



# Securitatea rețelelor

## - Prelegerea 0 -

### Informatii administrative

Ruxandra F. Olimid

Facultatea de Matematică și Informatică

Universitatea din București

# Cuprins

1. Cadre didactice
2. Ce aştept de la voi?
3. Organizare şi Evaluare
4. Structura cursului
5. Referinte bibliografice

# Cadre didactice



Ruxandra F. Olimid



[ruxandra.olimid@fmi.unibuc.ro](mailto:ruxandra.olimid@fmi.unibuc.ro)



[www.ruxandraolimid.weebly.com](http://www.ruxandraolimid.weebly.com)



# Cine sunteți voi?

QUESTIONS    RESPONSES

## SecRet - Cine sunteti voi?

Completați câteva informații despre voi.

Am facut cel putin un curs de criptografie.\*

Da

Nu

Other...

<https://goo.gl/forms/pEUosDgM7PzGkLYA2>

# Ce aştept de la voi?



Sunt prezent pentru că mă interesează!



Întreb pentru că vreau să ştiu!



Studiez individual sau în echipă



Promovez (cu o notă bună)

# Ce aşteptați voi de la mine?

<http://ruxandraolimid.weebly.com/feedback-from-students.html>

## Feedback from students

\* Indicates required field

### Feedback with respect to:

- Criptografie si securitate (2018-2019)
- Securitatea retelelor (2018-2019)
- Others

### Feedback\*

Trimite

# Organizare și Evaluare

## 1. Organizare

- 2h curs / săpt
- 2h laborator / 2 săpt

## 2. Evaluare

- 50 % examen (cu materiale)
- 15 % proiect laborator (**deadline!**)
- 20 % proiect curs (**deadline!**)
- 15 % laborator
- +10 % bonus curs
- +5% bonus proiect curs

## 3. Condiții de promovare

- $\geq 45\%$  din examen
- $\geq 45\%$  din total



Moodle: SECRET

# Structura cursului

## Principii & aspecte criptografice

- ✓ Notiuni generale de securitate ...
- ✓ Protocole, algoritmi criptografici ....
- ✓ ...

## Tehnologii & sisteme & securitate în practică

- ✓ Web security, Vulnerabilities & Attacks, Countermeasures, ...
- ✓ Firewalls, Intrusion Detection Systems (IDS), E-mail security, ... (?)

## Wireless ...

- ✓ WLAN: WEP, WPA, WPA2, 802.11i
- ✓ Mobile: GSM / (UMTS) / LTE / (5G?)
- ✓ ...

## ... Wired:

- ✓ SSL/TLS , SSH, IPSec, ... (?)

*Etică!*

# Schimbăm rolurile



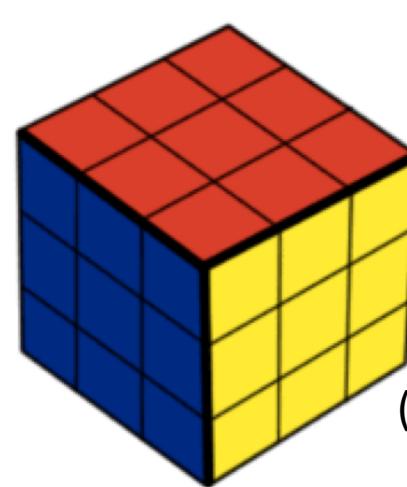
Reținem

- 10% din ce citim
- 20% din ce auzim
- 30% din ce vedem
- 50% din ce vedem și auzim
- 70% din ce discutam cu altii
- 80% din ce experimentam
- 95% din ce ii invatam pe altii

(William Glasser, psiholog)

Proberbe

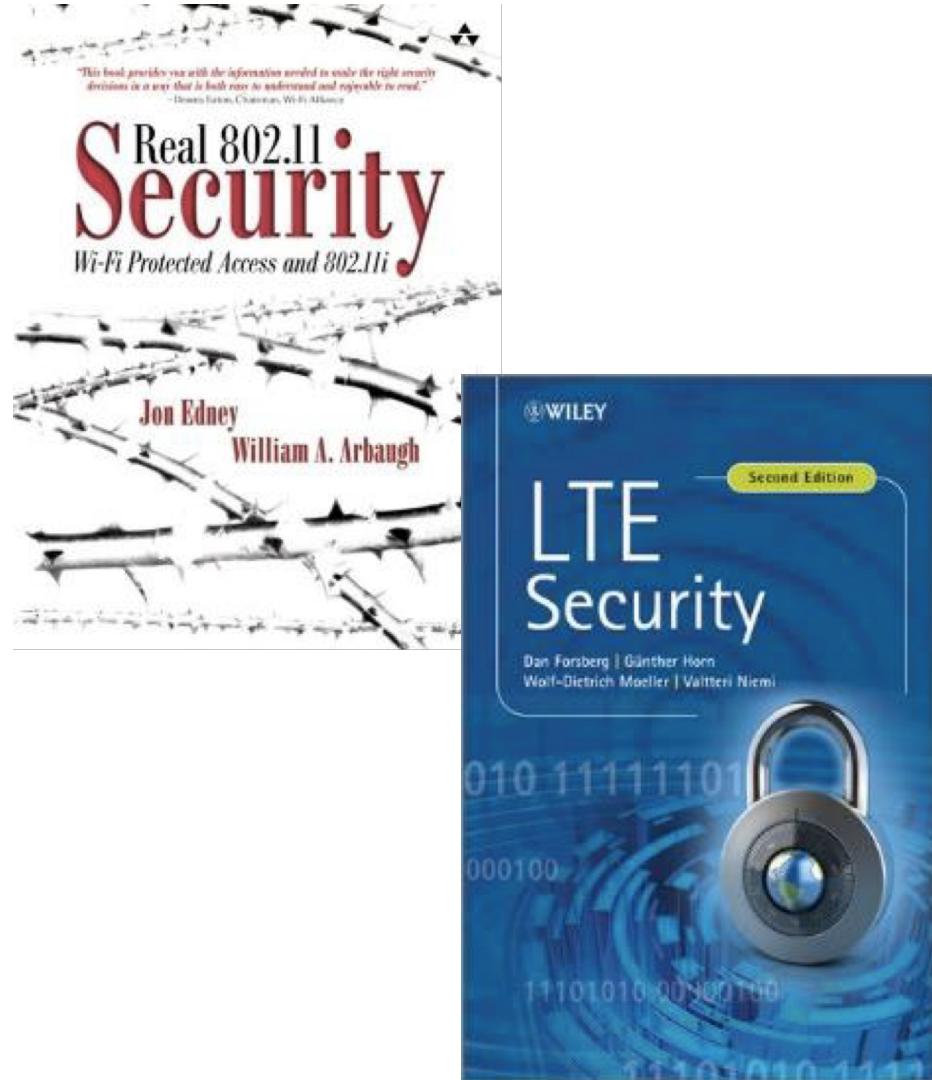
*latinești, românești, chinezesci ...*



(Ernő Rubik)

# Materiale. Referințe bibliografice

- Curs (slide-uri, alte materiale)
- Laborator
- Proiectele de curs
- Articole, standard
- Carti





# Securitatea rețelelor

## - Prelegerea 1 -

### Introducere (Wireless Security)

Ruxandra F. Olimid

Facultatea de Matematică și Informatică  
Universitatea din București

# Cuprins

1. Ce învățăm la securitatea wireless
2. De ce?
3. Prin ce diferă securitatea wireless de securitatea rețelelor cu fir?

# Despre

Rețele  
Wireless

WiFi  
(IEEE 802.11)

Rețele mobile

Altele

- Tehnologii, metode, protocoale de securitate
- Modele, principii de design
- Vulnerabilități și atcuri

Aspecte de  
etică!

# IEEE 802.11 Wireless LAN / Wi-Fi

Security Requirements

Security Principles

Security Architecture

Cryptography

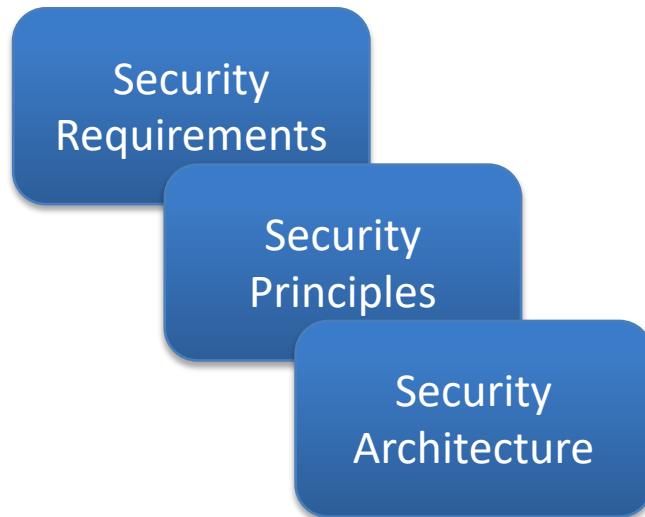


Vulnerabilities

Attacks

*Security aspects only! No pure networking!*

# Rețele mobile



# Aptitudini

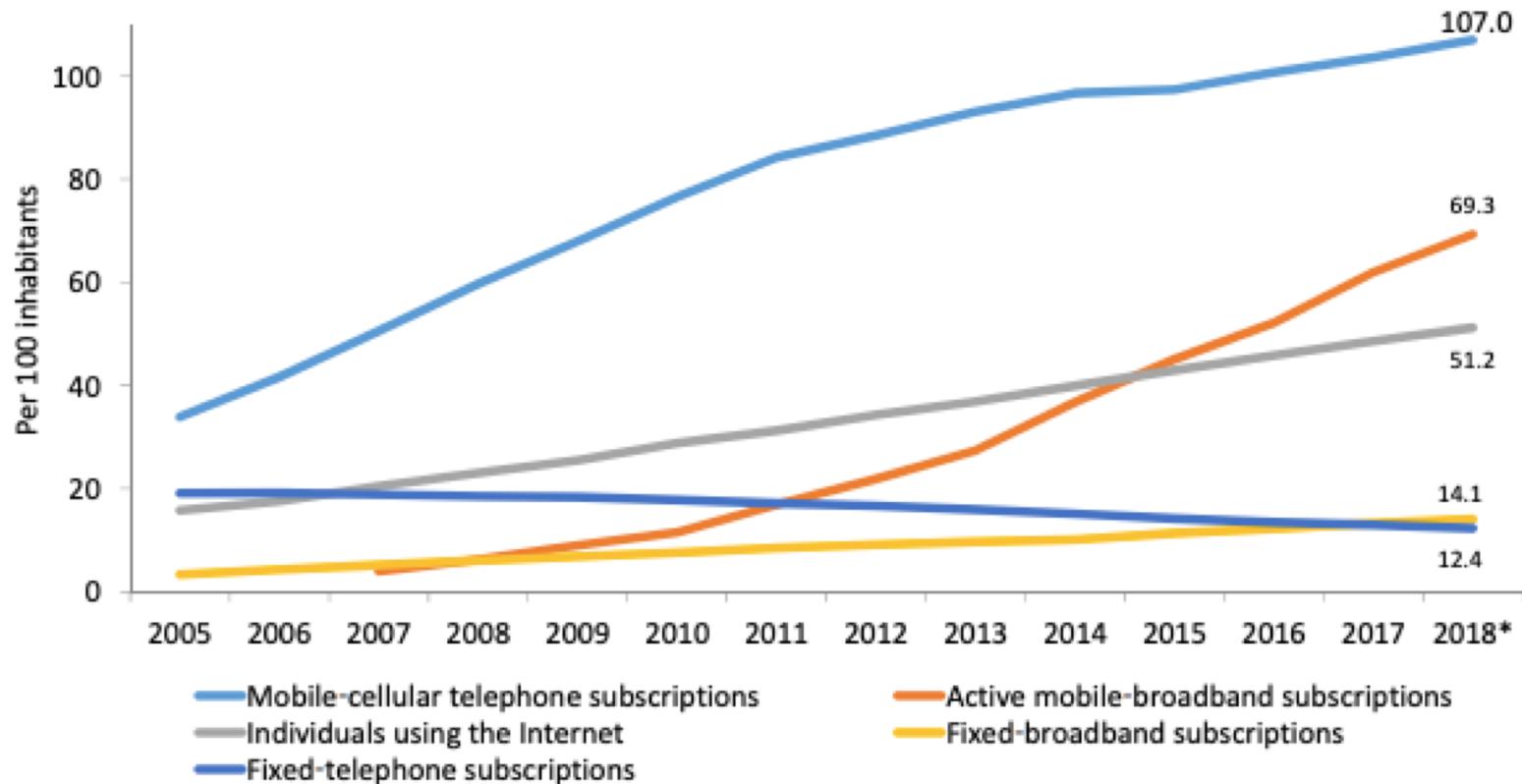
Rețele  
Wireless  
&  
Altele

- Dobândiți cunoștințe despre *wireless security*
- Aptitudini practice și analitice
- Lucru în echipă
- Studiu independent (proiecte, pregătirea examenului)
- Utilizarea unor tool-uri, programare,... gândiți ca un adversar!

# Motivație

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>

# Motivătie

## ITU: Measuring the Information Society Report 2018

### 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.<sup>370</sup> 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	13.0
Mobile-cellular sub. per 100 inhab.	114.6	120.4	103.6
Active mobile-broadband sub. per 100 inhab.	82.9	85.9	61.9
3G coverage (% of population)	100.0	98.3	87.9
LTE/WiMAX coverage (% of population)	83.2	89.6	76.3
Individuals using the Internet (%)	63.7	77.2	48.6
Households with a computer (%)	73.0	78.6	47.1
Households with Internet access (%)	76.5	80.6	54.7
International bandwidth per Internet user (kbit/s)	49.8	117.5	76.6
Fixed-broadband sub. per 100 inhab.	24.3	30.4	13.6
Fixed-broadband sub. by speed tiers, % distribution			
-256 kbit/s to 2 Mbit/s	0.5	0.6	4.2
-2 to 10 Mbit/s	8.0	12.4	13.2
-equal to or above 10 Mbit/s	91.4	87.0	82.6

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

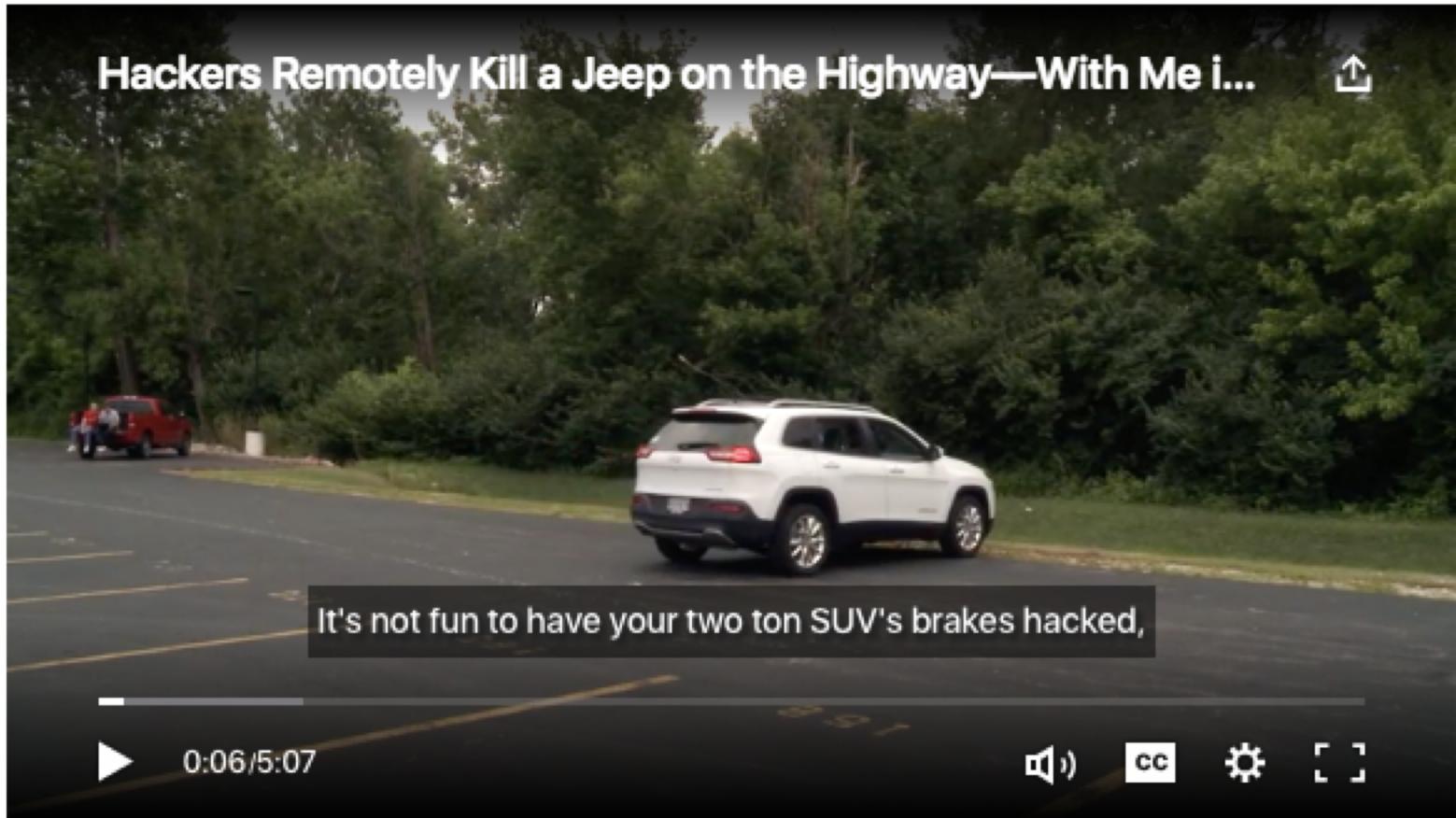
focus of the Government in recent years is on digitalization and broadband development. The National Strategy for the Romanian Digital Agenda 2020 illustrates the Government's efforts in this regard. In line with European targets, Romania aims at achieving 100 per cent of households with fixed-broadband 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.<sup>372</sup> 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.<sup>373</sup>

<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>

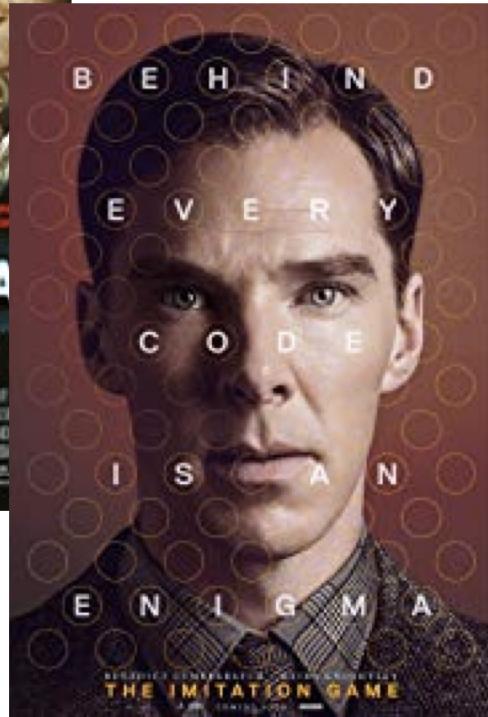
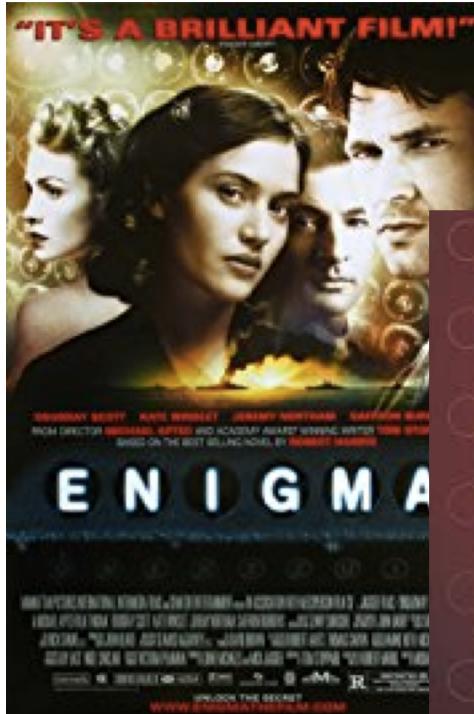
# Motivație

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



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

# Motivație



# Motivație

**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**

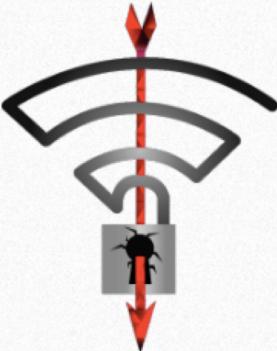
We built an IMSI Catcher that collects subscribers' identifiers (IMSI) in the area of NTNU and then makes the phone reconnect to the commercial network in 2 ways:

- 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](http://ruxandraolimid.weebly.com/uploads/2/0/1/0/20109229/final_Lte.pdf)

# Motivație



# 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>

# De ce este securitatea wireless diferită?

- **Teoretic:** nu diferă foarte mult de securitatea rețelelor cu fir
- **Practic:**
  - Access direct la mediul de transmisiune
  - Dificil de detectat atacuri pasive
  - Comunicație broadcast
  - Dinamicitate (roaming, mobility, etc.)
  - *Constraint devices* (putere de calcul, consum de energie, etc.)
  - Simplicitatea unor atacuri de tip Men-in-the-Middle (MitM), radio jamming, etc.
  - ...



# Securitatea rețelelor

## - Prelegerea 2 -

### IEEE 802.11 Wireless LAN / Wi-Fi Intro

Ruxandra F. Olimid

Facultatea de Matematică și Informatică

Universitatea din București

# Cuprins

1. IEEE 802.11 / Wi-Fi, istorie, evoluție
2. IEEE 802.11 Wireless LAN Architecture

# Despre

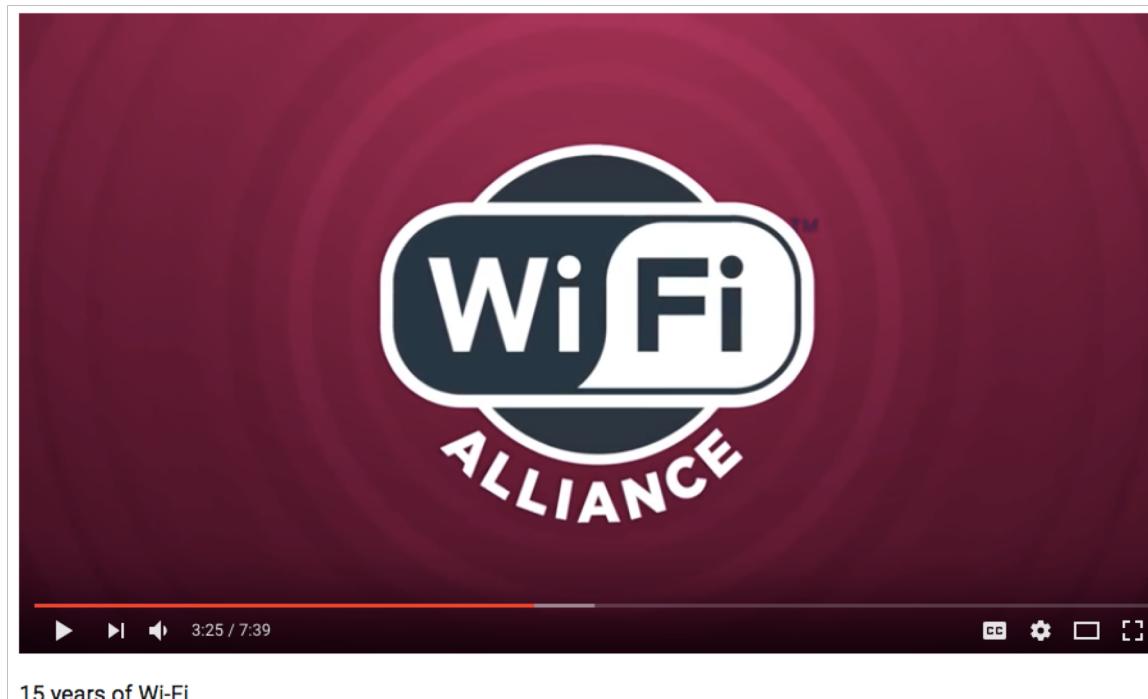
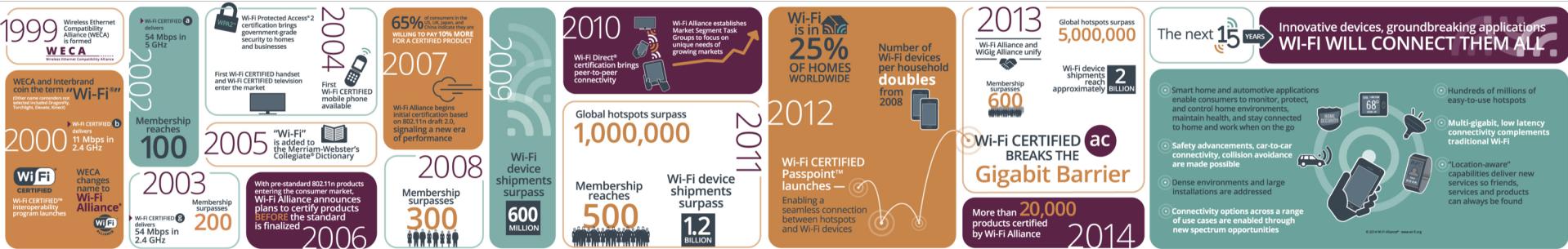
- **IEEE 802.11 Wireless LAN**: un set de specificații (la nivel Physical layer și MAC sublayer) pentru implementarea Wireless LAN (WLAN) networks



- **Wi-Fi**: (produse / echipamente ale) rețele(lor) wireless care implementează standardul IEEE 802.11; o tehnologie bazată pe IEEE 802.11; trademark al Wi-Fi Alliance

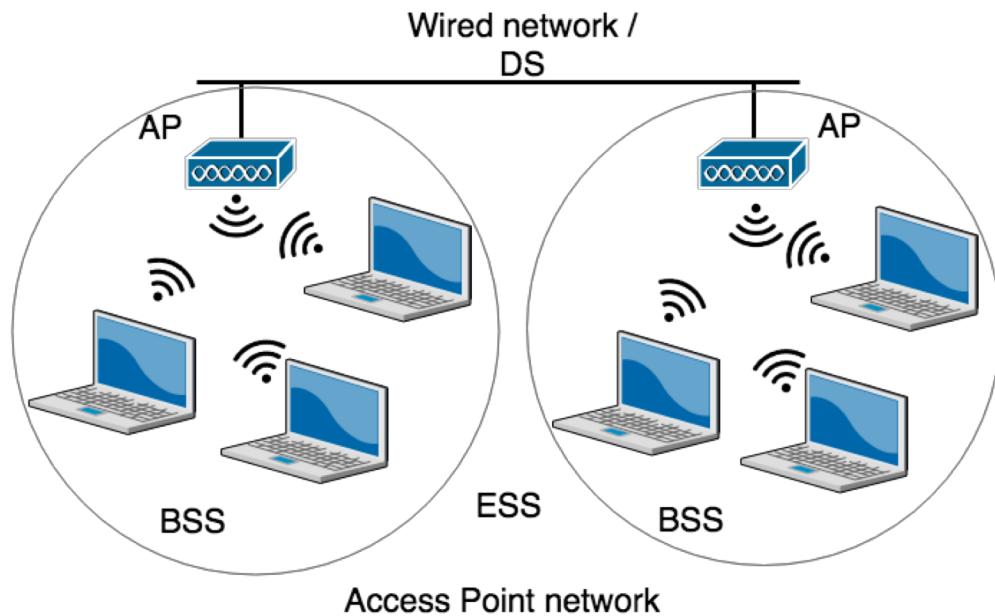
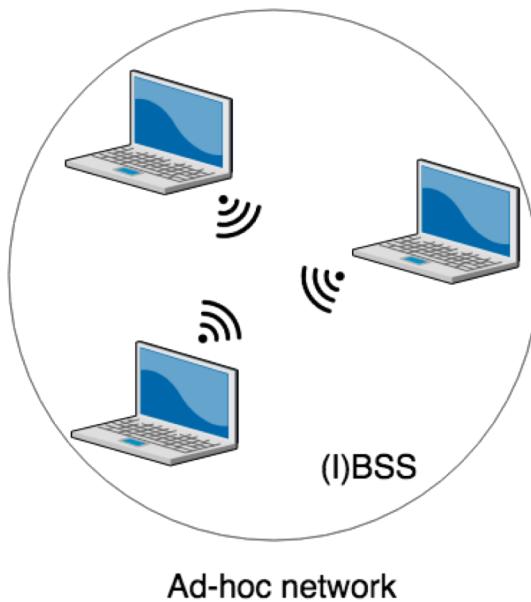


# Evoluția WiFi



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

# IEEE 802.11 Wireless LAN - Arhitectura



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

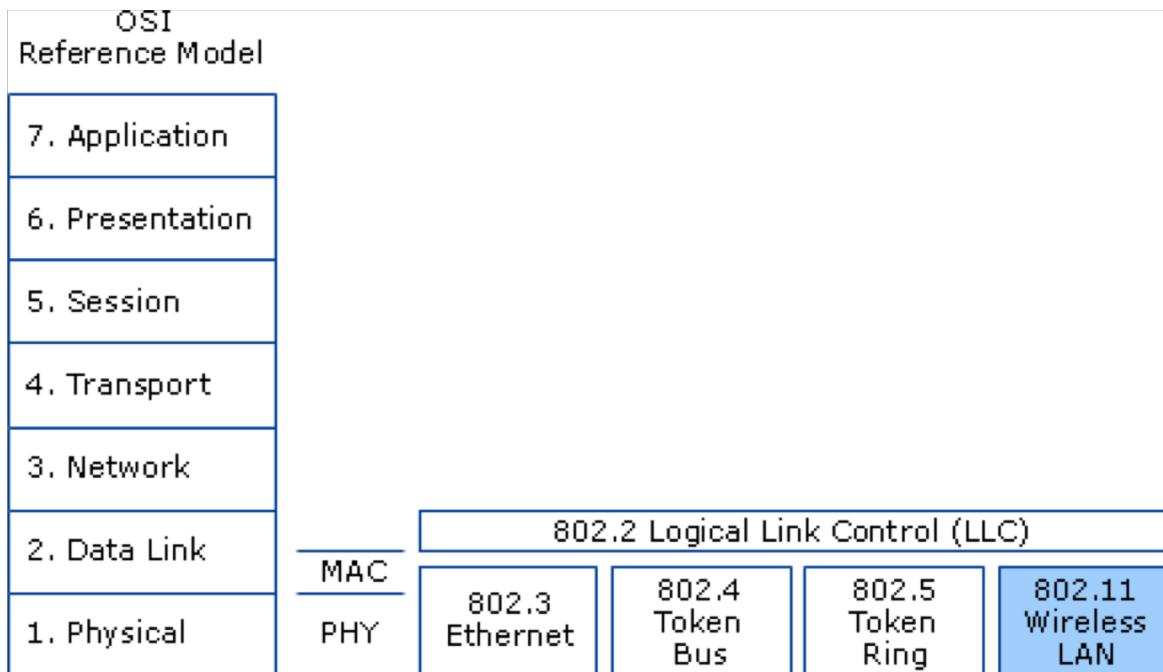
Tipuri de rețea:  

- Ad-hoc
- cu AP
- mesh

# IEEE 802.11 Wireless LAN - Arhitectura

- STA (Stations):
  - Laptopuri, Tablete, Smartphones...
- AP (Access Point):
  - Un dispozitiv care are rol de hub de comunicație
- BSS (Basic Service Set):
  - Identificat de un Service Set ID (SSID)
  - Fie STAs direct conectate (ad-hoc), fie STAs conectate la un AP
- ESS (Extended Service Set):
  - Identificat de un Extended SSID (ESSID)
  - Mai multe BSS conectate printr-o rețea cu fir

# IEEE 802.11 Wireless LAN vs. OSI

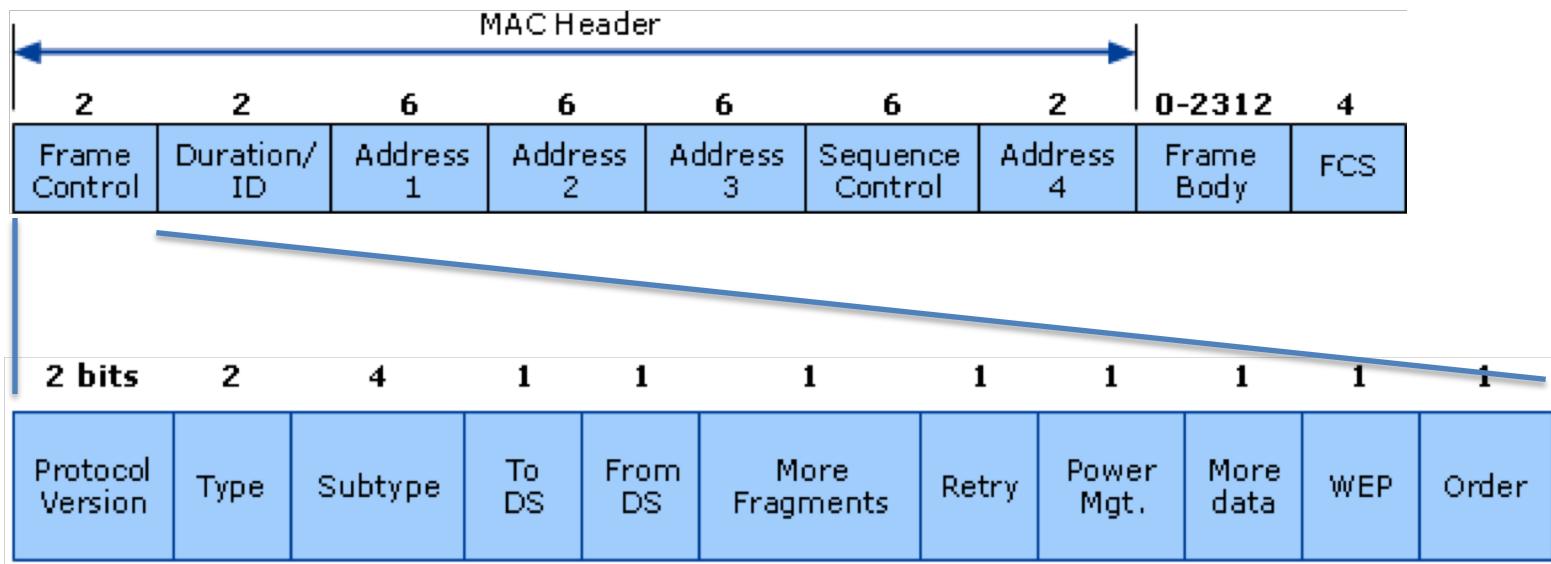


[Source: [https://technet.microsoft.com/pt-pt/library/cc757419\(v=ws.10\).aspx](https://technet.microsoft.com/pt-pt/library/cc757419(v=ws.10).aspx) ]

Definește în OSI :

- Physical layer (codarea / decodarea semnalelor, transmisie de biți, etc.)
- Media Access Control (MAC) sublayer al Data Link layer (grupeaza datele în frames, detectie de erori – 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



# Securitatea rețelelor

## - Prelegerea 3 -

# Wired Equivalent Privacy (WEP)

Ruxandra F. Olimid

Facultatea de Matematică și Informatică

Universitatea din București

# Cuprins

1. Descriere
2. Vulnerabilități și atacuri
3. Lecții de învățat

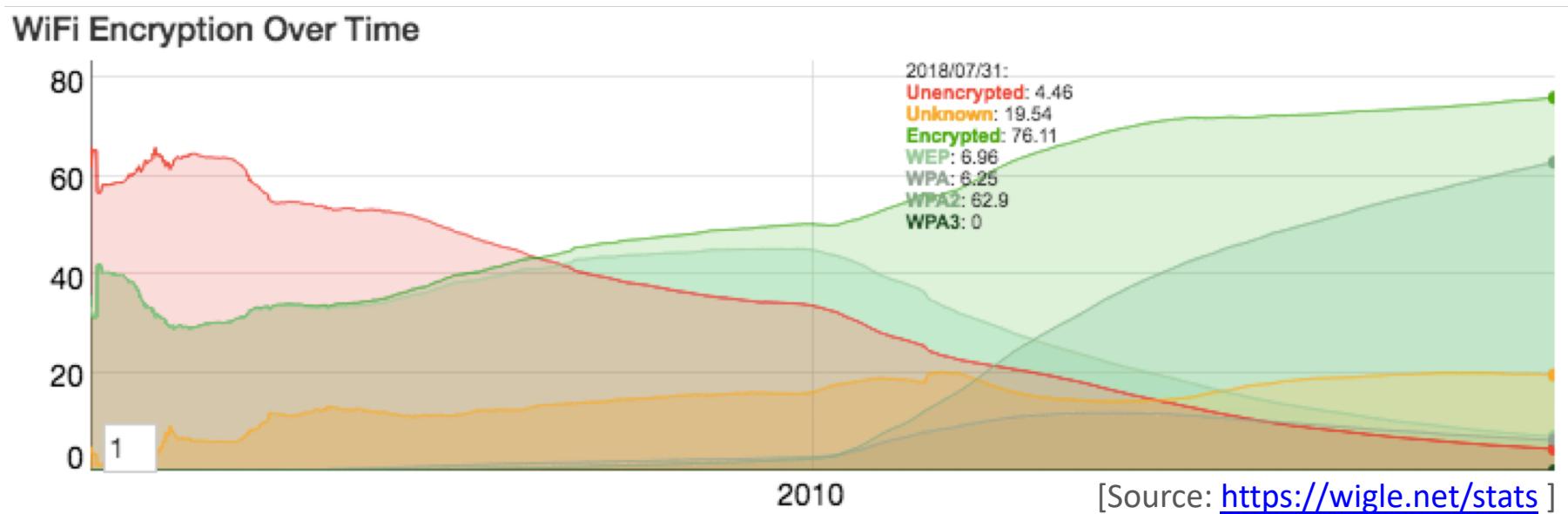
# IEEE 802.11 Security

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)

- Mecanismul original de securitate pentru IEEE 802.11 (1999)
- Deprecated din 2008, dar încă se utilizează
- Interesant de studiat ca un exemplu de AŞA NU ☺



# Obiective de securitate

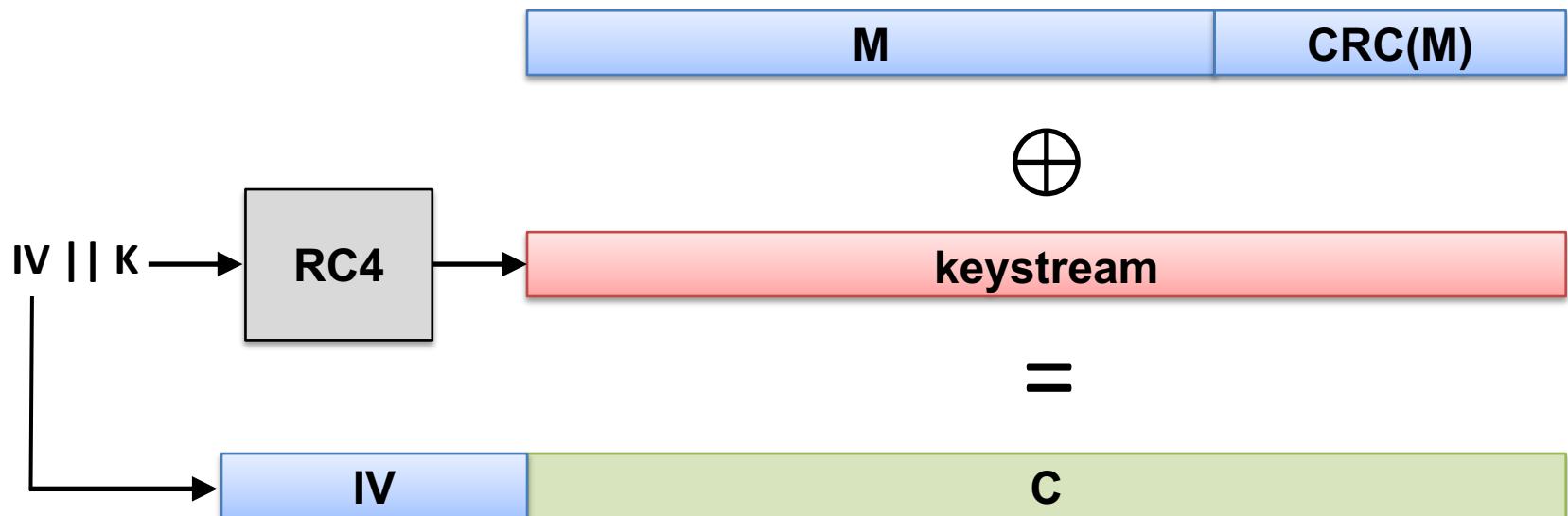
- Data confidentiality (confidențialitatea datelor):
  - Protejează împotriva ascultării (eavesdropping) pe canalul radio
- Data integrity (integritatea datelor):
  - Protejează împotriva introducerii și modificării mesajelor
- Network access control (control de access):
  - Protejează utilizarea resurselor WLAN
- Altele:
  - Exportabil
  - Eficient dpdv hardware și software

# Cum funcționează WEP?

# Idei de design

- Key management (managementul cheilor):
  - O singură cheie pentru toate dispozitivele dintr-un BSS
  - Export: chei pe 40 de biți
- Data confidentiality (confidențialitatea datelor):
  - Criptarea frame-urilor de date transmise pe mediul de comunicație wireless folosind cheia criptografică
- Data integrity (integritatea datelor):
  - Folosirea unei Cyclic Redundancy Check (CRC)

# Criptarea WEP (teorie)

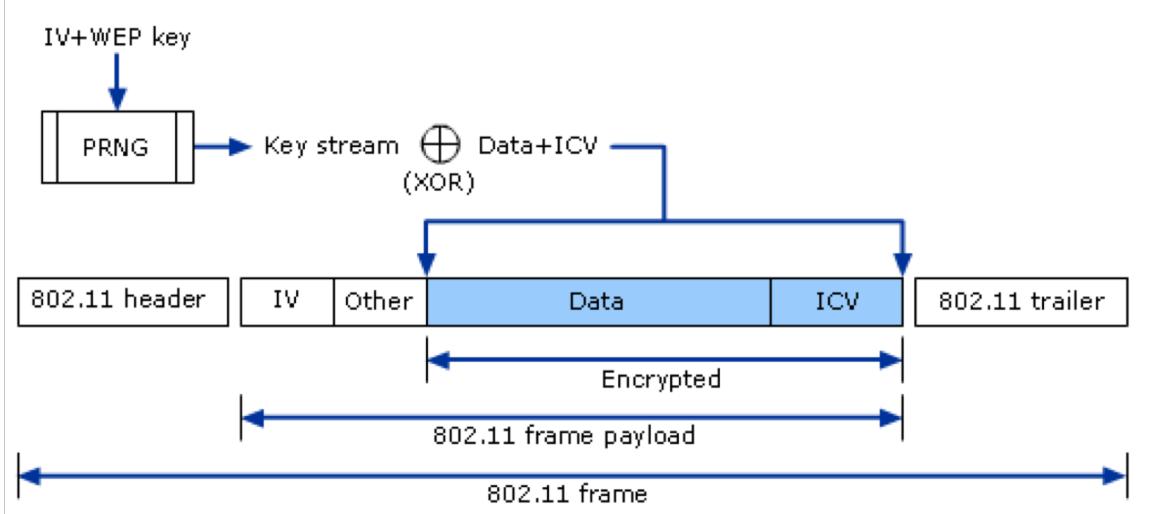


- Uses **RC4**
- IV: 24 bits, K: 104 bits (40 bits)
- IV is used in counter mode (0, 1, 2, ...)

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

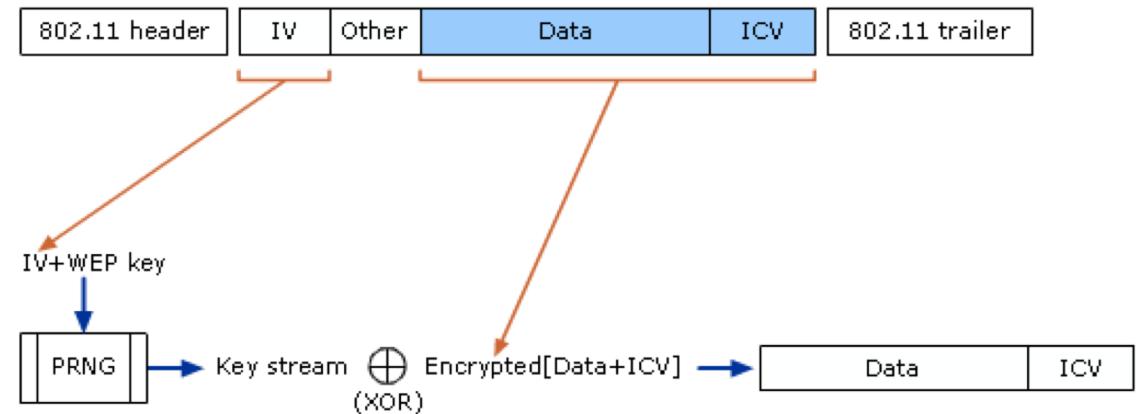
# Criptarea WEP (practică)

## WEP Encryption Process



IV: Initialization Vector  
PRNG: Pseudo-Random Number Generator  
ICV: Integrity Check Value

## 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) ]

# Autentificarea WEP



- **Auth Challenge:**
  - AP trimite o provocare (random) pe 128 biți (challenge)
- **Auth Response:**
  - STA criptează challenge-ul cu cheia secretă folosind WEP și trimite textul criptat către AP
- **Auth Success:**
  - AP decriptează și compară plaintext-ul cu challenge-ul; dacă sunt egale, autentificarea se realizează cu succes

# Ce probleme apar?

## Problema 1 - Autentificarea

Întrebare: Ce poate afla adversarul printr-un atac pasiv?

Răspuns: Un adversar pasiv ascultă (eavesdrops) plaintext-ul (challenge) și ciphertext-ul și determină *keystream* pentru un IV:

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

Întrebare: Este autentificarea sigură?

Răspuns: Nu! Adversarul știe *keystream* pentru un IV dat. Refolosește IV, XOR-ează *challenge* cu *keystream* găsit ca mai înainte și întoarce un text valid criptat către AP.

## Problema 1 - Autentificarea

Întrebare: Este autentificarea mutuală ([mutual authentication](#))?

Răspuns: Nu! STA nu autentifică AP.

Întrebare: Ce tip de atac facilitează asta?

Răspuns: În general absența autentificării mutuale favorizează apariția [rogue entities](#) (e.g., un AP fals care trimite challenge-uri și primește răspunsuri, adică un fel de [oracol de autentificare](#))

## Problema 2 - Linearitate

**Întrebare:** Considerăm că nu există CRC. Poate adversarul să schimbe anumiți biți din mesajul clar după cum dorește?

**Răspuns:** Da!

- interceptează  $c$ ;
- schimbă  $c$  în:

$$c' = c \oplus m'$$

- trimit  $c'$  în loc de  $c$

La destinație va ajunge

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

$m'$  are 1 pe pozițiile care se schimbă în  $m$ , și 0 altfel

CRC previne **erori** (neintenționate), nu **atacuri** (intenționate)!

## Problema 3 – Utilizarea multiplă a lui IV

**Întrebare:** Care este efectul imediat al utilizării aceluiași IV pentru o cheie fixă K?

**Răspuns:** Se obține același *keystream* (RC4 e determinist!)

**Întrebare:** În aceste condiții sistemul este sigur?

**Răspuns:** Nu!

$$c1 = m1 \parallel CRC(m1) \oplus keystream$$

$$c2 = m2 \parallel CRC(m2) \oplus keystream$$

$$\Rightarrow c1 \oplus c2 = m1 \parallel CRC(m1) \oplus m2 \parallel CRC(m2)$$

Exemplu: dacă adversarul știe  $m2$ , află imediat  $m1$

**Întrebare:** Câte valori posibile sunt pentru IV?

**Răspuns:**  $2^{24}$  , puține!

(se repetă la câteva ore; mai mult, AP poate seta IV la 0 la reset)

## Alte probleme...

- RC4 nu este un PRG sigur! Chei slabe, atacuri,...
- Replay attacks (nu există mecanism de protecție) ...
- Message injection (dacă se știe *keystream* pentru un IV)
- **Man-in-the-Middle (MitM)**: direct prin găsirea cheii, sau prin rogue AP (open auth. mode)

# Recuperarea cheii

## Smashing WEP in A Passive Attack

Pouyan Sepehrdad<sup>1</sup>, Petr Sušil<sup>2 \*</sup>, Serge Vaudenay<sup>2</sup>, and Martin Vuagnoux

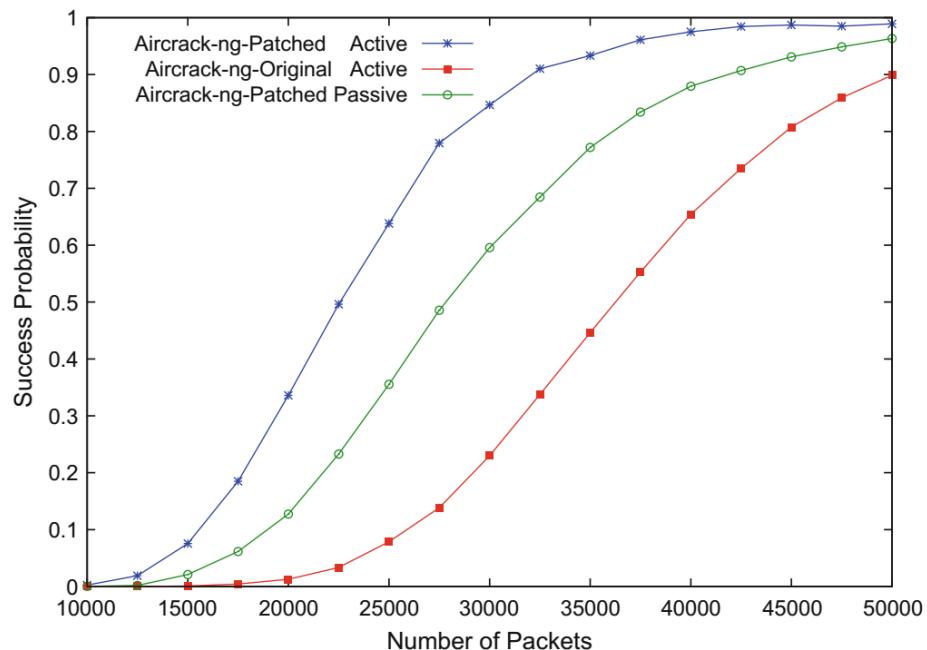
<sup>1</sup> Intel CRI-SC at TU-Darmstadt, Darmstadt, Germany

<sup>2</sup> EPFL, Lausanne, Switzerland

pouyan.sepehrdad@trust.cased.de,

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

martin@vuagnoux.com



**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...

- Obiective clare de design 
- Open standard 
- Utilizarea primitivelor criptografice bine cunoscute și studiate 
- Public review / analiză / competiții 

# Lecții de învățat...

- E dificil de realizat un protocol sigur
- Folosiți primitive criptografice cunoscute, analizate
- Faceți sistemul public ([principiul lui Kerckhoffs](#)); mai mult, analiza publică de securitate e importantă
- Folosiți definiții precise și demonstrații de securitate
- Adversarii nu sunt limitați de modele!



# Securitatea rețelelor

## - Prelegerea 4 -

### Wi-Fi Protected Access (WPA)

Ruxandra F. Olimid

Facultatea de Matematică și Informatică  
Universitatea din București

# Cuprins

1. Îmbunătățiri față de WEP
2. Descriere

# IEEE 802.11 Security

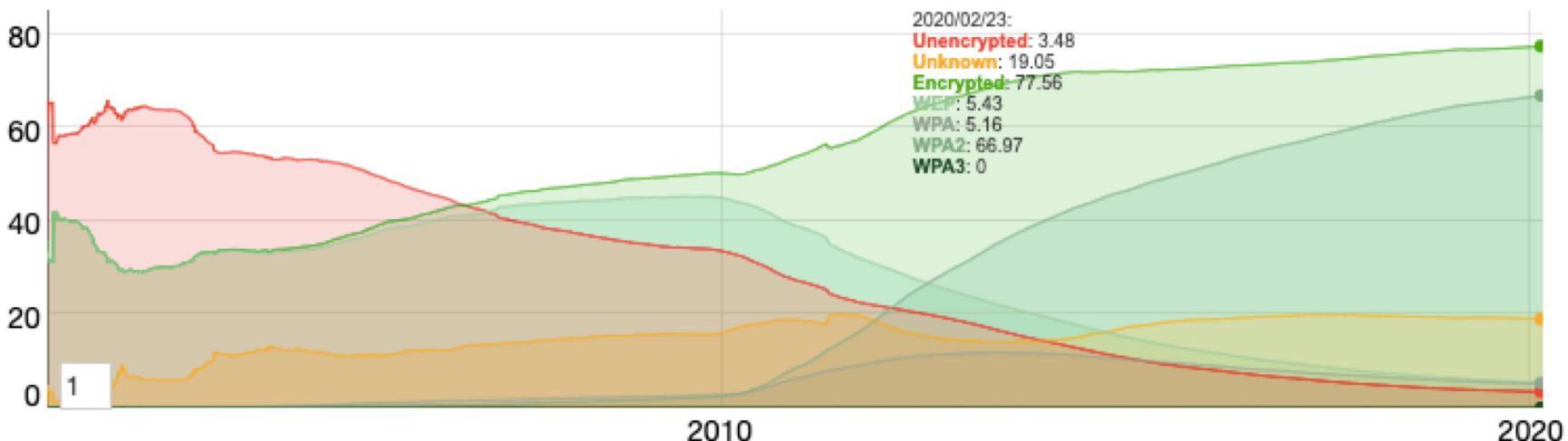
Improved security

- 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* al Wi-Fi Alliance (802.11i-draft) – soluție ușor de adoptat
- WEP + Temporal Key Integrity Protocol (TKIP)
- Deprecated din 2014, dar încă se utilizează

WiFi Encryption Over Time



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

# Reamintim WEP

- Nu oferă **confidențialitate**:
  - IV scurt ⇒ refolosire keystream RC4
  - Recuperarea cheii (< 60 secunde)
- Nu oferă **integritate**:
  - CRC nu este MAC!
- Nu oferă protecție împotriva **replay attack**
- Nu există un **management al cheilor**:
  - O singură cheie (104 biți) folosită la criptarea mesajelor
  - O singură cheie folosită de toți utilizatorii din WLAN

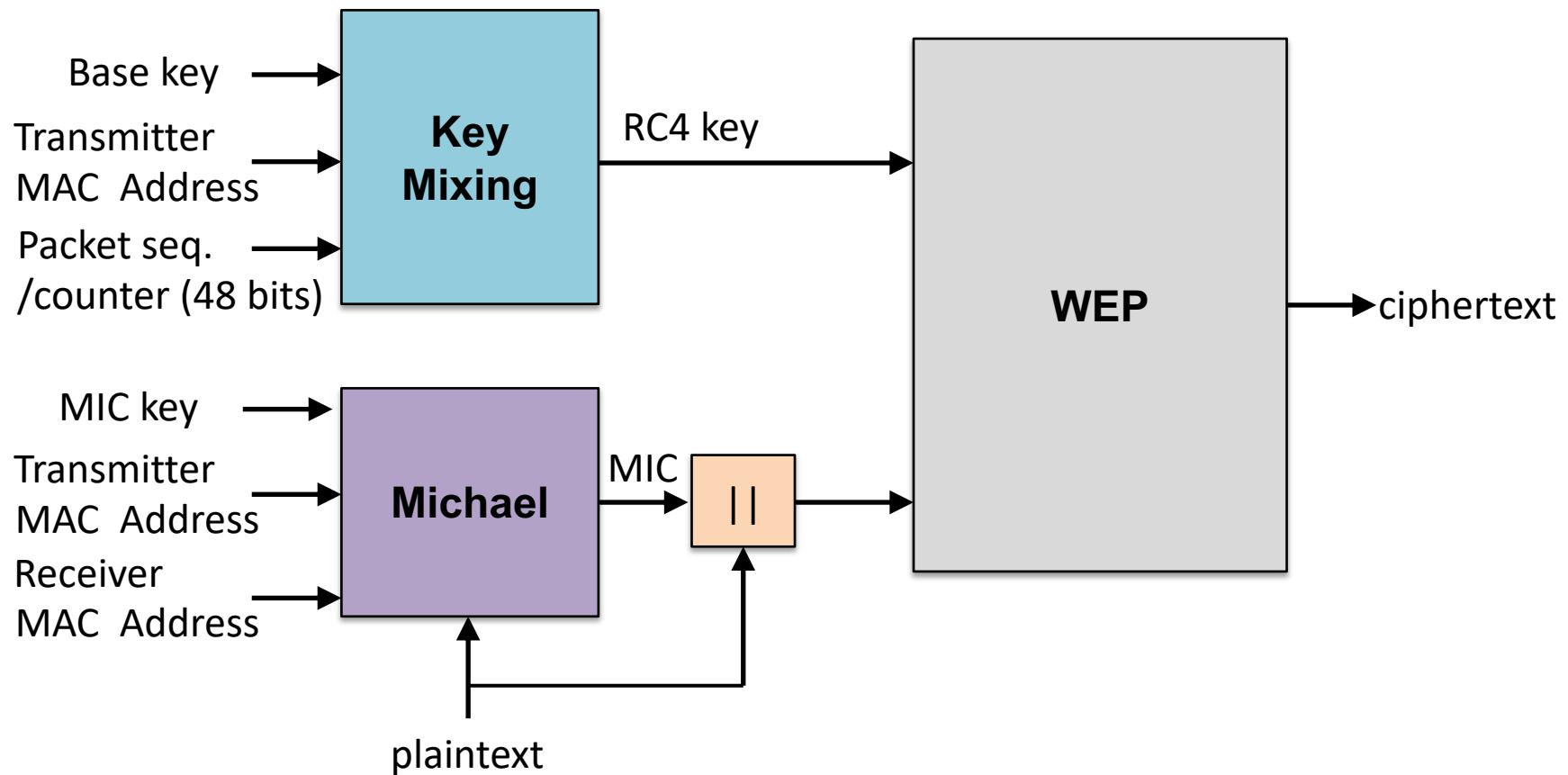
# Îmbunătățiri față de WEP

- Criptare:
  - TKIP pentru îmbunătățirea criptării WEP (e.g., o cheie nouă pentru fiecare pachet / frame)
  - Posibilitatea de a utiliza AES (optional, nu toate dispozitivele aveau suport AES)
- Integritate:
  - Michael, un nou algoritm
- Autentificare:
  - 802.1X (definit inițial pentru rețelele Ethernet, adoptat apoi la 802.11 WLAN)
  - 802.11 - autentificarea 802.1X e optională, WPA - autentificarea 802.1X e obligatorie
- Generarea și distribuția cheii:
  - 802.1X

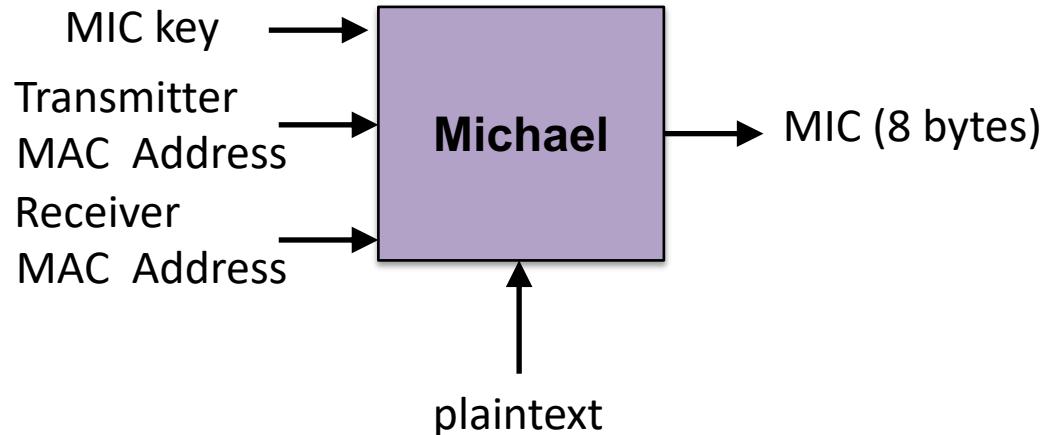
# TKIP

## (Temporary Key Integrity Protocol)

# TKIP (Temporary Key Integrity Protocol)



# Michael



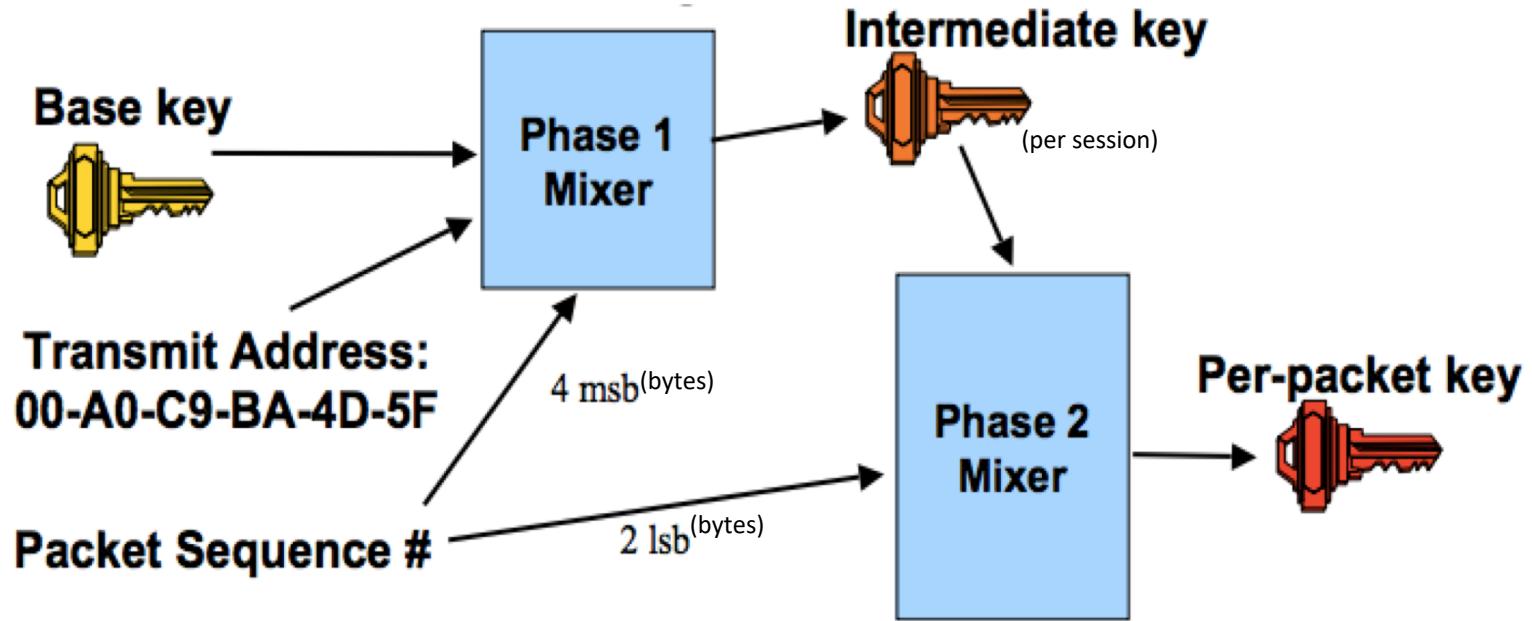
- **MIC key**: de fapt 2 chei de 64 biți fiecare (câte una pentru fiecare direcție de comunicație)
- **Output**: 64 biți (8 bytes)
- **Problemă**: nivelul de securitate - 20 biți;

**Întrebare:** De ce este asta o problemă?

**Răspuns:** Adversarul are șanse de aprox. 1 la un million să ghicească MIC ( $2^{20} = 1048576$ )

**Soluții?** Limitarea verificării MIC-ului de către adversary (delay de 1 min. la detectie atacuri). Apare o nouă problemă: **DoS!**

# TKIP (Temporary Key Integrity Protocol)



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

# TKIP (Temporary Key Integrity Protocol)

- Chei temporare:
  - 2 etape de mixare
  - Dependente de echipament, prin adresa MAC a transmițătorului
  - Dependente de *packet sequence* (48 biți, nu 24 cum avea IV in WEP)
- Scop:
  - Se evită reutilizarea keystream (cheile devin temporare) / **collision attacks**
  - Se evită retransmiterea pachetelor la refolosirea IV (spațiul posibil devine acum  $2^{48}$ ) / **replay attacks**

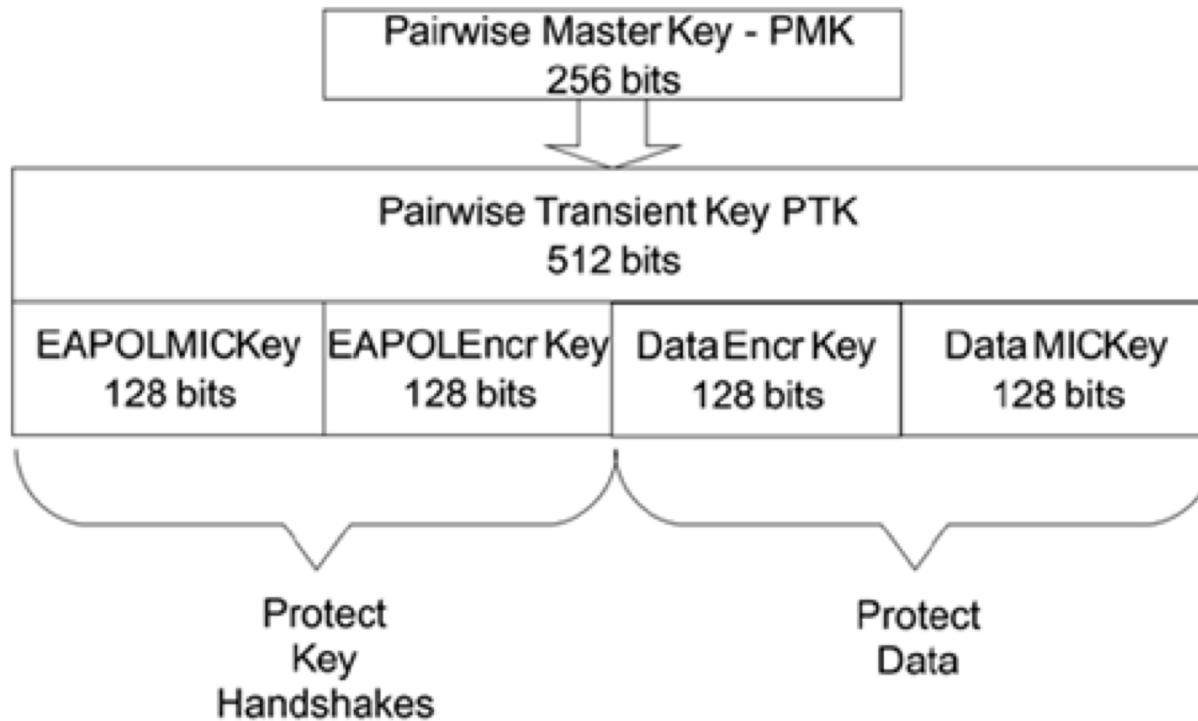
# TKIP (Temporary Key Integrity Protocol)

- Base key / PTK (Pairwise Transient Key):

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

- PMK (Pairwise Master Key) / 2 variante:
  - pre-shared key, 256 biți
  - 802.1X PMK e unică per STA, transmisă de serverul de autentificare către AP (*upper layer authentication*)

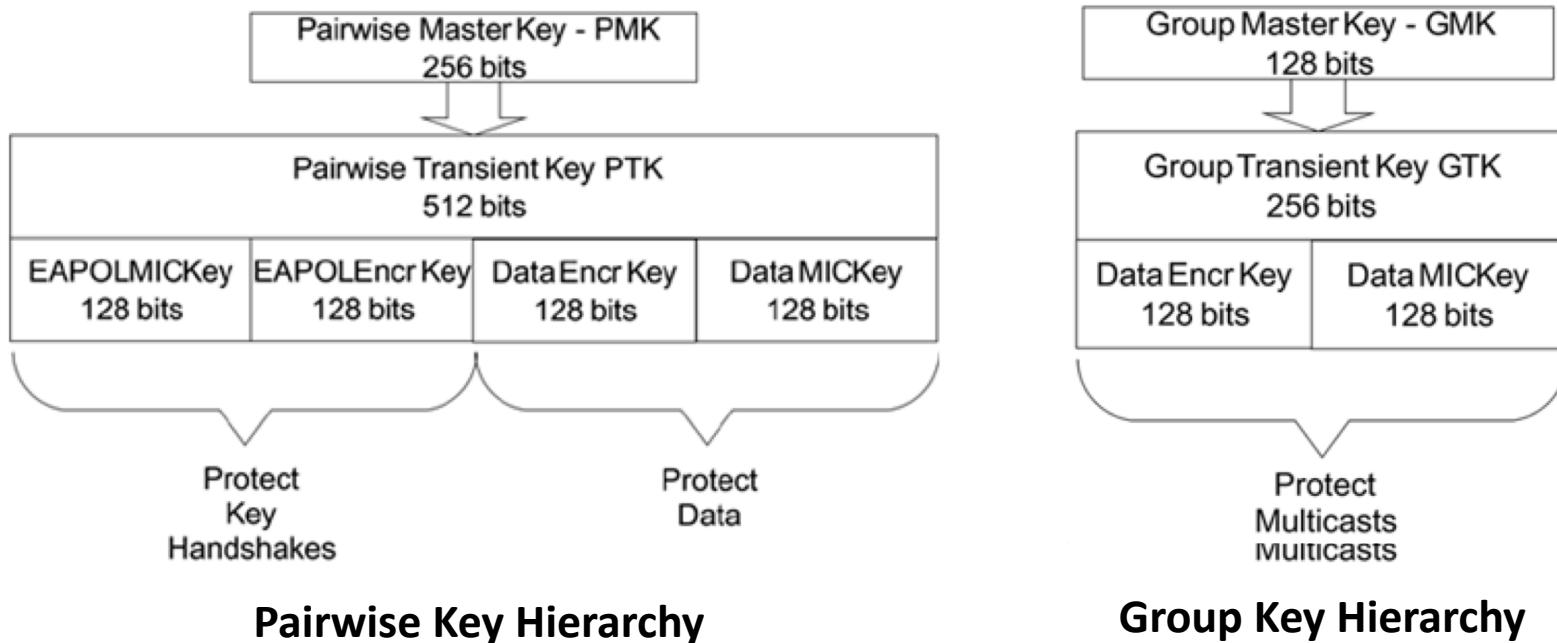
# TKIP Pairwise Key Hierarchy



[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

## Design WPA...

- Încearcă să adreseze toate problemele WEP
- Limitat de capacitatele dispozitivelor (software upgrade)
- Compatibil cu 802.11i (WPA ca draft 802.11i)



# Securitatea rețelelor

## - Prelegerea 5 -

## 802.1X & EAPOL

Ruxandra F. Olimid

Facultatea de Matematică și Informatică  
Universitatea din București

# Cuprins

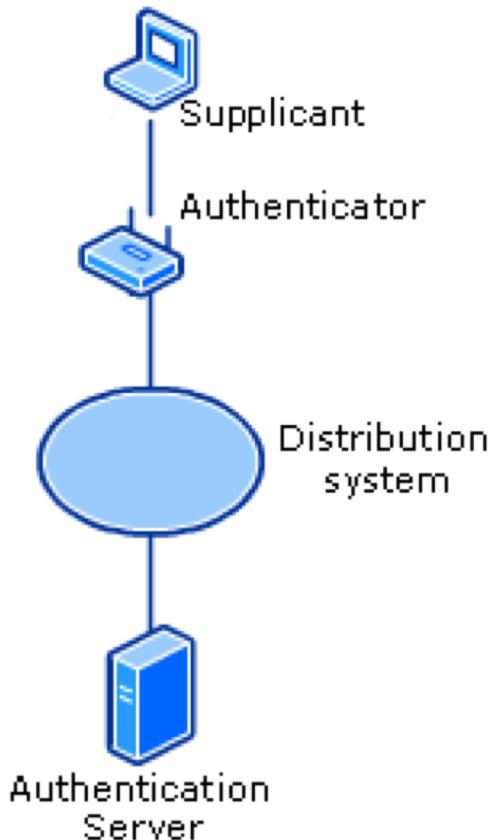
1. Arhitectură 802.1X
2. Secvență de autentificare EAPOL

# 802.1X

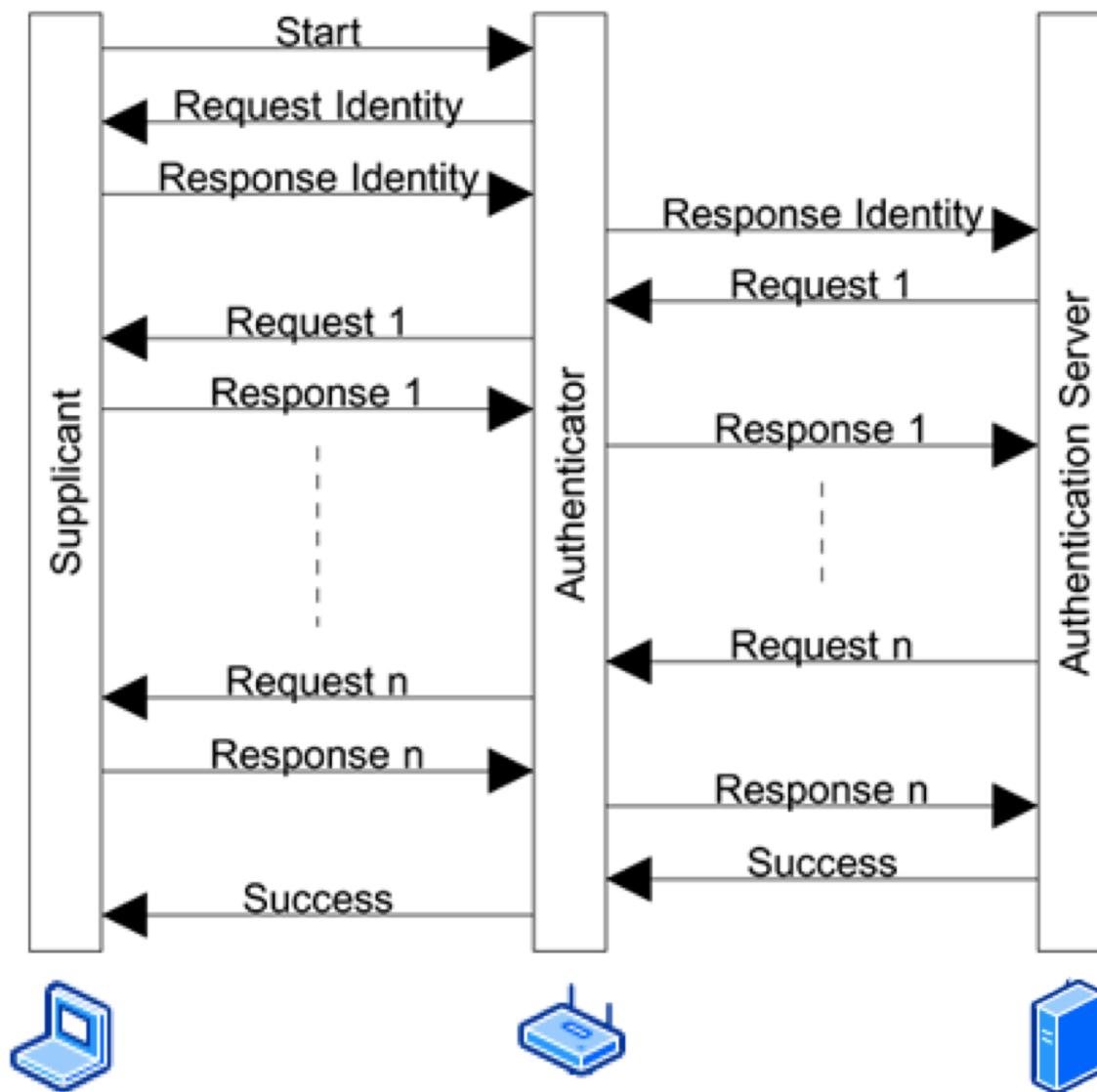
- Standard definit inițial pentru rețelele Ethernet, adoptat apoi la 802.11 WLAN
- Definește controlul accesului în rețea (pe bază de porturi), dar mai mult, oferă access autentificat în rețea
- Extensible Authentication Protocol (EAP) over LAN (EAPOL) este un mecanism de autentificare Point to Point Protocol (PPP) adoptat pentru utilizare în LAN.
- 802.1X folosește EAPOL pentru transmiterea mesajelor între entități.

# Arhitectura IEEE 802.1X

- **Supplicant:**
  - O entitate care cere acces la servicii; e.g.: un laptop
- **Authenticator:**
  - O entitate care realizează autentificarea înainte de a acorda acces la servicii (i.e. controlează “poarta de access”); e.g.: un AP
- **Authentication Server:**
  - Decide dacă supplicant-ul poate / nu poate accesa serviciile (prin verificarea credențialelor în numele authenticator-ului); e.g.: în AP (în general NU!), **RADIUS** (Remote Authentication Dial-In User Service)



# Sevență de autentificare EAPOL

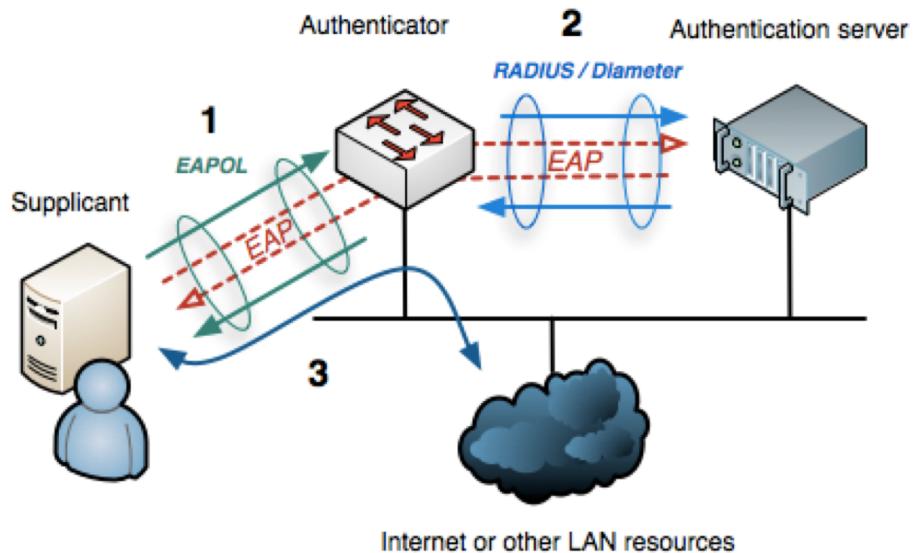
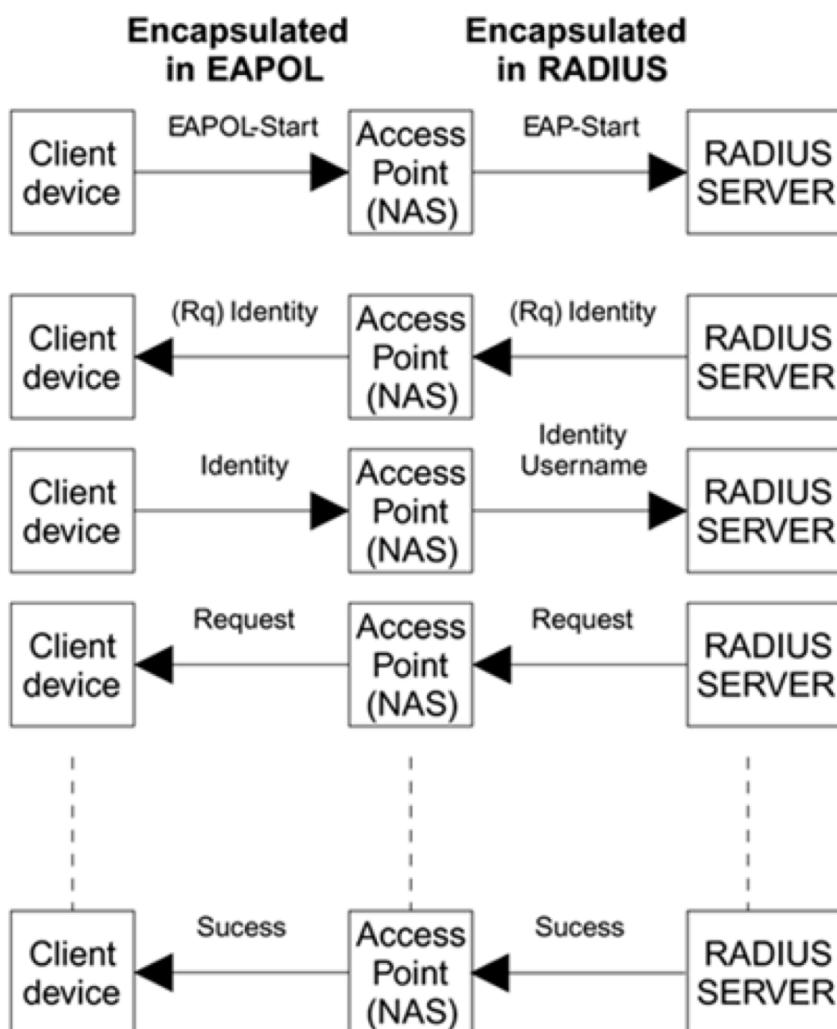


[Source: Course book, Edney &Arbaugh, Chapter 8]

## Autentificarea EAPOL

- Framework generic de autentificare
- Încapsulează protocoale specific (e.g., TLS, AKA)
- Scop: ambele părți dovedesc că știu același secret
- 4 mesaje specifice: *Request*, *Response*, *Success*, *Failure*

# Incapsularea EAPOL



[Source: [https://en.wikipedia.org/wiki/IEEE\\_802.1X](https://en.wikipedia.org/wiki/IEEE_802.1X)]

# RADIUS

- Remote Authentication Dial In User Service (RADIUS)
- Definește:
  - Un set de funcționalități comune pentru serverele de autentificare
  - Un protocol care permite accesarea acestor funcționalități
- Specificat de IETF
- EAP over RADIUS extension (RFC2869)
- Mecanism de tip Challenge-response

# Mai multe...

The video player interface shows a presentation slide from INE. The slide has a dark background with a geometric pattern. At the top right is the INE logo. The main title is "802.1x Purpose". Below it is a bulleted list: "» What problem does it solve?", "» Components", and a list of three components: "• Supplicant", "• Authenticator", and "• Authentication Server". Below the list is a diagram illustrating the components: a laptop labeled "Supplicant" is connected by a line to a blue rectangular box labeled "Authenticator", which is then connected to a yellow cloud-like shape representing "Authentication Server". The INE logo is also present on the server icon. At the bottom left of the slide is the text "Copyright © www.ine.com".

An Overview of 802.1x

Unlisted

[Source: <https://www.youtube.com/watch?v=3obzgqqlnL8>]



# Securitatea rețelelor

## - Prelegerea 6 -

### IEEE 802.11i RSN / WPA2

Ruxandra F. Olimid

Facultatea de Matematică și Informatică  
Universitatea din București

# Cuprins

1. Obiective de securitate
2. CCMP
3. Ierarhia de chei. 4-way handshake
4. Securitate

# IEEE 802.11 Security

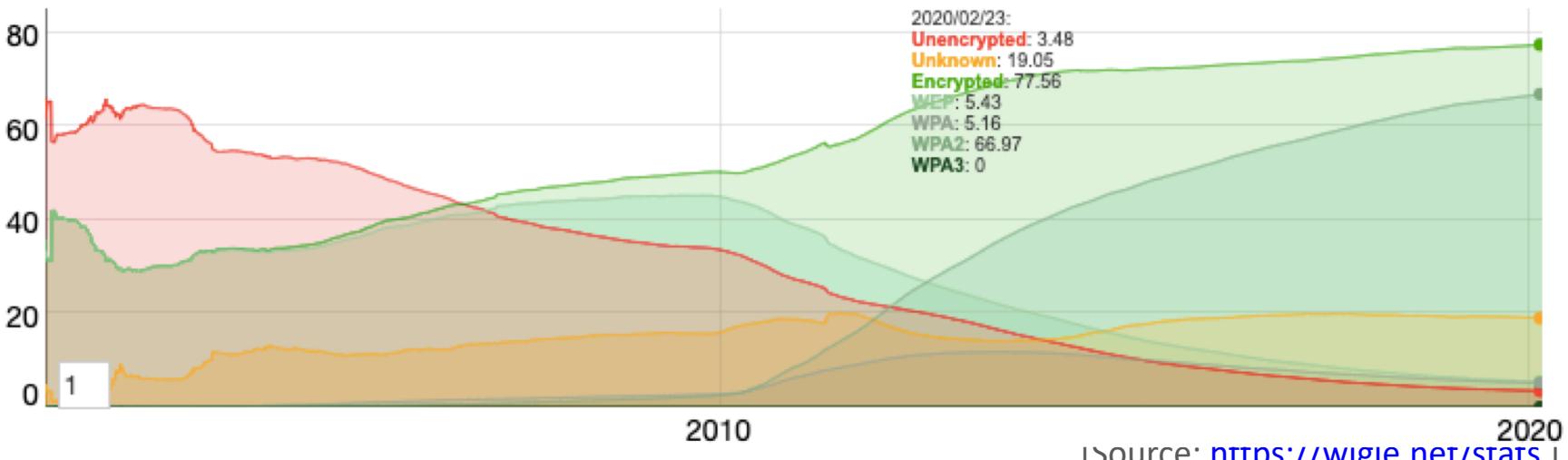
Improved security ↓

- 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 II (WPA2)

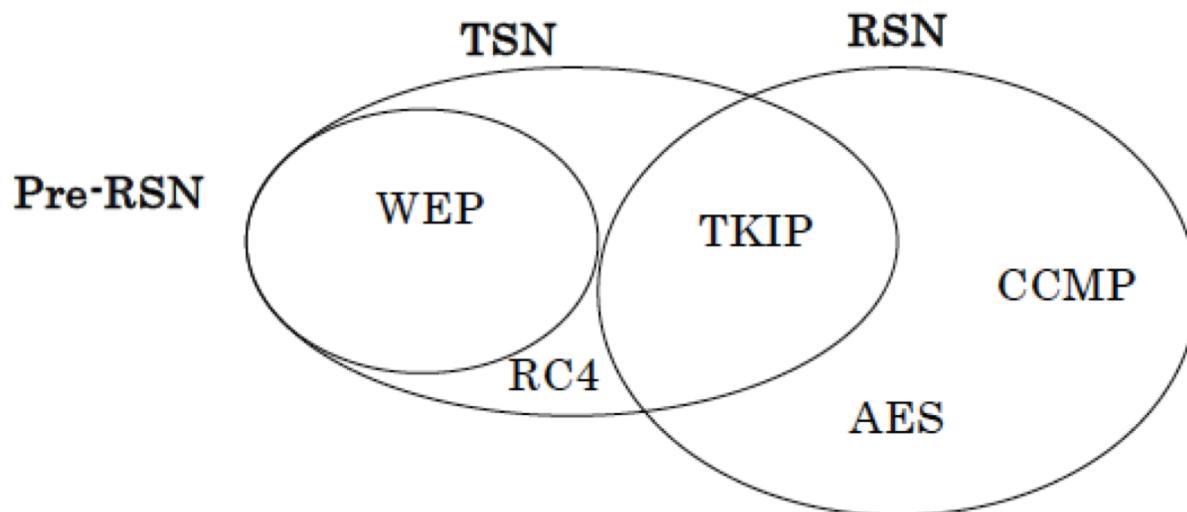
- Introdus de Wi-Fi Alliance în 2004 ca o soluție pe termen lung pentru înlocuirea WEP
- Cunoscut și ca 802.11i
- Folosit până la introducerea WPA3 (deși *key reinstallation attacks* au fost publicate în 2017)

WiFi Encryption Over Time



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

# WLAN Security Soup



RSN: Robust Security Network

TSN: Traditional Security Network

WEP: Wired Equivalent Privacy

TKIP: Temporal Key Integrity Protocol

RC4: Rivest Code 4

AES: Advanced Encryption Standard

CCMP: CCM Protocol

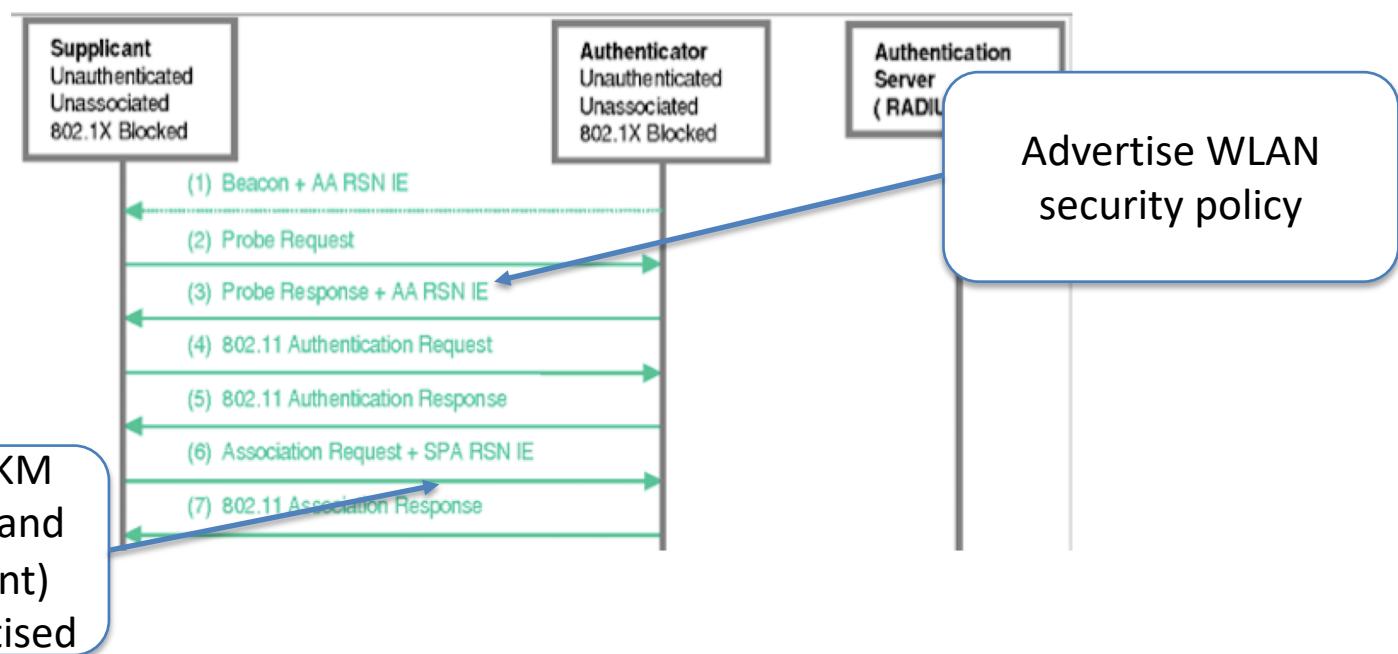
CCM: Counter mode with CBC MAC

CBC: Cipher Block Chaining

MAC: Message Authentication Code

# Robust Security Network (RSN)

- RSN: un protocol pentru stabilirea comunicațiilor sigure peste rețelele wireless 802.11
- **RSN Information Element (IE)**: structură de date pentru publicarea și negocierea capabilităților de securitate



# Robust Security Network (RSN)

Backward compatibility with WEP!

## Defined Ciphersuites

- 00-0F-AC:1 WEP-40
- 00-0F-AC:2 TKIP
- 00-0F-AC:4 AES-CCMP (default)
- 00-0F-AC:5 WEP-104
- Vendor OUI:Any Vendor specific
- Other Reserved

## Defined AKMs

- 00-0F-AC:1 802.1X Authentication + 4-Way Handshake
- 00-0F-AC:2 PSK + 4-Way Handshake
- Vendor OUI:Any Vendor specific
- Other Reserved

## RSN IE

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

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		

# Obiective de securitate

Încearcă să adreseze problemele din WEP

- **Confidențialitate**  
Folosește **Advanced Encryption Standard (AES)**, în loc de RC4
- **Integritatea și autentificarea mesajelor**  
Folosește 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](http://ieee802.org/16/liaison/docs/80211-05_0123r1.pdf) ]

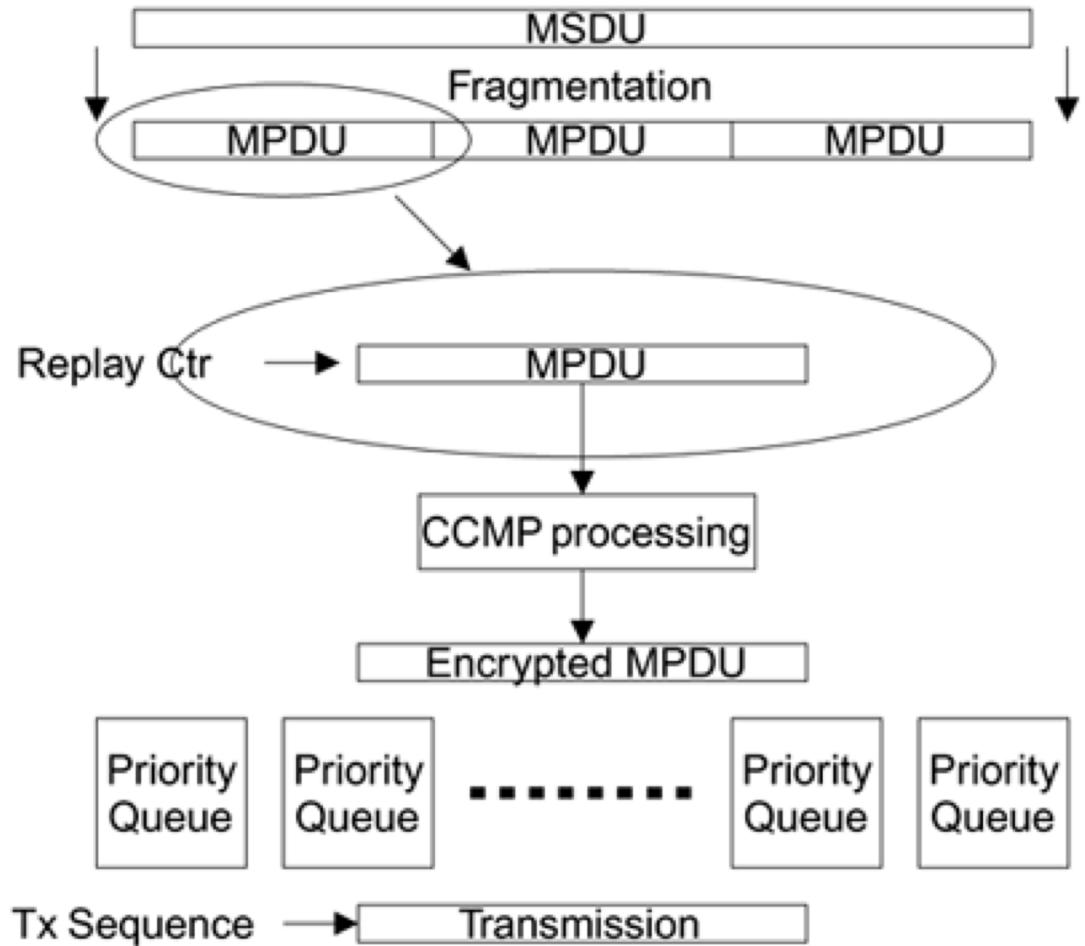
# Security Goals

Încearcă să adreseze problemele din WEP

- Reply detection  
Packet Number (PN), replay counter
- Key management protocols  
Similar cu WPA
- Access control  
Folosește arhitectura **802.1X**

CCMP  
(Counter Mode Cipher Block Chaining Message  
Authentication Code Protocol )

# CCMP



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

MSDU: MAP Service Data Unit

MPDU: MAC Protocol Data Unit

# CCM Mode

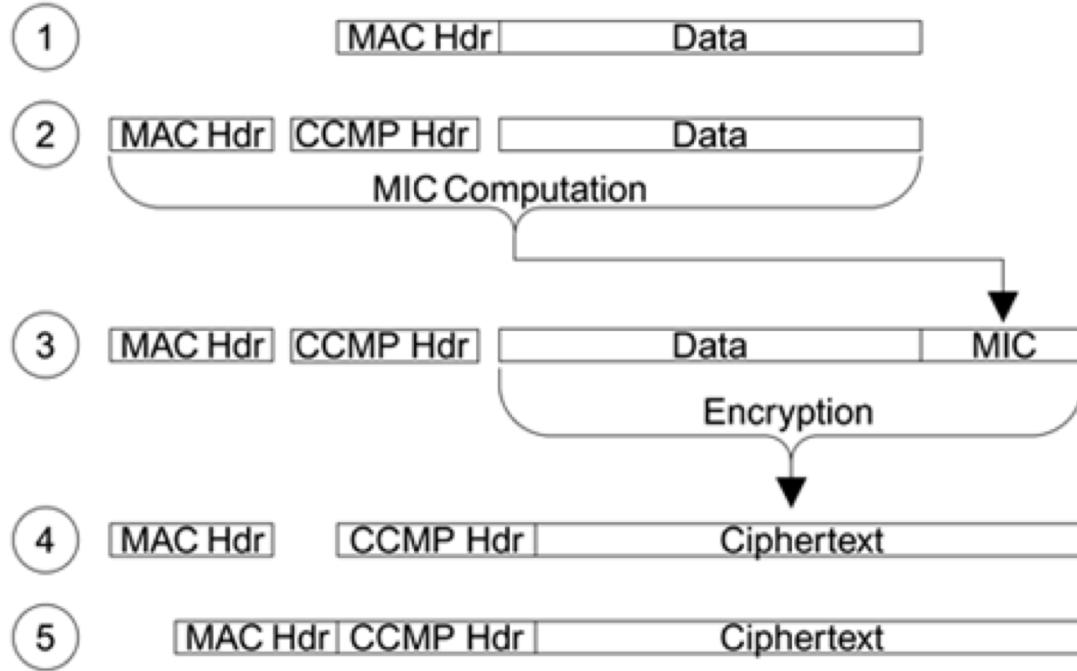
- *Authenticated encryption (with associated data)* care combină modul CTR mode cu CBC-MAC:
  - adaugă un CBC-MAC la header, lungimea header-ului și plaintext
  - cripteză în mod CTR (mesajul clar cu 1,2,3... și MIC cu valoarea counter 0)
- Folosește o singură cheie (*temporal key* partajată de STA și AP) și presupune 128-bit blocks



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

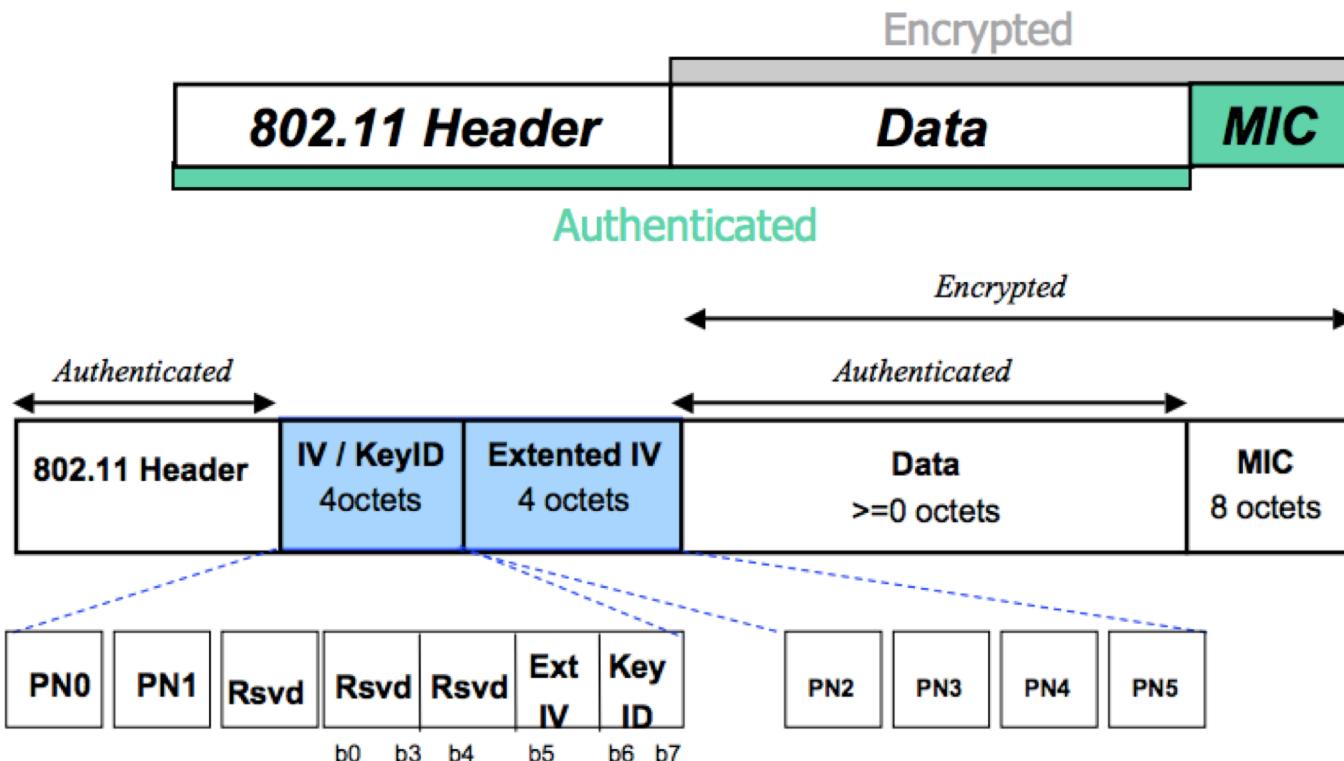
# CCMP

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



- 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

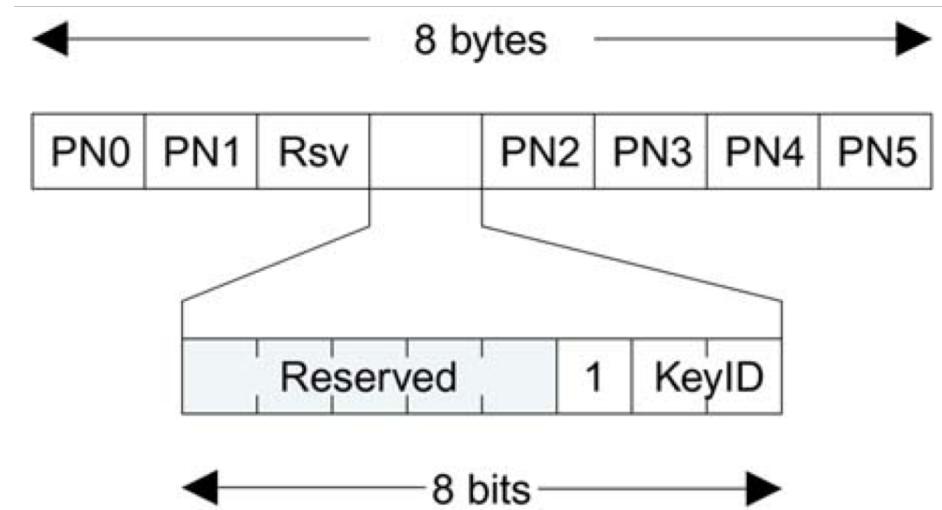


[Source: IEEE 802.11i Overview [http://ieee802.org/16/liaison/docs/80211-05\\_0123r1.pdf](http://ieee802.org/16/liaison/docs/80211-05_0123r1.pdf) ]

# CCMP Header

Rol:

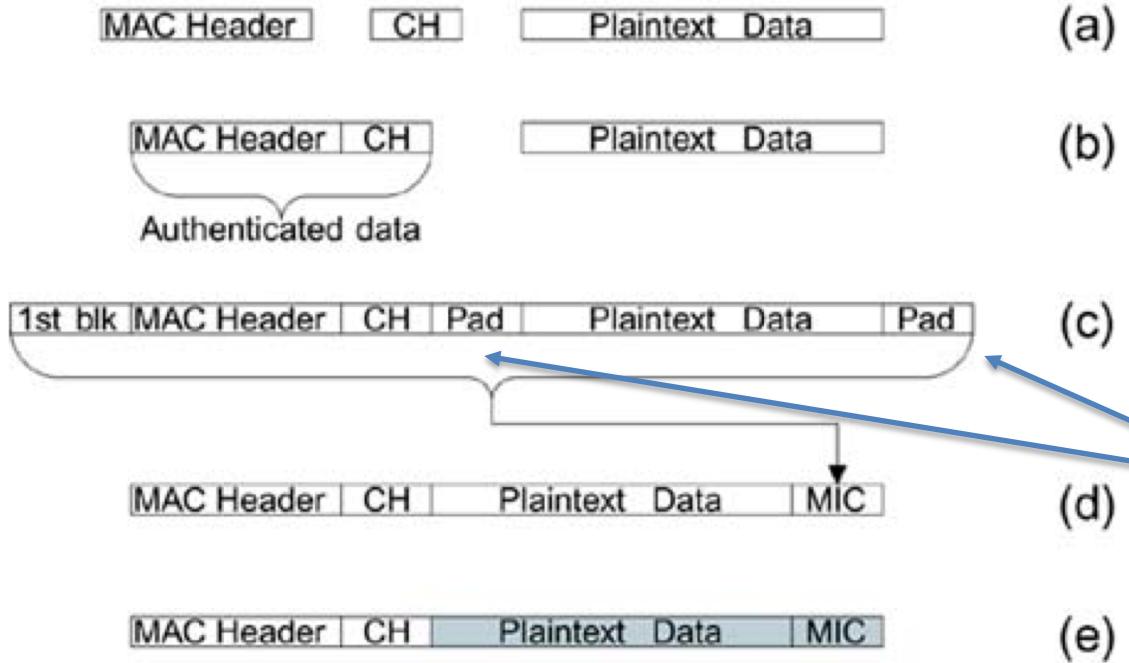
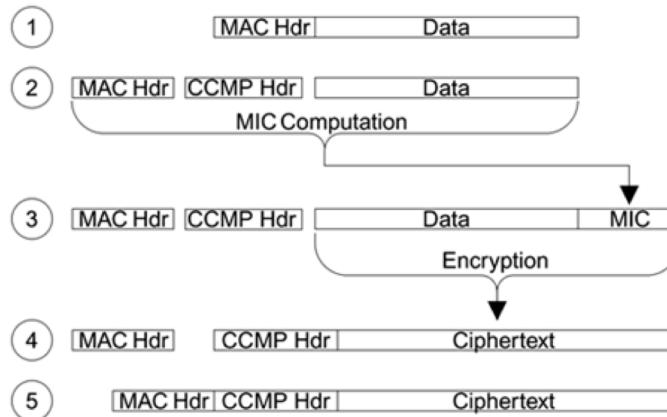
- Conține **Packet Number (PN)** care oferă *replay protection* și oferă la recepție nonce-ul necesar la decriptare
- În caz de multicast, transmite cheia de grup folosită la criptare



- 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]

# CCMP



CCMP requires both the Authenticated Data and Plaintext can be divided in exact blocks of 128 bits; for this padding with 0 is used

: Encrypted  
: Unencrypted

CH: CCMP Header

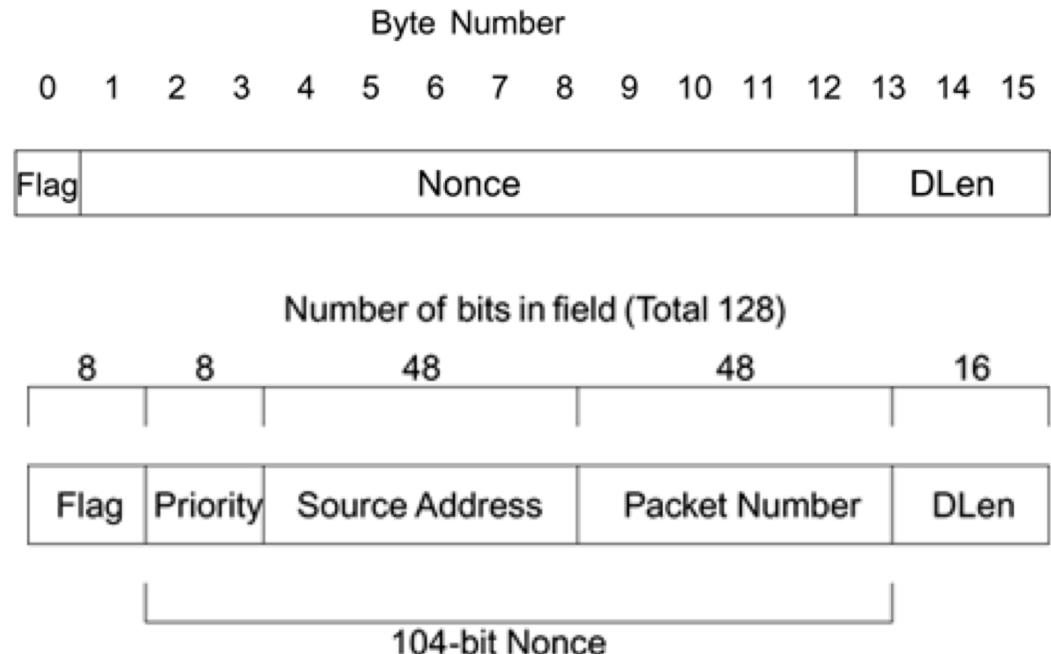
[Source: Course book, Edney & Arbaugh, Chapter 12]

# Calculul MIC

- Folosește **CBC-MAC**, cu un bloc de start (*starting block*)
- 64-bit (8 bytes) MIC, ultimii 64 bits sunt ignorați (aruncați)

**Starting block (IV)** se formează astfel:

- **Flag: 01011001** (fixed)
- **Nonce:** conține PN și adresa sursă pentru a garanta unicitate (PN ar fi putut fi deja utilizat de una dintre părțile comunicante într-o altă conversație); priority poate face referire la tipuri diferite (audio, video, etc.);
- **DLen:** lungimea datelor (Data Length)



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

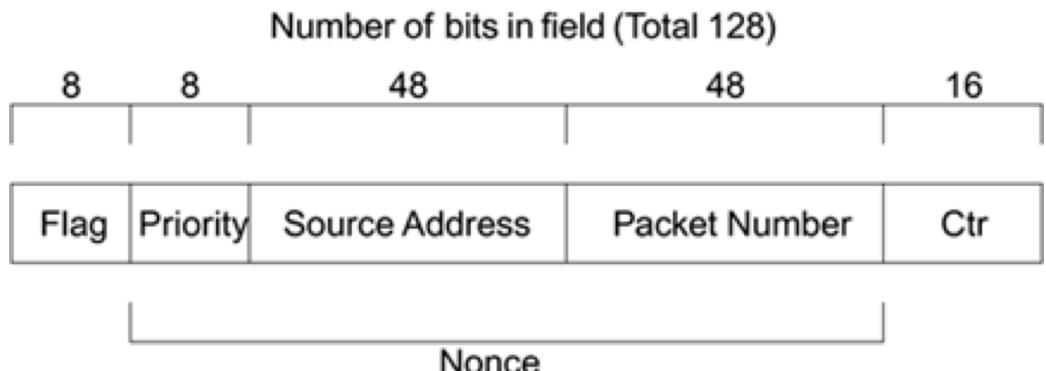
# Criptarea MPDU

- Folosește **CTR-AES**

## Counter block

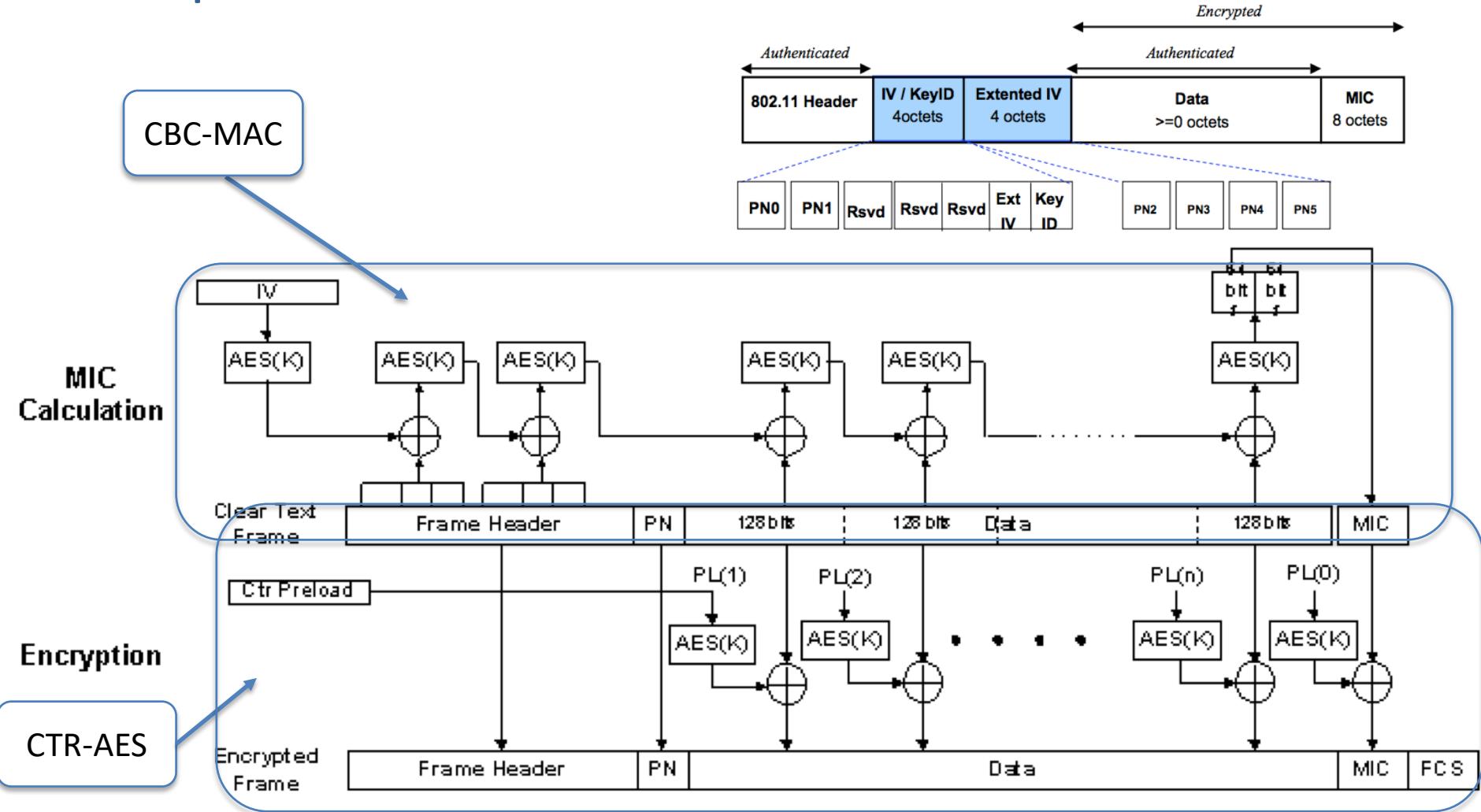
(PL0, PL1...):

- **Flag:** 01011001 (fixat)
- **Nonce:** conține PN și adresa sursă pentru a garanta unicitate (PN ar fi putut fi deja utilizat de una dintre părțile comunicante într-o altă conversație); priority poate face referire la tipuri diferite (audio, video, etc.);
- **Ctr:** starts at 1 and increases



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

# Encapsularea CCMP



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

# Key hierarchy

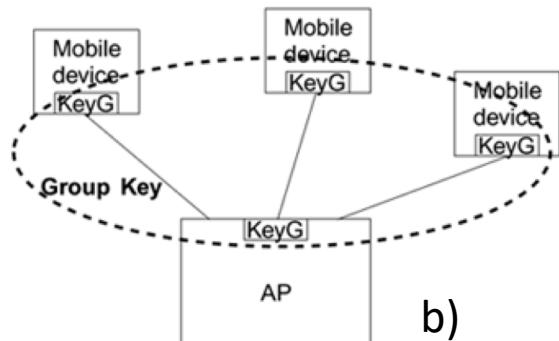
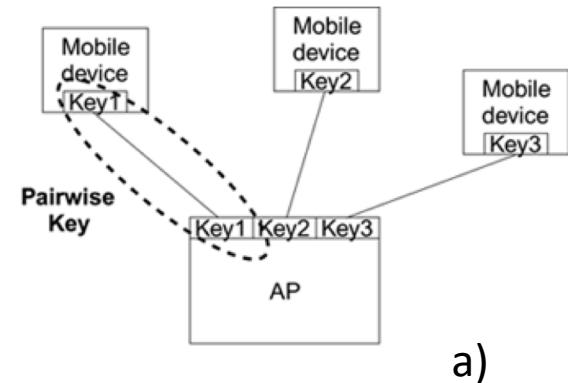
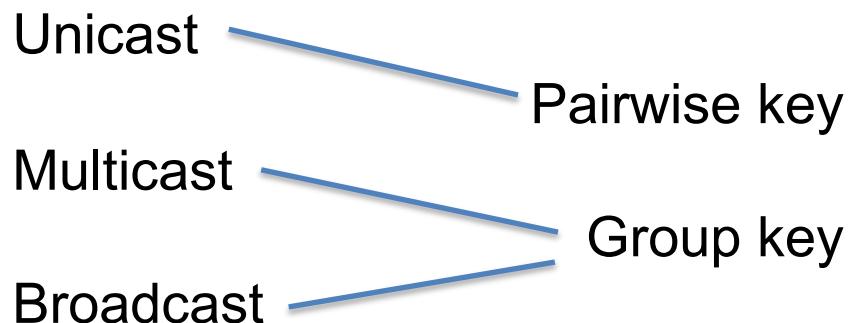
# Chei

Întrebare: Care dintre figurile din dreapta ilustrează *pairwise key* și care o cheie de grup (*group key*)?

Răspuns: a) Pairwise key; b) Group key

Question: Trasați corespondența dintre tipul mesajelor și tipul de cheie

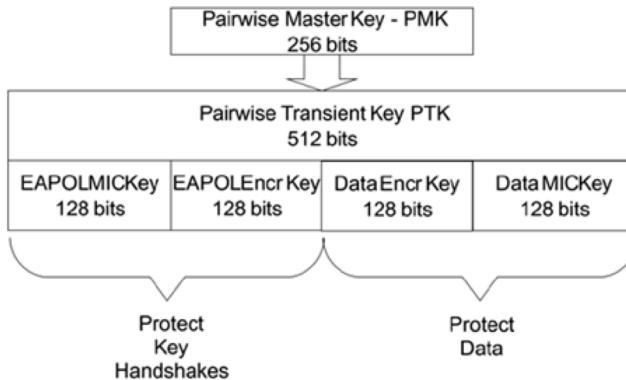
Answer:



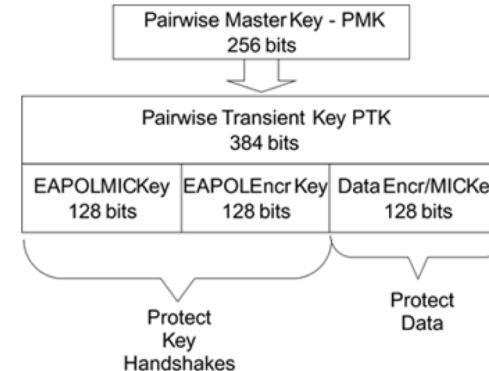
# Key Hierarchy (WPA TKIP vs WPA2/RSN AES-CCMP)

Pairwise

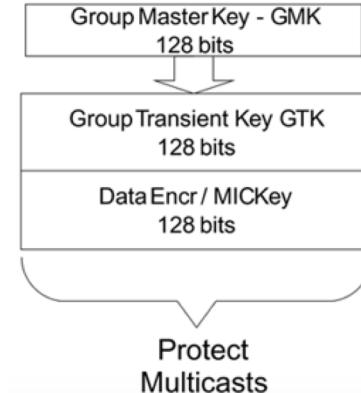
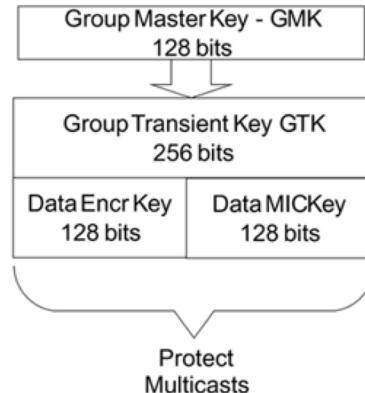
## WPA TKIP



## WPA2-RSN AES-CCMP



Group



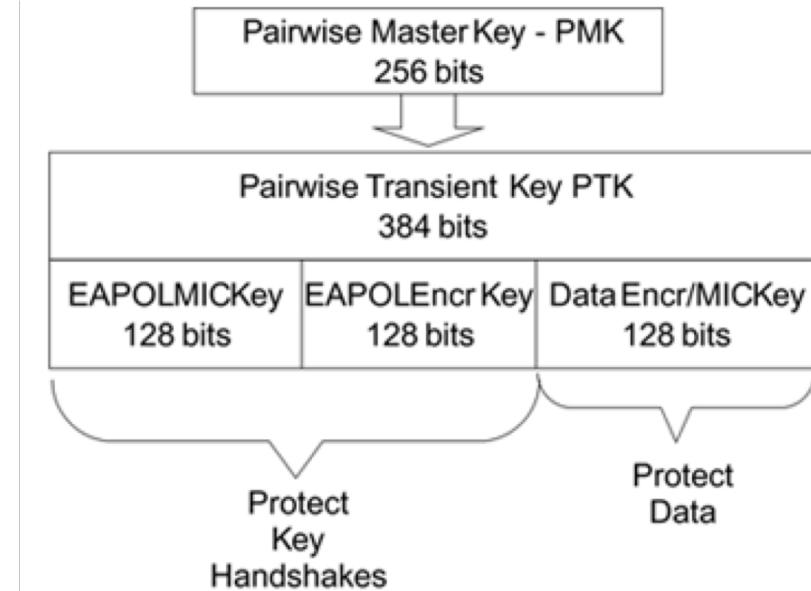
[Source: Course book, Edney & Arbaugh, Chapter 10]

More details in the course book – Edney & Arbaugh, Chapter 10

# Pairwise WPA2/RSN AES-CCMP Key Hierarchy

- **Pairwise Master Key (PMK):**

- 256 bits, cheie simetrică
- Preshared sau *upper layers authentication* (e.g.: transmis catre AP de serverul de autentificare)



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

- **Pairwise Transient Key (PTK):**

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

- **Temporal Keys:**

- 3 chei (128 bits):
  - EAPOL-keys: encryption key, integrity key
  - Data encryption and data integrity key (**o singură cheie!**)

# Group WPA2/RSN AES-CCMP Key Hierarchy

- Folosită pentru comunicare multicast and broadcast

- **Group Master Key (GMK):**
  - 256 bits, cheie simetrică
  - Generată de AP

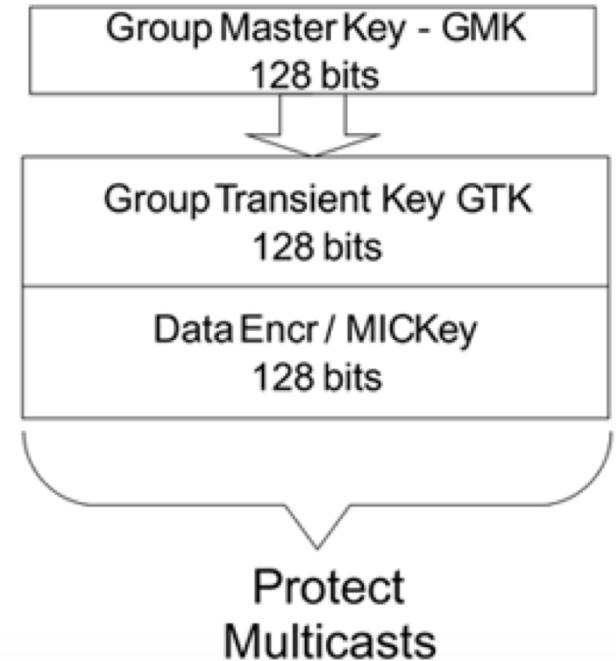
- **Group Transient Keys (GTK):**

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

- **Temporal Key:**

- Cheia pentru criptare și protecție a integrității pe 128 bits  
**(o singură cheie!)**

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



## 802.11 Key Derivation Function (KDF)

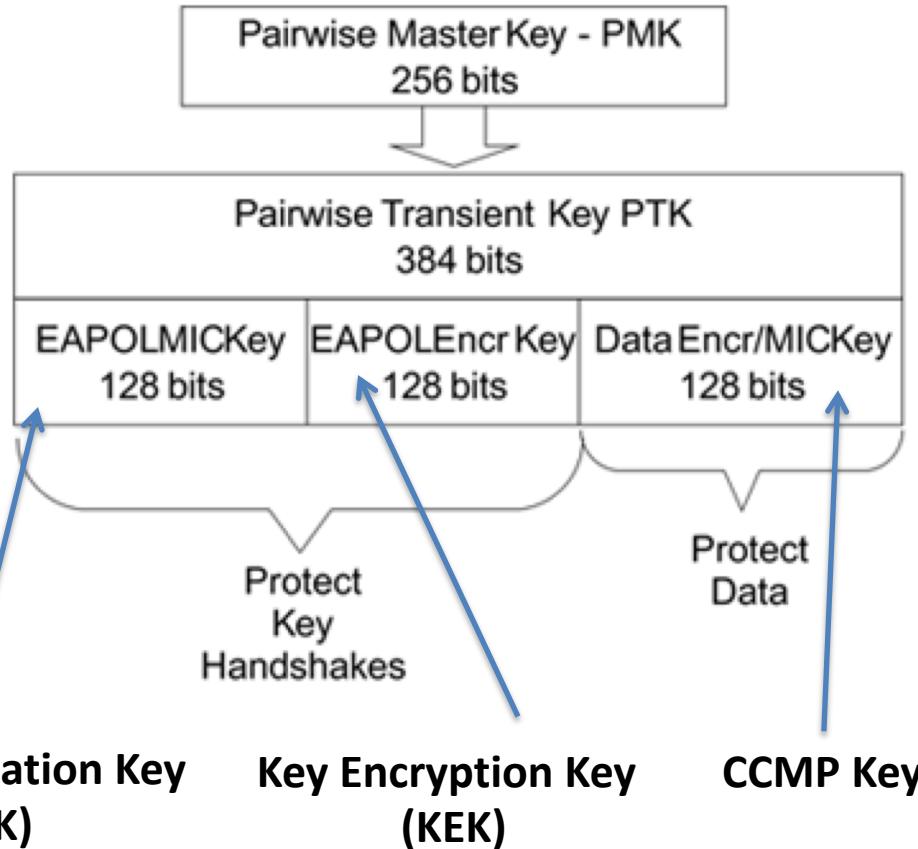
- $\text{PTK} \leftarrow \text{KDF}(\text{PMK},$

$$\min\{\text{Addr}_{AP}, \text{Addr}_{STA}\} \parallel \max\{\text{Addr}_{AP}, \text{Addr}_{STA}\}$$
$$\min\{N_{AP}, N_{STA}\} \parallel \max\{N_{AP}, N_{STA}\})$$

)

- KDF - **HMAC-SHA-1**

# Pairwise WPA2/RSN Key Hierarchy

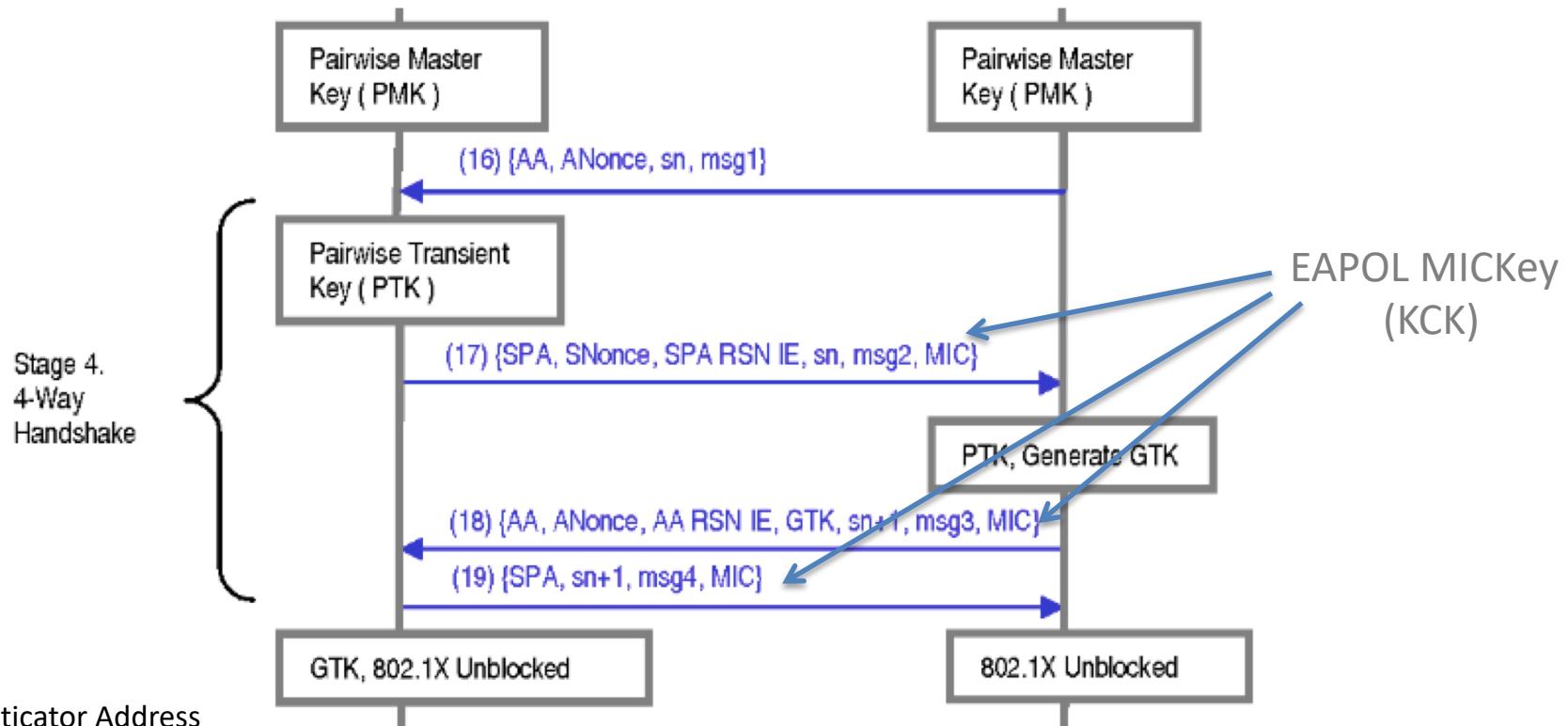


Folosite numai în 4WHS:

**KCK:** Pentru MAC handshake messages

**KEK:** Pentru criptarea cheii de grup

# 4-Way Handshake protocol



AA: Authenticator Address

SA: Suplicant Address

ANonce: nonce generated by  
the Authenticator (AP)

SNonce: nonce generated by  
the Suplicant (STA)

sn: sequence number

Encrypted data communication follows

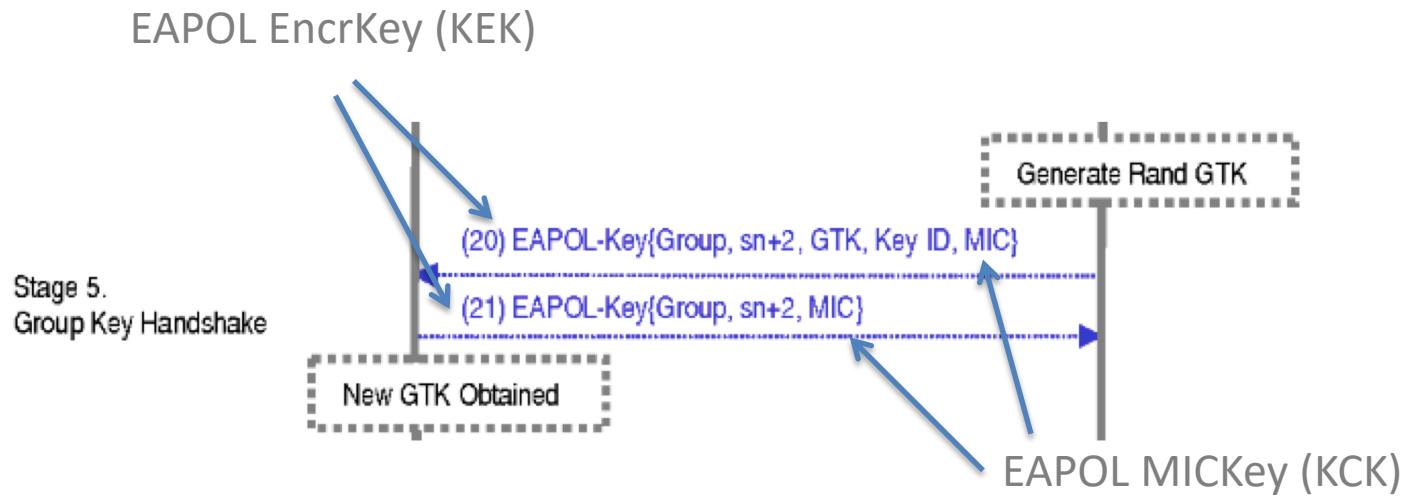
[Source: He and Mitchell Security Analysis and Improvements for IEEE 802.11i

<https://theory.stanford.edu/~jcm/papers/NDSS05.pdf> ]

## 4WHS - Proprietăți

- Nu prezintă **forward secrecy**
  - PMK + MAC-uri + Nonces sunt destul pentru a determina PTK
  - Se pot decripta comunicari trecute, înregistrate
- Vulnerabilitate la *dictionary attacks*
  - Dacă PMK este derivată din parole slabe
  - Captură MACs + Nonces → ghicește password → determină 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

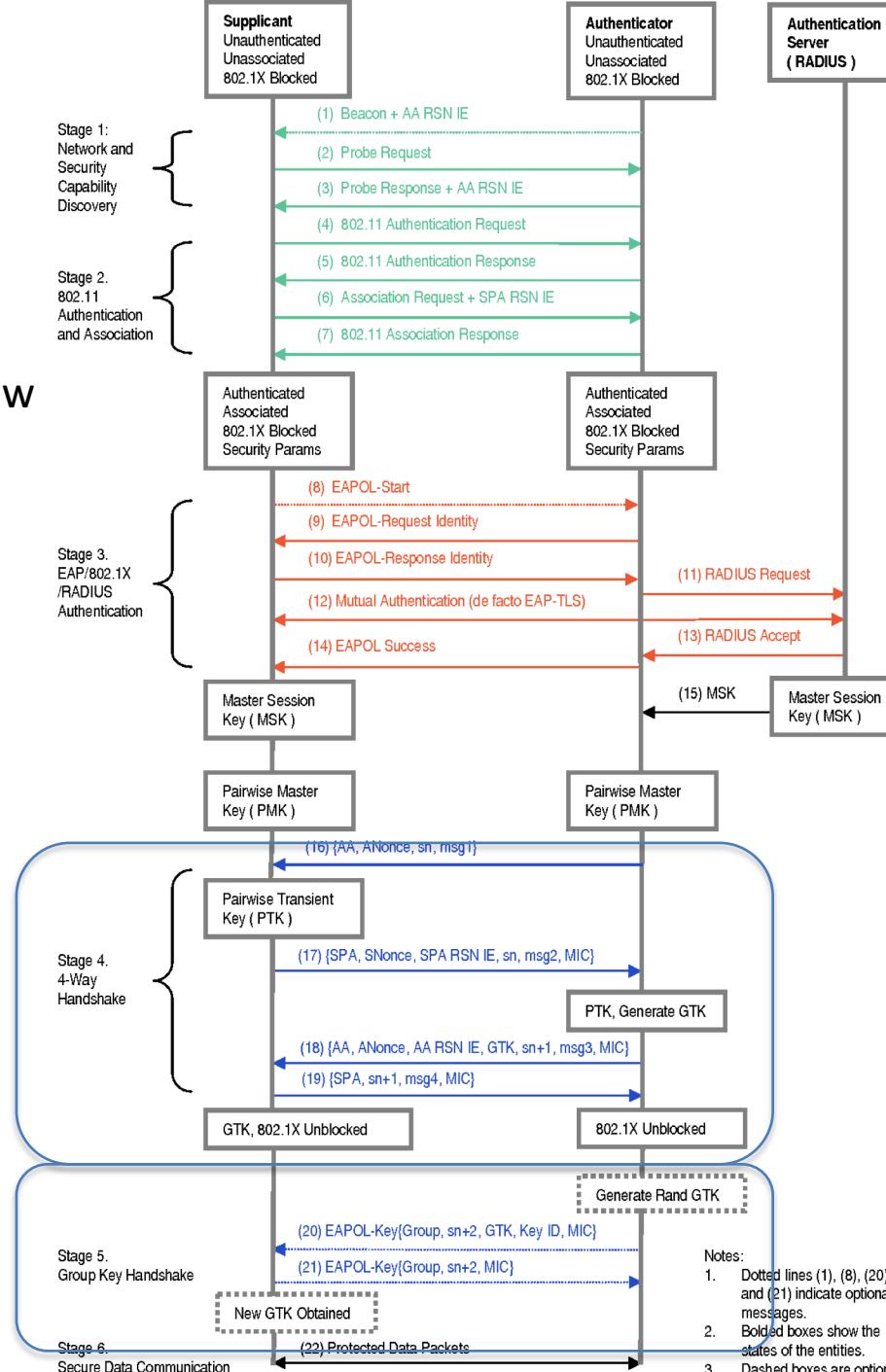
RSN IE: RSN Identification Element (set of capabilities)

AA: Authenticator Address

SA: Suplicant Address

ANonce: nonce generated by the Authenticator (AP)

SNonce: nonce generated by the Suplicant (STA)

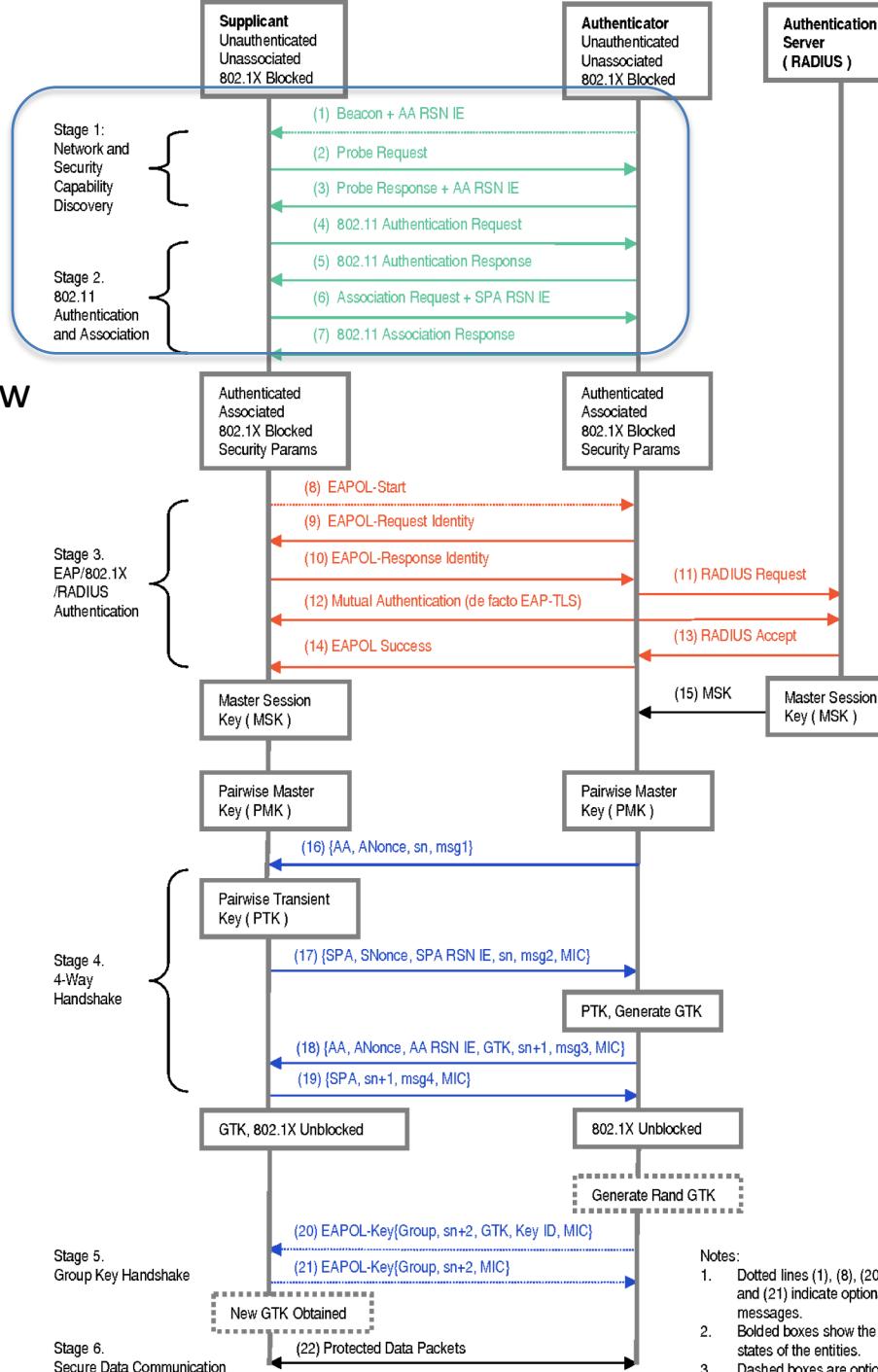


[Source: He and Mitchell Security Analysis and Improvements for IEEE 802.11i  
<https://theory.stanford.edu/~icm/papers/NDSS05.pdf> ]

# 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/~icm/papers/NDSS05.pdf> ]

# RSN/ WPA2

## Association Overview

Both parties  
prove to know the  
same MSK

RSN IE: RSN Identification

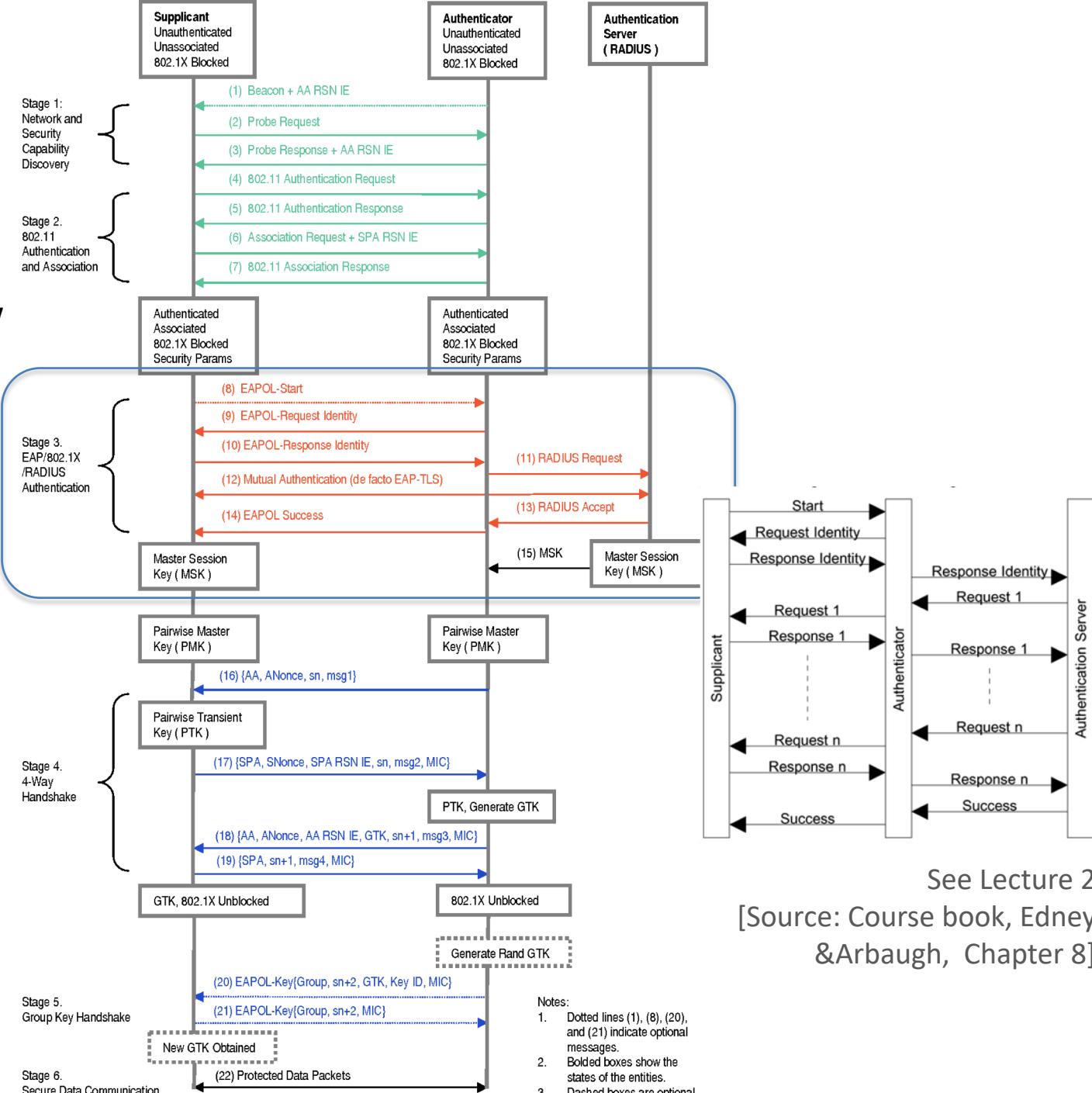
Element (set of capabilities)

AA: Authenticator Address

SA: Supplicant Address

ANonce: nonce generated by  
the Authenticator (AP)

SNonce: nonce generated by  
the Supplicant (STA)



See Lecture 2

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

# RSN/ WPA2

## Association Overview

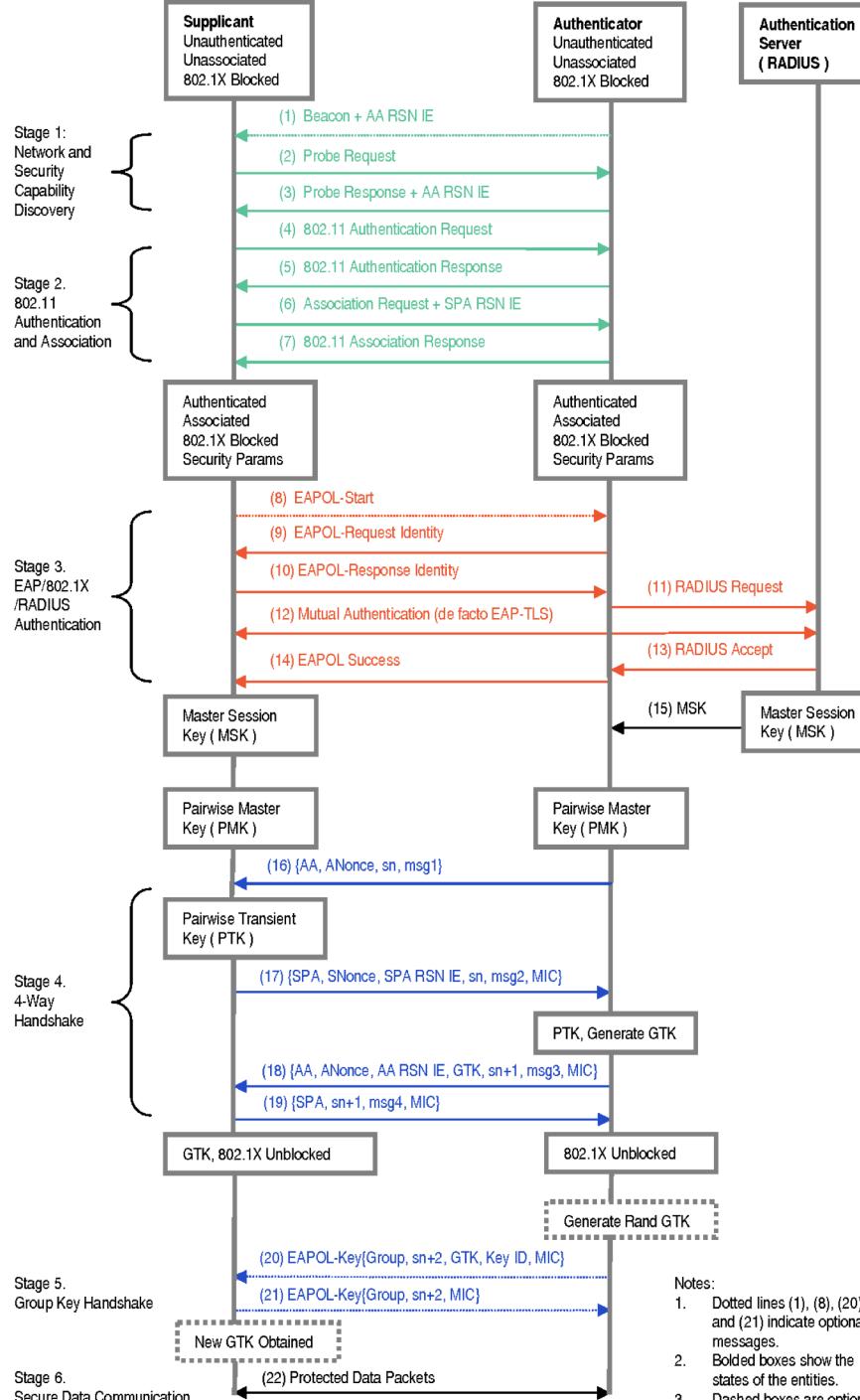
RSN IE: RSN Identification Element (set of capabilities)

AA: Authenticator Address

SA: Suplicant Address

ANonce: nonce generated by the Authenticator (AP)

SNonce: nonce generated by the Suplicant (STA)

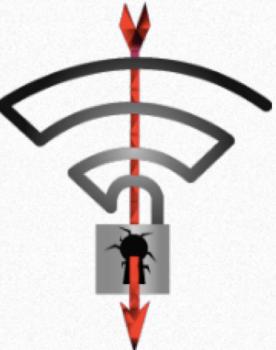


[Source: He and Mitchell Security Analysis and Improvements for IEEE 802.11i  
<https://theory.stanford.edu/~icm/papers/NDSS05.pdf> ]

# Securitate

# Securitate

- 802.11i protejează numai frame-uri de date (nu control, etc.)
- Fară *forward secrecy*
- ...



# 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>

# Overview

Interesant de citit: 802.11i overview - doc.: IEEE 802.11-04/0123r1  
[http://ieee802.org/16/liaison/docs/80211-05\\_0123r1.pdf](http://ieee802.org/16/liaison/docs/80211-05_0123r1.pdf)



# Securitatea rețelelor

## - Prelegerea 7 -

### Upper Layer Authentication

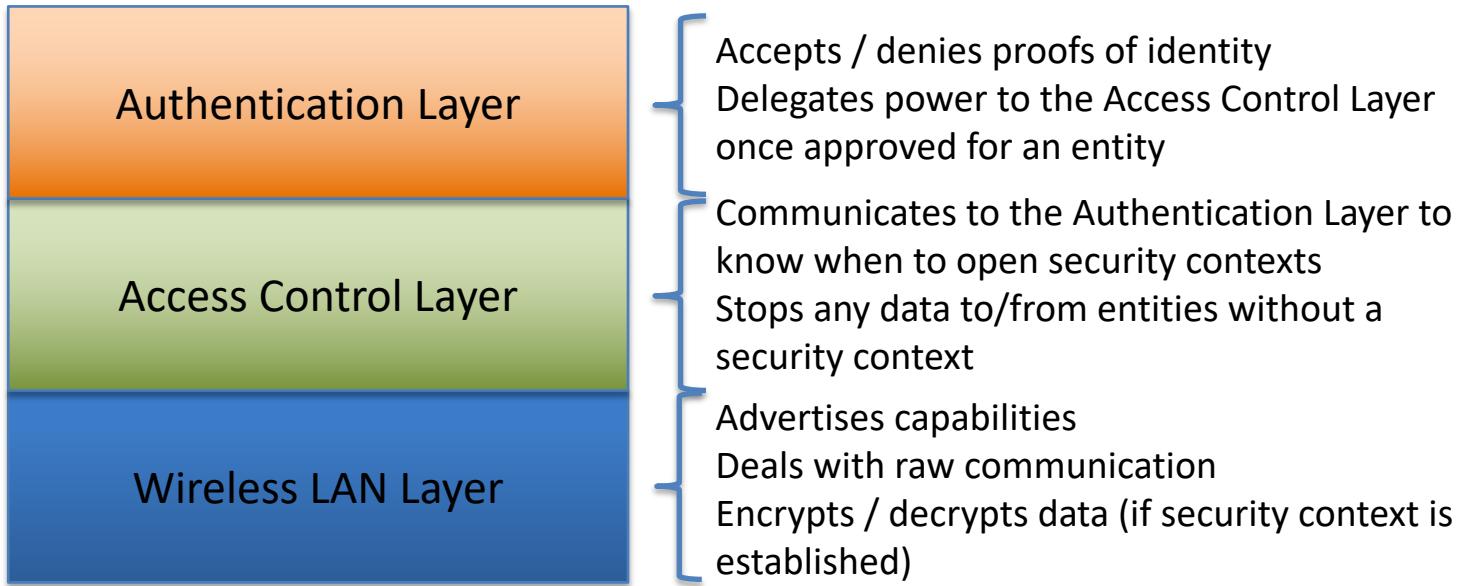
Ruxandra F. Olimid

Facultatea de Matematică și Informatică  
Universitatea din București

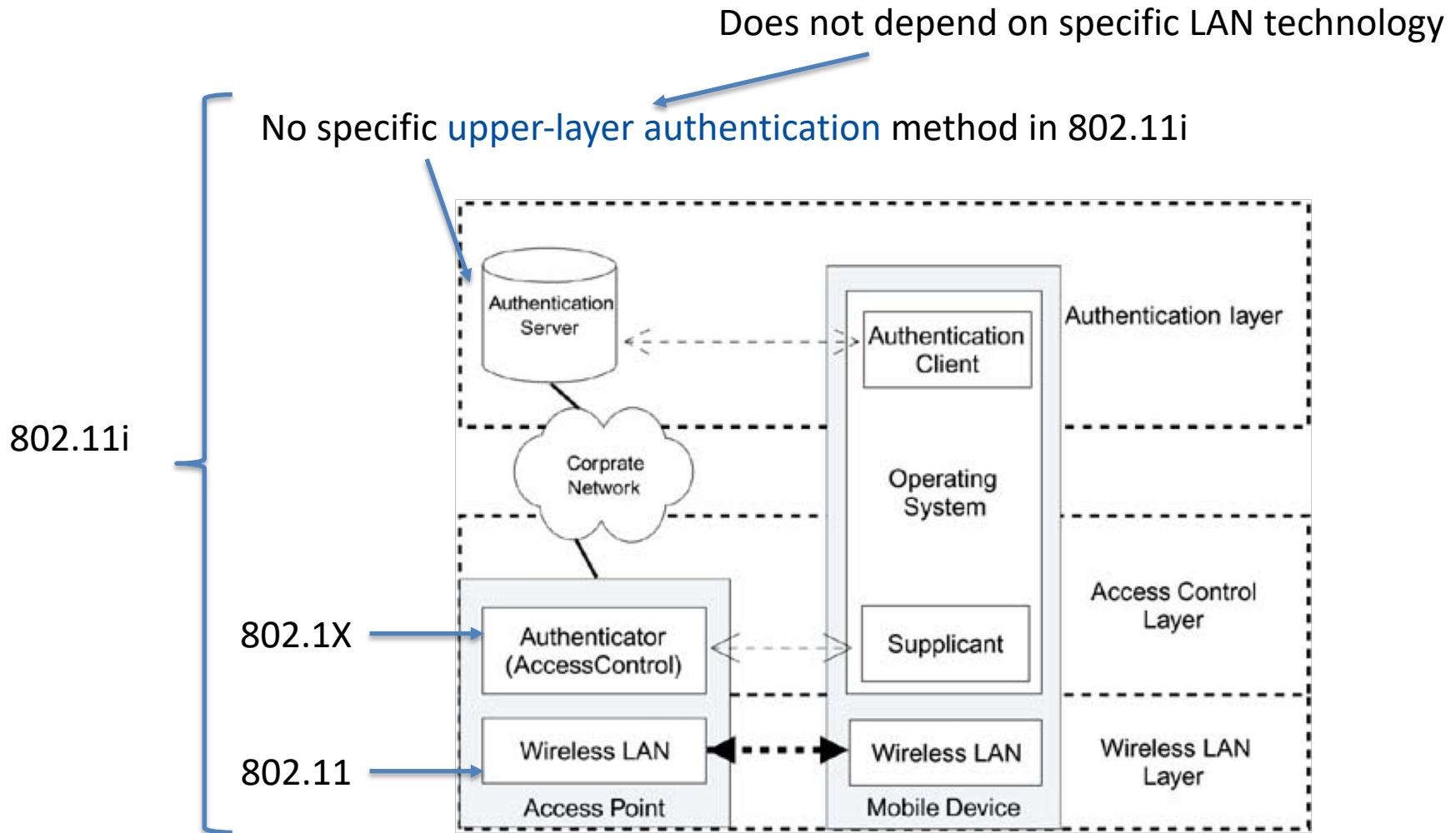
# Cuprins

1. Nivele de securitate
2. WPA2-Personal (WPA2-PSK) and WPA2-Enterprise
3. Upper-layer authentication

# Nivele de securitate



# Nivele de securitate



[Source: Course book, Edney & Arbaugh, Chapter 7]

# RSN/ WPA2

## Association Overview

Upper-layer authentication:  
**Ambele parti demonstreaza ca stiu aceeasi MSK**

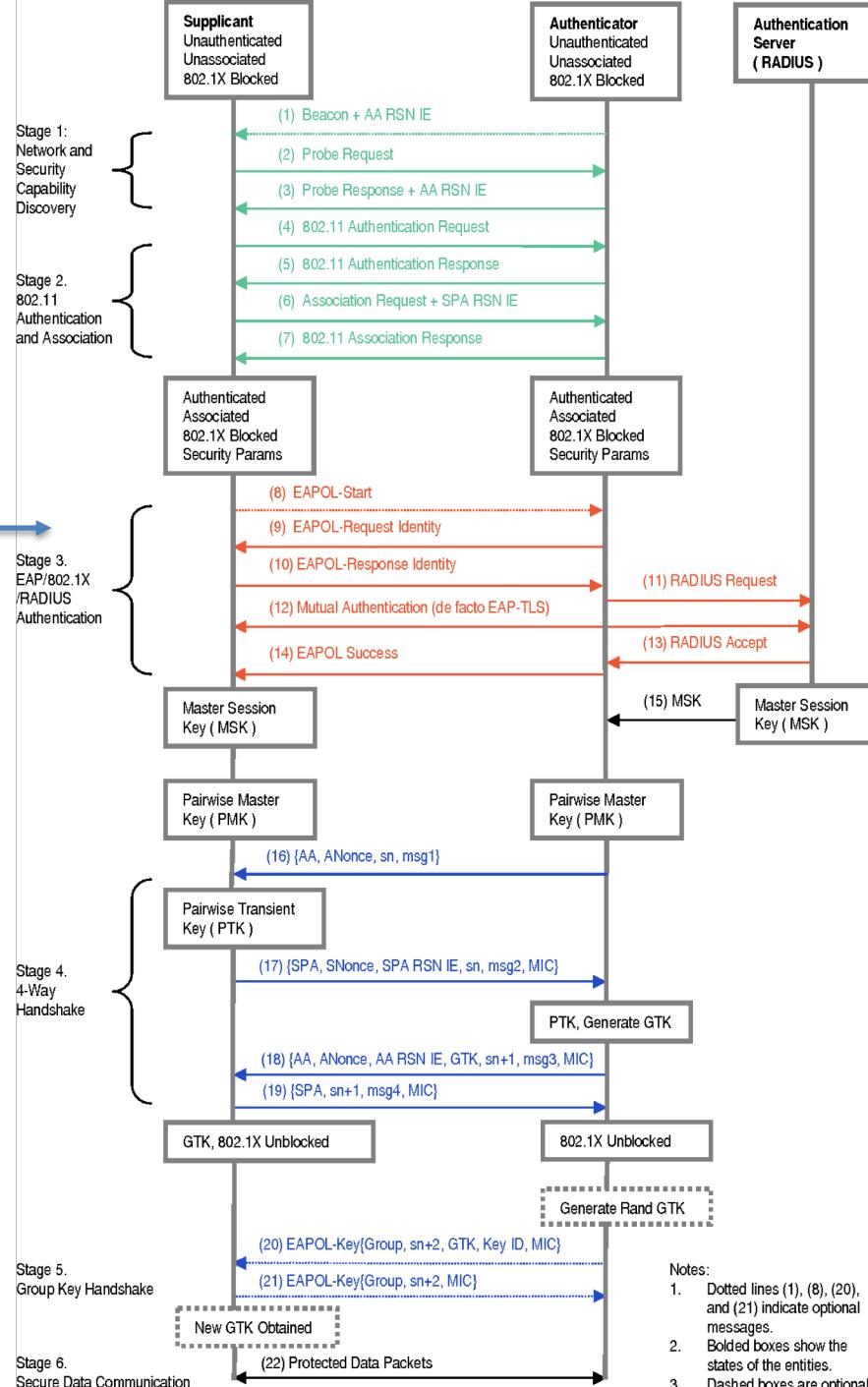
RSN IE: RSN Identification Element (set of capabilities)

AA: Authenticator Address

SA: Suplicant Address

ANonce: nonce generated by the Authenticator (AP)

SNonce: nonce generated by the Suplicant (STA)



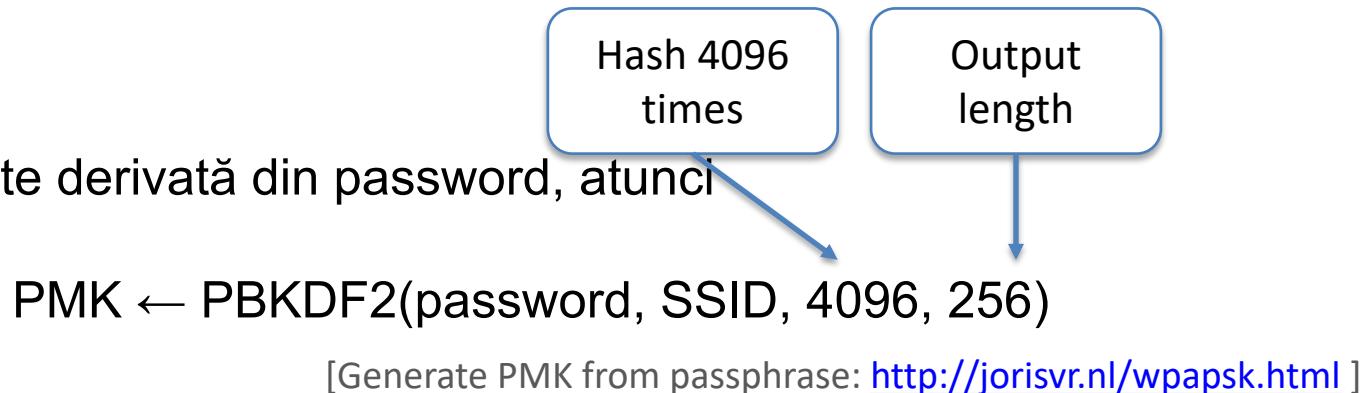
[Source: He and Mitchell Security Analysis and Improvements for IEEE 802.11i  
<https://theory.stanford.edu/~icm/papers/NDSS05.pdf> ]

# Upper-layer Authentication

- Scop:
  - Demonstrează că fiecare parte cunoaște o cheie / parolă secretă asociată identității sale (e.g.: password)
  - Oferă chei necesare pentru un context de securitate (*security context*)
  - Satisfac obiectivele fără să scurgă informație despre cheia / parola asociată
- **Întrebare:** Cum se partajează PMK între entitățile din WLAN?
- Cu Pre-Shared Key (PSK)  **WPA2-Personal (WPA2-PSK)**  
• Cu authentication server  **WPA2-Enterprise**

# WPA2-PSK: Problema 1 – Scalabilitate, Dinamicitate

- Aceeași valoare PSK (=PMK) pentru toate entitățile din WLAN



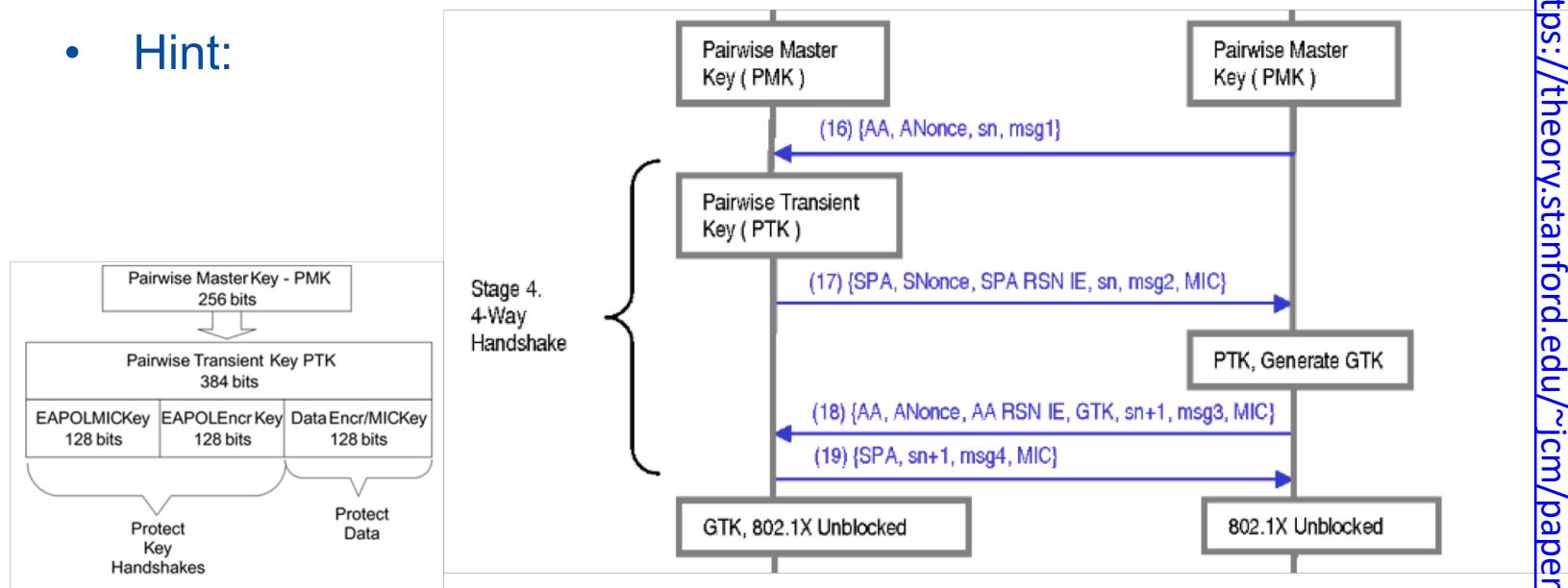
- Dacă PMK este derivată din password, atunci

- **Întrebare:** Ce probleme vedeți aici?
- **Răspuns:**

- PSK trebuie să fie manual instalată pe APs și STAs, deci **nu e scalabil** (?!)
- La modificarea password, toate echipamentele trebuie update
- Dacă un echipament este compromis, toate sunt compromise

# WPA2-PSK: Problema 2 - Insider Attack

- Întrebare: De ce WPA2-PSK e vulnerabil la *insider attack*?
- Hint:



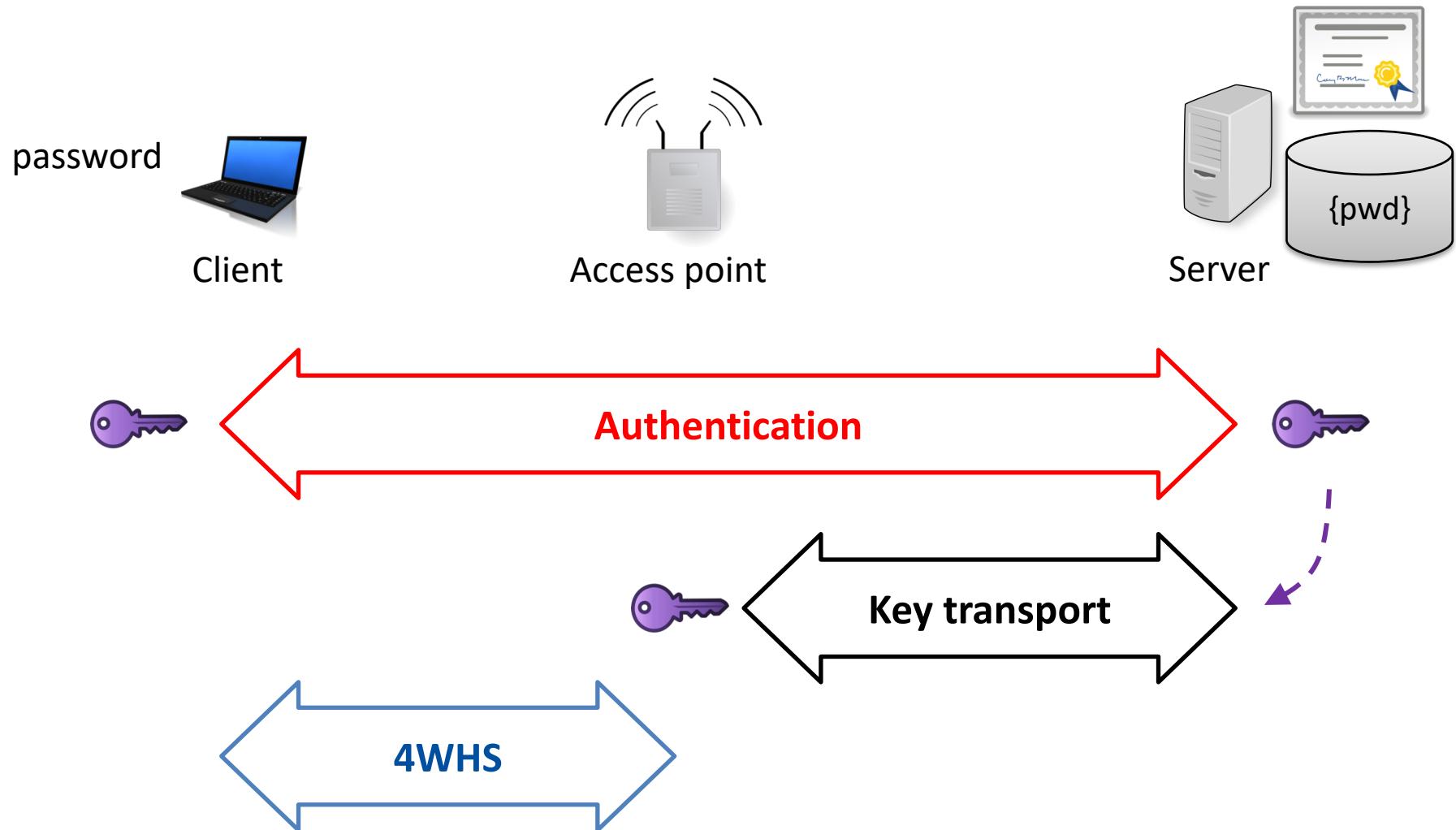
- Răspuns: Un *insider* poate să asculte valorile nonce și determină cheia CCMP, deci atât confidențialitatea cât și integritatea sunt compromise

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

## WPA2-PSK: Problema 3 - Outsider Attack

- **Întrebare:** De ce este WPA2-PSK vulnerabil (*outsider attack*) dacă PSK este o parolă slabă?
- **Răspuns:** E vulnerabil la *dictionary attack*

# WPA2-Enterprise

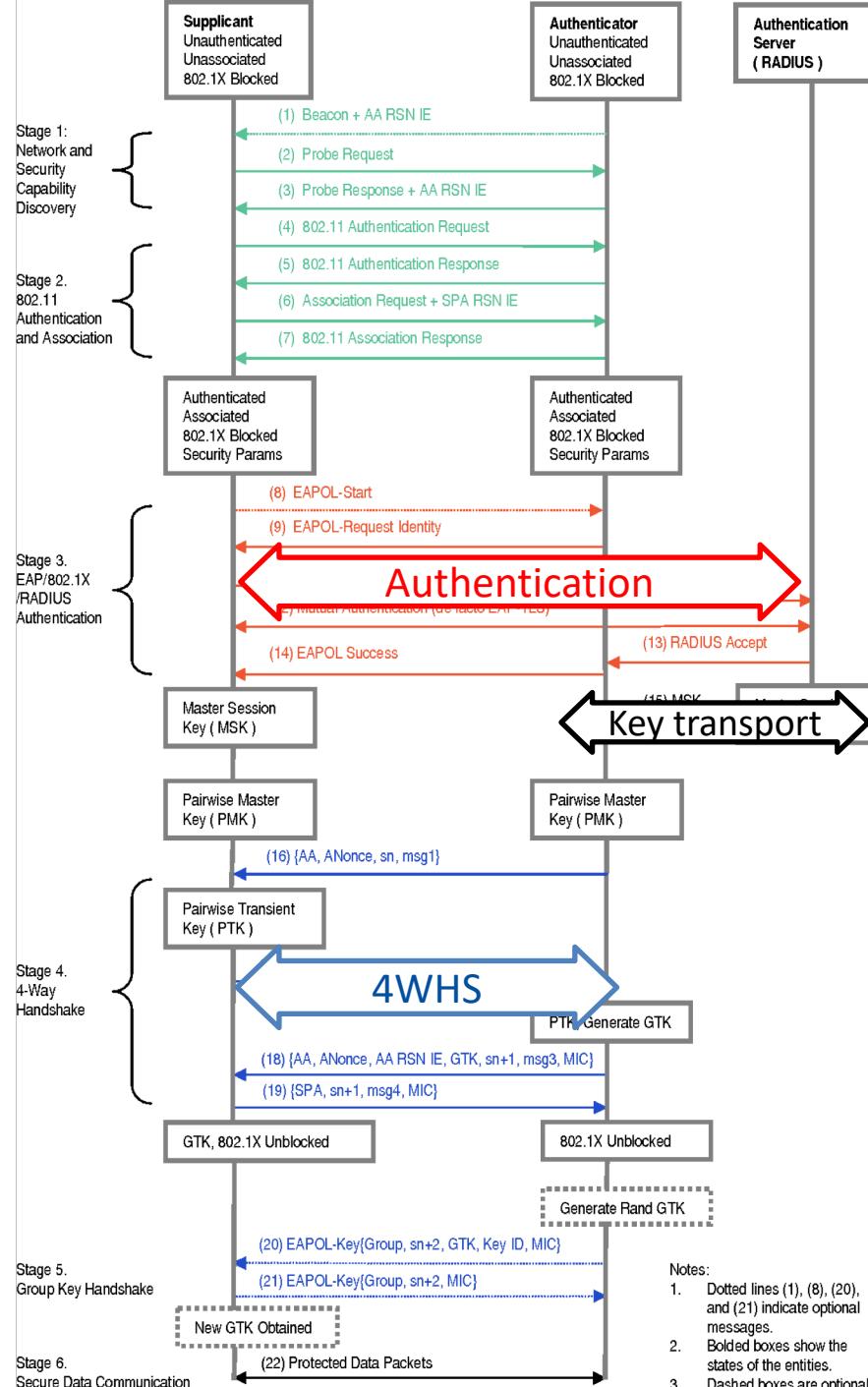


[Slide ack: Håkon Jacobsen]

# RSN/ WPA2

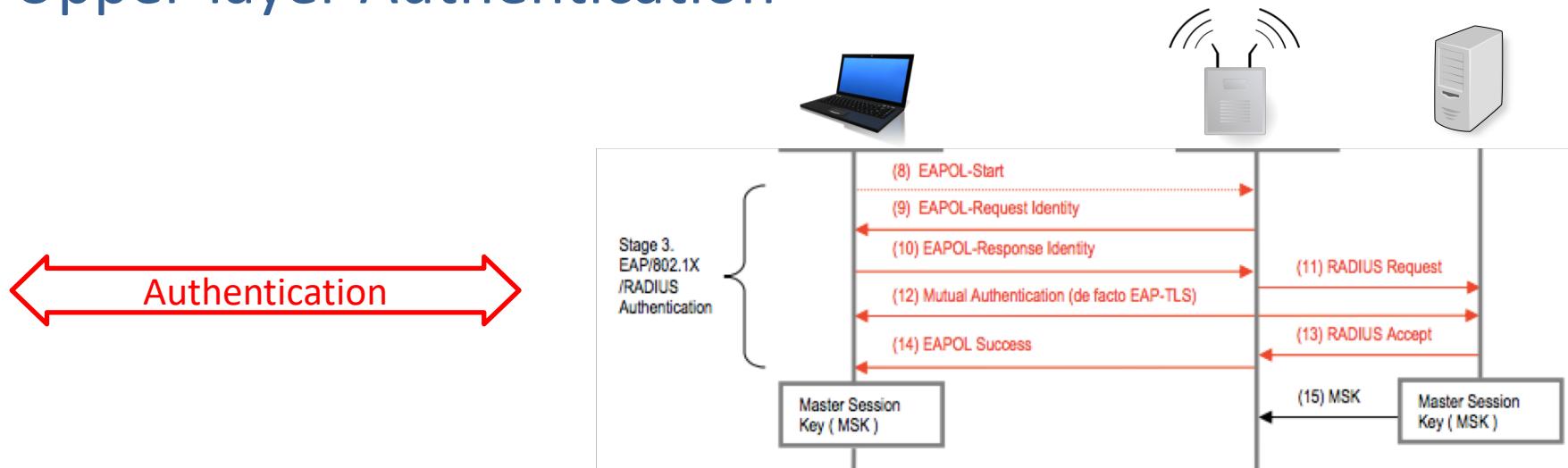
## Association Overview

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/~icm/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)

# EAP Methods

802.1X EAP Types	MD5 --- Message Digest 5	TLS --- Transport Level Security	TTLS --- Tunneled Transport Level Security	PEAP --- Protected Transport Level Security	FAST --- Flexible Authentication via Secure Tunneling	LEAP --- Lightweight Extensible Authentication Protocol
Client-side certificate required	no	yes	no	no	no (PAC)	no
Server-side certificate required	no	yes	no	yes	no (PAC)	no
WEP key management	no	yes	yes	yes	yes	yes
Rogue AP detection	no	no	no	no	yes	yes
Provider	MS	MS	Funk	MS	Cisco	Cisco
Authentication Attributes	One way	Mutual	Mutual	Mutual	Mutual	Mutual
Deployment Difficulty	Easy	Difficult (because of client certificate deployment)	Moderate	Moderate	Moderate	Moderate
Wi-Fi Security	Poor	Very High	High	High	High	High when strong passwords are used.

[Source: Intel - 802.1X Overview and EAP Types

<https://www.intel.com/content/www/us/en/support/articles/000006999/network-and-i-o/wireless-networking.html> ]



# Securitatea rețelelor

- Prelegerea 8 -

Global System for Mobile Communication  
(GSM)

Ruxandra F. Olimid

Facultatea de Matematică și Informatică  
Universitatea din București

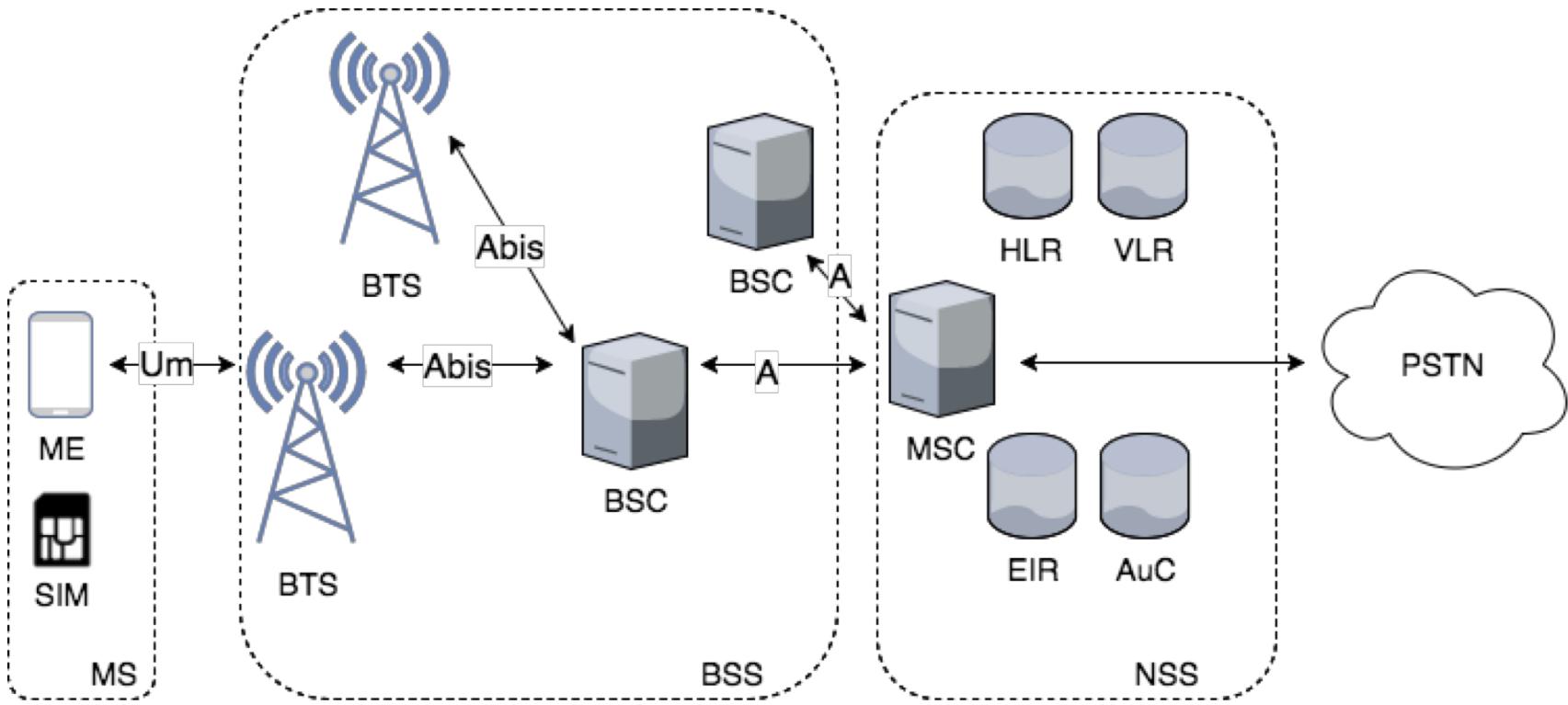
# Cuprins

1. Arhitectura GSM
2. Arhitectura de Securitate GSM
3. Principii de Securitate si implementare
4. Vulnerabilități și atacuri



[Source: <http://www.gsm-history.org/54.html>]

# Architectura GSM



MS: Mobile Station

ME: Mobile Equipment

SIM: Subscriber Identity Module

PSTN: Public Switched Telephone Network

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

# Architectura GSM

- **MS (Mobile Station):**
  - Mobile Equipment (ME) și Subscriber's Identity Module (SIM)
- **BSS (Base Station Subsystem):**
  - Conține BTS-uri și BSC-uri
  - BSC este un element central care controlează rețeaua radio, menține conectivitatea radio cu mai multe BTS-uri și realizează conectarea la 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 este elementul de rețea principal din NSS pentru realizarea apelurilor, fiind responsabil de call control, BSS control, și interconectarea cu alte rețele (PSTN)

# Architectura GSM

- **VLR (Visitor Location Register):**
  - Stochează informație despre subscriberii care sunt deserviți de MSC (păstrează copii ale datelor din HLR, crescând eficiența: scade numărul de mesaje schimbat între MSC și HLR)
  - De obicei nu este independent, ci o componentă software a MSC
- **HLR (Home Location Register):**
  - Este baza de date principală în GSM
  - Conține informații despre fiecare subscriber: IMSI, număr de telefon - Mobile Station International Subscriber Directory Number (MSISDN), servicii disponibile subscriberului, locație, etc.
- **AuC (Authentication Center):**
  - Pentru fiecare subscriber, stochează cheia permanentă  $K_i$ , care este de asemenea stocată și în SIM
  - Generează vectorii de autentificare (RAND, SRES,  $K_C$ )

# Architectura GSM

- **EIR (Equipment Identity Register):**

- Inventariază echipamentele din rețeaua mobilă, care sunt identificate prin IMEI
- Păstrează 3 liste:



- *White list*: conține echipamentele care sunt acceptate de operator și pot accesa fără restricții rețeaua mobile



- *Black list*: conține echipamentele care au fost raportate ca furate sau care au dovedit că afectează funcționalitatea rețelei și sunt restrictionate să acceseze rețeaua mobilă



- *Gray list*: conține echipamentele care nu sunt total compliant cu operatorul, dar pot accesa rețeaua sub supraveghere

# GSM –Principii de securitate

**Scop:** Rețeaua GSM trebuie să fie la fel de sigură ca rețeaua fixă (PSTN) ...  
...dar, securitatea nu trebuie să aibă un impact

Vom întâlni aceeași limitare la LTE, unde 3GPP nu a considerat PKI o soluție fiabilă

## Principii de securitate în GSM:

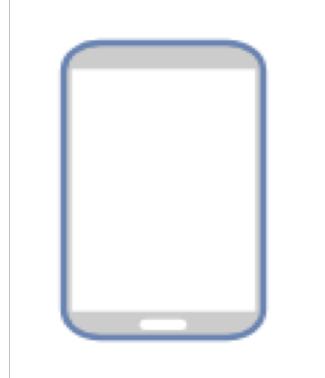
- **Controlul accesului la MS:** permite accesul autorizat al utilizatorului la stația mobilă
- **Anonimitatea abonaților (privacy):** păstrează identitatea abonaților (precum și locația, apelurile, etc.) ascunsă unor entități neautorizate
- **Autentificarea abonaților:** abonații trebuie să dovedească identitatea pentru a avea drept de access la serviciile mobile
- **Confidențialitatea:** păstrarea confidențialității pe link-ul radio

# GSM –Principii de securitate

## Vulnerabilități în securitatea GSM:

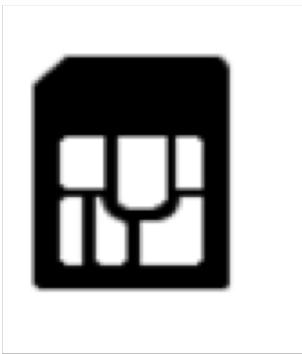
- *Kerckhoffs' principle*: algoritmii criptografici nu au fost făcuți publici (e.g., A5/1, A5/2)
- *Chei criptografice scurte*: vulnerabilitate la *brute force* (*căutare exhaustivă*)
- *Criptare limitată*: datele sunt criptate doar pe o porțiune
- *Autentificare unilaterală*: Stația mobilă nu autentifică rețeaua, doar rețeaua autentifică stația mobilă
- Nu se tratează *integritatea datelor*
- *Atacuri active*; e.g.: IMSI Catchers, când un adversar imparsonează un BTS
- *Utilizatorii nu sunt (în general) notificați despre nivelul de securitate*

# Echipamentul mobil



- **Identificare:**
  - **IMEI** (International Mobile Equipment Identity), un număr care identifică telefonul mobil (slot-ul SIM); este scris pe echipament, și poate fi afișat prin apelarea \*#06#
  - **IMEISV** (IMEI Software Version) de obicei înlătură ultimul digit (check digit) din IMEI și adaugă 2 digits pentru SVN (Software Version Number)
- **Controlul accesului (access control):**
  - IMEI poate fi utilizat pentru a preveni conectivitatea la rețea pentru telefoanele furate (prin adăugare în black list)
  - Autentificarea biometrică; e.g., fingerprint recognition, voice recognition
  - Mecanisme de deblocare a ecranului; e.g., coduri, patterns

# SIM



## Identificare:

- **IMSI** (International Mobile Subscriber Identity), un identificator global al abonatului (subscriber-ului)  $\cong 15$  digits
- **ICCID** (Integrated Circuit Card ID) identificatorul pentru SIM fizic, printat pe SIM
- **Controlul accesului:**
  - **PIN** (Personal Identification Number), o secvență de numere necesare pentru deblocarea SIM
  - **PUK** (Personal Unlocking Key), un cod necesar când PIN a fost introdus greșit de prea multe ori

## 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

List of MCCs and MNCs: <http://mcc-mnc.com/>

# SIM



## Autentificare și confidențialitate:

- **IMSI** (International Mobile Subscriber Identity)
- **TMSI** (Temporary Mobile Subscriber Identity), un id temporar folosit pentru minimalizarea expunerii IMSI
- $K_i$  o cheie permanentă pe 128 biți
- Mecanisme criptografice: un mecanism de tip *challenge-response* care folosește cheia permanentă pentru autentificarea abonaților și un *algoritm de derivare al cheilor* pentru confidențialitatea comunicației

Cardul SIM trebuie să fie tamper-resistant (i.e. un adversary nu poate să citească / modifice informația sigură stocată în SIM). În caz contrar, cardul SIM devine vulnerabil la cloning attacks caz în care adversarul crează copii ale cardului SIM pentru utilizare în diferite scopuri (eavesdropping, inițierea de apeluri, etc.)

\*Terminologie: Initial, cardul fizic se numea el însuși SIM, mai târziu a preluat denumirea de UICC (Universal Integrated Circuit Card) iar prin SIM se înțeleg aplicațiile care sunt prezente pe card

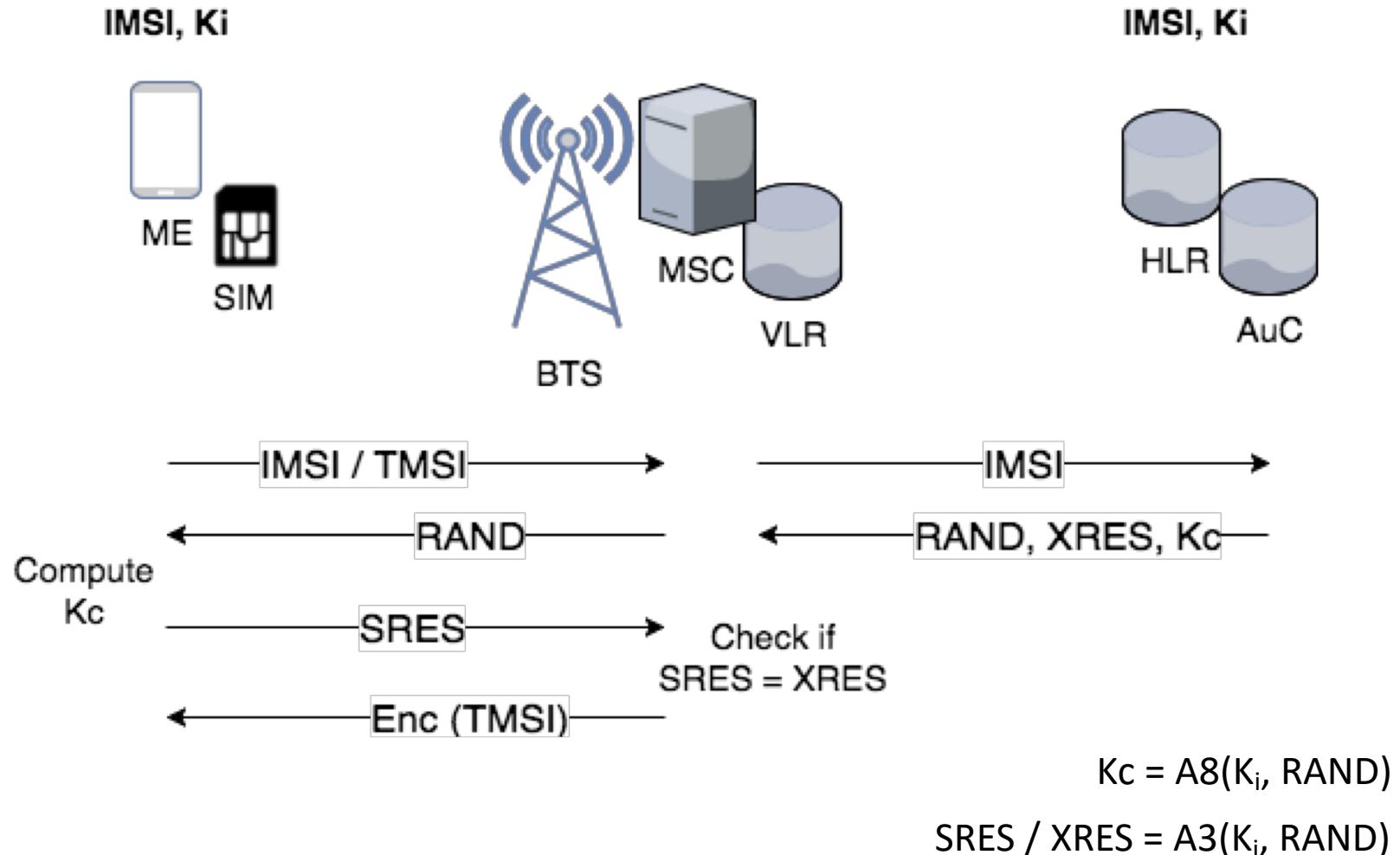
# Anonimitatea abonaților

- **Scop:** Menținerea privată a identității abonaților (și indirect prezența / absența lor într-o locație, etc.)
- Un abonat se poate identifica prin :
  - **IMSI** – identitatea permanentă
  - **TMSI** – identitatea temporară
- **Principii:**
  - Introduce TMSI ca o modalitate de a reduce expunerea IMSI pe interfața radio
    - e.g., IMSI identifică în mod unic un abonat și interceptarea acestuia este suficientă pentru a dovedi prezența într-o locație
  - TMSI este alocat stației mobile când se autentifică în rețea; este local în *visiting network* (VLR păstrează corespondența IMSI – TMSI); MS stochează TMSI în SIM pentru reutilizare după restart
  - TMSI trebuie să fie realocat la anumite intervale de tip (operator specific) – tradeoff securitate vs. eficiență; dacă TMSI nu este schimbat în mod constant, atunci va devi el însuși o vulnerabilitate

# Autentificarea abonaților

- **Scop:** Demonstrează identitatea utilizatorilor în rețea pentru a previni accesul neautorizat
- Mecanismul de autentificare folosește
  - Cheia permanentă  $K_i$ , unică per abonat, stocată în
    - SIM (**la abonat**)
    - AuC (**în rețeaua operatorului**)
  - Algoritmi criptografici: **A3** (autentificare), **A8** (generarea cheilor)
- **Principii:**
  - $K_i$  nu părăsește cele 2 locații (SIM, AuC);
  - Autentificarea constă în verificarea că se cunoaște  $K_i$ , *challenge-response mechanism*
  - Visiting network nu știe  $K_i$ , deci are nevoie de ajutor de la home network pentru autentificare
  - Acum este derivată cheia  $K_c$  care va fi utilizată ulterior pentru criptare

# Autentificarea abonaților



# Triplete de autentificare

- **Scop:** Permit visiting network să autentifice MS fără să cunoască  $K_i$  și cresc eficiența prin folosirea unor seturi de triplete (batches)
- Un triplet folosit pentru autentificare este
$$(RAND, XRES, K_c)$$
unde  $XRES = A3(K_i, RAND)$  and  $Kc = A8(K_i, RAND)$
- **Operation:**
  - AuC produce seturi de triplete pentru fiecare MS, fiecare cu o valoare diferita RAND și le trimit către HLR
  - Pentru un singur request, VLR primește un set de triplete de la HLR (pentru a evita comunicația deasă între VLR și HLR)
  - Dacă VLR nu mai are triplete, cere altele de la HLR (nu este permis să se refolosească triplete)

# Criptare / Decriptare

Se cipărează comunicația între stația mobile și BTS (apeluri și informații sensitive precum TMSI, MSISDN, etc.)

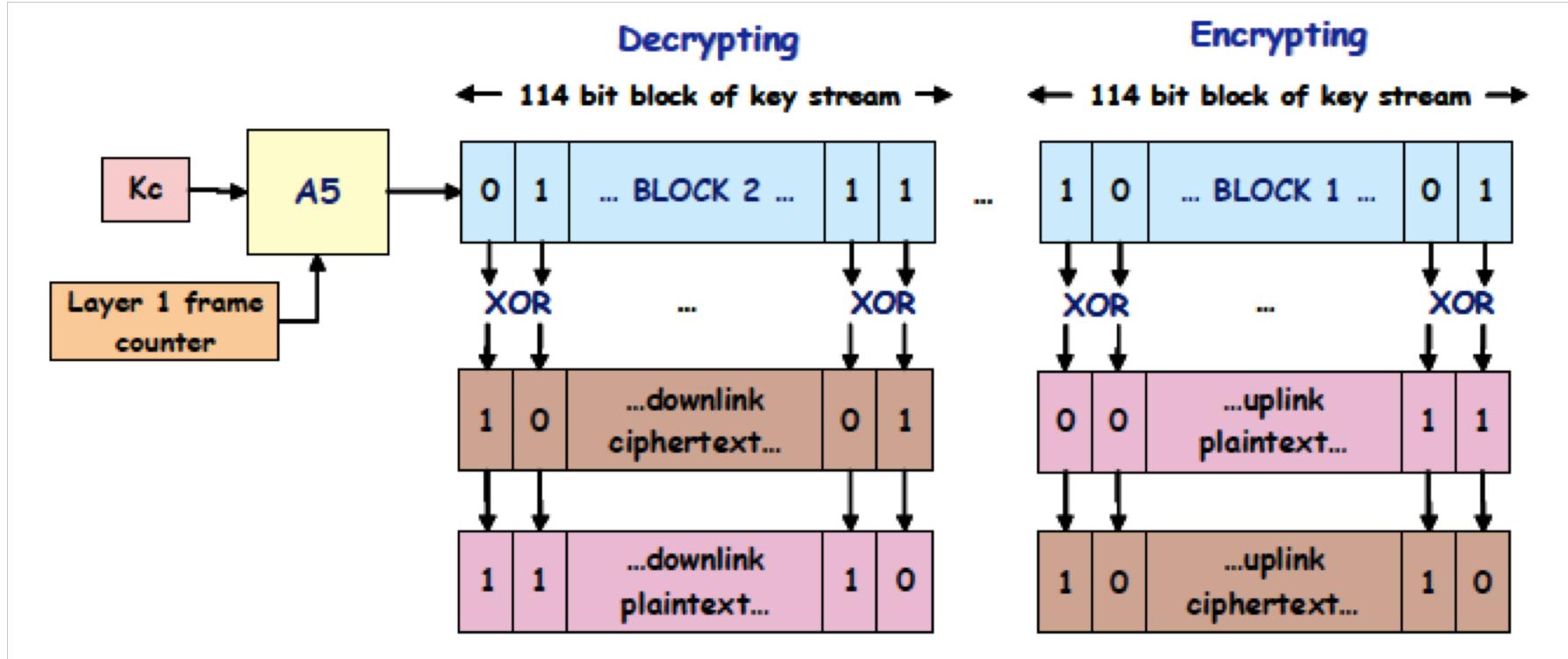
- Criptarea GSM folosește:
  - Cheia  $K_c$ , derivată în cadrul mecanismului de autentificare
  - Algoritmul de criptare: **A5** (criptare radio)
- **Principii:**
  - Criptarea are loc doar pe linkul radio până la BTS (!)
  - Algoritmul de criptare folosește ca input cheia de sesiune  $K_c$  derivată în cadrul mecanismului de autentificare
- **Funcționare:**
  - Cheia  $K_c$  este folosită ca și cheie de criptare pentru un sistem fluid (care utilizează LFSR):

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

# Criptare / Decriptare

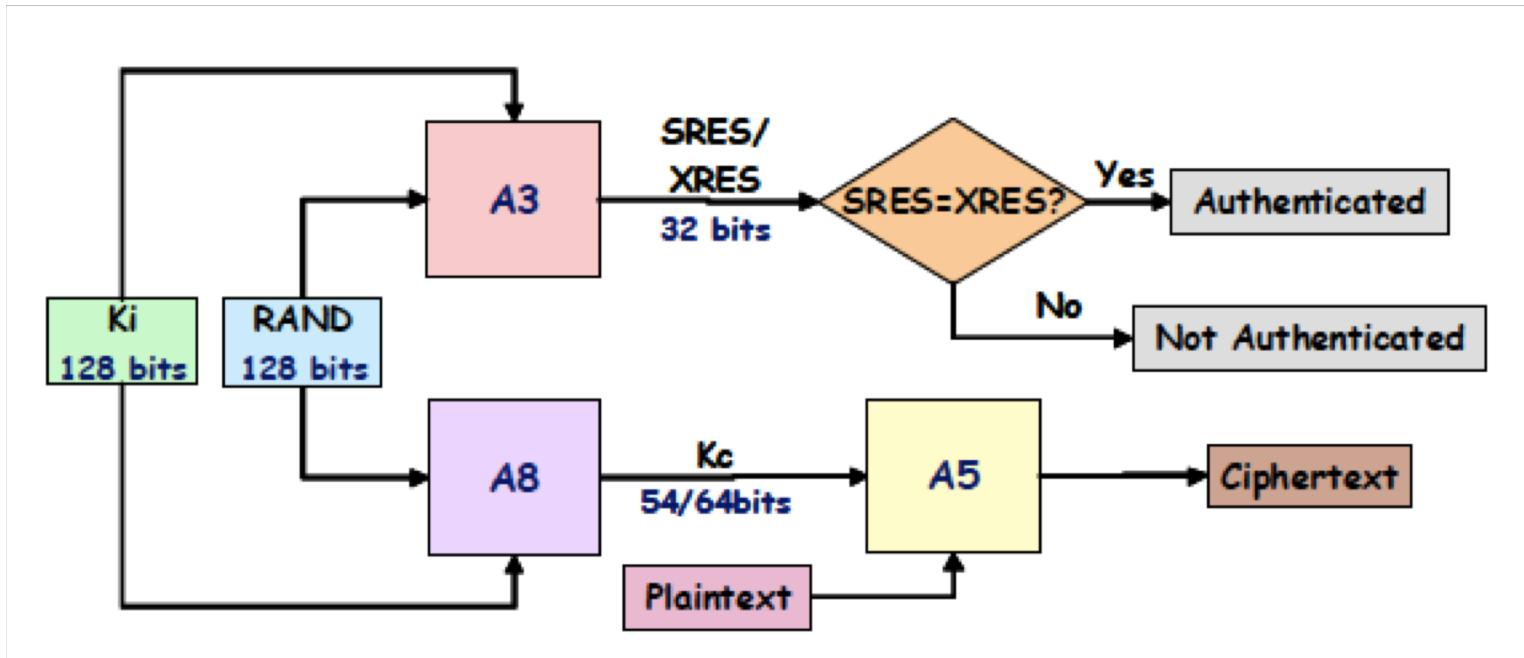
- Atât A5/1 cât și A5/2 nu au fost publici inițial (încalcarea principiului lui Kerckhoffs)
- A5 este **stream ciphers**, deci criptarea se realizează bit cu bit
- Un *frame counter* (22 bits) este folosit ca input adițional cu cheia  $K_c$
- **Vulnerabilitate!** *Frame counter* se repetă la fiecare  $2^{22}$  frames (approx. la fiecare 3.5 hours), deci keystream se repeat dacă  $K_c$  nu este modificat între timp
- GSM este *full duplex*: pentru fiecare frame, primii 114 biți (Block1) sunt folosiți pentru criptarea datelor transmise, următorii 114 biți (Block2) sunt folosiți pentru decriptarea datelor care sunt primite

# Criptare / Decriptare



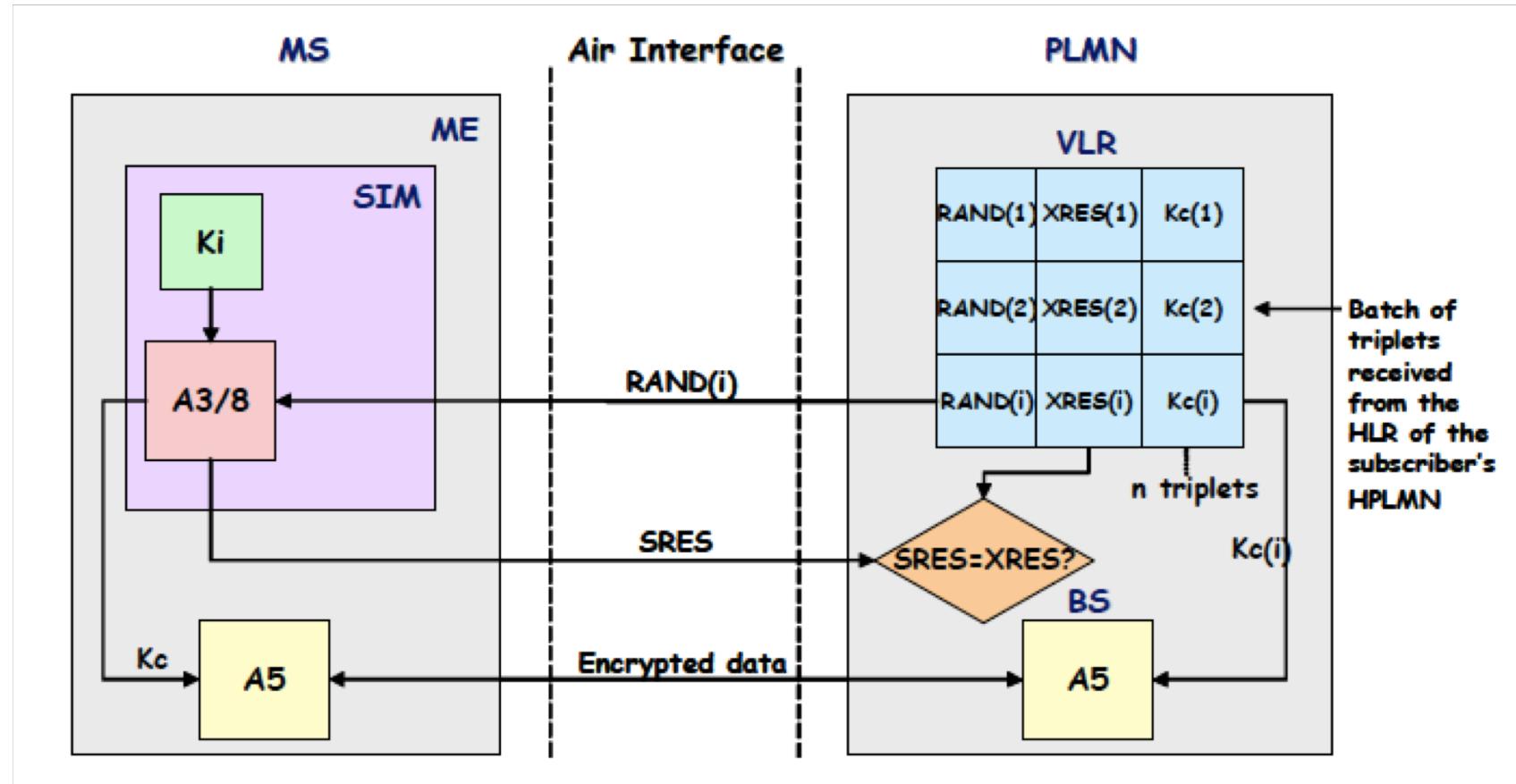
[Source: P.S.Pagliusi – A Contemporany Foreword on GSM Security, InfraSec '02]

# Overview I



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

# Overview II



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

# Criptografie

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!)

# GSM – Principii de securitate

- **Modularitate:**
  - GSM este modular în sensul că acceptă ca algoritmi să fie înlocuiți, cât timp păstrează aceeași structură input/output
  - A5 se referă la o familie de algoritmi; e.g.: A5/1, A5/2, A5/3 (64-biți  $K_c$ ); A5/0 (fără criptare), A5/4 (128-biți  $K_c$ ) – unii se folosesc și pentru UMTS (e.g.: A5/3)
- **Standardizare:**
  - A5 trebuie să fie standardizat (e.g., MS trebuie să comunice cu BTS în roaming)
  - A3, A8 nu trebuie neapărat să fie standardizați, pentru că ambele părți (SIM și AuC) aparțin aceluiași operator mobil; tutuși, 3GPP dă ca exemplu setul de algoritmi TS55.205

# GSM –Principii de securitate

- **Folosirea SIM ca modul de securitate:**
  - Autentificarea și confidențialitatea sunt realizate pe baza cheii secrete ( $K_i$ )
  - SIM stochează informații private ale abonatului ( $K_i$ , IMSI) și algoritmii criptografici (A3, A8)
  - SIM trebuie să fie *tamper-resistant*
- **Securitatea în visiting network:**
  - Cheia  $K_i$  trebuie să nu fie cunoscută de *visitor network*
  - Tripleții de autentificare asigură autentificarea în *visitor networks*
- **Cerințe referitoare la algoritmi:**
  - Imposibil (computațional) de ghicit SRES
  - Imposibil (computațional) de găsit  $K_i$ ,  $K_c$  din datele interceptate
  - ... (rezumări care exclud atacuri triviale)

# Atacuri și vulnerabilități

- **Atacuri pasive:**
  - Adversarul ascultă pe canalul de comunicație și determină IMSI
  - Atacul este posibil pentru că IMSI este transmis în clar când MS nu deține un TMSI sau nu poate fi identificat prin TMSI
- **Atacuri active:**
  - Adversarul cere IMSI de la MS
  - **IMSI Catcher:** adversarul imparsonează o stație BTS legitimă și cere MS pentru IMSI
  - Atacul este posibil pentru că MS nu autentifică rețeaua – criteriul de selecție al celului este puterea semnalului
  - Vom învăța mai multe despre IMSI Catchers când vom studia LTE

# Atacuri și vulnerabilități

- Criptanaliză:
  - Lungimea cheii
    - Lungimea cheii  $K_c$  (54/64 bits) este prea mică
    - Prin căutare exhaustivă (brute force) se poate sparge cheia în câteva ore
  - **COMP128** a fost spart în 1998 (de Wagner and Goldberg, dar aparent atacul era cunoscut de operatori)
    - Atac cu text clar ales (chosen plaintext attack):  $K_i$  se poate găsi când se cunosc aprox. 16000 perechi RAND-SRES
    - Moduri de a colecta perechi RAND-SRES:
      - Acces direct la SIM, conectare la un emulator de telefon (2-10 ore)
      - Folosirea unui BTS fals (durează mai mult, dar nu necesită acces fizic la SIM)

# Atacuri și vulnerabilități

- Criptanaliză:
  - **A5/1** a fost spart în 1999 (de Biryukov, Shamir, apoi atacul a fost îmbunătățit împreună cu Wagner)
    - Time-memory trade-off:
      - *Faza de preprocesare:* Se realizează o bază de date cu stări și chei fluide ale sistemului fluid
      - *Faza de atac:* se caută secvențe ale cheii fluide în baza de date; dacă se găsește o secvență, starea sistemului fluid este cea din baza de date (cu probabilitate mare)
      - 2s de text clar cunoscut (uplink și downlink) pentru succes
  - **A5/2** a fost criptanalizat în 1999 (Goldberg, Wagner, Green), 2003 (Barkan, Biham, Keller), etc.

# Atacuri și vulnerabilități

- **Linkuri radio:**
  - Conexiunea BTS – BSC link poate fi și wireless, ceea ce o face susceptibilă la eavesdropping
  - Atacul este posibil pentru că securitatea GSM nu presupune criptare pe linkul BTS-BSC (criptarea se realizează doar pe portiunea MS – BTS)
- **Engineering attacks:**
  - Atacuri asupra cardului, side-channel attacks
  - Atacuri software
- **Opționalitate:**
  - Criptarea a fost introdusă ca opțională
  - Foarte puține terminale informează utilizatorul dacă are loc criptare sau nu

# De la GSM la GPRS

- Tehnologic:
  - **GSM**: comutare de circuite (*circuit-switched*)
  - **GPRS (General Packet Radio Service)**: comutare de pachete (*packet-switched*)
- Criptarea:
  - **GSM**: doar pâna la BTS, la nivel 1 (physical), algoritmul A5
  - **GPRS**: până la SGSN (în rețeaua core), la nivel 2 (LLC, Logical Link Control), GEA (GPRS Encryption Algorithm)
- **GEA**:
  - LLC counter (32 bits) se folosește în loc de frame counter (22 bits)
  - Cheia fluidă (keystream) este de lungime variabilă (vs. 54/64 bits in GSM)
  - GEA1, GEA2, GEA3 (64 bits), GEA4 (128 bits)

# De reținut!

1. Aplicați principiul lui Kerckhoffs (faceți sistemele criptografice publice)
2. Gândiți soluțiile pentru viitor (e.g., folosiți chei criptografice sufficient de lungi, gândiți-vă la legea lui Moore)
3. Trade-off între eficiență / utilizabilitate și securitate (pot să apară vulnerabilități)
4. Nu subestimați adversarul (e.g., atacurile active nu erau considerate fesabile)



# Securitatea rețelelor

- Prelegerea 9 -

Universal Mobile Telecommunication System  
(UMTS)

Ruxandra F. Olimid

Facultatea de Matematică și Informatică

Universitatea din București

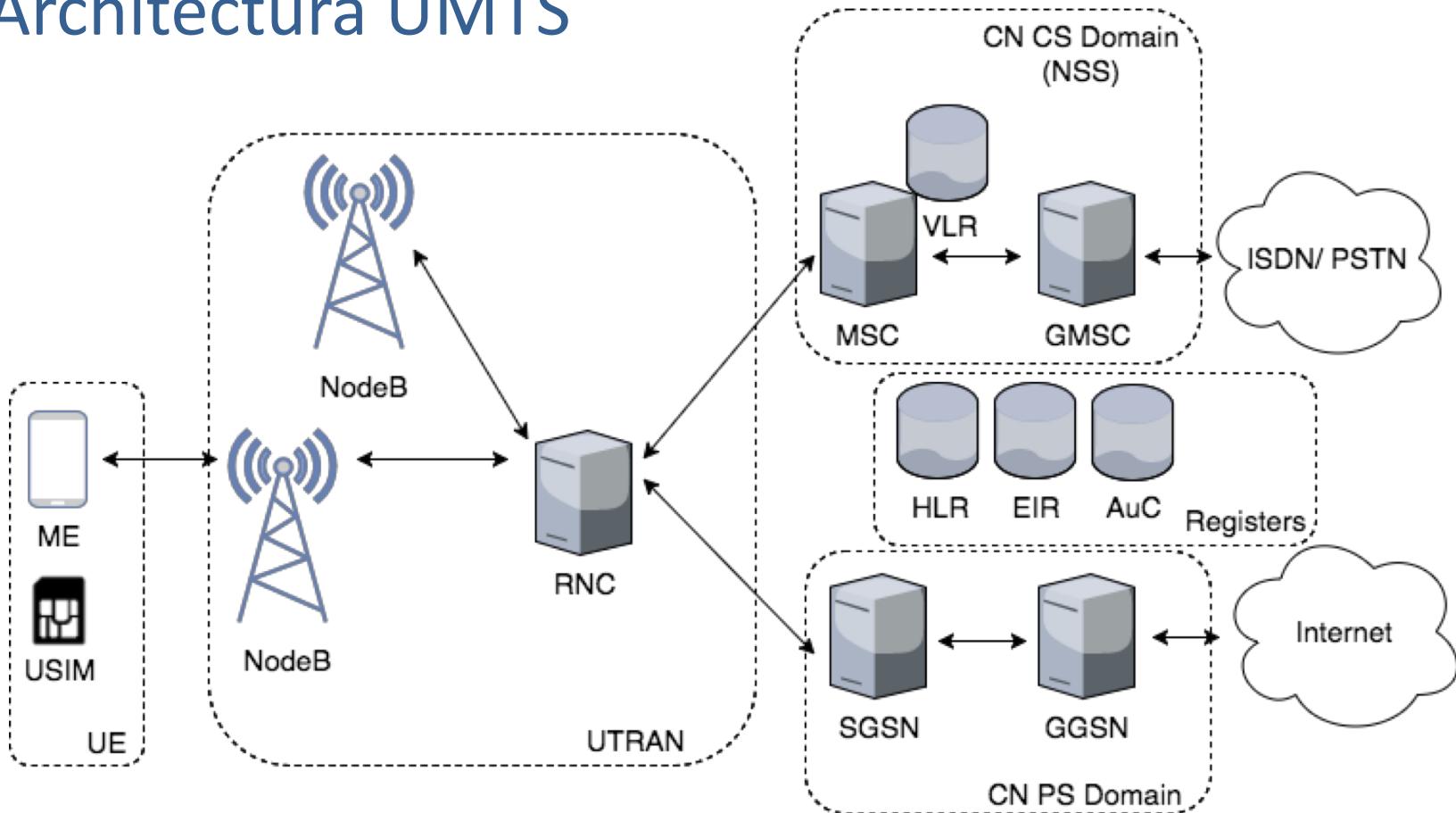
# Cuprins

1. Arhitectura UMTS
2. Principii de Securitate si implementare
3. Man-in-the-Middle Attack



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

# Architectura UMTS



UE: User Equipment

ME: Mobile Equipment

USIM: Universal SIM

UTRAN: UMTS Terrestrial Radio

Access Network

RNC: Radio Network Controller

ISDN: Integrated Services Digital Network

PSTN: Public Switched Telephone Network

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

# Architectura UMTS (vs.GSM)

- **UE (User Equipment):**
  - Consistă în Mobile Equipment (ME) și Universal Subscriber's Identity Module (USIM)
  - Observați schimbarea denumirii: MS vs. UE, SIM vs USIM
- **UTRAN (UMTS Terrestrial Radio Access Network):**
  - NodeB este stația de bază în UMTS (coresponde BTS în GSM)
  - RNC (Radio Network Controller) este controller în UMTS (coresponde BSC în GSM)
- **Elementele de autentificare:**
  - VLR, HLR, EIR, AuC rămân din GSM

# Architectura UMTS (vs.GSM)

- Partea de core este acum împărțită în funcție de tehnologia folosită: *packet switched* și *circuit switched*
- **CN CS Domain (Core Network Circuit Switched Domain):**
  - Corespunde NSS din GSM
  - Realizează conectivitatea cu ISDN / PSTN
- **CN PS Domain (Core Network Packet Switched Domain):**
  - Este nou în UMTS, fiind responsabil de switching și controlul abonaților pentru tehnologia packet switching
  - Realizează conectivitatea la internet

# UMTS – Principii de securitate

- Preluate din GSM:
  - Autentificarea abonaților, utilizarea (U)SIM
  - Criptarea pe interfața radio (pentru *confidentiality*)
  - Folosirea identităților temporare (pentru *privacy of subscribers*)
  - Păstrarea regiștrilor: HLR, VLR, AuC
- Gândit să reziste atacurilor din GSM

# GSM – Recapitulare

## Vulnerabilități în securitatea GSM:

- *Kerckhoffs' principle*: algoritmii criptografici nu au fost făcuți publici (e.g., A5/1, A5/2)
- *Chei criptografice scurte*: vulnerabilitate la *brute force* (*căutare exhaustivă*)
- *Criptare limitată*: datele sunt criptate doar pe o porțiune
- *Autentificare unilaterală*: Stația mobilă nu autentifică rețeaua, doar rețeaua autentifică stația mobilă
- Nu se tratează *integritatea datelor*
- *Atacuri active*; e.g.: IMSI Catchers, când un adversar imparsonează un BTS
- *Utilizatorii nu sunt (în general) notificați despre nivelul de securitate*

# UMTS – Principii de securitate

Vulnerabilități în securitatea GSM:

Se tratează în UMTS!

- *Kerckhoffs' principle*: algoritmii criptografici nu au fost făcuți publici (e.g.,
  - Algoritmii criptografici sunt publici
- *Chei criptografice scurte*: vulnerabilitate la *brute force* (*căutare*)
  - Chei criptografice mai lungi (128 bits)
- *Criptare limitată*: datele sunt criptate doar pe o portiune
  - Criptarea datelor până la RNC
- *Autentificare unilaterală*: Stația mobilă nu autentifică rețeaua, doar
  - *Autentificare mutuală (UE și rețeaua se autentifică reciproc)*
- ~~Nu se tratează integritatea datelor~~
  - Se introduc Message Authentication Code (MAC)
- *Atacuri active*; e.g.: IMSI Catchers, când un adversar imparsonează un BTS
- *Utilizatorii nu sunt (în general) notificați despre nivelul de securitate*

# UMTS – Principii de securitate

- Noi principii de Securitate, ca îmbunătățire față de GSM:
  - ... (slide precedent)
  - Algoritmul de criptare KASUMI este exportat în întreaga lume
  - UE și rețeaua negociază pentru a agreea algoritmii de criptare și integritate utilizări
  - Se introduce SQN (SeQuence Number) în tripleții de autentificare (în AUTN) pentru a evita *replay attacks* și pentru a asigura *key freshness*

# UMTS – Principii de securitate

## Vulnerabilități în UMTS:

- *Atacurile active sunt posibile*; e.g.: IMSI Catchers, când un adversary impersionează un NodeB
- *Utilizatorii nu sunt (în general) anunțați de nivelul de securitate*
- *End-to-end (UE-to-UE) security nu se consideră*
- *Vulnerabilități în protocolul de autentificare* (nu se utilizează PKI)

Le vom reîntâlnii la LTE!

# Man-in-the-Middle Attack

# UMTS – Man-in-the-Middle Attack

- **Scop:** se realizează un atac de tip MitM (Man-in-the-Middle) împotriva UMTS - tot traficul inițiat de stația mobilă (UE) se transmite prin intermediul adversarului, care are acces la informație
- **Idea de bază:**
  - Adversarul obține un token de autentificare din rețea, și îl folosește să imparsoneze o stație GSM către abonatul UMTS
- **Atacul este posibil pentru că:**
  - Interconectarea GSM / UMTS permite
  - GSM nu suportă protecție de integritate, deci adversarul poate să păcăleasca UE să nu folosească criptare
- Atacul a fost introdus de **Meyer și Wetzel** în 2004

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

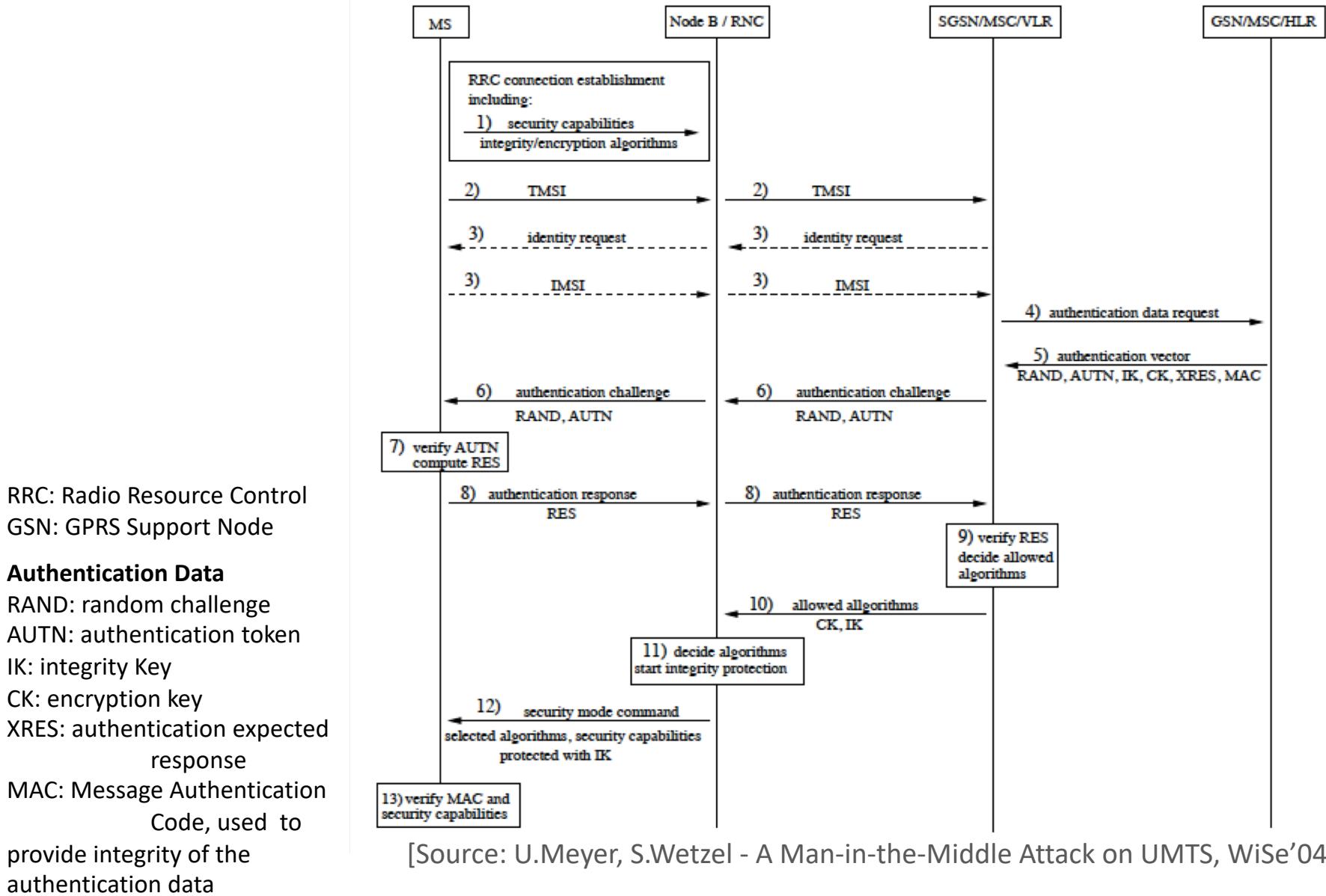
# UMTS – Man-in-the-Middle Attack

- MitM este ușor în **GSM**:
  - Nu are loc autentificarea *serving network* de către abonat, aşa încât un adversary poate să imploreze BTS
  - Un adversary poate să imploreze victima MS către BTS doar prin forward-area traficului de autentificare
- Adversarul dobândește acces la informație prin păcălirea ambelor părți să nu folosească criptare (i.e., să folosească A5/0)
- Dacă atacul e posibil în GSM, e normal că **abonații UMTS care folosesc GSM rămân vulnerabili**
- ... dar abonații UMTS sunt vulnerabili și dacă rămân în rețeaua UMTS și se aplică autentificarea UMTS
- **Roll-back attack:** *un atac care folosește slăbiciunea unor versiuni mai vechi care trebuie să rămână valide din necesități de compatibilitate*

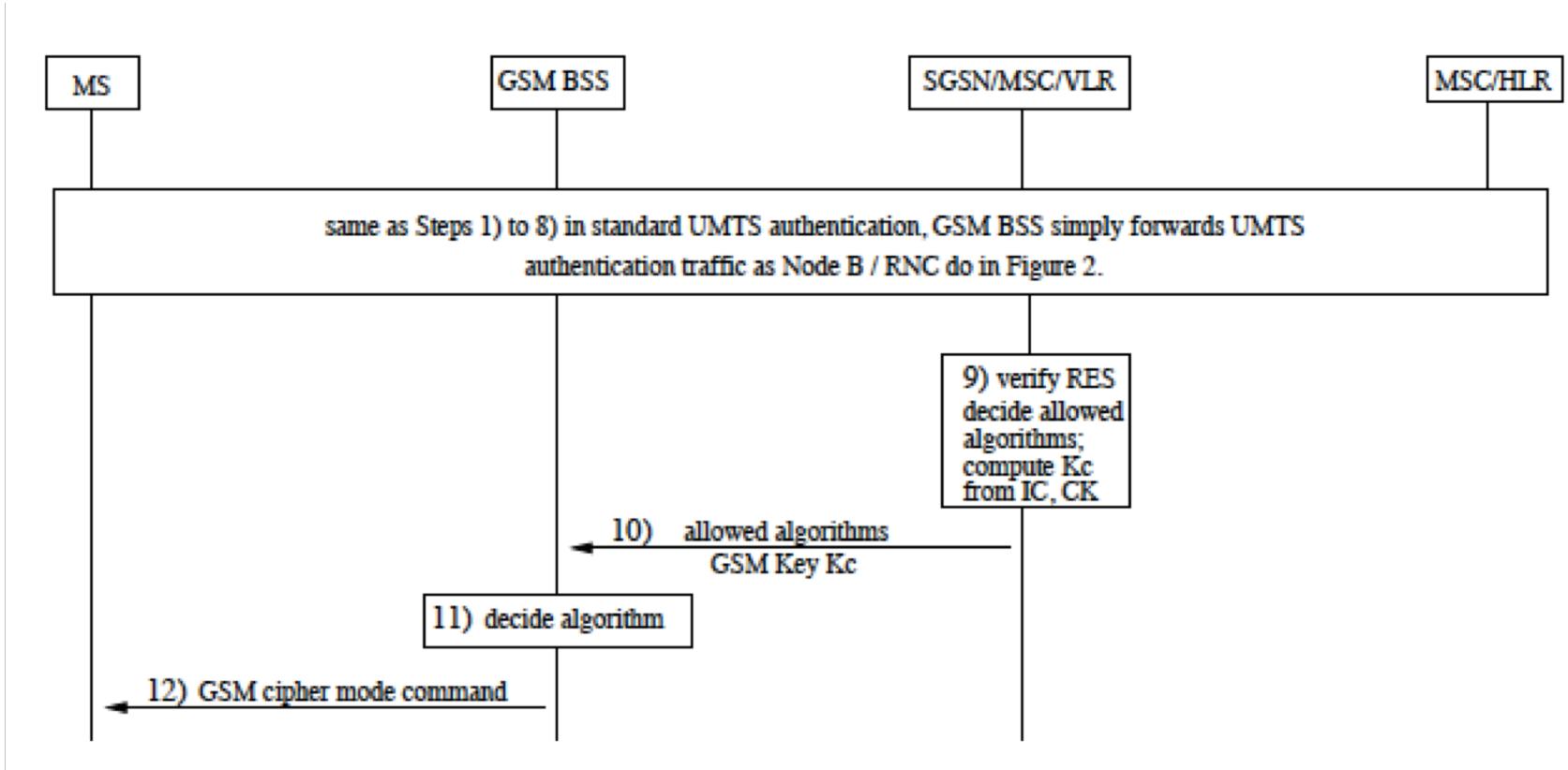
# UMTS – Man-in-the-Middle Attack

- 2 tipuri de autentificare sunt de interes pentru atac:
  - **UE (UMTS) – NodeB (UMTS)**: un abonat UMTS se conectează în rețeaua UMTS prin intermediul NodeB
  - **UE (UMTS) - BTS (GSM)**: un abonat UMTS cu un UE care permite conectivitate la GSM se conectează la *serving network* prin BTS

# AKA: UE (UMTS) – NodeB (UMTS)



# AKA: UE (UMTS) – BTS (GSM)



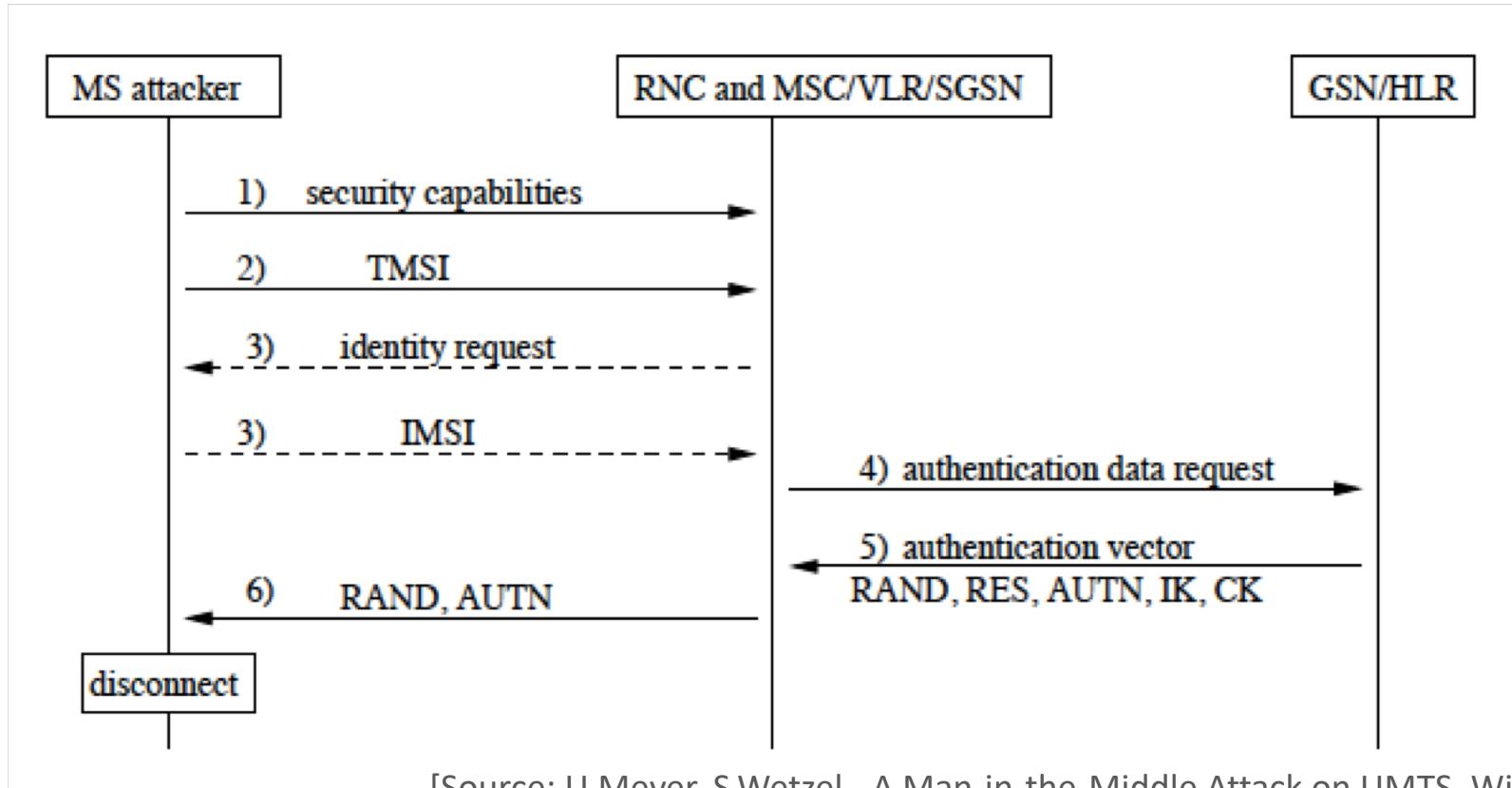
[Source: U.Meyer, S.Wetzel - A Man-in-the-Middle Attack on UMTS, WiSe'04 ]

**Mesajul din pasul 12 poate fi modificat de adversar pentru ca nu are protecție la integritate (GSM does not support integrity protection)**

# UMTS – Man-in-the-Middle Attack

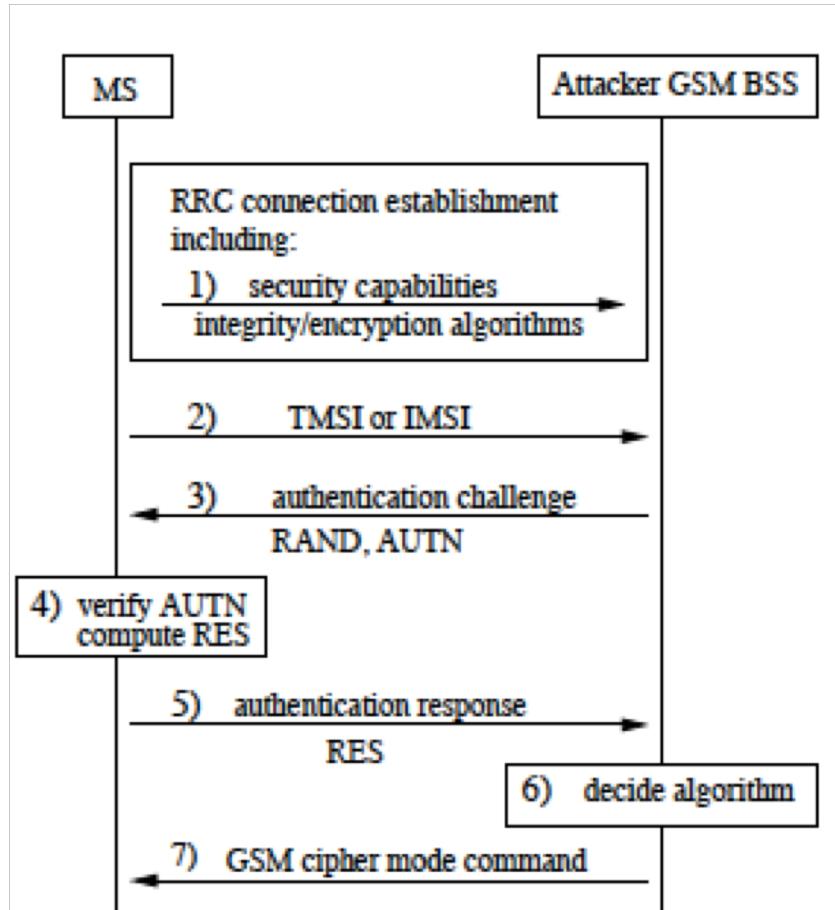
- Atacul constă în 2 faze (+1):
  - **Faza 0:** adversarul găsește IMSI victimei (și capabilitățile criptografice)
    - Este fesabil, prin inițierea procedurii de autentificare înainte de atac (IMSI Catcher)
  - **Faza 1:** adversarul acționează în locul victimei pentru a prelua un token de autentificare valid AUTN (de la rețea)
  - **Phase 2:** adversarul imparsionează un BTS (GSM) pentru a face victimă să se conecteze la acest BTS fals

# Faza 1



**Faza 1:** adversarul acționează în locul victimei pentru a prelua un token de autentificare valid AUTN (de la rețea)

## Faza 2



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

**Faza 2:** adversarul imparsionează un BTS (GSM) pentru a face victimă să se conecteze la acest BTS fals

# UMTS – Man-in-the-Middle Attack

- Adversarul poate decide să folosească A5/0 (fără criptare), dacă acest lucru e acceptat de MS/UE (în faza 1, *security capabilities*)
- Atacul nu funcționează dacă are loc o altă autentificare între Faza 1 și Faza 2, altfel SQN poate fi *out of range*
- Atacul nu permite impersonarea ambelor părți MS/UE și BTS/NodeB în același timp

# De reținut!

1. Învățam din erori (UMTS a fost realizat astfel încât să reziste atacurilor GSM)
2. Backward compatibility introduce probleme de multe ori
3. Noi noțiuni, aspect ale securității UMTS



# Securitatea rețelelor

## - Prelegerea 9 -

## Long Term Evolution (LTE)

Ruxandra F. Olimid

Facultatea de Matematică și Informatică  
Universitatea din București

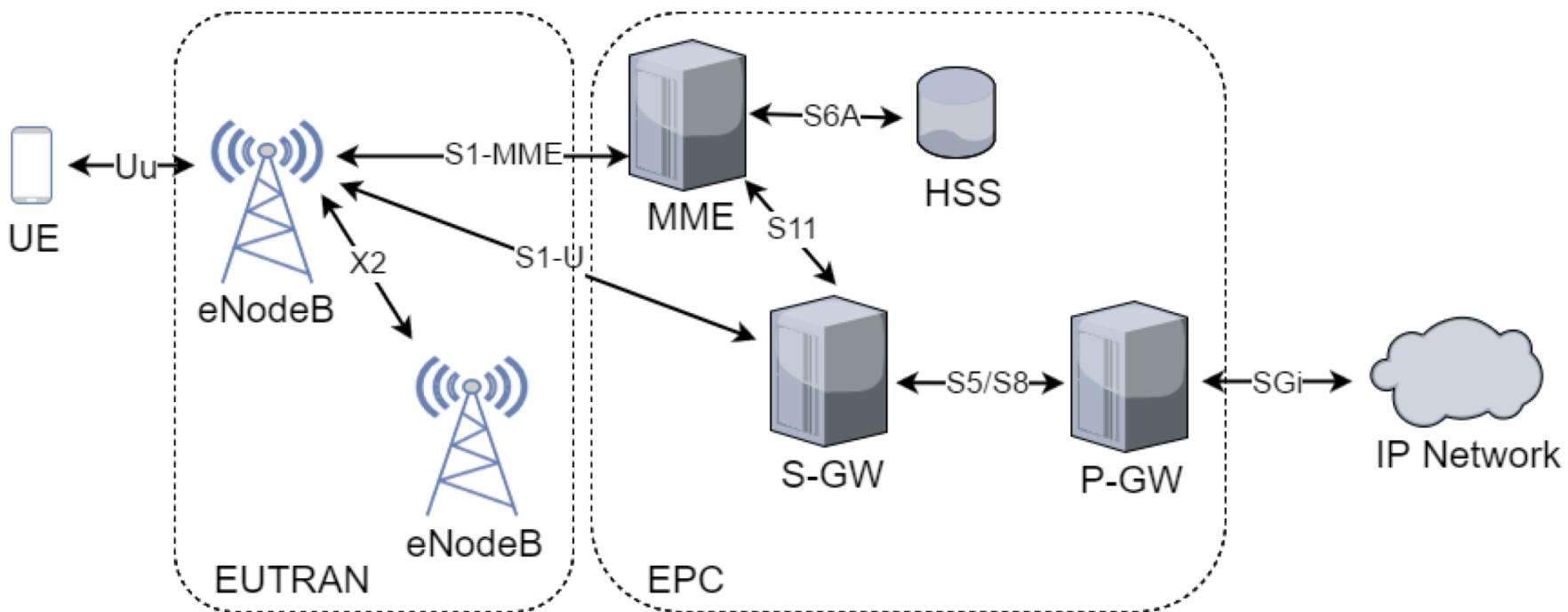
# Cuprins

1. Arhitectura LTE
2. Arhitectura de Securitate LTE
3. Principii de Securitate si implementare
4. Key hierarchy
5. AKA
6. Standarde de securitate



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

# 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

# Architectura LTE

- **UE (User Equipment):**
  - Consistă în Mobile Equipment (ME) și Universal Subscriber's Identity Module (USIM)
- **EUTRAN (Evolved UTRAN):**
  - Cuprinde mai multe eNodeB (enhanced NodeB)
  - Ca diferență față de generațiile anterioare, eNodeB pot comunica direct
- **EPC (Evolved Packet Core):**
  - MME este responsabil de 2G / 3G handover, autentificarea și alocarea resurselor pentru UE. MME are rol în managementul mobilității UE, când eNodeN nu pot face asta direct
  - S-GW este punctul de interconectare EUTRAN - EPC, responsabil pentru rutarea pachetelor, buffering, forwarding, etc., cu rol în mobilitatea 3GPP
  - P-GW este interfața spre rețelele externe PDN

# Terminologie

- **LTE (Long Term Evolution):**
  - Noua tehnologie radio
- **SAE/LTE (System Architecture Evolution / LTE):**
  - Denumirea întregului sistem: tehnologia LTE cu acces la tehnologii precedente precum 2G, 3G
  - LTE include EUTRAN, iar SAE include EPC
- **EPS (Evolved Packet System):**
  - Termenul ethnic pentru SAE/LTE, dar se cunoaște sub denumirea generică **LTE**

# Identificarea UE

- Similar cu GSM, UMTS (GUTI similar cu TMSI)
- MME asignează GUTI în procedura Attach Accept sau Tracking Area Update Accept
- MME poate să asigneze GUTI în GUTI Reallocation procedure

**GUTI** (Global Unique Temporary UE Identity)

GUMMEI (Globally Unique MME Identifier)				M-TMSI (MME Temporary Subscriber Identifier)
MCC (Mobile Country Code)	MNC (Mobile Network Code)	MMEI (MME Identifier)		
		MMEGI (MME Group ID)	MMEC (MME Code)	

Identifica MME care aloca GUTI

Identifica UE in cadrul MME

# EPS Cerințe de securitate

- **Cerințe de securitate la nivel înalt și servicii:**
  - EPS ar trebui să ofere autenticitatea informațiilor între terminal și rețea
  - EPS trebuie să se asigure că utilizatorii neautorizați nu pot stabili o comunicare prin sistem
  - EPS trebuie să permită rețelei să își ascundă structura internă față de terminal
  - Politicile de securitate ar trebui să fie sub controlul operatorului (home network)
  - EPS oferă sprijin pentru interceptarea legală (lawful interception)
  - EPS suportă apelurile de urgență
  - USIM Rel-99 sau mai nou este necesar pentru autentificare

# EPS Cerințe de securitate

- **Privacy:**
  - *EPS va furniza mai multe niveluri adecvate de confidențialitate a utilizatorilor pentru comunicare, locație și identitate*
  - *Conținutul de comunicare, originea și destinația sunt protejate împotriva dezvăluirii către părți neautorizate*
  - *EPS trebuie să poată ascunde identitățile utilizatorilor față de părțile neautorizate*
  - *EPS trebuie să poată ascunde locația utilizatorilor față de părțile neautorizate*

# Funcționalități preluate din 2G/3G

- Funcționalități preluate din GSM and UMTS:
  - Abonare autentificare, utilizarea de USIM (IMEI stocate în ME și IMSI stocate în UICC)
  - Autentificare reciprocă (de la UMTS)
  - Criptarea pe interfața radio (pentru confidențialitate), care rămâne însă opțională pentru operatorul rețelei
  - Utilizarea identităților temporare (pentru confidențialitatea abonaților)
  - Vizibilitatea și configurabilitatea securității la UE (de exemplu, indicatorul de criptare) este opțional
  - Lawful interception

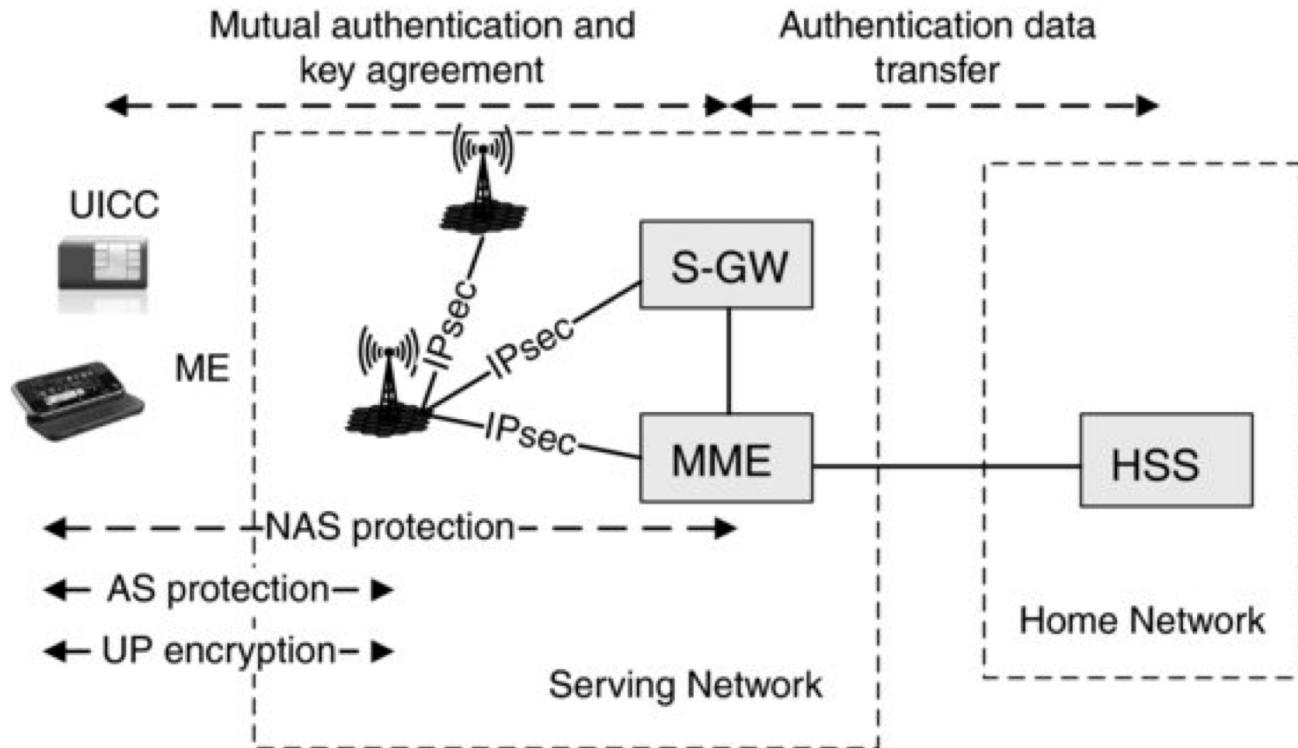
# Noi funcționalități

- Îmbunătățiri:
  - Punctul final pentru criptare în partea de rețea rămâne eNodeB, dar cerințe de securitate fizică sunt introduse pentru eNodeB (în UMTS este RNC, dar în GSM este BTS)
  - Nu există niciun mecanism de integritate pentru datele utilizatorului (motivul: riscul de a manipula datele utilizatorilor este considerat prea scăzut pentru a introduce o atitudine semnificativă prin protecția integrității, în special pentru voce)
  - Noua ierarhie de chei, mai elaborată
  - Îmbunătățiri ale algoritmilor și protocoalelor criptografice

# EPS - Arhitectura de securitate

- Protecția rețelei are loc în 2 planuri:
  - *Signalling plane*
  - *User plane*
- Există mecanisme de confidențialitate și integritate:
  - **Confidențialitate:** pentru ambele planuri (**signalling plane, user plane**)
  - **Integritate:** doar pentru **signalling plane**

# EPS - Arhitectura de securitate



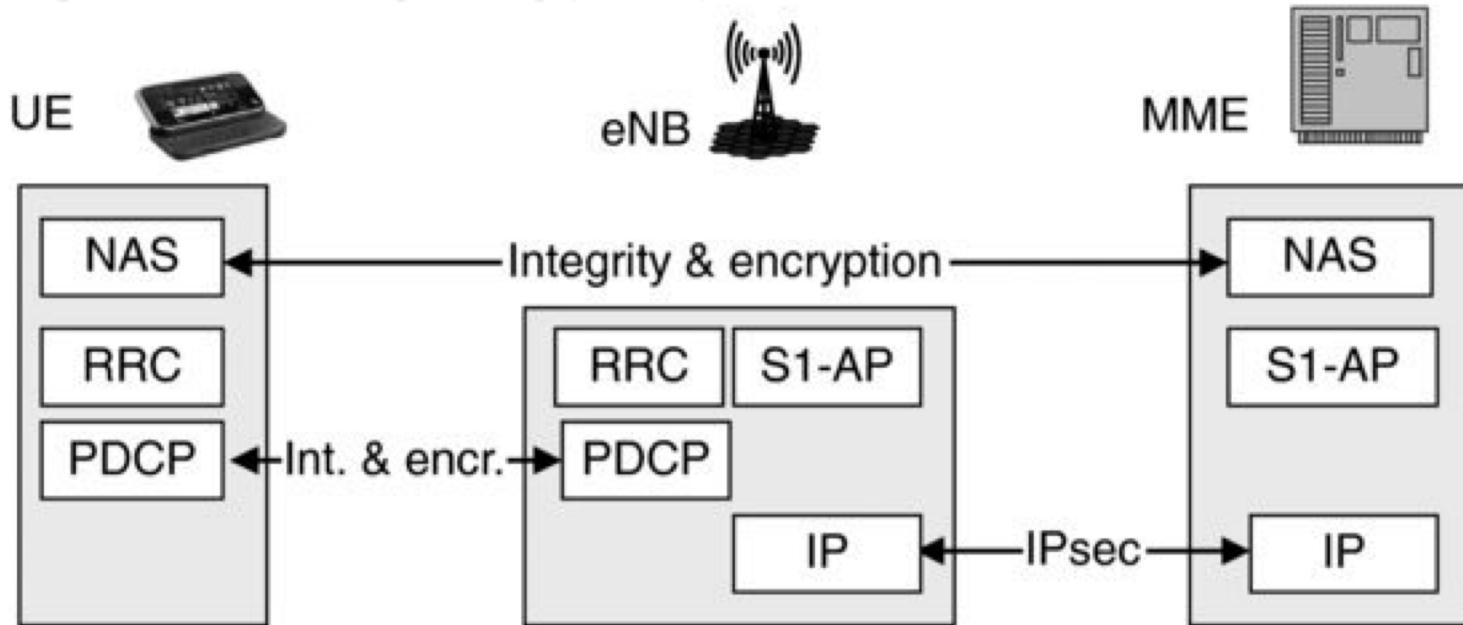
[Source: D.Forsberg et al. – LTE Security, Wiley 2012]

NAS: Non-Access Stratum

AS: Access Stratum

UP: User Plane

# EPS Signalling Plane Protection



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

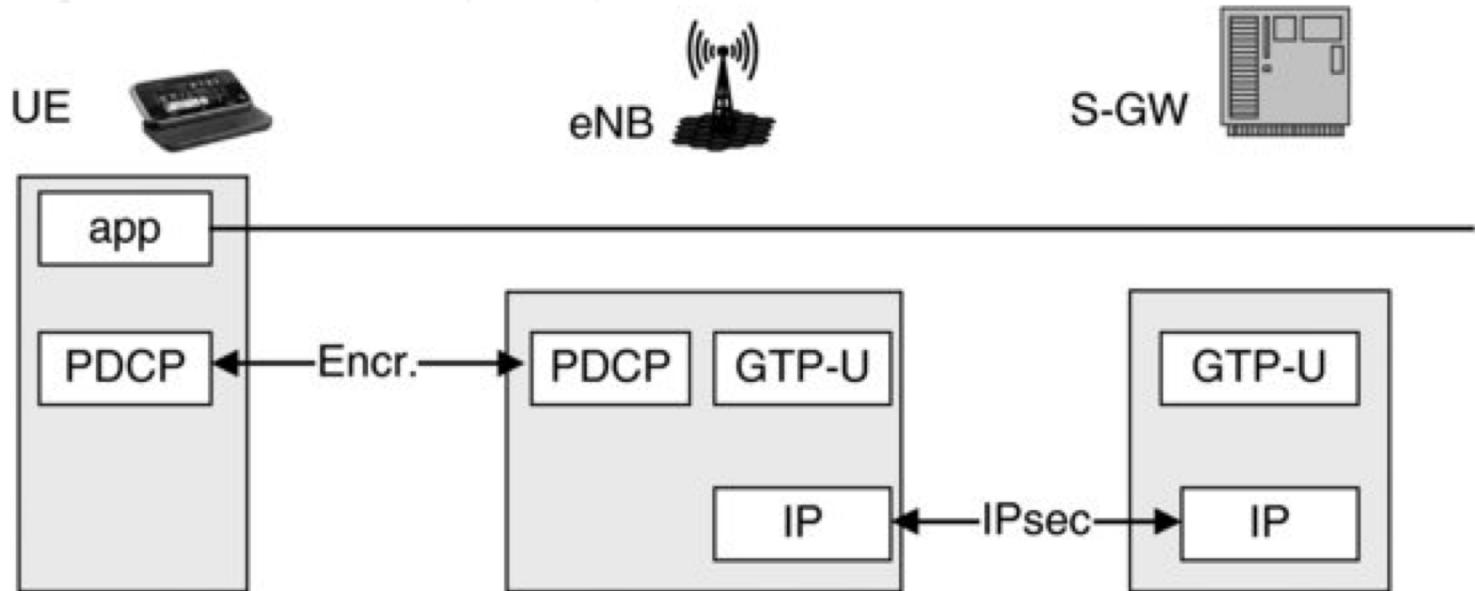
NAS: Non-Access Stratum

RRC: Radio Resource Control

PDCP: Packet Data Convergence Protocol

IP: Internet Protocol

# EPS User Plane Protection



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

PDCP: Packet Data Convergence Protocol

GTP: GPRS Tunneling Protocol

*Confidentialitatea este optională pentru ambele planuri!*

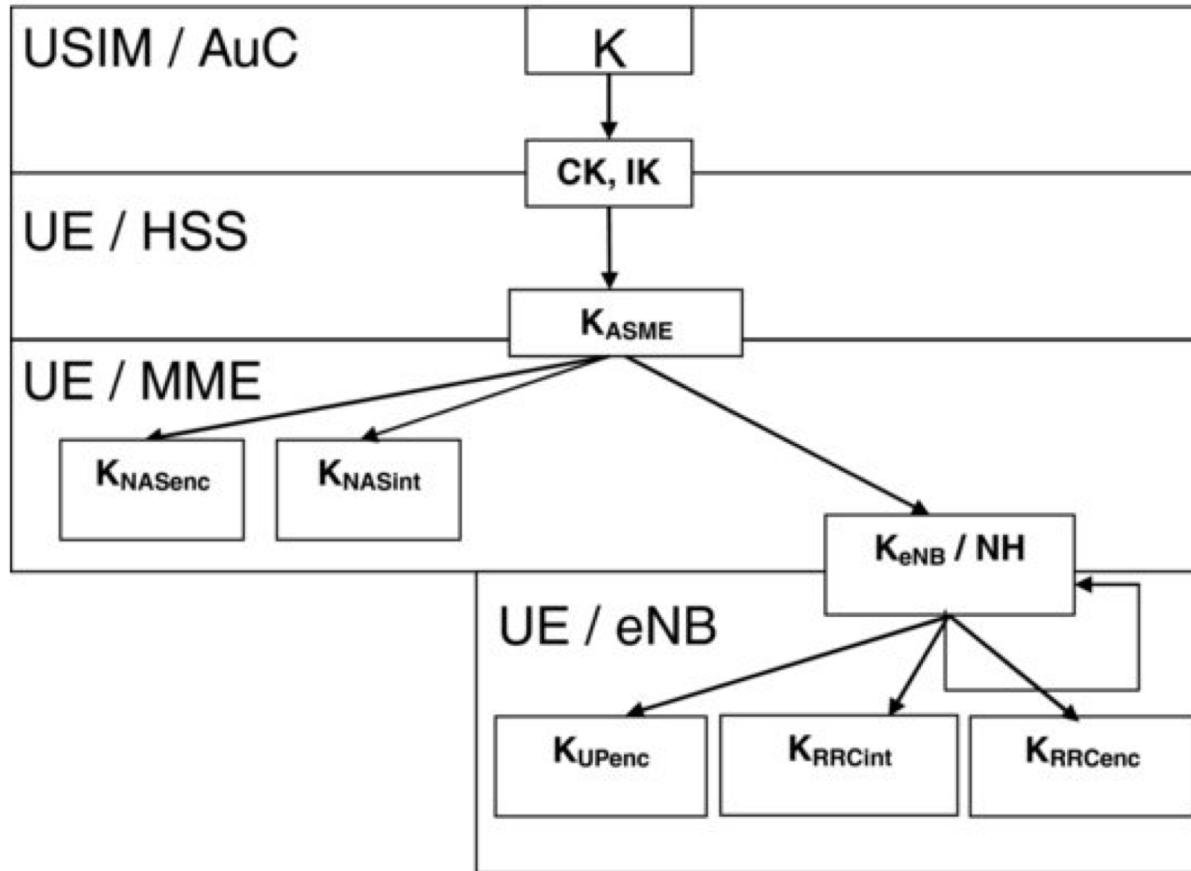
# Key Hierarchy

## (Ierarhia de chei)

# Key Hierarchy

- MME preia datele de autentificare din HSS
- MME trigger-ează Authentication and Key Agreement (AKA) protocol with the UE, rezultând o cheie  $K_{ASME}$
- 2 chei derivate se folosesc pentru confidențialitate ( $K_{NASenc}$ ) și integritate ( $K_{NASint}$ ) pentru signalling plane, în comunicația MME / UE - **NAS protection**
- O cheie este transmisă către eNodeB ( $K_{eNB}$ ), din care sunt derivate alte 3 chei:
  - 2 chei pentru confidențialitate ( $K_{RRCint}$ ) și integritate ( $K_{RRCenc}$ ) pentru signalling plane, în comunicația eNodeB / UE - **AS protection**
  - 1 cheie ( $K_{UPenc}$ ) pentru protecția confidențialității al user plane, în comunicația eNodeB / UE

# Key Hierarchy



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

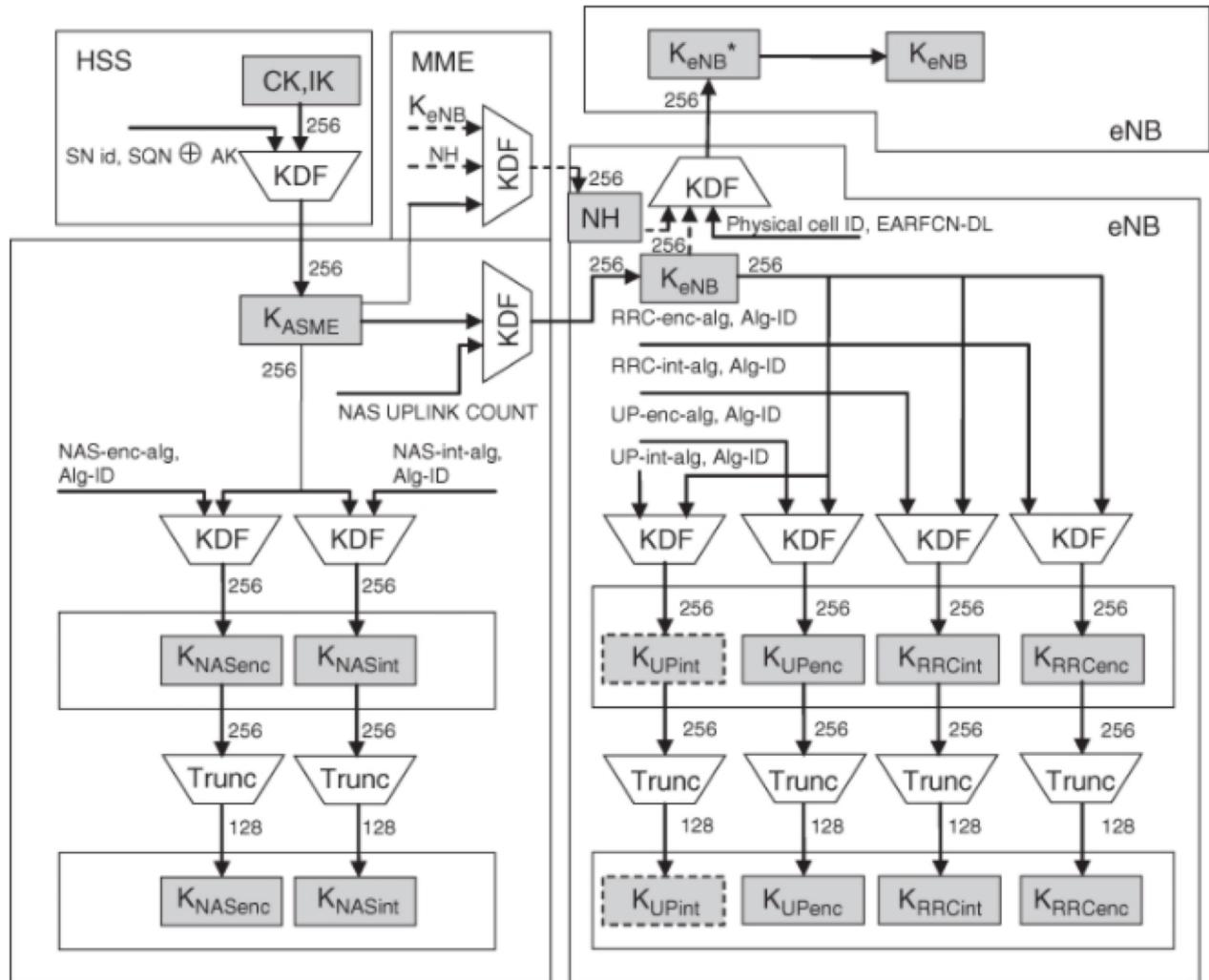
# Key Hierarchy

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

# Key Hierarchy

- Principiul separării cheilor (Cryptographic key separation):
  - Fiecare cheie este utilizată doar pentru un singur context (de exemplu: criptarea traficului de semnalizare)
  - Împiedică extinderea **key leakage**: cunoașterea cheilor într-un singur context nu ajută la găsirea cheii într-un alt context
- Key freshness:
  - Cheile pot fi schimbatе fără a modifica alte chei (e.g.: schimbarea  $K_{eNB}$  nu necesită schimbarea  $K_{ASME}$ )
  - Schimbarea cheilor se poate face mai des
- ... ca **disavantaj**: complexitate crescută

# Key Hierarchy



**Întrebare:** Se pot schimba  $K_{NASenc}$ ,  $K_{NASint}$  cu menținerea  $K_{ASME}$ ? Cum?

*Se schimbă alți parametrii, precum NAS-enc/int-alg Alg\_ID*

# EPS AKA

## (Authentication and Key Agreement)

# EPS AKA

SN id: Serving Network Identity

AV: Authentication Vector

AUTN: Authentication Token

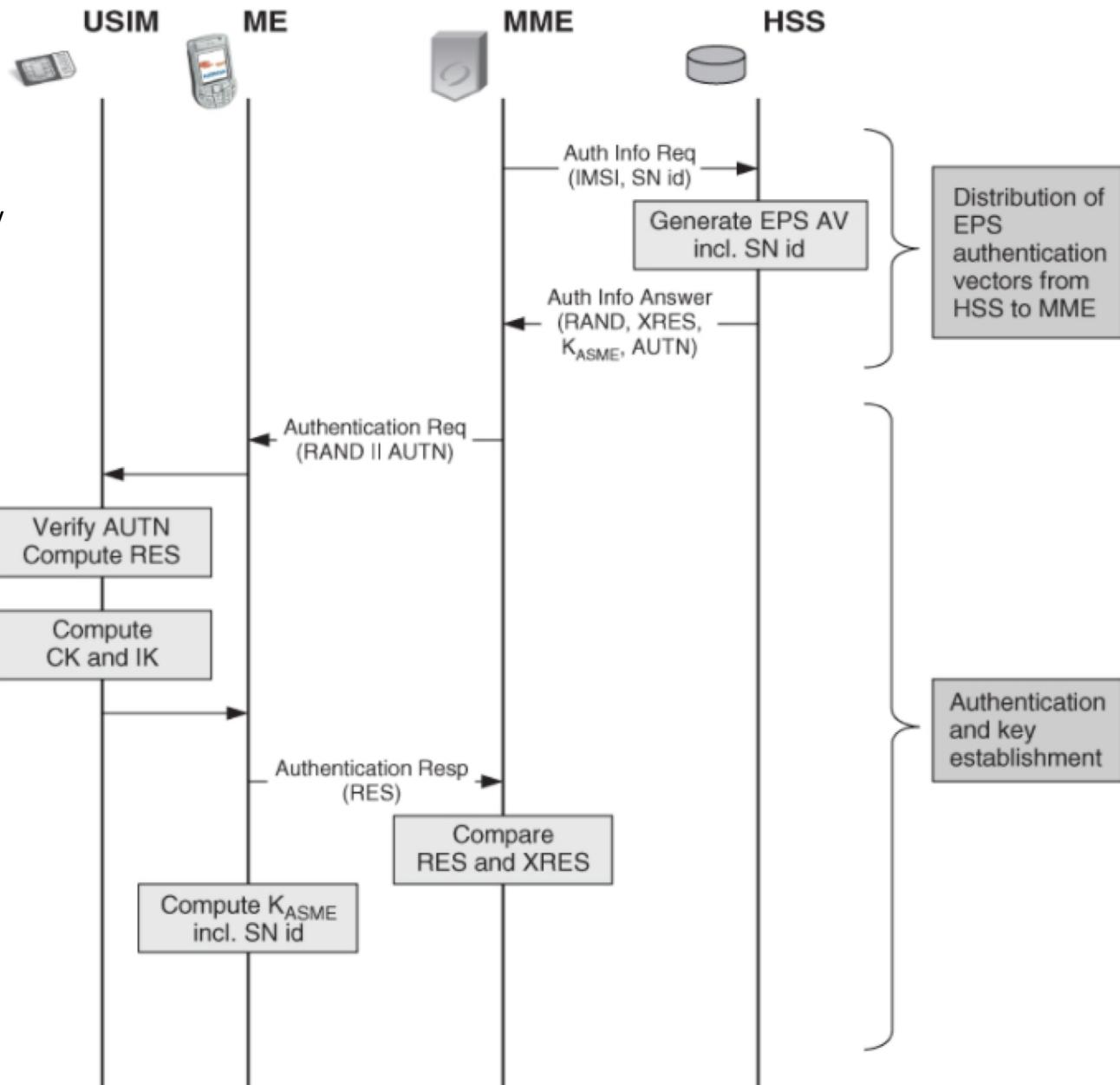
RES: Response

XRES: Expected Response

CK: Ciphering Key

IK: Integrity Key

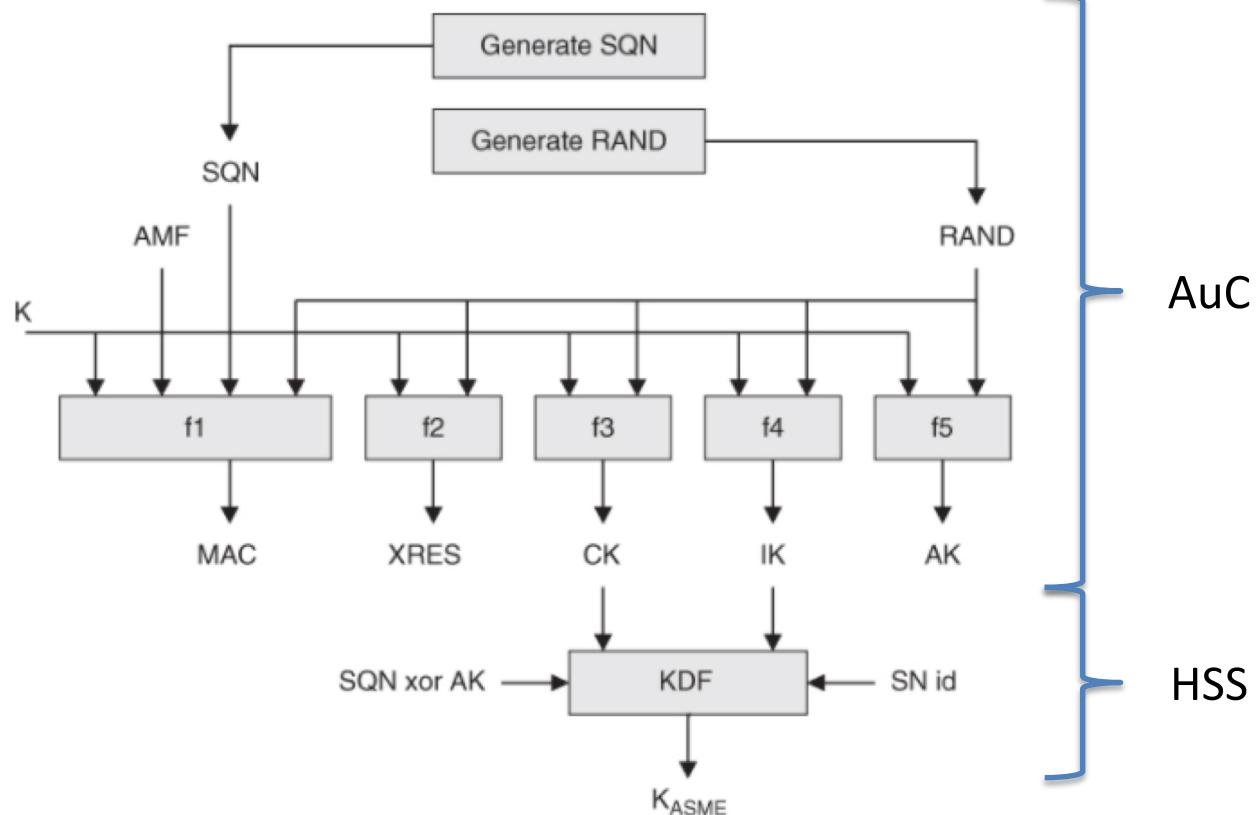
ASME: Access Security Management Entity



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

# EPS AKA - Network Side

AMF: Authentication Management Field  
AK: Anonymity Key



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

EPS AV:  
(RAND, XRES, K<sub>ASME</sub>, AUTN)

AUTN := SQN xor AK || AMF || MAC

UMTS AV := RAND || XRES || CK || IK || AUTN

EPS AV := RAND || XRES || K<sub>ASME</sub> || AUTN

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

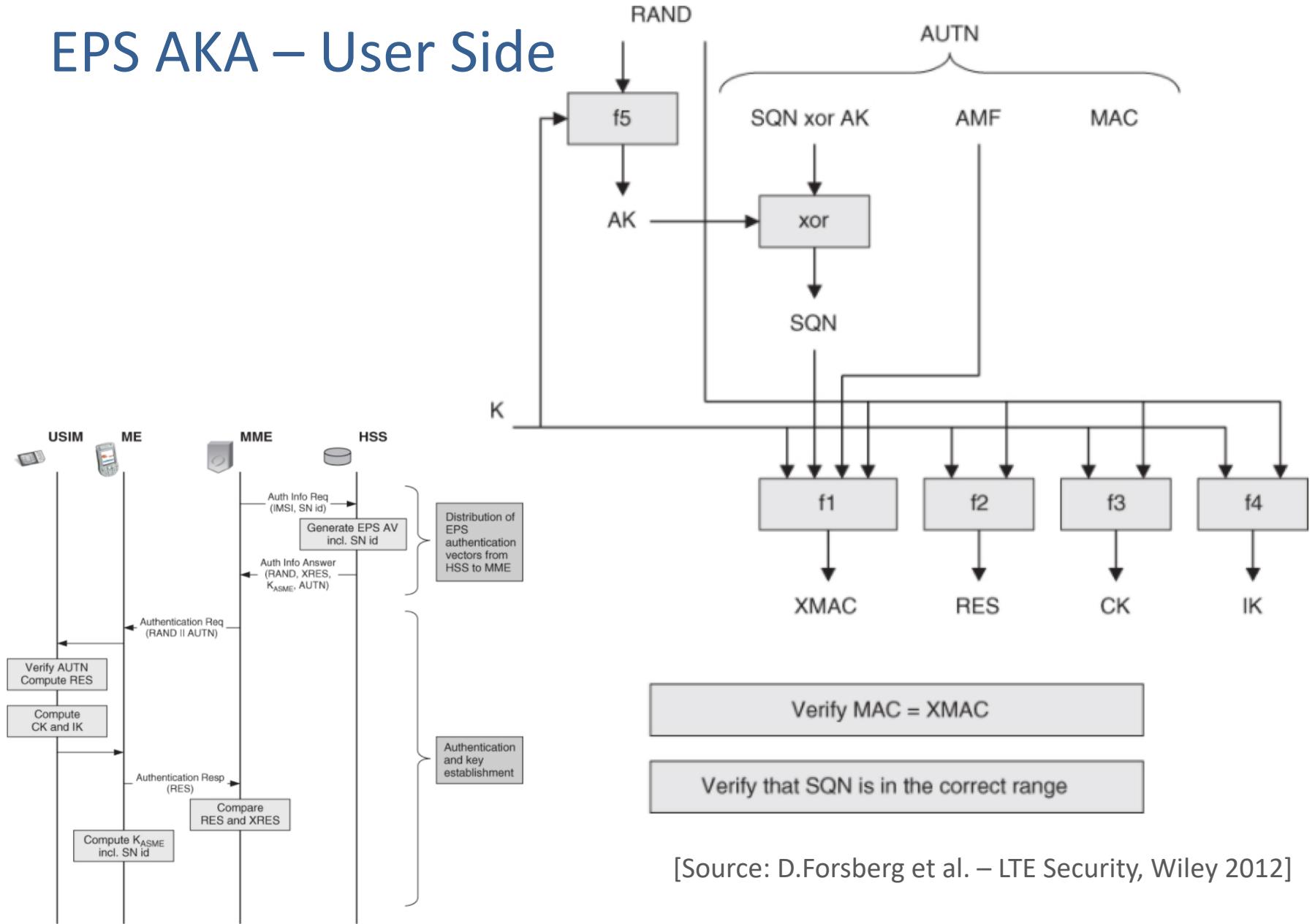
## EPS AKA – Network Side

- Recomandarea este de a trimite un singur AV la un moment dat (nu mai mult) ...  
... deoarece necesitatea de a solicita AV proaspăt este redusă din cauza existenței  $K_{ASME}$ , care nu este expusă deoarece CK și IK au fost expuse în UMTS
- Nu se refolosesc atunci când UE se mută într-o altă rețea ...  
... deoarece ID-ul SN este introdus în KDF
- Fiecare AV este folosit o singură dată
- CK și IK nu părăsesc HSS
- Specific operatorului: dacă  $AK=0$ , atunci  $AK \text{ XOR } SQN = SQN$  (când operatorul decide că nu este necesar să se ascundă SQN)

# EPS AKA – Network Side

- Ambii vectori de autentificare (AV) UMTS și EPS sunt generați
- AuC generează vectorii de autentificare AVs în același mod ca și pentru UMTS
- HSS derivă  $K_{ASME}$  din CK și IK
- AuC generează un nou SQN și o secvență aleatoare RAND
- **AMF (Authentication Management Field):**
  - Indică algoritmul folosit pentru generarea auth vector dacă sunt mai mulți
  - Setează valori limită pentru timpul de viață al cheilor
  - Primul bit este 1 pentru a marca faptul că AV este pentru utilizare EPS

# EPS AKA – User Side



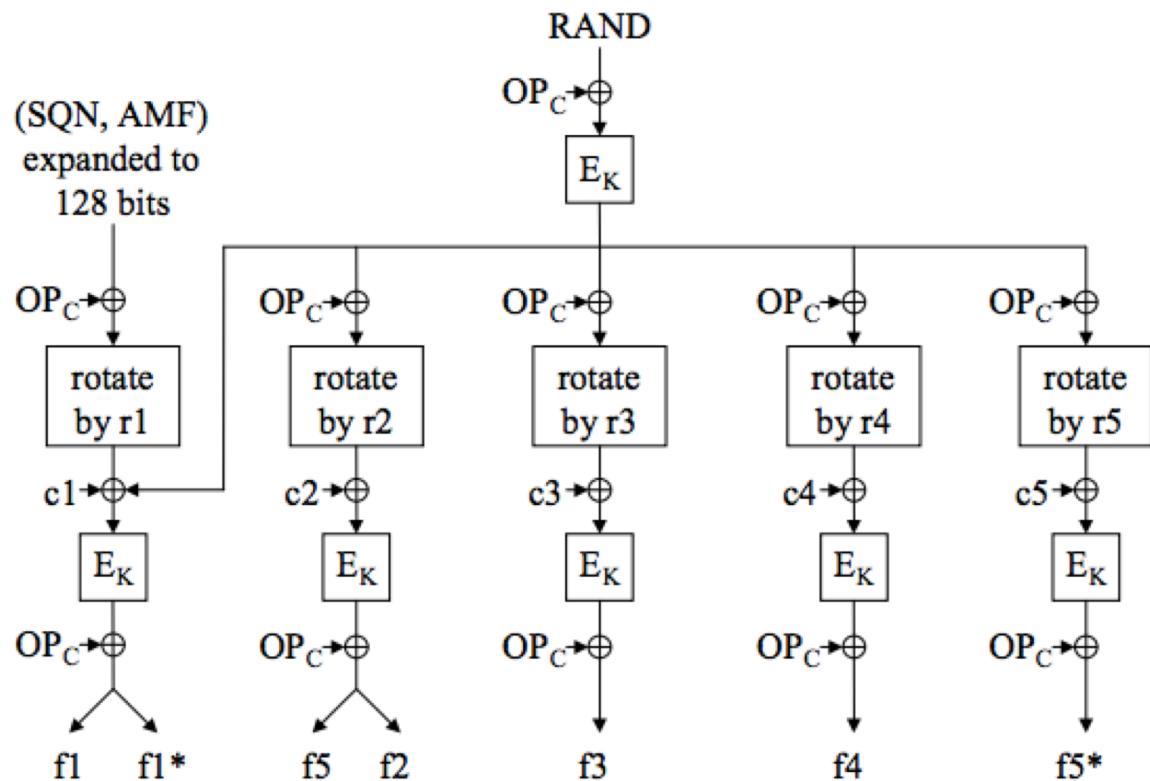
# EPS AKA – User Side

- Verificarea SQN nu a fost standardizată (generarea și verificarea au loc în rețeaua home network, astfel încât aceasta poate fi specifică operatorului)
- Cerințe pentru SQN:
  - Nu trebuie să se utilizeze niciun SQN de două ori: USIM nu ar trebui să accepte 2 AUTN cu același SQN după verificarea AUTN
  - Permite, într-un anumit prag, out of order SQN no.
  - Respinge SQN prea vechi dacă se bazează pe timp
- Verificarea este realizată în USIM

# Un exemplu: MILENAGE

OP<sub>C</sub>: Operator variable derived (128 bits)  
 r1...r5: fixed rotations constants  
 c1...c5: fixed addition constants  
 E<sub>K</sub>: encryption with key K

Note: f1\*, f5\* used in case sync.failure at auth. (see Sect.7.2.3, Auth.failures) in the book



Definition of f1, f1\*, f2, f3, f4, f5 and f5\*

f0

the random challenge generating function;

f1 the network authentication function;

f1\* the re-synchronisation message authentication function;

f2 the user authentication function;

f3 the cipher key derivation function;

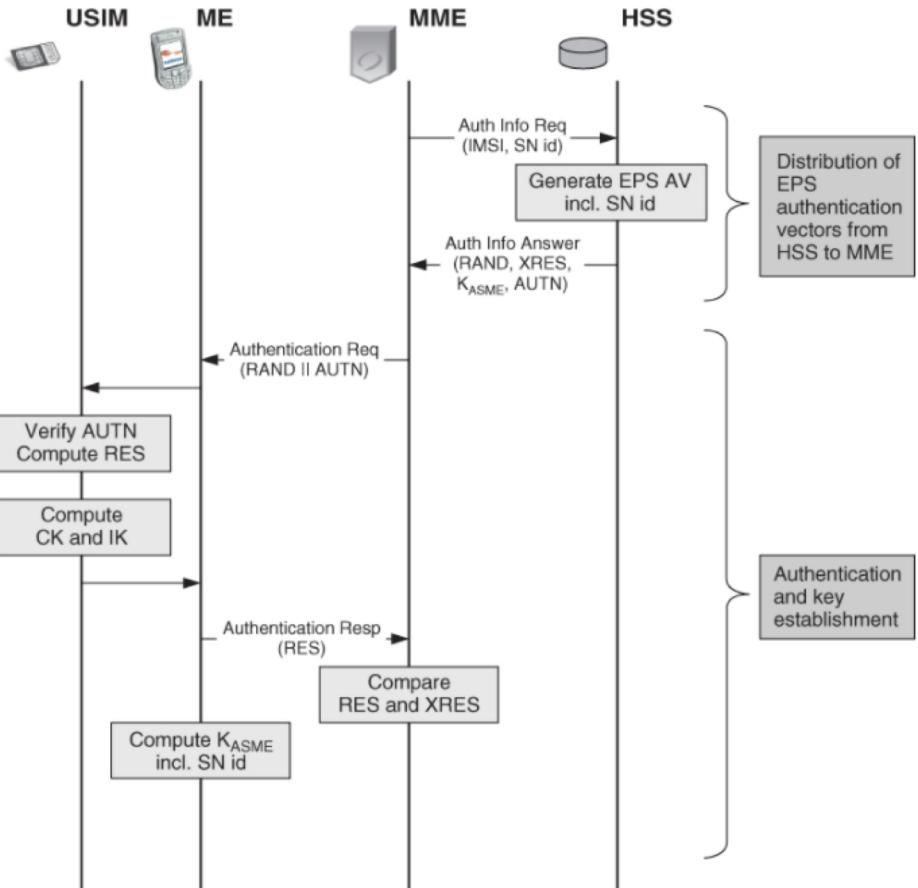
f4 the integrity key derivation function;

f5 the anonymity key derivation function.

f5\*

f5\* the anonymity key derivation function for the re-synchronisation message.

# EPS AKA – User Side



- Dacă USIM suportă GSM, convertește (CK, IK) într-o cheie GSM  $K_c$

# Algoritmi criptografici

# Principii

- **Flexibilitatea algoritmilor:** algoritmii criptografici ar trebui înlocuiți fără dificultăți
  - Permite îndepărtarea algoritmilor depășiți
  - Numărul de algoritmi ar trebui să fie mic (pentru motive de sincronizare și gestionare), dar nu doar 1 ...
  - ... pentru că dacă un algoritm este spart să se folosească un altul
- **Diversitatea algoritmilor:** proiectarea algoritmilor ar trebui să difere cât mai mult posibil
  - *De ce? Unde ați mai întâlnit acest principiu în cripto?*
  - Scenarii de urgență

# Emergency / Scenarii de urgență

- **Null algorithm:** nu oferă protecție criptografică
  - Trebuie să existe pentru scenarii de urgență
  - Problema din perspectiva securității, deoarece poate fi declanșată aceasta utilizare în cazurile în care protecția ar trebui activată
- **Turn-off principle:** **protecția criptografică ar trebui să fie activată în mod implicit și numai la cerere (în cazul scenariilor speciale) ar trebui să fie oprită**
- **EEA0 (EPS Encryption Algorithm):** identitatea (i.e. textul criptat este același cu textul clar)
- **EIA0 (EPS Integrity Algorithm) :** o secvență de 32 biți de 0 se adaugă mesajului
  - Motiv: **păstrați scenariile protejate și ne-protejate cât mai asemănătoare posibil** (de exemplu: aceeași lungime)

# Confidențialitate

- Aceeași structură pentru protecția NAS și AS
- 128-EEA1: **SNOW 3G** adaptată pentru arhitectura de securitate EPS
  - Chei pe 128 bits
- 128-EEA2: **AES** / Kasumi
  - Chei pe 128 bits
  - CTR mode

# Integritate

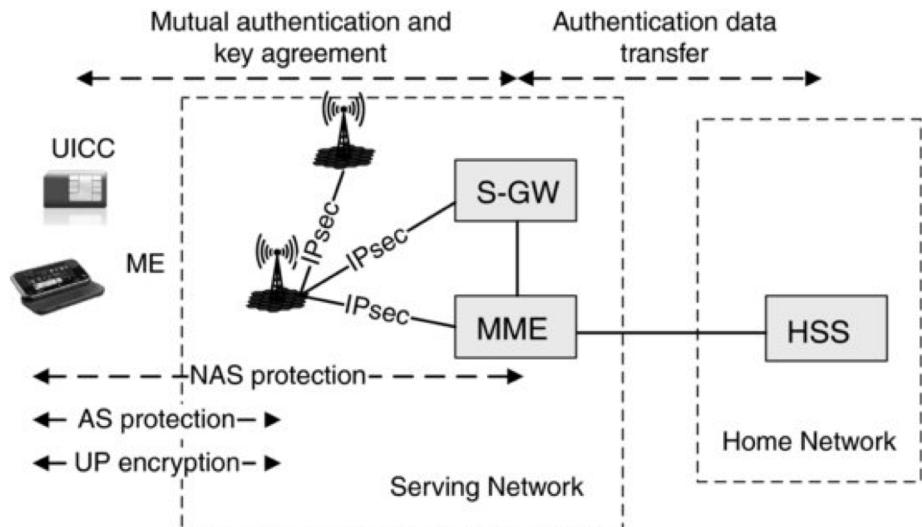
- Aceleași principiu ca și pentru confidențialitate
- **128-EIA1: UIA 2 (SNOW 3G)** adapted to the EPS security architecture
  - Chei pe 128 bits
- **128-EIA2: Cipher-based MAC (AES)**
  - Chei pe 128 bits
- Lungimea cheii în denumire implică faptul că alte lungimi ale cheilor (de exemplu: 192, 256) pot fi utilizate în cazul unei îmbunătățiri a securității

# Derivarea cheilor

- **One-way**: un adversar nu poate folosi o cheie pentru a obține o cheie situată superioară în ierarhie
- **Independentă**: 2 chei deriveate din aceeași cheie ar trebui să fie independente
- **SHA-256** în **HMAC mode**

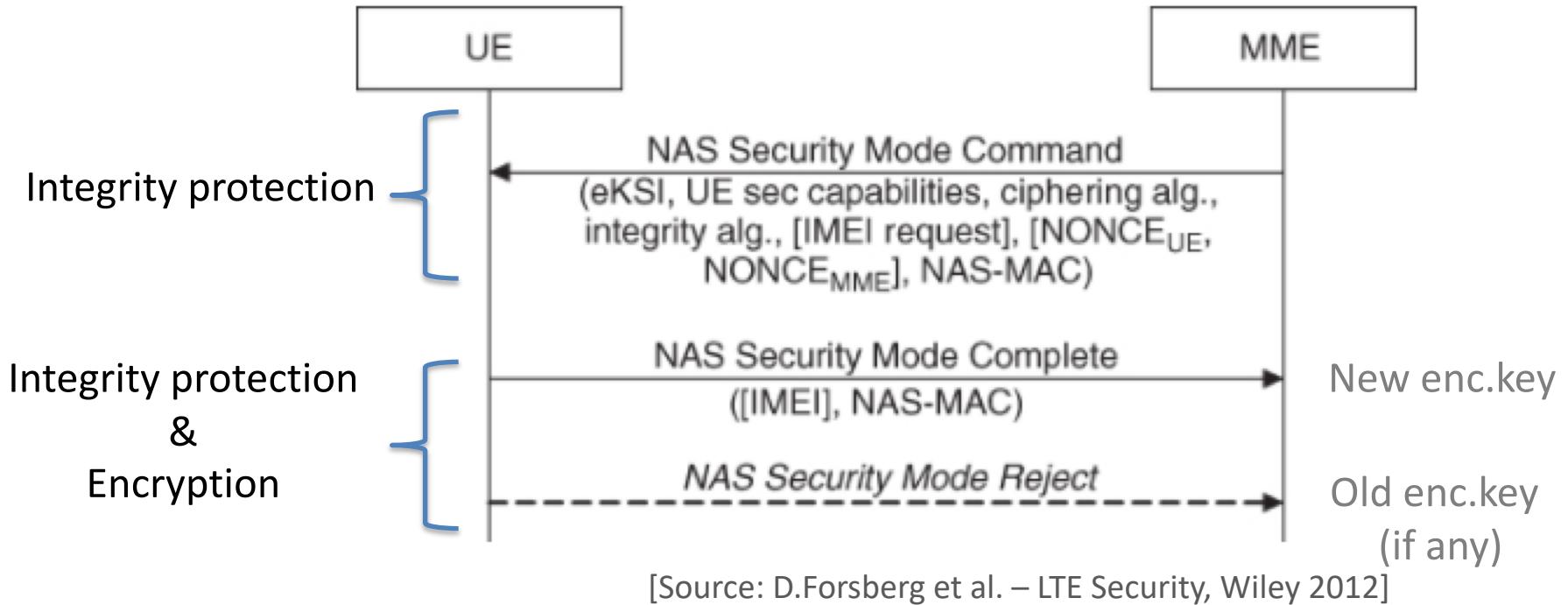
# Negocierea algoritmilor

- Algoritmii sunt **negociați separat** pentru AS (între UE și eNodeB) și NAS (între UE și MME)
- Negocierile se bazează pe capabilitățile UE și o listă de algoritmi criptografici permisi în eNodeB, respectiv MME în ordinea priorită
- eNodeB și MME sunt responsabile pentru selectarea nivelului AS, respectiv a algoritmilor nivelului NAS, după ce UE își trimit capabilitățile în procedura de atașare
- Selectia este indicată în **AS Security Mode Command**, respectiv **NAS Security Mode Commands**



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

# NAS Signalling Protection

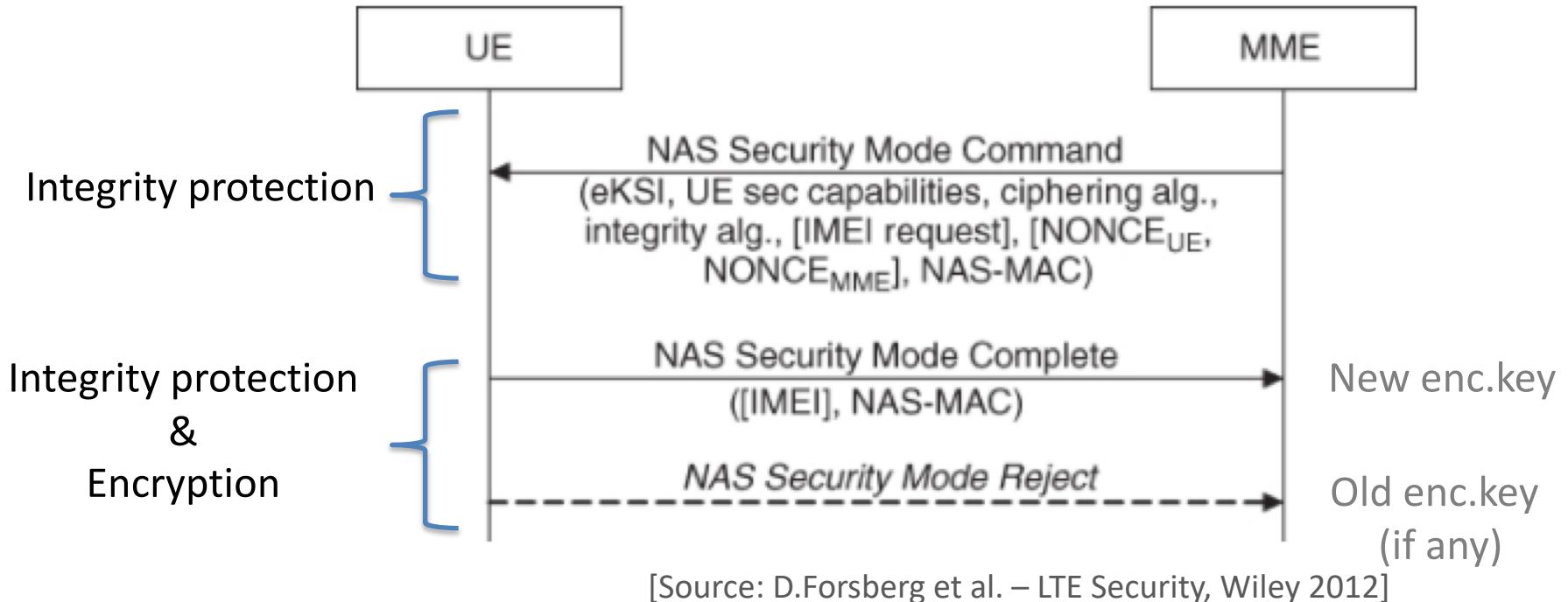


eKSI: key set identifier that identifies the key  $K_{ASME}$

NONCE<sub>UE</sub>, NONCE<sub>MME</sub>: used for mobility

**Întrebare:** De ce NAS Security Mode Command nu este criptată?  
*UE nu știe algoritmul și cheia pentru decriptare*

# NAS Signalling Protection



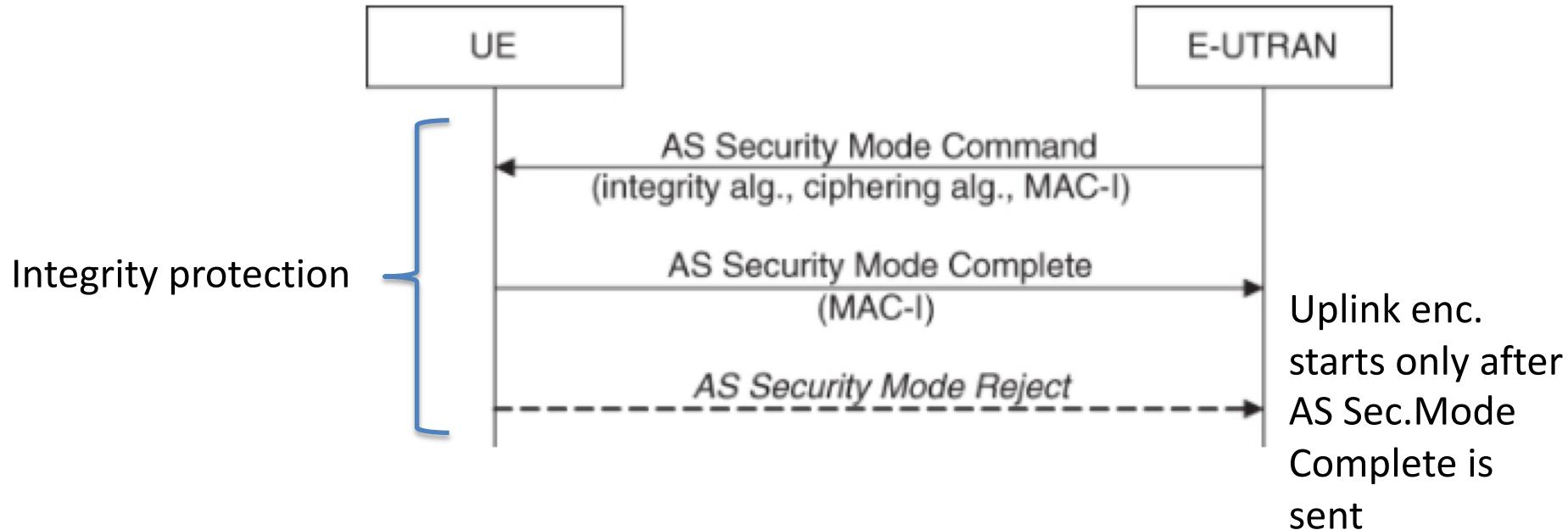
eKSI: key set identifier that identifies the key  $K_{ASME}$

NONCE<sub>UE</sub>, NONCE<sub>MME</sub>: used for mobility

**Întrebare:** De ce este NAS Security Mode Complete criptat?

*Pentru a nu expune IMEI*

# AS Signalling Protection



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

Întrebare: De ce este AS Security Mode Complete nu este criptat?

*Nu conține informație privată*

# Standard de Securitate EPS



- 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