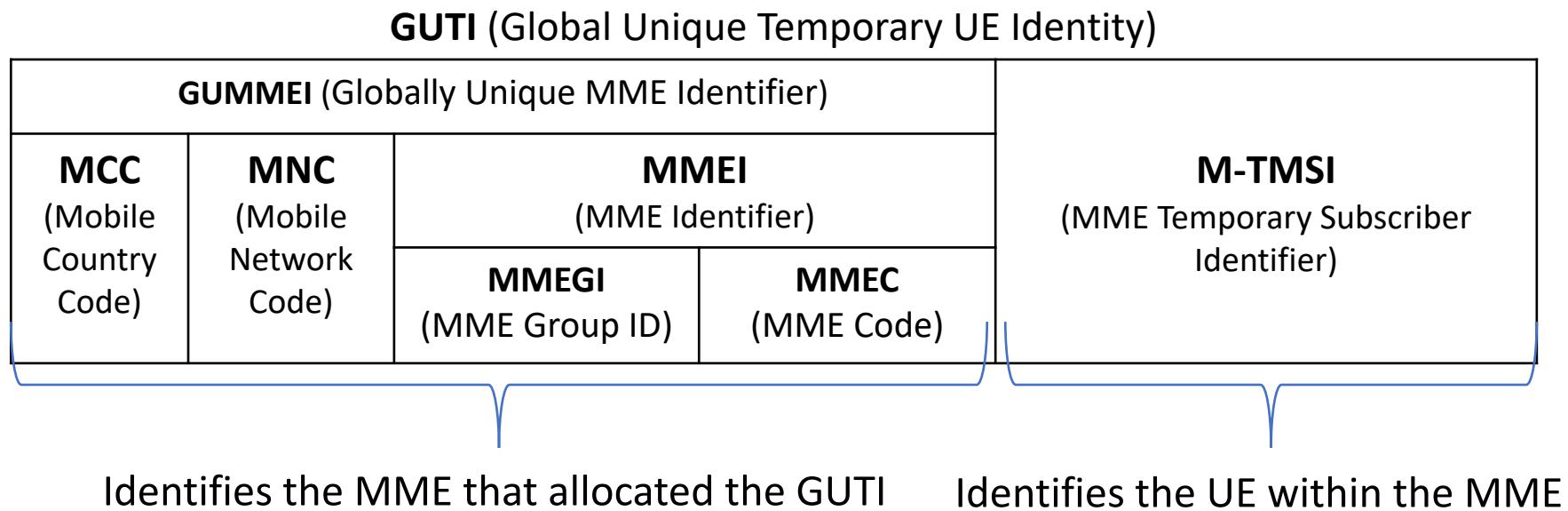
UE Identification



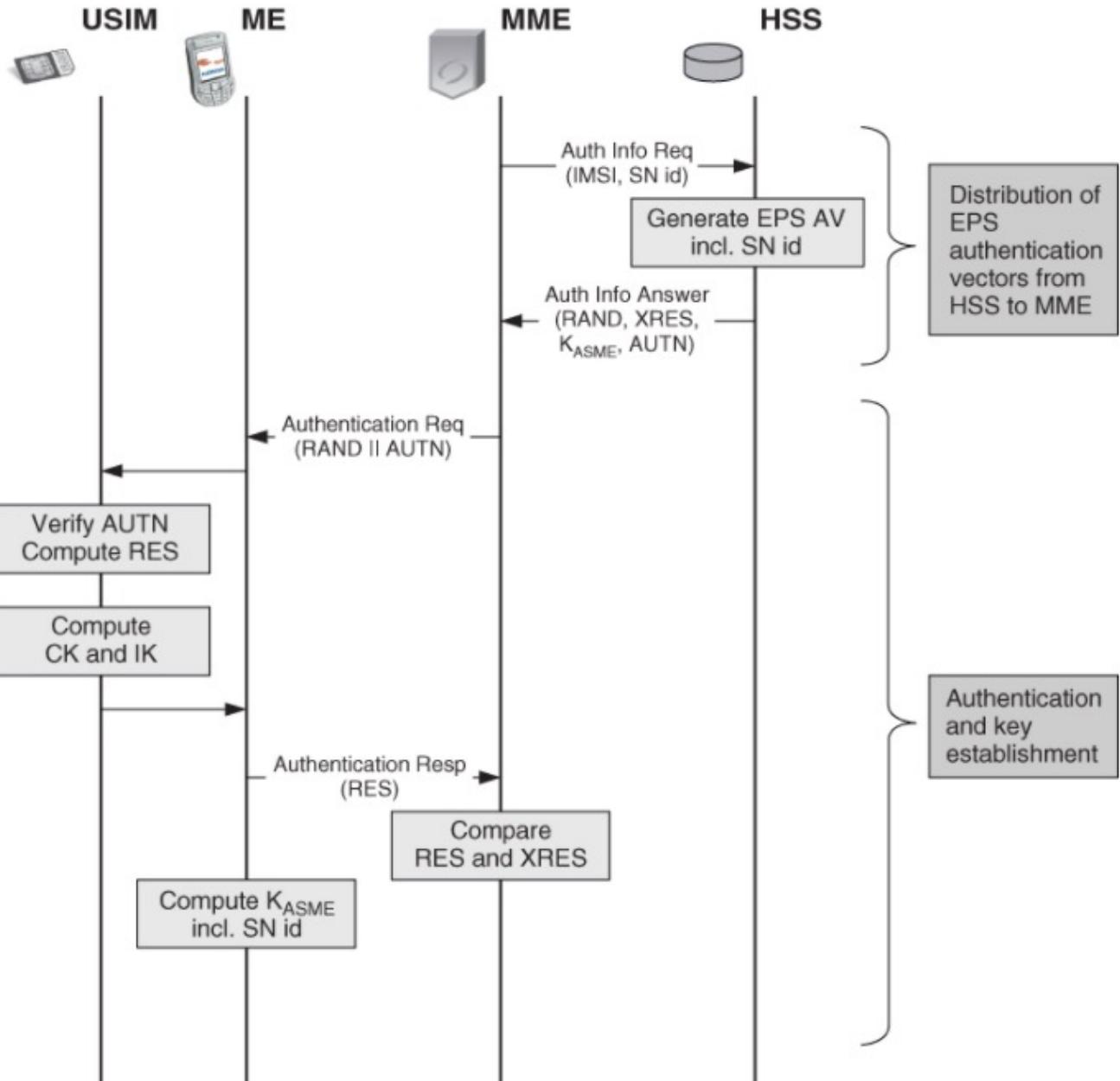
- Similar to identification in GSM and UMTS
 - **IMSI**
 - **IMEI , IMEI SV**
- **GUTI** (Global Unique Temporary UE Identity), allocated to provide user identity confidentiality
 - Similar to TMSI in GSM
- **C-RNTI** (Cell Radio Network Temporary Identifier) with security role in handover preparation

UE Identification

- MME assigns a GUTI to the UE in Attach Accept or Tracking Area Update Accept messages
- MME can also assign GUTI in a separate GUTI Reallocation procedure



EPS AKA



SN id: Serving Network Identity

AV: Authentication Vector

AUTN: Authentication Token

RES: Response

XRES: Expected Response

CK: Ciphering Key

IK: Integrity Key

ASME: Access Security Management Entity

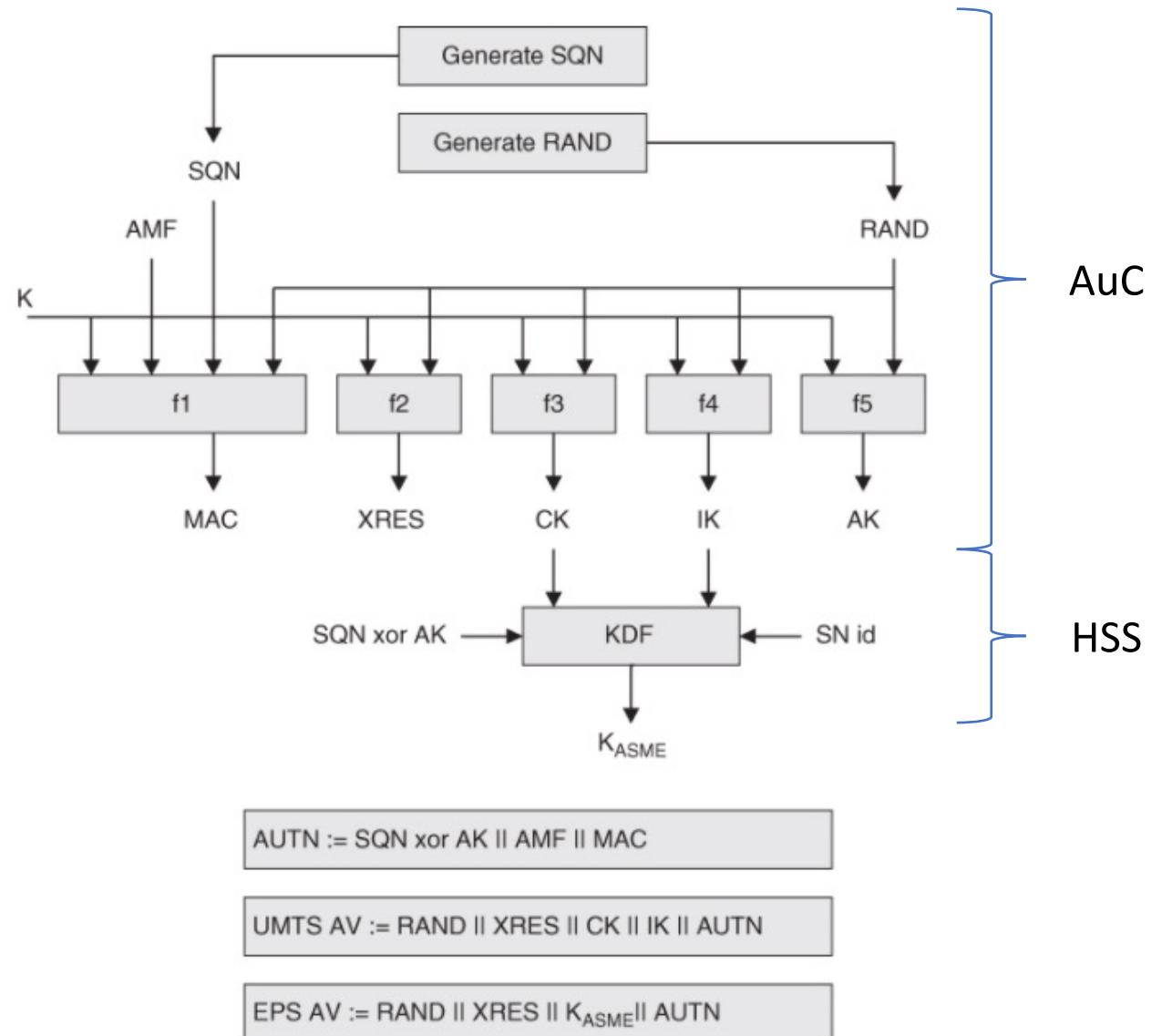
EPS AKA – Network side

- The recommendation is to send a single AV at a time (not more)...
... because the need to request fresh AV is reduced due to the existence of the K_{ASME} , which is not exposed as the CK and IK were exposed in UMTS
- Precomputed AV are not longer used when the UE moves to another network...
... because the SN id is input to the KDF
- Each AV is used only once
- CK and IK do not leave the HSS
- Operator specific: if $AK=0$, then $AK \text{ XOR } SQN = SQN$ (if the operator decides no need for concealment of SQN is required)

EPS AKA – Network side

UMTS AV:
(RAND, XRES, CK, IK, AUTN)

EPS AV:
(RAND, XRES, K_{ASME} , AUTN)



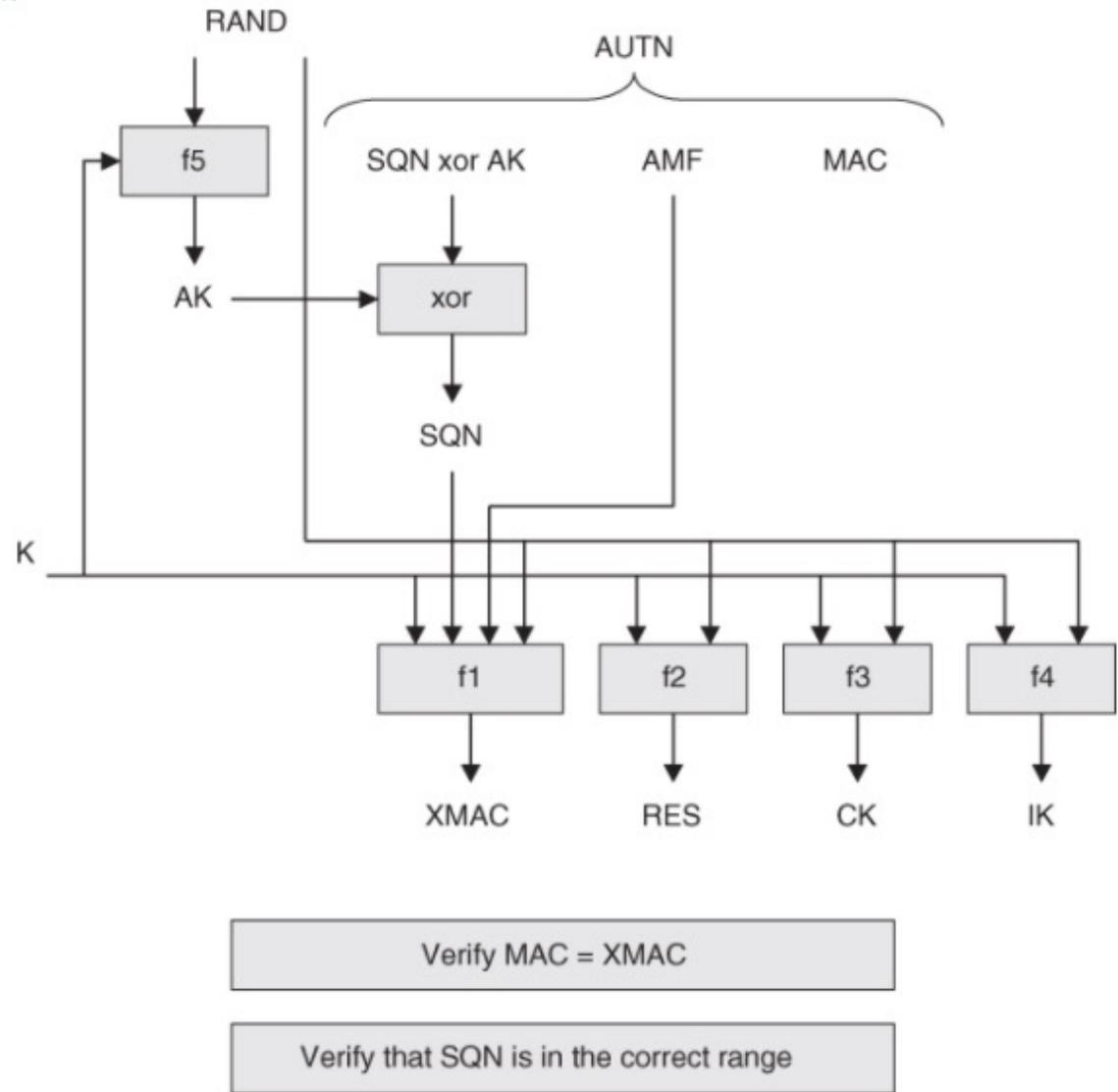
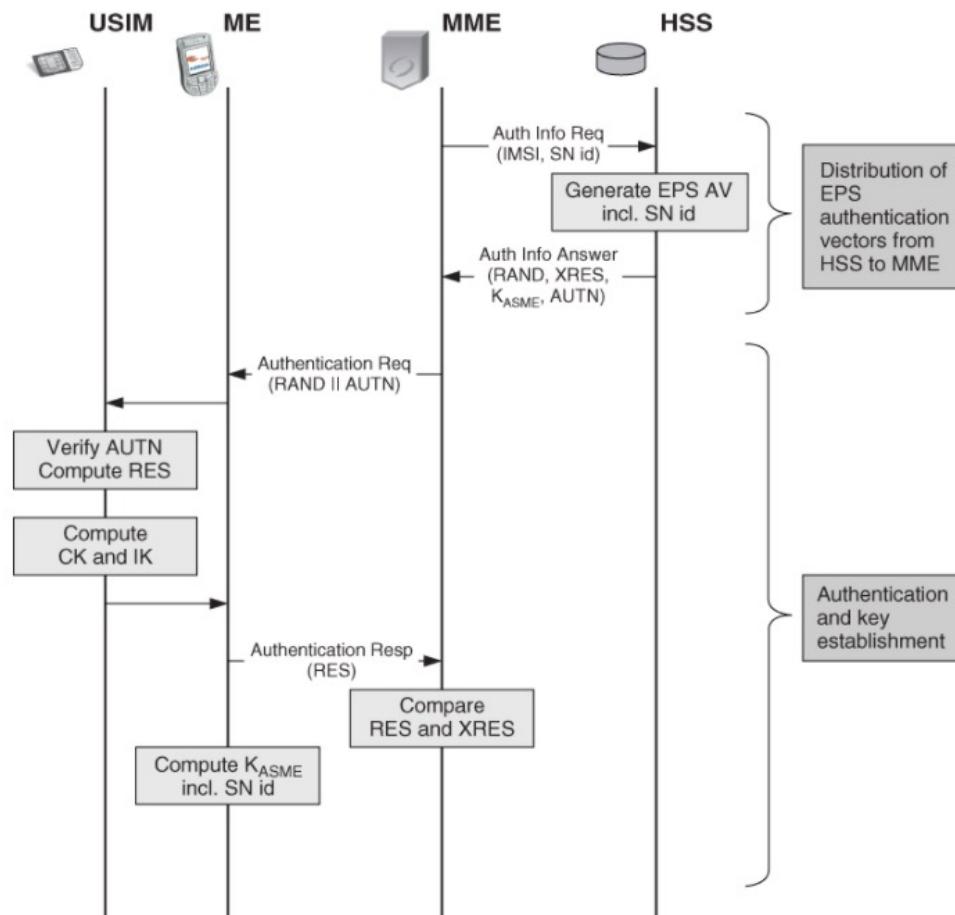
AMF: Authentication
Management Field
AK: Anonymity Key

[Source: D.Forsberg et al. – LTE Security, Wiley 2012]

EPS AKA – Network side

- Both UMTS and EPS authentication vectors are generated
- The AuC generates the AVs in exactly the same way as for UMTS
- The HSS derives the K_{ASME} from CK and IK
- The AuC generates fresh SQN and unpredictable random RAND
- **AMF (Authentication Management Field):**
 - Indicates the algorithm used to generate a particular auth vector when several exist
 - Sets threshold values for key lifetimes
 - First bit is set to 1 to mark that the AV is for EPS use (this should be checked in the MME)

EPS AKA – User side

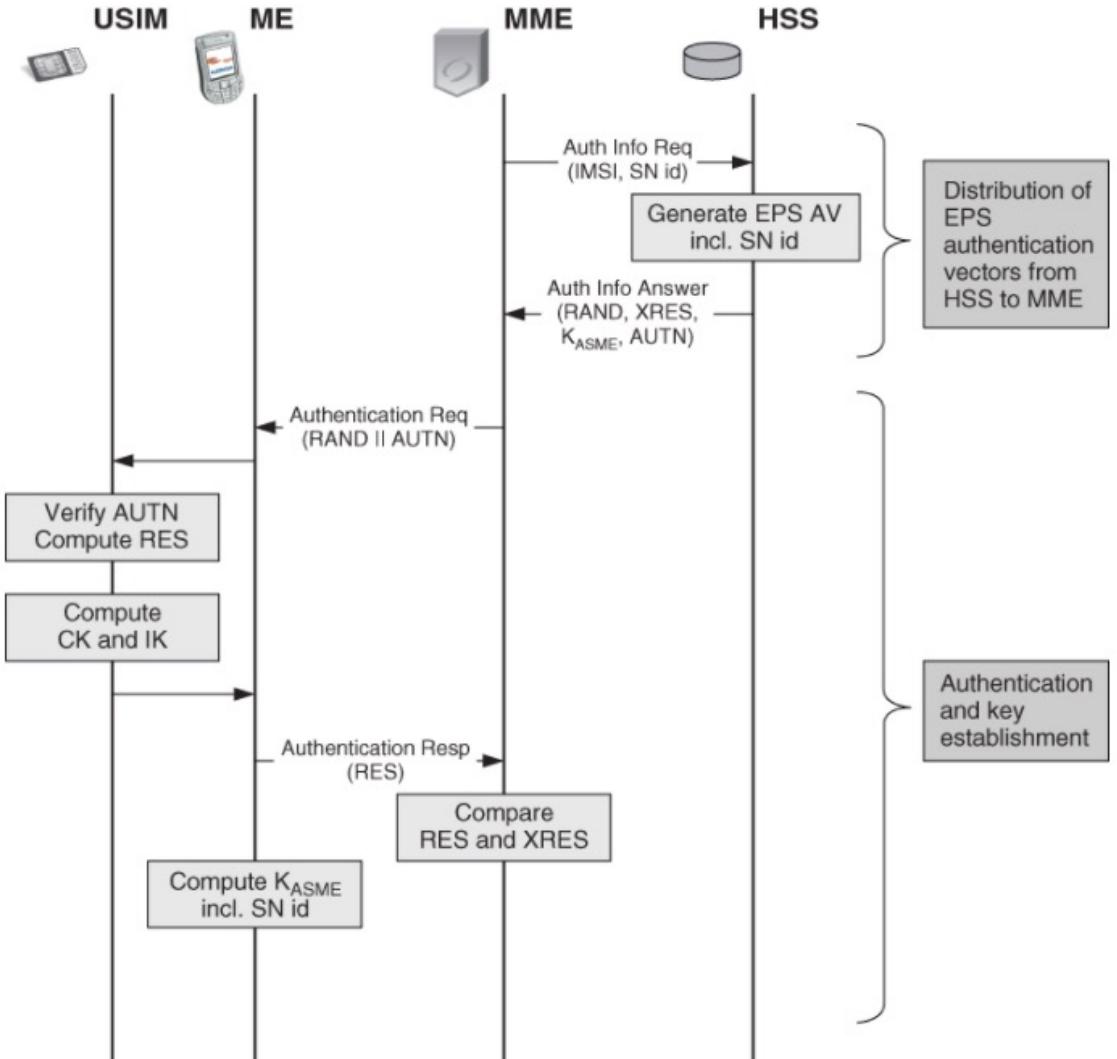


[Source: D.Forsberg et al. – LTE Security, Wiley 2012]

EPS AKA – User side

- SQN verification has not been standardized (generation and verification takes place in the home network, so it can be operator specific)
- Requirements for SQN:
 - No SQN should be used twice: USIM should not accept 2 AUTN with the same SQN after AUTN was verified
 - Allow, in a given threshold, out of order SQN numbers
(might not accept a SQN if the jump from the last one is too big)
 - Reject too old time-based SQN
- Verification is performed in the USIM

EPS AKA – User side



- If USIM supports GSM, then it converts (CK, IK) to a GSM key K_c and sends it to the ME

Handover and Roaming

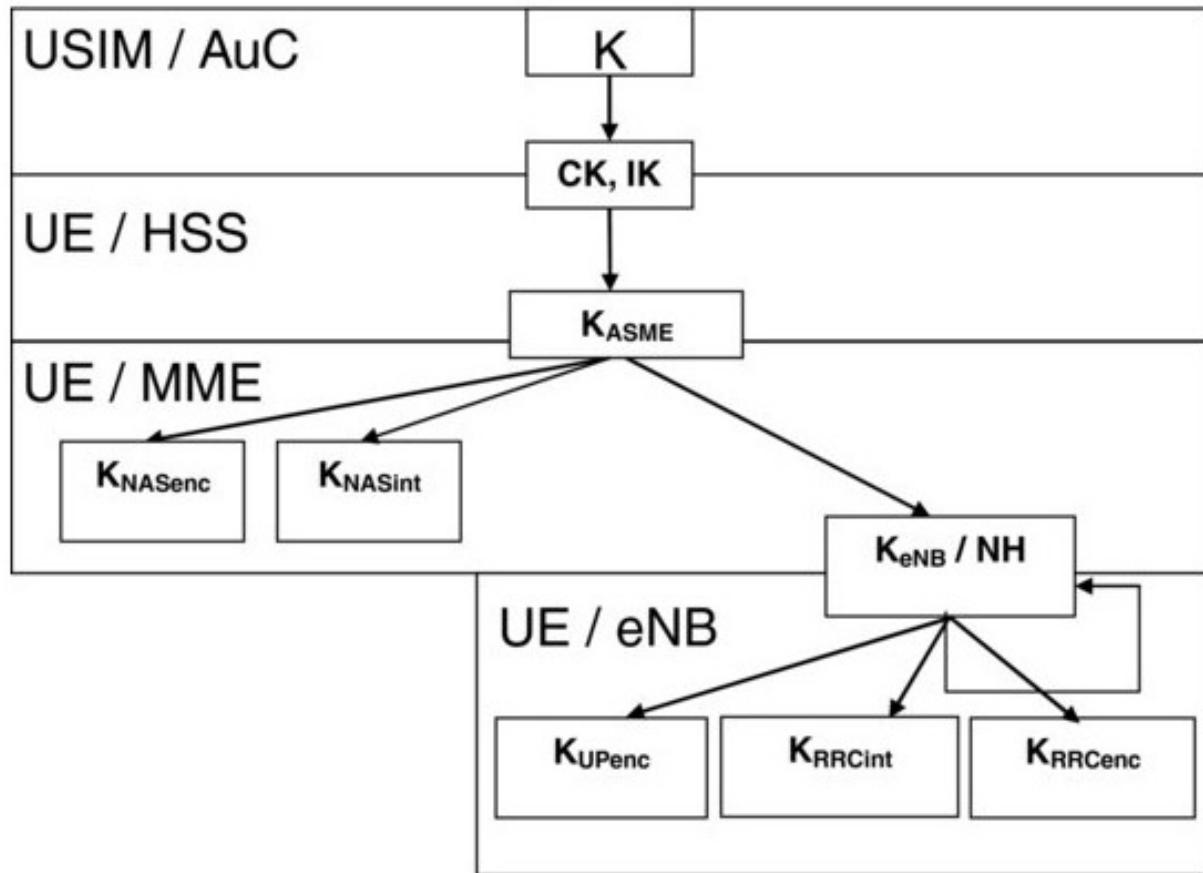
- When the UE changes MME, it identifies itself by GUTI in the Attach Request and Tracking Area Update Request
- The MME is unaware of the GUTI, so it has 2 possibilities:
 - *Request the IMSI* – breaks confidentiality!
 - *Ask the old MME to translate the GUTI to IMSI*
- Data exchanged between the old and the new MME in 2 scenarios:
 - *Old and new MME are in the same network* ([Handover](#))
 - Transfer the EPS security context*
 - The old MME transfers the remaining AVs (if any)
 - *Old and new MME are in networks of different operators* ([Roaming](#))
 - The current security context* is allowed, depending on the security of the networks (EPS to EPS only)
 - The old MME does not transfer the remaining AVs (if any), because they are not good in the new network

Security Context

- A **security context** is a set of parameters agreed by 2 parties when they engage in a secured communication
- Contains: algorithm identifiers, cryptographic keys, etc.

Key hierarchy (remember!)

Key	Length	Info
K	128 bits	Key shared between the subscriber and the network operator, stored in the USIM and AuC; permanent key of the subscriber
CK, IK	128 bits	Ciphering key CK and integrity key IK are for UMTS interconnection
K_{ASME}	256 bits	A local master key of the subscriber from which all other keys will be derived; Shared between the UE and the MME
K_{NASenc} , K_{NASint}	128 / 256 bits	Ciphering key K_{NASenc} and integrity key K_{NASint} for NAS protection
K_{eNB} / NH	256 bits	Intermediate key stored in the eNodeB NH (Next Hop) is used in handover
K_{RRCenc} , K_{RRCint}	128 / 256 bits	Ciphering key K_{RRCenc} and integrity key K_{RRCint} for AS protection
K_{UPenc}	128 / 256 bits	Ciphering key K_{UPenc} for user data



[Source: D.Forsberg et al. – LTE Security, Wiley 2012]

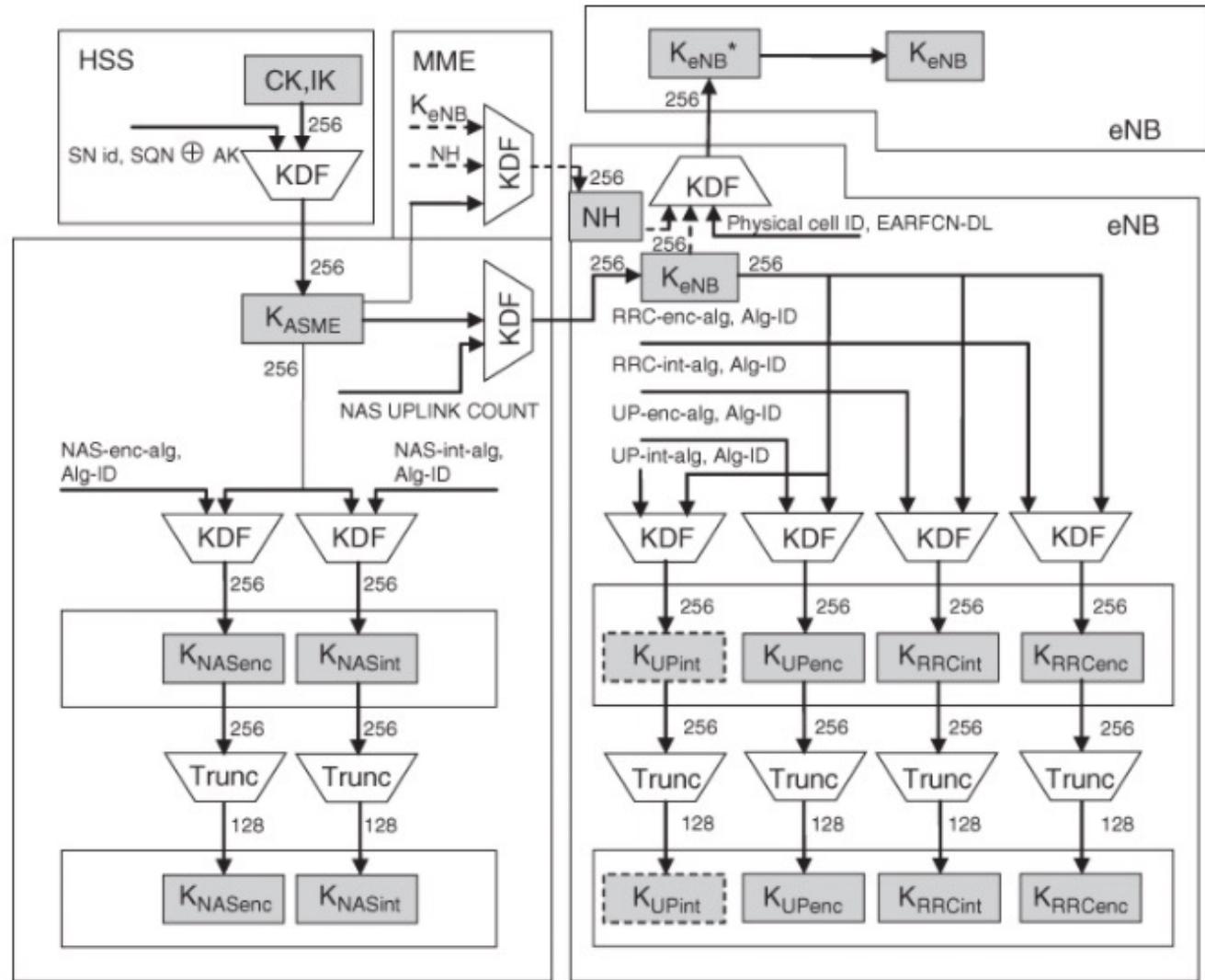
Key hierarchy

- K_{ASME} is derived in the ME (not the USIM!) and the HSS => its derivation must be standardized; others not necessarily
- KDF used to derive keys in the hierarchy must be **one-way; why?**
- KDF based on **HMAC-SHA-256**
- Encryption and integrity keys (K_{NASenc} , K_{NASint} , K_{RRCint} , K_{RRCenc} , K_{UPenc}) are on 256 bits and truncated to 128 last significant bits (EPS accepts both 256 and 128 bits keys)
- Keys are derived in hierarchical manner, with additional parameters as input (e.g.: SN id, SQN xor AK, etc.) – the params are all **assumed to be known by a potential attacker** because they are sent in clear or easy computable from unencrypted communication

Key hierarchy

- A principle that brings **advantages**:
 - **Cryptographic key separation**:
 - Each key is used to one context only (e.g.: encryption of signalling traffic)
 - Prevents **expanding of leakage**: leakage of keys in one context do not help finding the key in another context
 - **Related key attacks**: the attacker can ask the exchange of the key in a way that he predetermines the relation between the old and new keys
 - **Key freshness**:
 - Keys can be renewed without affecting other keys (e.g.: renew of K_{eNB} does not require renewal of the K_{ASME} , X2 handover)
 - Renewal of keys takes place more often
 - ... and **disadvantages**: added complexity

Key hierarchy



Question: Can K_{NASenc}, K_{NASint} be refreshed without refreshing the K_{ASME} ? How?

Just by changing the other param, NAS-enc/int-alg Alg_ID

Cryptography

- **Algorithm agility / flexibility:** the cryptographic **algorithms should be replaced** without much difficulty
 - Allows removal of out-dated algorithms
 - The number of algorithms should be keep small (for synchronization and management reasons), but more than 1...
 - ... because if one algorithms fails (is broken), others will be used
- **Algorithms diversity:** **the design** of the algorithms **should differ** from each other as much as possible
 - *Why? Where did you encounter this principle before (in crypto)?*
- Emergency scenarios

Emergency

- Null algorithm: provides no cryptographic protection
 - Must exist for emergency cases
 - **Problematic** from security perspective because it can be triggered in cases where protection should be enabled
- Turn-off principle: the **cryptographic protection should be by default on**, and only by request (on special scenarios) should be turned off
- EEA0 (EPS Encryption Algorithm): the identity function (i.e. ciphertext equals the cleartext)
- EIA0 (EPS Integrity Algorithm) : a **32-bit string of 0's** is appended to the message
 - Reason: **keep the protected and non-protected scenarios as similar as possible** (e.g.: same length)

Confidentiality

- Same structure for NAS and AS protection
- Out-of-the shelf algorithms (easier than to invite submission and go through a selection process) ...
- ... keeping in mind **reusability** from 3G (compatibility reasons)
- **128-EEA1: SNOW 3G** adapted to the EPS security architecture
 - 128 bits keys
- **128-EEA2: AES**
 - 128 bits keys
 - Counter mode

Integrity

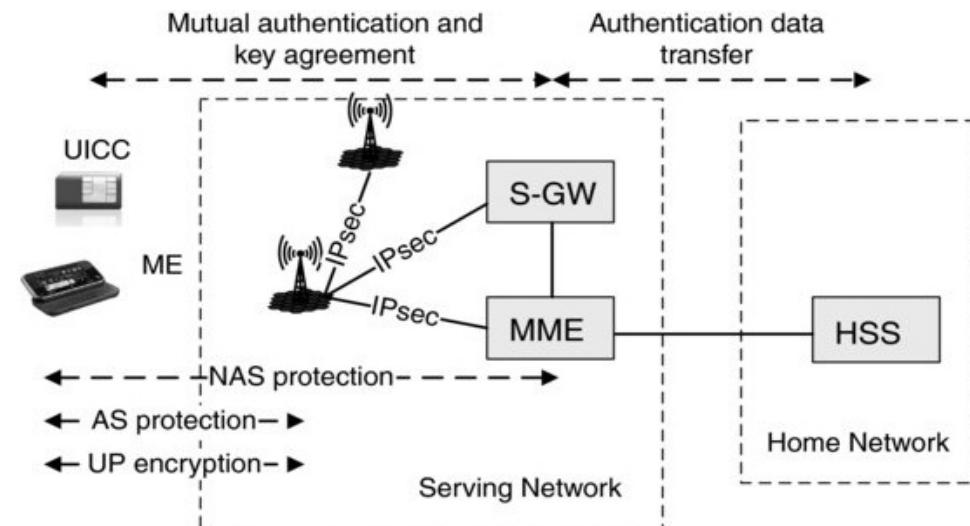
- Same principles as for confidentiality
- Usage of the same main cryptographic blocks (re-usability)
- **128-EIA1: UIA 2 (SNOW 3G)** adapted to the EPS security architecture
 - 128 bits keys
- **128-EIA2: Cipher- based MAC (AES)**
 - 128 bits keys
- The key length in the naming implies that other key lengths (e.g.:192, 256) can be used in case of improved security

Key derivation

- **One-way**: an adversary cannot use one key to derive a key located upper in the hierarchy
- **Independence**: 2 keys derived from the same key should be independent
- **SHA-256** used in the **HMAC** mode

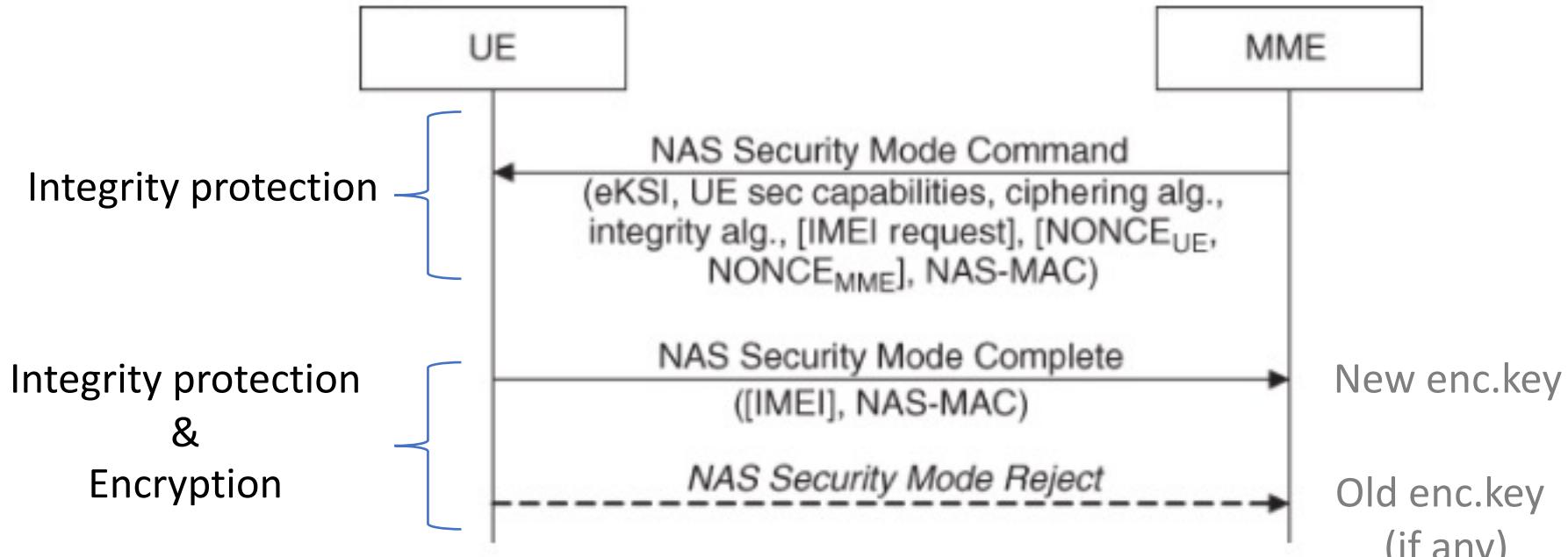
Algorithm negotiation

- Algorithms are **negotiated separately** for AS (between UE and eNodeB) and NAS (between UE and MME)
- Negotiation is based on the UE capabilities and a list of allowed cryptographic algorithms in the eNodeB, respectively MME in priority order
- eNodeB and MME are responsible for selecting the AS level, respectively the NAS level algorithms, after UE sends its capabilities in the attachment procedure
- Selection is indicated in **AS Security Mode Command**, respectively **NAS Security Mode Commands**



[Source: D.Forsberg et al. – LTE Security, Wiley 2012]

NAS signalling protection



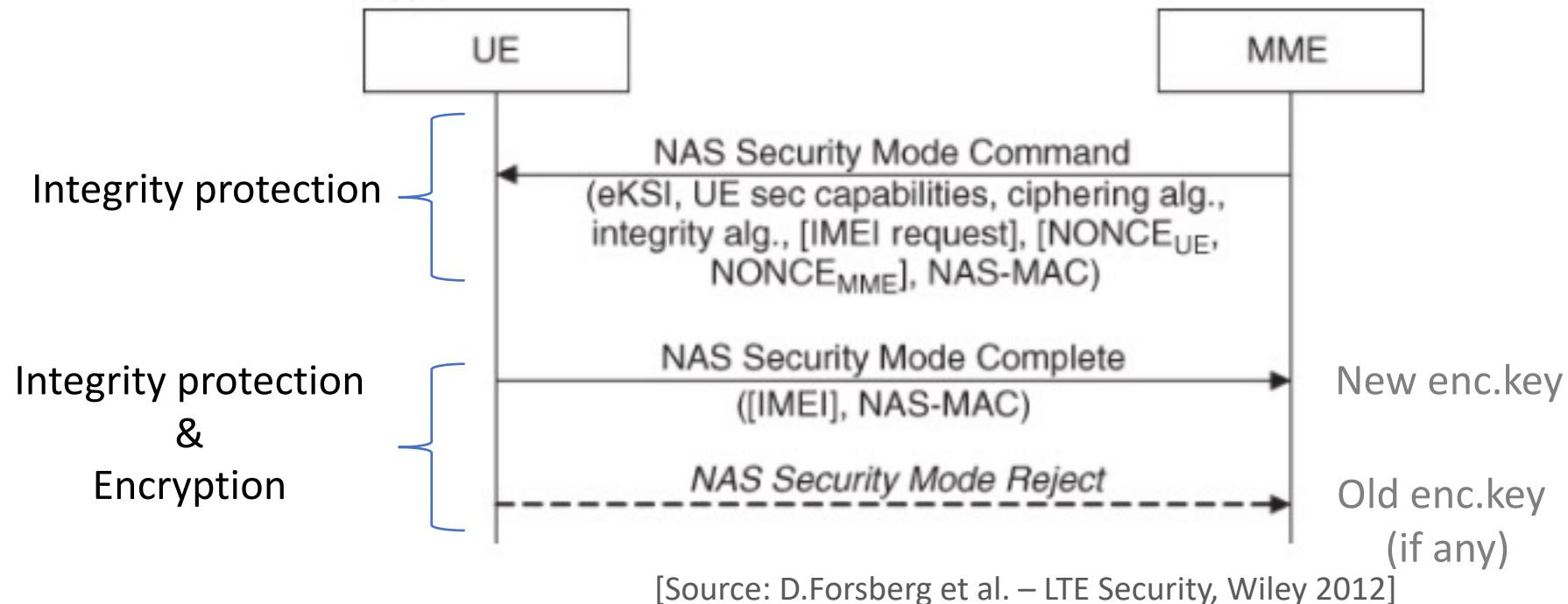
eKSI: key set identifier that identifies the key K_{ASME}

NONCE_{UE} , $\text{NONCE}_{\text{MME}}$: used for mobility

Question: Why is the NAS Security Mode Command not encrypted?

The UE does not know what algorithm and key to use for decryption

NAS signalling protection



eKSI: key set identifier that identifies the key K_{ASME}

NONCE_{UE} , $\text{NONCE}_{\text{MME}}$: used for mobility

Question: Why is the NAS Security Mode Complete encrypted?

To not expose IMEI

NAS signalling protection

- **Integrity and replay protection** are part of the NAS protocol itself
- **Integrity** algorithm's **input** params:
 - K_{NASint} , 128 bits key
 - COUNT, 32 bits
 - DIRECTION, 1 bit indicating upstream or downstream signalling
 - BEARER, constant value – used for similarity with AS

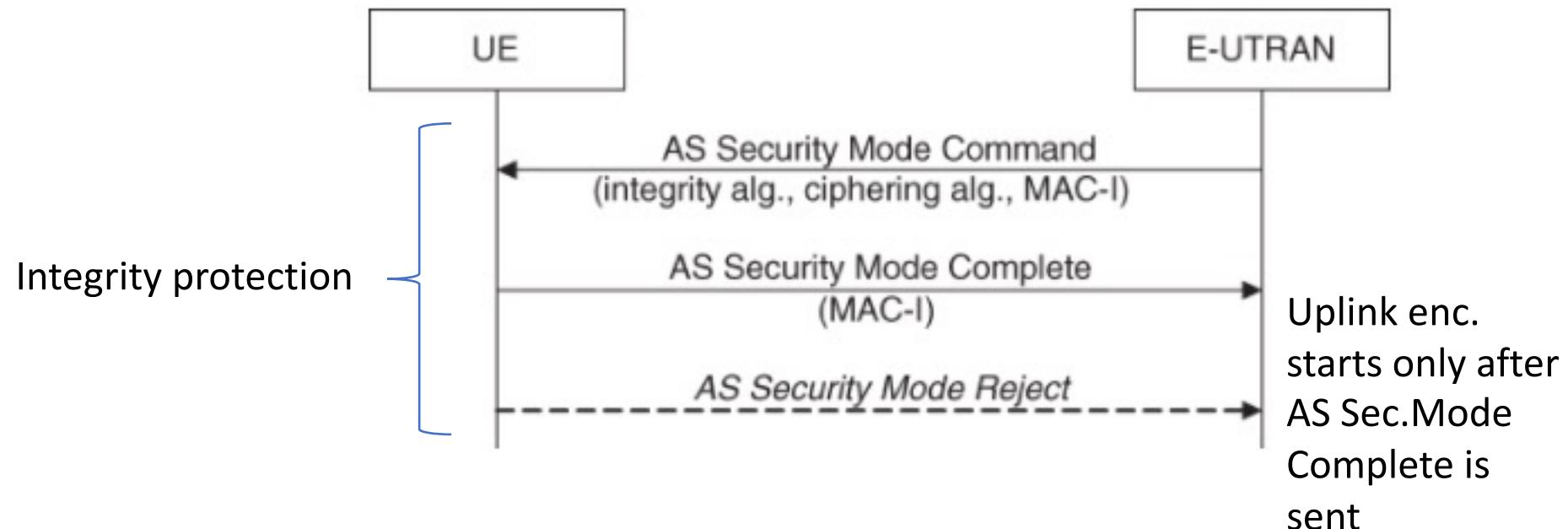
COUNT = 0x00 || NAS OVERFLOW || NAS SQN

- NAS OVERFLOW, 16 bits – incremented every time NAS SQN overflows
- **Integrity** algorithm's **output**:
 - NAS-MAC, 32 bits
- For efficiency reasons, NAS Service Request message uses 16 bits NAS-MAC (e.g.: when UE responds to paging from the MME)

NAS signalling protection

- **General rule:** messages that are not integrity protected are discarded in the UE and MME once the NAS protection has been activated
- **Exceptions:** emergency calls, etc.
- **Ciphering:** same inputs, except K_{NASenc} instead of K_{NASint} and an additional parameter LENGTH that specifies the length of the keystream to be generated

AS signalling protection



Question: Why is the AS Security Mode Complete not encrypted?

No need, it contains no private information

AS signalling and User data protection

- Radio Resource Control (RRC): the AS level signalling protocol
- The security is implemented in the PDCP (Packet Data Convergence Protocol) layer, which carries both RRC and user data
- Integrity algorithm's **input** params:
 - K_{RRCint} , 128 bits key
 - COUNT, 32 bits, for each radio bearer (PDCP seg.no).
 - DIRECTION, 1 bit, indicating upstream or downstream
 - BEARER, 5 bits indicating the radio bearer identity, mapped from RRC bearer identity:

Same inputs as for NAS, but a different key and BEARER not constant

Signalling Radio Bearers (SRB):	SRB0 RRC control messages not protected	SRB1 RRC control messages protected after sec. activation	SRB2 NAS messages Always protected
Data Radio Bearers (DRB)	multiple ciphered, but not integrity-protected		

- Integrity algorithm's **output**:
 - MAC-I, 32 bits

AS signalling and User data protection

- **Ciphering:** same inputs, except $K_{RRC_{enc}}$ instead of $K_{RRC_{int}}$ and an additional parameter LENGTH that specifies the length of the keystream to be generated

NAS vs AS Security Mode Commands (SMC)

AS (Access Stratum)

- Signalling protection **and user data protection**
- Security is implemented in the **PDCP protocol**
- It is **not possible** to change algorithms using AS Security Mode Command
- Encryption starts **after** the AS Security Mode Complete
- **Several bearers** (there are several AS level connections between UE and eNodeB)

NAS (Non-Access Stratum)

- Signalling protection
- Security is implemented in the **NAS protocol itself**
- It is **possible** to change algorithms using NAS Security Mode Command
- Encryption starts **with** the NAS Security Mode Complete
- **One bearer of constant value** (there is only one NAS level connection between UE and MME)

To remember!

1. The principles of EPS AKA
2. The advantages of key hierarchy
3. Principles to select and use cryptographic algorithms
4. Implementation in LTE



Network Security

- Lecture 12 -

5G

Adela Georgescu

Faculty of Mathematics and Computer Science
University of Bucharest

*slides belonging to Ruxandra Olimid

Outline

- Arhitecture
- EPS AKA
- Key hierarchy
- Cryptographical aspects
- New concepts

5G Security

Figure 1: Standardisation organisations of relevance for 5G security



[ENISA – Security in 5G Specifications – Controls in 3GPP

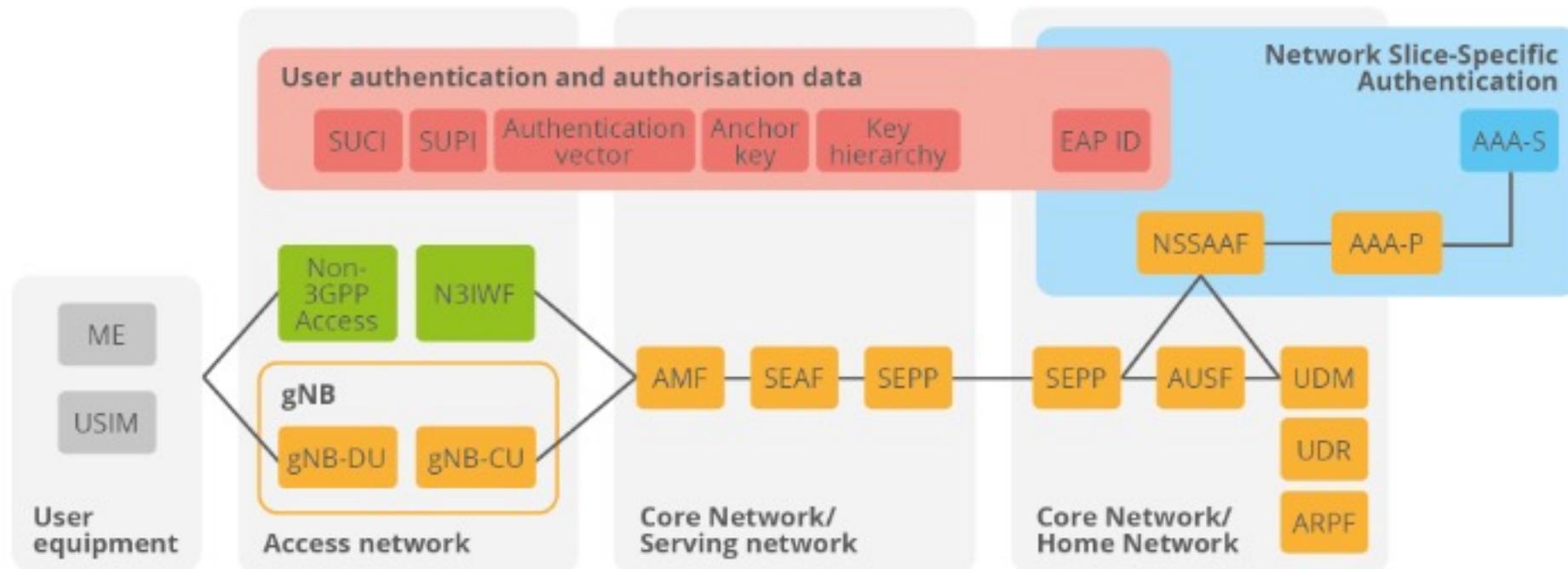
Available at: <https://www.enisa.europa.eu/publications/security-in-5g-specifications>]

3GPP Security Standards

TS 33.501	Security architecture and procedures for 5G System
TS 33.511	Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class
TS 33.512	5G Security Assurance Specification (SCAS); Access and Mobility management Function (AMF)
TS 33.513	5G Security Assurance Specification (SCAS); User Plane Function (UPF)
TS 33.514	5G Security Assurance Specification (SCAS) for the Unified Data Management (UDM) network product class
TS 33.515	5G Security Assurance Specification (SCAS) for the Session Management Function (SMF) network product class
TS 33.516	5G Security Assurance Specification (SCAS) for the Authentication Server Function (AUSF) network product class
TS 33.517	5G Security Assurance Specification (SCAS) for the Security Edge Protection Proxy (SEPP) network product class
TS 33.518	5G Security Assurance Specification (SCAS) for the Network Repository Function (NRF) network product class
TS 33.519	5G Security Assurance Specification (SCAS) for the Network Exposure Function (NEF) network product class
TS 33.520	5G Security Assurance Specification (SCAS); Non-3GPP InterWorking Function (N3IWF)
TS 33.521	5G Security Assurance Specification (SCAS); Network Data Analytics Function (NWDAF)
TS 33.522	5G Security Assurance Specification (SCAS); Service Communication Proxy (SECOP)
TS 33.535	Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in the 5G System (5GS)

Security Architecture

Figure 8: Security architecture zoom-in from the ENISA 5G Threat Landscape 2020



[ENISA – Security in 5G Specifications – Controls in 3GPP

Available at: <https://www.enisa.europa.eu/publications/security-in-5g-specifications>]

UE Privacy

SUCI: Subscription Concealed Identifier

SUPI: Subscription Permanent Identifier

GUTI: Globally Unique Temporary UE Identity

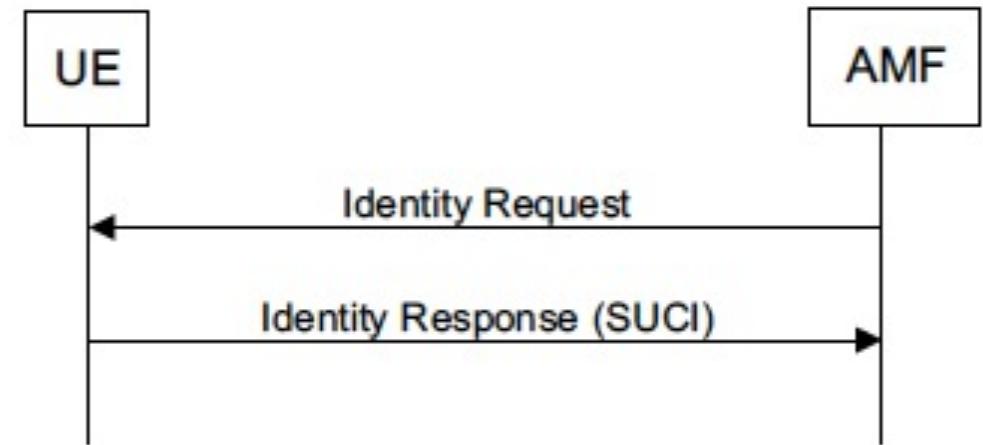
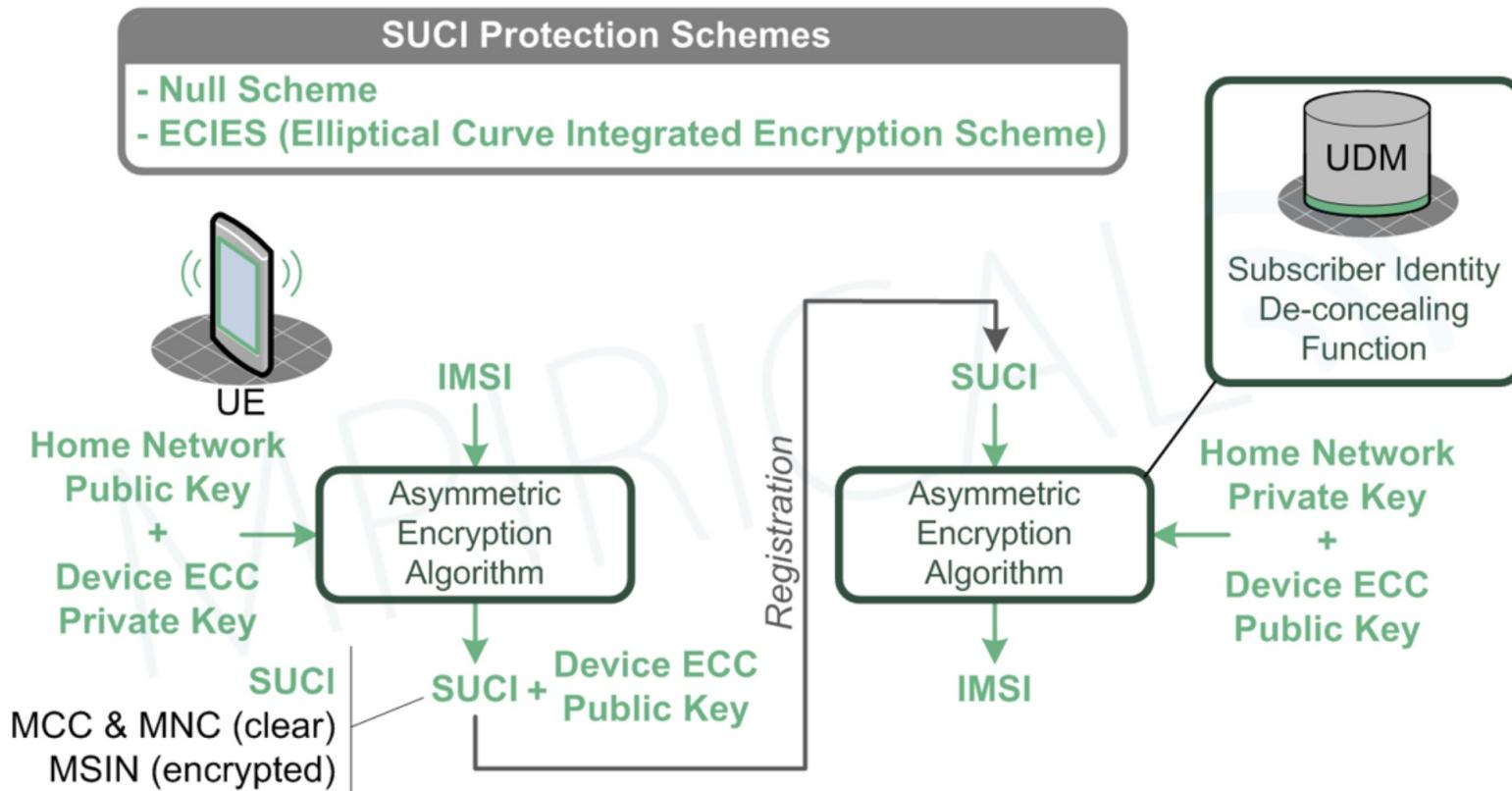


Figure 6.12.4-1: Subscription identifier query

[Source: 3GPP TS 33.501 V17.1.0 (2021-03)]

Protection of SUPI by encryption



[Source: <https://www.mpirical.com/blog/5g-anonymity-and-the-suci>]

Protection of SUPI – SUCI – encryption

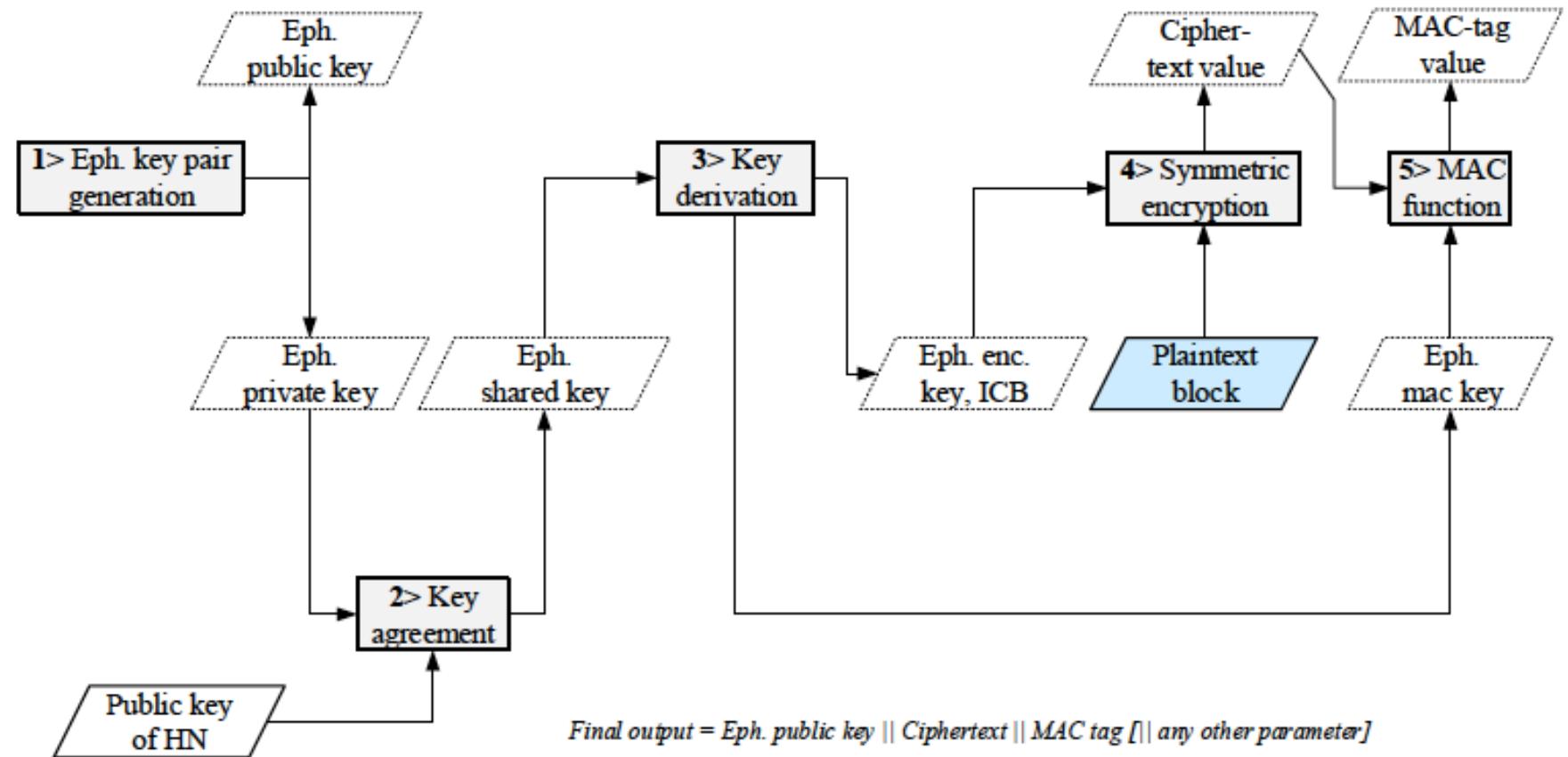


Figure C.3.2-1: Encryption based on ECIES at UE

[Source: 3GPP TS 33.501 V17.1.0 (2021-03)]

Protection of SUPI – SUCI - decryption

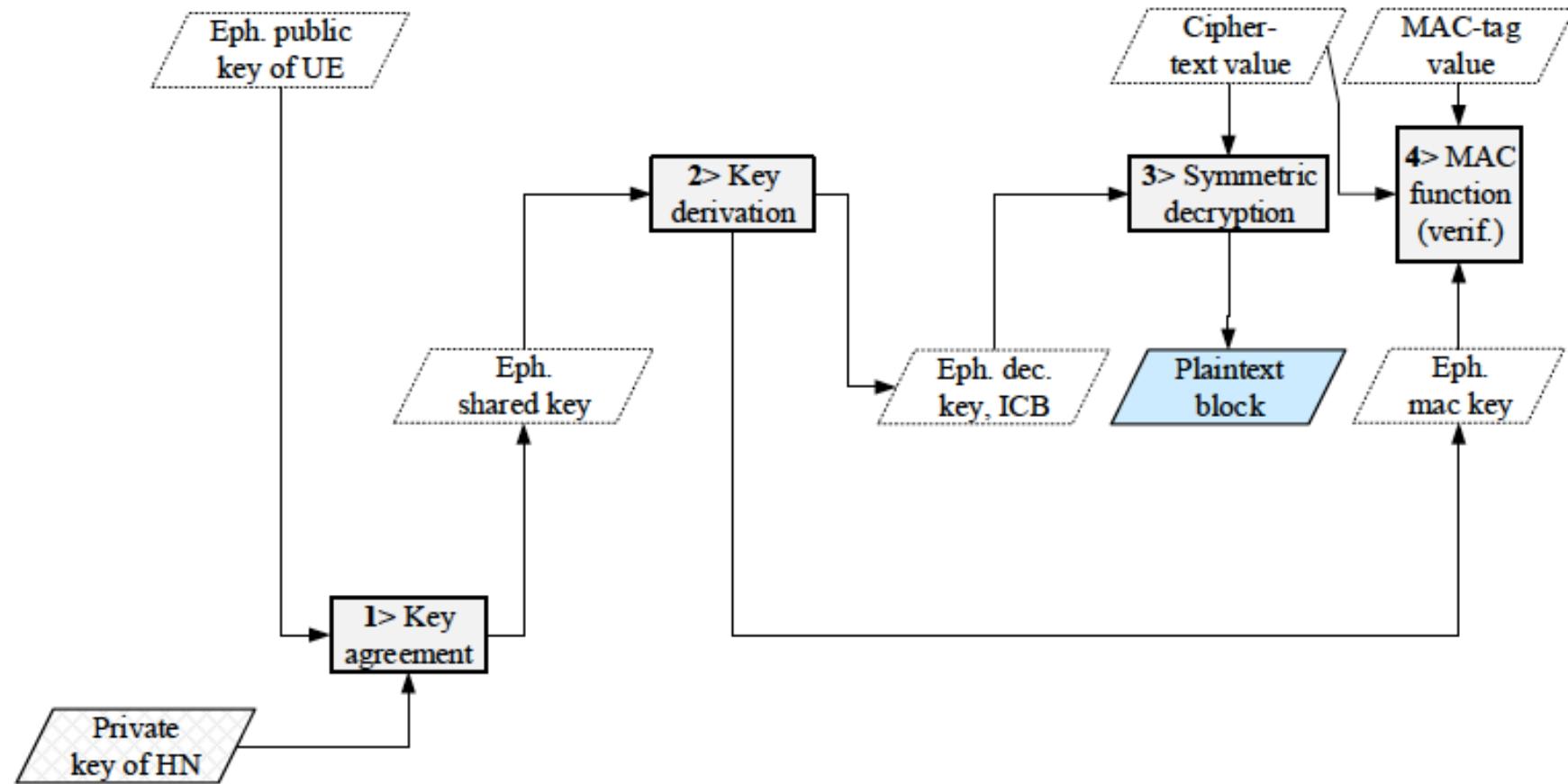
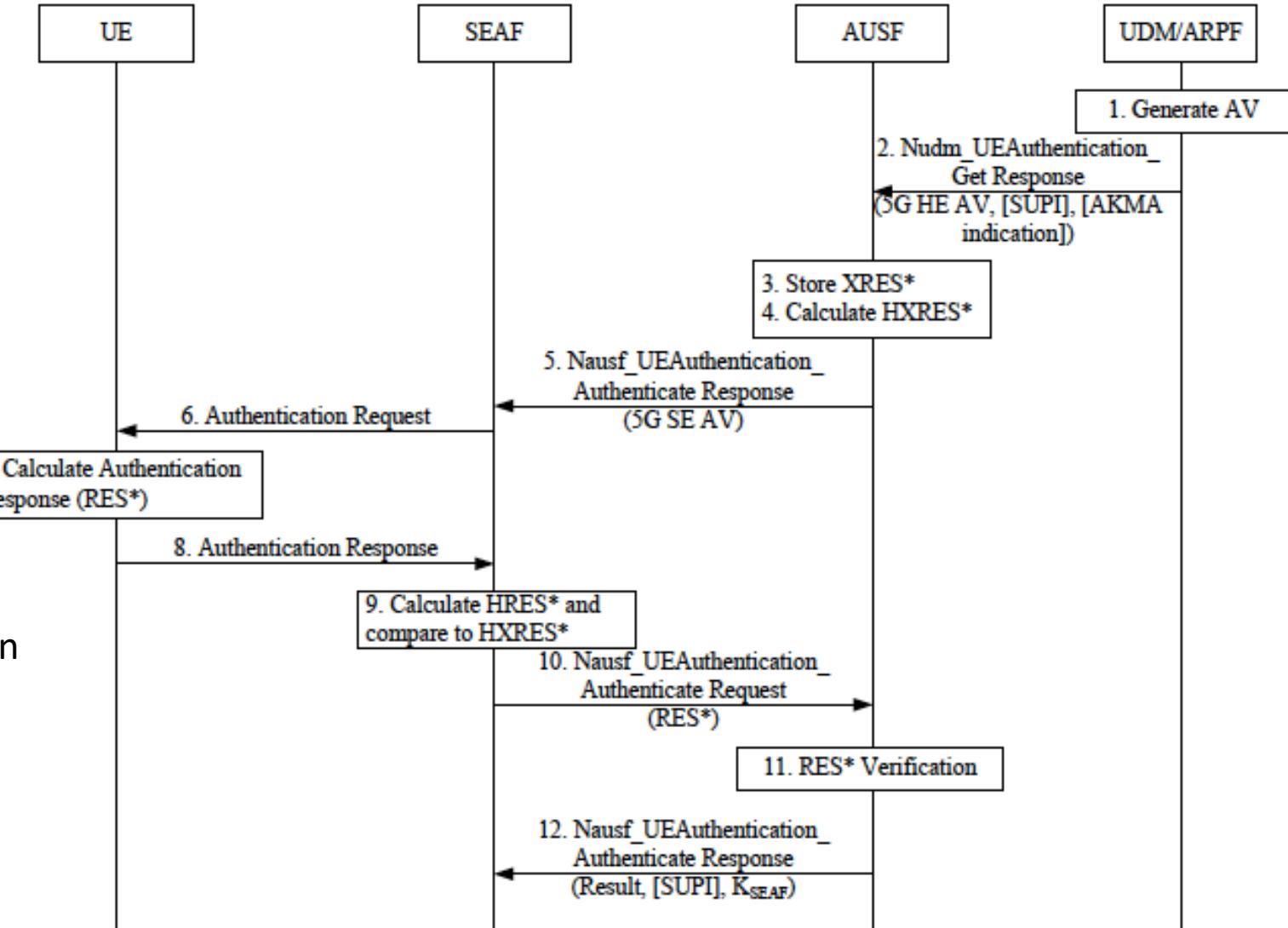


Figure C.3.3-1: Decryption based on ECIES at home network

[Source: 3GPP TS 33.501 V17.1.0 (2021-03)]

5G-AKA

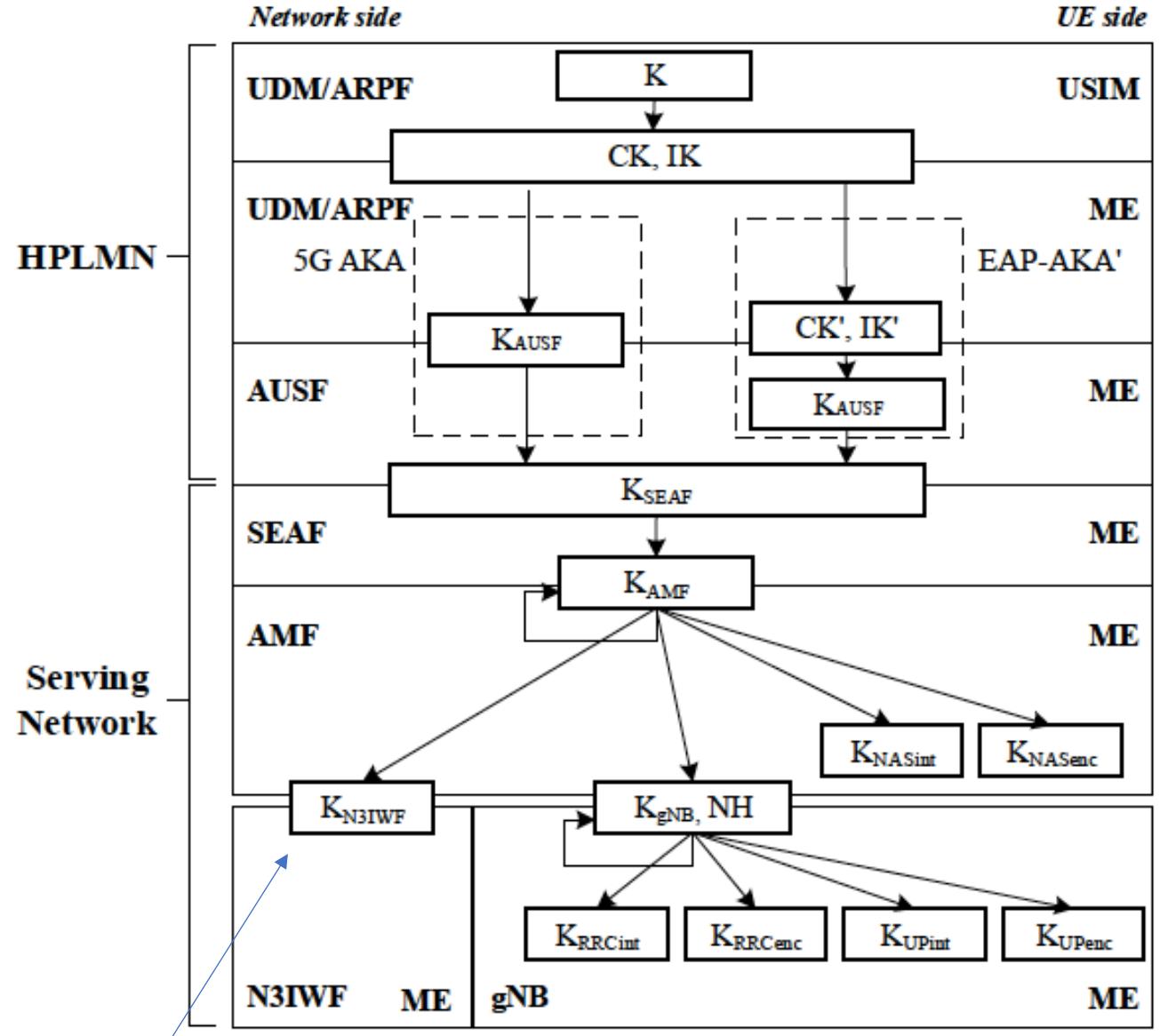


AUSF: AUthentication Server Function
ARPF: Authentication credential
Repository and Processing Function
SIDF: Subscription Identifier De-concealing Function
SEAF: SEcurity Anchor Function

Figure 6.1.3.2-1: Authentication procedure for 5G AKA

Key Hierarchy

AUSF: AUthentication Server Function
 ARPF: Authentication credential
 Repository and Processing Function
 SEAF: SEcurity Anchor Function
 AMF Access and Mobility Management Function



[Source: 3GPP TS 33.501 V17.1.0 (2021-03)]

Non-3GPP

Figure 6.2.1-1: Key hierarchy generation in 5GS

Cryptographical Aspects

5.2.2 User data and signalling data confidentiality

The UE shall support ciphering of user data between the UE and the gNB.

The UE shall activate ciphering of user data based on the indication sent by the gNB.

The UE shall support ciphering of RRC and NAS-signalling.

The UE shall implement the following ciphering algorithms:

NEA0, 128-NEA1, 128-NEA2 as defined in Annex D of the present document.

The UE may implement the following ciphering algorithm:

128-NEA3 as defined in Annex D of the present document.

The UE shall implement the ciphering algorithms as specified in TS 33.401 [10] if it supports E-UTRA connected to 5GC.

Confidentiality protection of the user data between the UE and the gNB is optional to use.

Confidentiality protection of the RRC-signalling, and NAS-signalling is optional to use.

Confidentiality protection should be used whenever regulations permit.

"0000 ₂ "	NEA0	Null ciphering algorithm;
"0001 ₂ "	128-NEA1	128-bit SNOW 3G based algorithm;
"0010 ₂ "	128-NEA2	128-bit AES based algorithm; and
"0011 ₂ "	128-NEA3	128-bit ZUC based algorithm.

Cryptographical Aspects

5.2.3 User data and signalling data integrity

"0000 ₂ "	NIA0	Null Integrity Protection algorithm;
"0001 ₂ "	128-NIA1	128-bit SNOW 3G based algorithm;
"0010 ₂ "	128-NIA2	128-bit AES based algorithm; and
"0011 ₂ "	128-NIA3	128-bit ZUC based algorithm.

The UE shall support integrity protection and replay protection of user data between the UE and the gNB. The UE shall support integrity protection of user data at any data rate, up to and including, the highest data rate supported by the UE.

The UE shall activate integrity protection of user data based on the indication sent by the gNB.

The UE shall support integrity protection and replay protection of RRC and NAS-signalling.

The UE shall implement the following integrity protection algorithms:

NIA0, 128-NIA1, 128-NIA2 as defined in Annex D of the present document.

The UE may implement the following integrity protection algorithm:

128-NIA3 as defined in Annex D of the present document.

The UE shall implement the integrity algorithms as specified in TS 33.401 [10] if it supports E-UTRA connected to 5GC.

Integrity protection of the user data between the UE and the gNB is optional to use.

NOTE: Integrity protection of user plane adds the overhead of the packet size and increases the processing load both in the UE and the gNB.

Integrity protection of the RRC-signalling, and NAS-signalling is mandatory to use, except in the following cases:

All NAS signalling messages except those explicitly listed in TS 24.501 [35] as exceptions shall be integrity-protected.

All RRC signalling messages except those explicitly listed in TS 38.331 [22] as exceptions shall be integrity-protected with an integrity protection algorithm different from NIA0, except for unauthenticated emergency calls.

The UE shall implement NIA0 for integrity protection of NAS and RRC signalling. NIA0 is only allowed for unauthenticated emergency session as specified in clause 10.2.2.

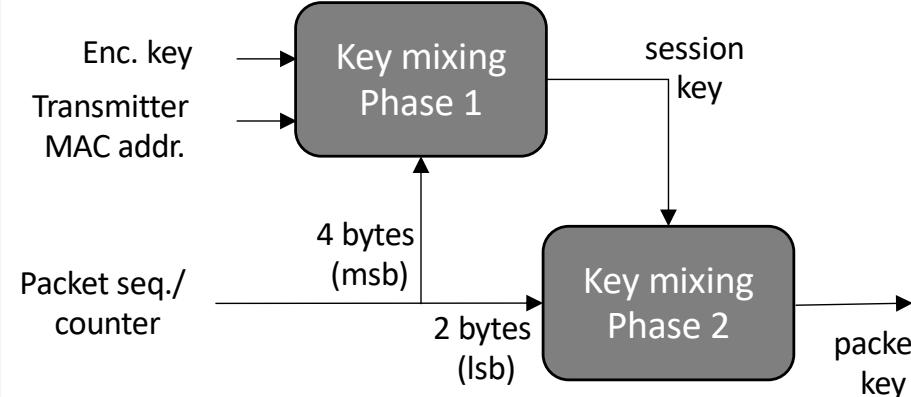
Wi-Fi Protected Access (WPA) -

Sizes

Packet seq.: 48 bits

MIC: 64 bits

Key Mixing



Integrity: MIC instead of CRC



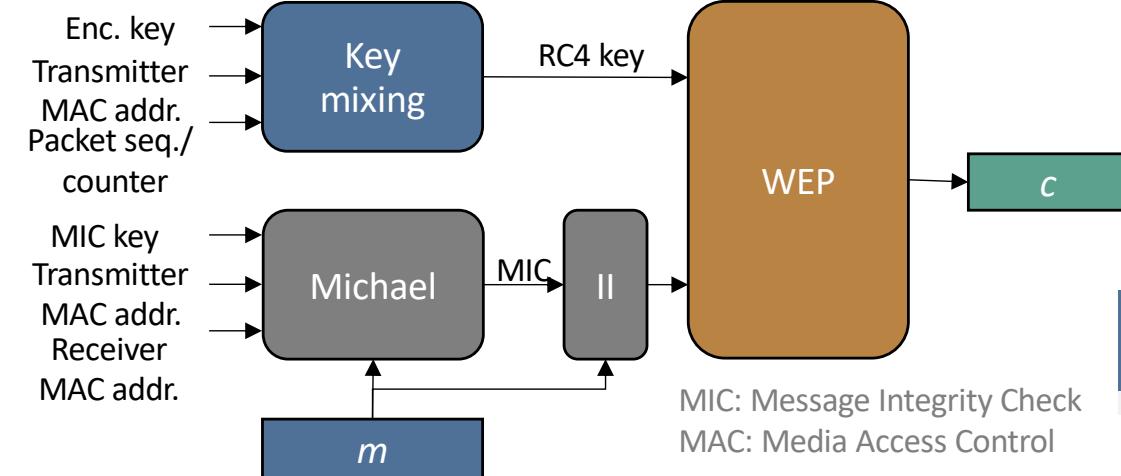
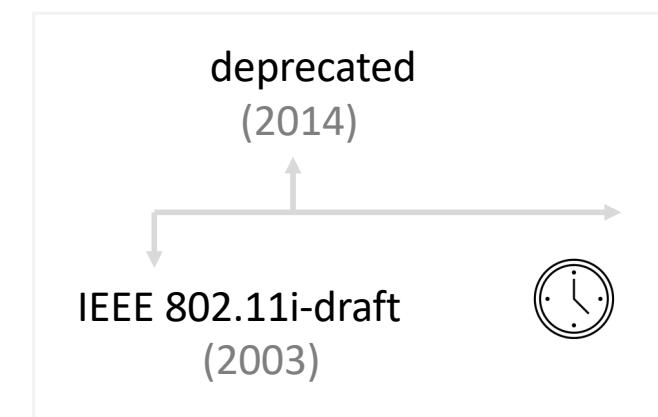
Lengths: larger (e.g., Packet seq. vs. IV)



Key management: key per package (packet no. to avoid replay attacks)



Attacks



MIC: Message Integrity Check

MAC: Media Access Control

KCK: Key Confirmation Key

KEK: Key Encryption Key

TK: Temporal Keys

13

Temporal Key Integrity Protocol (TKIP)

Pairwise Master Key - PMK (256 bits)

Pairwise Transient Key PTK (512 bits)

EAPOLMICKey
(128 bits)
(KCK)

EAPOLEncKey
(128 bits)
(KEK)

DataEncKey
(128 bits)
(TK)

DataMICKey
(128 bits)
(TK)

TKIP Pairwise Key Hierarchy

$$PTK = f(PMK, \text{Nonce}_{AP}, \text{Nonce}_{STA}, MAC_{AP}, MAC_{STA})$$

Group Master Key - GMK (128 bits)

Group Transient Key GTK (256 bits)

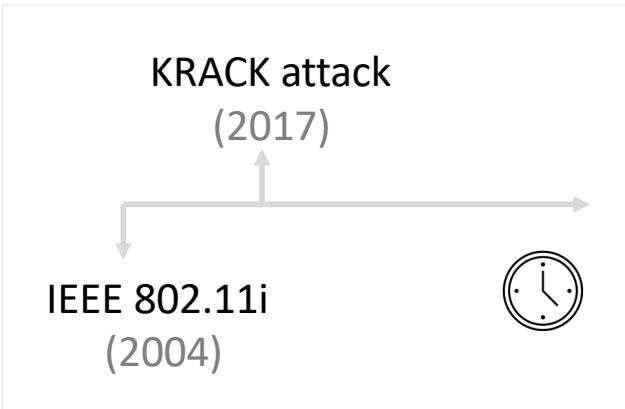
DataEncKey
(128 bits)

DataMICKey
(128 bits)

TKIP Group Key Hierarchy

$$GTK = f(GMK, \text{Nonce}_{AP}, MAC_{AP})$$

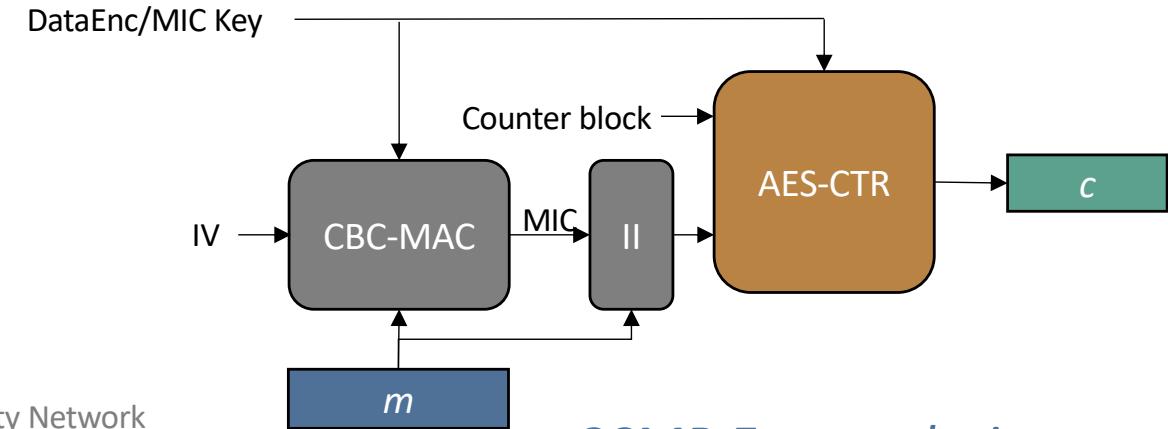
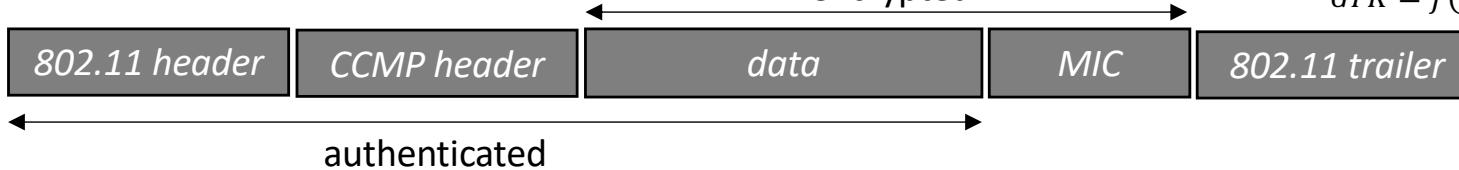
Wi-Fi Protected Access 2 (WPA2) -



RSN	TKIP	RSN: Robust Security Network MIC: Message Integrity Check MAC: Media Access Control CCMP: CTR mode with CBC-MAC Protocol
	AES	

+ Integrity: CBC-MAC (AES)	Counter block (CB) (128 bits) 01011001 <table border="1"><tr><td>Flag</td><td>Priority</td><td>Source Address</td><td>Packet No.</td><td>Counter</td></tr><tr><td>(8 bits)</td><td>(8 bits)</td><td>(48 bits)</td><td>(48 bits)</td><td>(16 bits) 1+</td></tr></table>	Flag	Priority	Source Address	Packet No.	Counter	(8 bits)	(8 bits)	(48 bits)	(48 bits)	(16 bits) 1+
Flag	Priority	Source Address	Packet No.	Counter							
(8 bits)	(8 bits)	(48 bits)	(48 bits)	(16 bits) 1+							
+ Confidentiality: AES-CTR	Initialization Vector (IV) (128 bits) 01011001 <table border="1"><tr><td>Flag</td><td>Priority</td><td>Source Address</td><td>Packet No.</td><td>Data Length</td></tr><tr><td>(8 bits)</td><td>(8 bits)</td><td>(48 bits)</td><td>(48 bits)</td><td>(16 bits)</td></tr></table>	Flag	Priority	Source Address	Packet No.	Data Length	(8 bits)	(8 bits)	(48 bits)	(48 bits)	(16 bits)
Flag	Priority	Source Address	Packet No.	Data Length							
(8 bits)	(8 bits)	(48 bits)	(48 bits)	(16 bits)							
- Attacks: KRACK, Kr00k, etc.	CCMP Header (64 bits) rrrrr1xy <table border="1"><tr><td>Packet No.0-1 (2x8 bits)</td><td>Reserved (8 bits)</td><td>KeyID (8 bits)</td><td>Packet No.2-5 (4x8 bits)</td></tr></table> r:reserved ; xy: KeyID (2 bits)	Packet No.0-1 (2x8 bits)	Reserved (8 bits)	KeyID (8 bits)	Packet No.2-5 (4x8 bits)						
Packet No.0-1 (2x8 bits)	Reserved (8 bits)	KeyID (8 bits)	Packet No.2-5 (4x8 bits)								
↻ Backwards compatibility: WEP, TKIP											

802.11 frame



17

CCMP Encapsulation Advanced Encryption Standard (AES)

Pairwise Master Key - PMK (256 bits)

Pairwise Transient Key PTK (384 bits)

EAPOLMICkey (128 bits)	EAPOLEncKey (128 bits)	DataEnc/MIC Key (128 bits)
------------------------	------------------------	----------------------------

AES Pairwise Key Hierarchy

$$PTK = f(PMK, \text{Nonce}_{AP}, \text{Nonce}_{STA}, MAC_{AP}, MAC_{STA})$$

Group Master Key - GMK (128 bits)

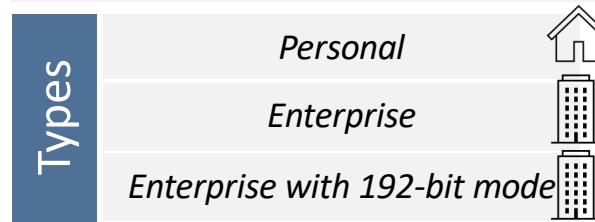
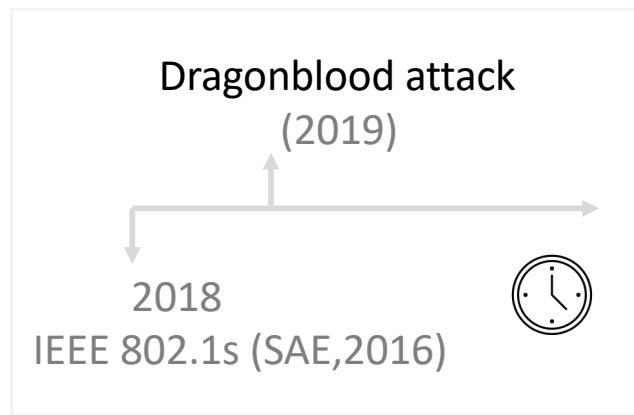
Group Transient Key GTK (128 bits)

DataEnc/MIC Key (128 bits)

AES Group Key Hierarchy

$$GTK = f(GMK, \text{Nonce}_{AP}, MAC_{AP})$$

Wi-Fi Protected Access 3 (WPA3) -



- + Better cryptography
- + Forward secrecy
- + Management frame protection
- + Open Wi-Fi Networks:
unauth. data encryption
- Attacks: downgrade (WPA2),
side-channels vs. DoS,
Dragonblood, etc.

SAE: Simultaneous Authentication of Equals
 DoS: Denial of Service
 PAKE: Password Authentication Key Exchange
 EC: Elliptic Curve
 KDF: Key Derivation Function

