Lecture 22

Cellular Networks Security

Nicola Laurenti December 11, 2020

Lecture 22— Contents

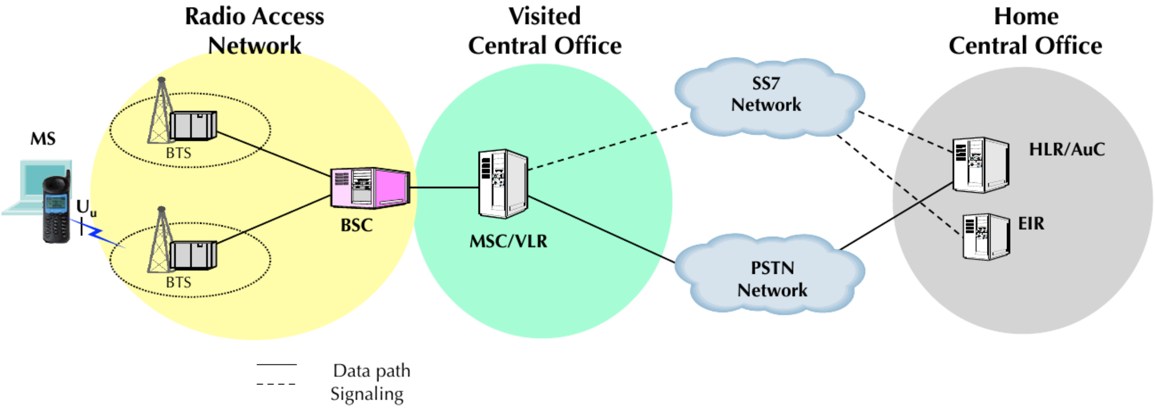
2nd generation cellular networks: GSM

3rd generation cellular networks: UMTS

4th generation cellular networks: LTE

5th generation cellular networks

GSM refererence architecture



GSM security fundamentals

Security services

GSM security was designed to provide the following services:

user privacy against attackers trying to identify and/or trace a specific user's location

access control against network usage by unauthorized entities

user authentication against billing frauds

user data secrecy against eavesdropping on the radio channel

...no data integrity protection

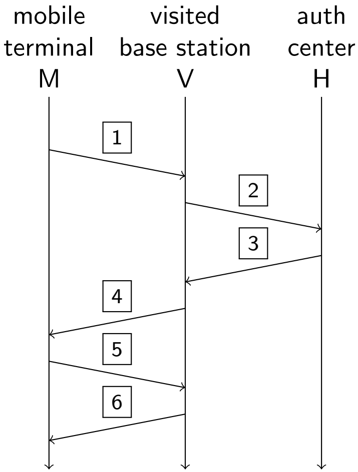
Long term credentials

The long term credentials for a user A are his/her International mobile subscriber identity (IMSI) id_A and his master secret key k_A.
The pair $(\mathrm{id}_\mathsf{A}, k_\mathsf{A})$ is stored in the user owned Subscriber identity module (SIM) and in the corresponding Authenticaton center

GSM security design principles

- protection of the (mobile – base station) radio link only
- completely new cryptographic functions (not publicly discussed before standardization)
- non mutual entity authentication: only the mobile user is authenticated
- interactive authentication protocol to be performed between mobile and visited BSC
- long term credentials are not shared with the visited BSC (may belong to another operator)
- assignment of a temporary pseudonym to mobile
- low complexity encryption / decryption

GSM mobile user authentication protocol



$\boxed{1}$ $\mathsf{M} \to \mathsf{V}$: $\mathrm{id}_\mathsf{M}, \mathrm{id}_\mathsf{H}$

$\boxed{2}$ $\mathsf{V} \to \mathsf{H}$: $\mathrm{id}_\mathsf{M}, \mathrm{id}_\mathsf{V}$

$\boxed{3}$ H : for $n = 1, \ldots, N$:

generate random challenge (128 bit) $c_n \sim \mathcal{U}(\mathcal{C})$

compute expected response (32 bit) $\hat{r}_n = A3(k_\mathsf{M}, c_n)$

compute session key (64 bit) $\hat{k}'_n = A8(k_\mathsf{M}, c_n)$

$\mathsf{H} \to \mathsf{V}$: $[c_1, \hat{r}_1, \hat{k}'_1, \ldots, c_N, \hat{r}_N, \hat{k}'_N]$

$\boxed{4}$ $\mathsf{V} \to \mathsf{M}$: c_1

$\boxed{5}$ M : compute response $r_1 = A3(k_\mathsf{M}, c_1)$

compute session key $k'_1 = A8(k_\mathsf{M}, c_1)$

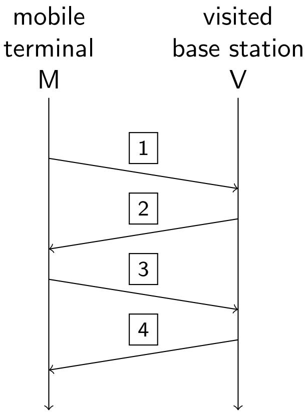
$\mathsf{M} \to \mathsf{V}$: r_1

$\boxed{6}$ V : if $r_1 = \hat{r}_1$, accept M and generate temporary $\mathrm{id}'_{\mathsf{M},1}$

$\mathsf{V} \to \mathsf{M}$: $[\mathrm{id}_\mathsf{V}, \mathrm{id}'_{\mathsf{M},1}]$

GSM re-authentication protocol

With the same VLR V:



$\boxed{1}$ M $\rightarrow$ V : $\mathrm{id}'_{\mathsf{M,n}}, \mathrm{id}_{\mathsf{V}}$

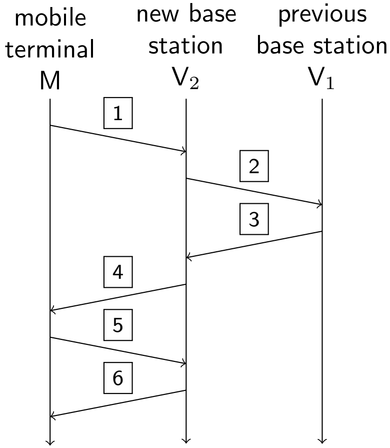
$\boxed{2}$ V $\rightarrow$ M : c_{n+1}

$\boxed{3}$ M : compute $r_{n+1} = A3(k_{\mathsf{M}}, c_{n+1})$ and $k'_{n+1} = A8(k_{\mathsf{M}}, c_{n+1})$
M $\rightarrow$ V : r_{n+1}

$\boxed{4}$ V : if $\hat{r}_{n+1} = \hat{r}_{n+1}$, accept M and generate temporary $\mathrm{id}'_{\mathsf{M,n+1}}$
V $\rightarrow$ M : $[\mathrm{id}_{\mathsf{V}}, \mathrm{id}'_{\mathsf{M,n+1}}]$

GSM re-authentication protocol

Handover from a VLR V_1 to another VLR V_2:



$\boxed{1}$ $M \to V_2$: $\mathrm{id}'_{M,n}, \mathrm{id}_{V_1}$

$\boxed{2}$ $V_2 \to V_1$: $\mathrm{id}'_{M,n}, \mathrm{id}_{V_1}$

$\boxed{3}$ $V_1 \to V_2$: $\mathrm{id}'_{M,n}, \mathrm{id}_M, [c_{n+1}, \hat{r}_{n+1}, \hat{k}'_{n+1}, \ldots, c_N, \hat{r}_N, \hat{k}'_N]$

$\boxed{4}$ $V_2 \to M$: c_{n+1}

$\boxed{5}$ M : compute $r_{n+1} = A3(k_M, c_{n+1})$ and $k'_{n+1} = A8(k_M, c_{n+1})$
$M \to V_2$: r_{n+1}

$\boxed{6}$ V_2 : if $r_{n+1} = \hat{r}_{n+1}$, accept M and generate temporary $\mathrm{id}'_{M,n+1}$
$V_2 \to M$: $[\mathrm{id}_{V_2}, \mathrm{id}'_{M,n+1}]$

GSM encryption

GSM provides 4 encryption modes: A5/0 (none), A5/1 (good), A5/2 (weak), A5/3 (strong)
A5/1 is a binary stream cipher

$$\mathcal{A}_u = \mathcal{A}_x = \mathcal{A}_z = \mathcal{A}_k = \mathcal{A}_s = \mathbb{B} = \{0,1\}$$

The global state comprises the state of the 3 LFSRs (19-bit, 22-bit, and 23-bit), both state and key are 64-bit long

$$\mathcal{K} = \mathcal{A}_k^{\ell_k} = \mathbb{B}^{\ell_k} \quad , \quad \mathcal{S} = \mathcal{S}_1 \times \mathcal{S}_2 \times \mathcal{S}_3 \quad , \quad \boldsymbol{s}_n = [\boldsymbol{s}_{1,n}, \boldsymbol{s}_{2,n}, \boldsymbol{s}_{3,n}] \quad , \quad \mathcal{S}_i = \mathbb{B}^{\ell_i}$$

$$\boldsymbol{s}_{i,n} = [s_{i,n}(0), \ldots, s_{i,n}(\ell_i - 1)] \quad , \quad \ell_1 = 19, \ell_2 = 22, \ell_3 = 23 \quad , \quad \ell_s = \ell_1 + \ell_2 + \ell_3 = 64$$

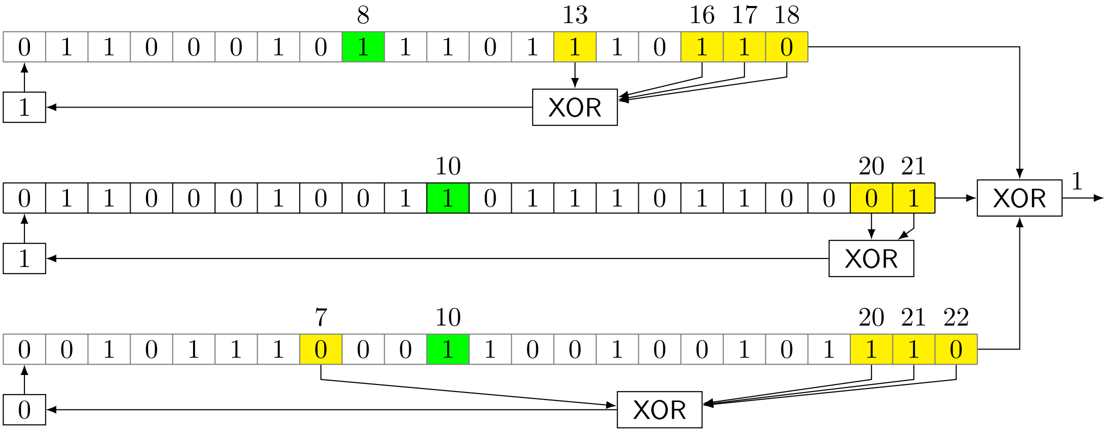
Key stream generation

$$h \,:\, z_n = s_{1,n}(\ell_1 - 1) \oplus s_{2,n}(\ell_2 - 1) \oplus s_{3,n}(\ell_3 - 1)$$

depends on current state (XOR the last bit from each LFSR), not on key.

State update each register i advances only if $s_{i,n}(c_i) = s_{j,n}(c_j)$ for some other $j \neq i$ (at each step either all or only two LFSRs advance)

The GSM cipher A5/1: structure



The GSM cipher A5/1: vulnerabilities

Specific vulnerabilities

- State update of A5/1 is not one-to-one
- Long time with the same BSC, states will concentrate
- 64 bit key / state are too short

$\rightarrow$

Biased birthday state guessing attack

1. precompute the 64-bit outputs that correspond to the most likely states
2. observe until any of them appears in the actual transmission
3. the state is known

The security level of k'_{M} was initially set to 54 bits (with 10-bit zero padding), then extended to 64 actual bits

GSM security vulnerabilities

In the authentication protocol

- No authentication of V to M $\Rightarrow$ M will respond to any challenge
- Weakness of the A3 function: for some $c_n = \gamma_i$, r_n leaks information about k_M
- A3 is used in a time invariant way

→

k_M recovery attack

- By simulating a fake base station in the vicinity of the victim mobile,
- or by directly accessing the victim SIM (phone resellers, repair shops, ...)

an attacker can submit challenges $\{\gamma_i\}$ and recover k_M (aka SIM cloning)

In the security negotiation

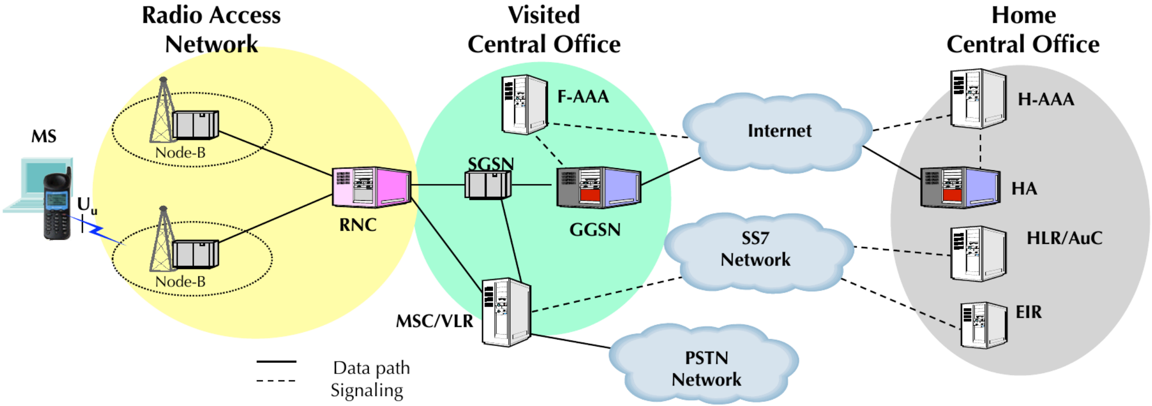
- Negotiation of the encryption mechanism (which A5/X) is carried out between V and M without H being aware
- M cannot enforce a minimum security level

→

Security downgrade attack

- a forged V' can force a low security level (A5/2) or sometimes none (A5/0)

UMTS refererence architecture



UMTS security fundamentals

Security services

In addition to the security services already provided by GSM, UMTS was designed to provide the following services:

mutual authentication between mobile user and network

user data integrity against forging/modification in the radio channel

key management with ephemeral keys

Moreover, it was designed to use stronger cryptographic mechanisms

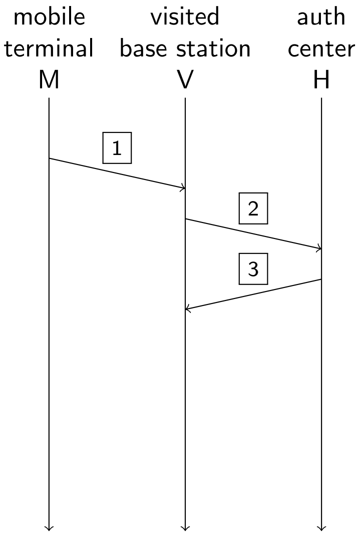
Long term credentials

The long term credentials for a user A are his/her International mobile subscriber identity (IMSI) id_A and his master secret key k_A.
The pair $(\mathrm{id}_\mathsf{A}, k_\mathsf{A})$ is stored in the user owned Subscriber identity module (USIM) and in the corresponding Authenticaton center (AuC)

UMTS security design principles

- protection of the (mobile – base station) radio link only
- robust cryptographic functions (publicly discussed before standardization)
- mutual entity authentication: also the network authenticates itself to the mobile user
- interactive authentication protocol to be performed between mobile and visited BSC
- long term credentials are not shared with the visited BSC (may belong to another operator)
- assignment of a temporary pseudonym to mobile
- low complexity encryption / decryption, signing / verification

UMTS entity authentication protocol



$\boxed{1}$ $\mathsf{M} \rightarrow \mathsf{V}$: $\mathrm{id}_{\mathsf{M}}, \mathrm{id}_{\mathsf{H}}$

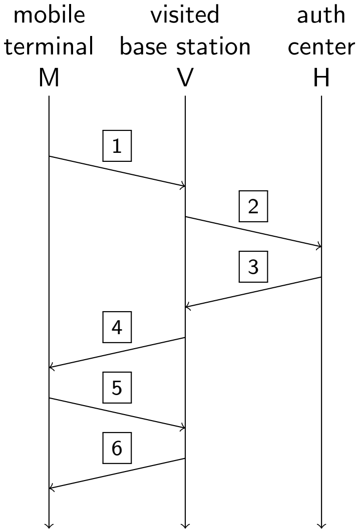
$\boxed{2}$ $\mathsf{V} \rightarrow \mathsf{H}$: $\mathrm{id}_{\mathsf{M}}, \mathrm{id}_{\mathsf{V}}$

$\boxed{3}$ H : for $n = 1, \ldots, N$:

- generate random challenge (128 bit) $c_n \sim \mathcal{U}(\mathcal{C})$
- compute expected response (32 bit) $\hat{r}_n = f_2(k_{\mathsf{M}}, c_n)$
- compute session keys for
  - encryption (128 bit) $k'_{\mathsf{C},n} = f_3(k_{\mathsf{M}}, c_n)$
  - data MAC (128 bit) $k'_{\mathsf{I},n} = f_4(k_{\mathsf{M}}, c_n)$
  - anonymity (48 bit) $k'_{\mathsf{A},n} = f_5(k_{\mathsf{M}}, c_n)$
- step sequence number (48 bit) $s_{\mathsf{M},n}$
- update security parameters (16 bit) y_n
- compute A+IP tag $t_n = f_1(k_{\mathsf{M}}, c_n, y_n, s_{\mathsf{M},n})$
- compute network auth token $a_n = [k'_{\mathsf{A},n} \oplus s_{\mathsf{M},n}, y_n, t_n]$

$\mathsf{H} \rightarrow \mathsf{V}$: $[c_1, \hat{r}_1, k'_{\mathsf{C},1}, k'_{\mathsf{I},1}, a_1, \ldots, c_N, \ldots, a_N]$

UMTS entity authentication protocol



$\boxed{4}$ V → M : (c_1, a_1)

$\boxed{5}$ M : compute anonymity key $k'_{\mathsf{A},1} = f_5(k_\mathsf{M}, c_1)$

retrieve $s_{\mathsf{M},1}$, y_1, and t_1 from a_1 and $k'_{\mathsf{A},1}$

compute $\hat{t}_1 = f_1(k_\mathsf{M}, c_1, y_1, s_{\mathsf{M},1})$

if $t_1 = \hat{t}_1$, and $s_{\mathsf{M},1}$ is consistent

accept V as legitimate

compute session keys

$k'_{\mathsf{C},1} = f_3(k_\mathsf{M}, c_1), k'_{\mathsf{I},1} = f_4(k_\mathsf{M}, c_1)$

compute response $r_1 = f_2(k_\mathsf{M}, c_1)$

M → V : r_1

$\boxed{6}$ V : if $r_1 = \hat{r}_1$, accept M and generate temporary $\mathrm{id}'_{\mathsf{M},1}$

V → M : $[\mathrm{id}_\mathsf{V}, \mathrm{id}'_{\mathsf{M},1}]$

UMTS cryptographic mechanisms: key derivation functions

- The functions $f_1, \ldots, f_5$ are operator dependent and implemented in the USIM and AuC
- They shoud be good one-way (e.g., cryptographic hash) functions
- They should prevent preimage attacks con k_{M}, even if the challenge c_i is known
- They should "look uncorrelated", i.e. the ouptut of one f_i should not leak information about that of the others

UMTS cryptographic mechanisms: encryption and authentication codes

Both encryption and message A+IP mechanism are implemented in the UE and the RNC.

Suite 1

Developed by 3GPP as of UMTS Release '99, and based on the symmetric block cipher Kasumi (patent Mitsubishi), a Feistel cipher with $2\ell = 64$-bit blocks, $\ell_k = 64$-bit keys and $n = 8$ rounds

Encryption (UEA1) Function f_8 uses Kasumi in counter (CTR) mode with the current key $k'_{\mathsf{C},n}$

Message authentication code (UIA1) Function f_9 uses Kasumi in CBC-MAC mode with the current key $k'_{\mathsf{I},n}$, tag t is truncated to 32 bits

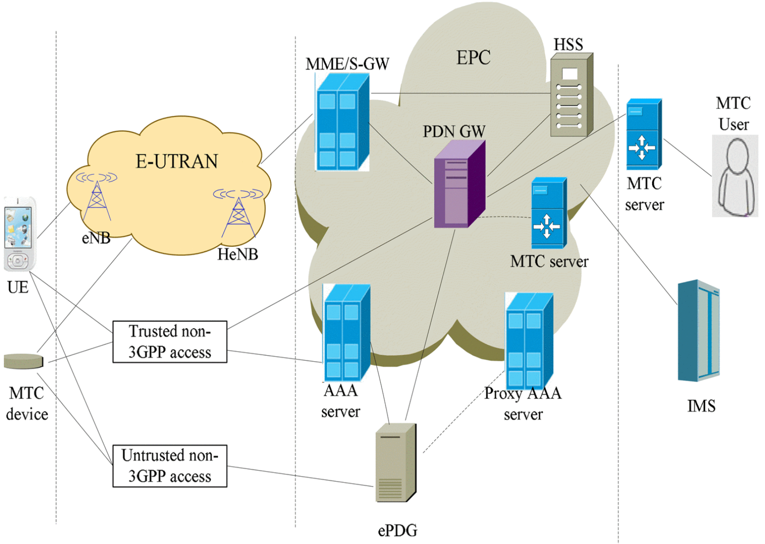
Suite 2

Later, in 2006 two new mechanisms were released that make use of SNOW 3G, an additive stream cipher based on a LFSR, with 32-bit symbols $\mathcal{A}_u = \mathcal{A}_x = \mathcal{A}_k = \mathcal{A}_s = \mathcal{A}_z = \mathrm{GF}(2^{32})$, 608-bit state $\boldsymbol{s}_n \in \mathcal{S} = \mathcal{A}_s^{19}$, a 128-bit key, $\boldsymbol{k} \in \mathcal{K} = \mathcal{A}_k^4$ and a 128-bit initialization vector $\boldsymbol{v} \in \mathcal{K}$

Encryption (UEA2) Function f_8 uses SNOW 3G as a stream cipher with the current key $k'_{\mathsf{C},n}$

Message authentication code (UIA2) Function f_9 uses SNOW 3G with the current key $k'_{\mathsf{I},n}$, tag t is truncated to the last 32 bits

LTE reference architecture



Main blocks

- Evolved Packet Core (EPC)
- Evolved Universal Terrestrial Radio Access Network (E-UTRAN)
- IP multimedia subsystem (IMS) network

New entities

- Machine Type Communication (MTC)
- Home eNodeB (HeNB)
- non-3GPP access networks
- evolved packet data gateway (ePDG)

Security in the LTE standard

LTE security extends its domain beyond the UE-eNB radio link

Security domains

network access protection of 3GPP radio link between UE and EPC

user domain protection of internal connection between USIM and UE

network domain protection of wired network aong nodes

application domain protection at the application layer

non 3GPP domain protection of non-3GPP radio link between UE and EPC

Security in the LTE standard

Security features

LTE has been designed with the following enhanced security features wrt UMTS:

new AKA for mutual authentication between the User Equipment (UE) and the Mobility Management Entity (MME)

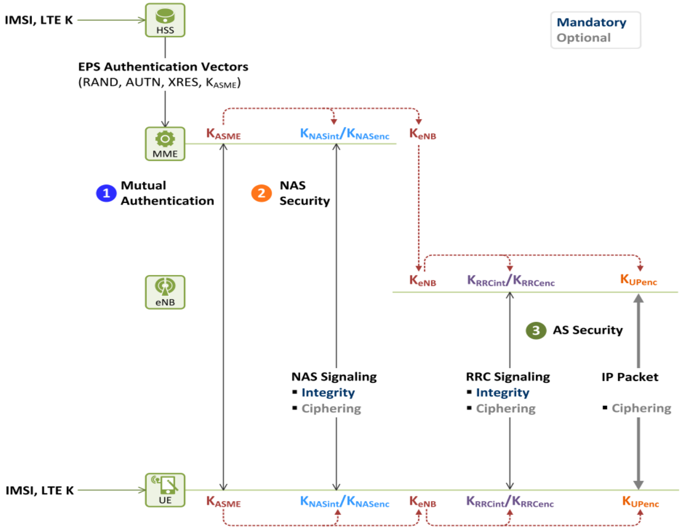
new key hierarchy with keys shared only between USIM $\leftrightarrow$ AuC, USIM $\leftrightarrow$ HSS, UE $\leftrightarrow$ MME, UE $\leftrightarrow$ eNB

new handover key management mechanism

Long term credentials

The long term credentials for a user A are his/her International mobile subscriber identity (IMSI) id_{A} and his LTE secret key k_{A}.
The pair $(\mathrm{id}_{\mathsf{A}}, k_{\mathsf{A}})$ is stored in the user owned Universal subscriber identity module (USIM) and in his/her Authenticaton center (AuC)

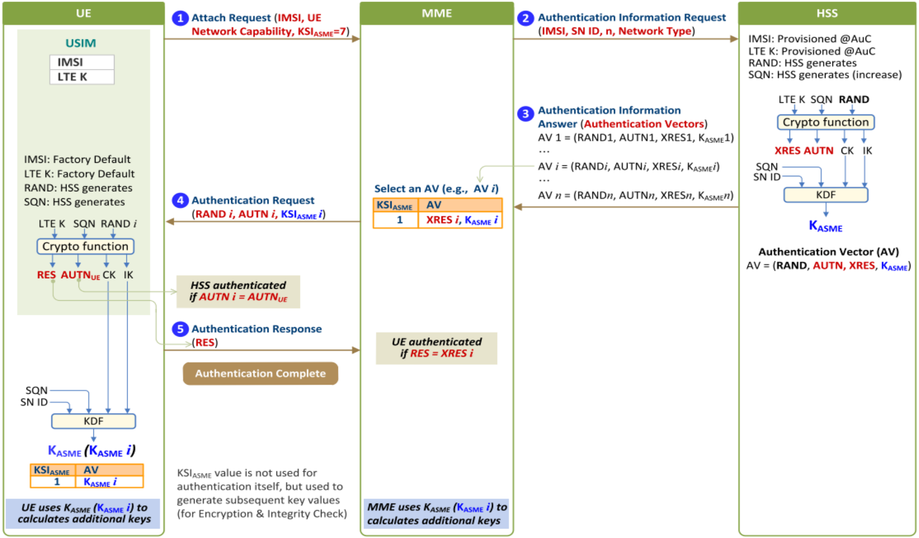
Overview of EPS Authentication and Key Agreement



EPS-AKA main steps

1. LTE mutual authentication between MME and UE
2. Non access stratum (NAS) KA negotiating mechanisms and establishing keys between MME and UE
3. Access stratum (AS) KA negotiating mechanisms establishing keys between eNBs and UE (both for C- and U-plane).

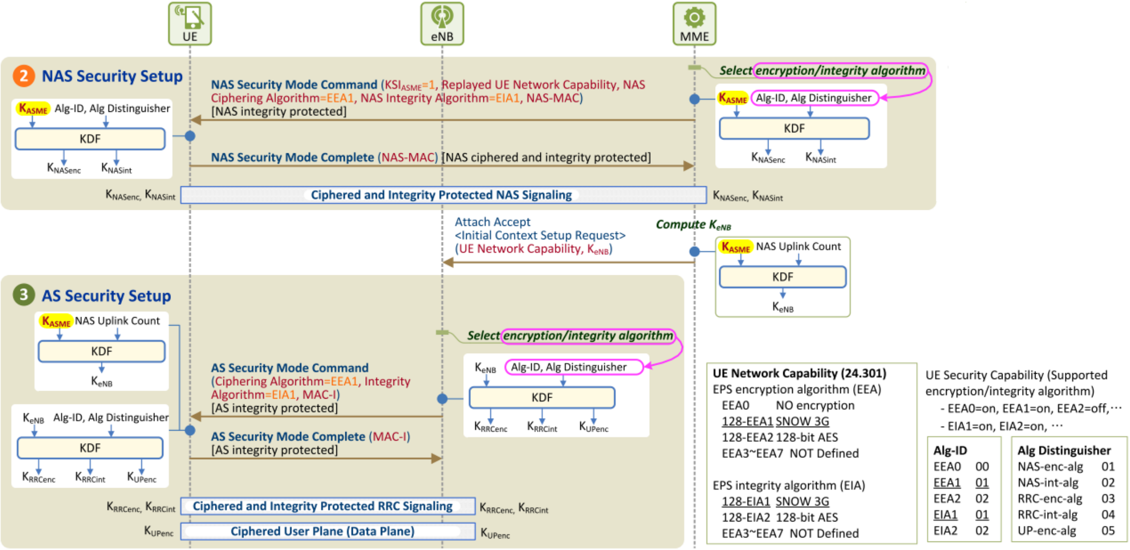
LTE authentication protocol



Protocol steps

1. Attach request
2. Request for auth info
3. Answer with auth info
4. Auth request
5. Auth response
6. Auth complete
7. Key derivation

NAS and AS security negotiation



Key handover among eNBs

Motivation

k_{eNB} should be unique for each eNB and known only by that specific base station.

- user's mobility forces a change of the serving eNB.
- backward security: the new eNB does not know the previous k_{eNB}
- 2-step forward security: the old eNB knows the next k_{eNB} but won't know the following.

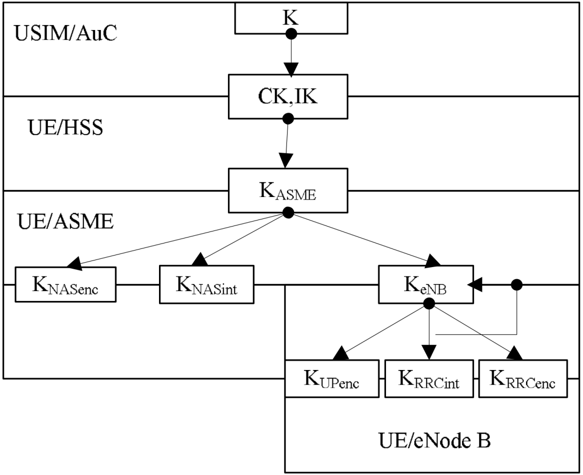
Handover techniques

A Next Hop key k_{NH} is used: unique for each eNB and delivered and updated by MME.

Horizontal key derivation obtain new $k_{\text{eNB},t+1}$ by applying a one-way function to the old one:
$k_{\text{eNB},t+1} = h_\alpha(k_{\text{eNB},t})$.

Vertical key derivation when a base station has a fresh NH key, it obtains the new k_{eNB} as:
$k_{\text{eNB},t+1} = h_\alpha(k_{\text{NH}})$.

LTE key hierarchy

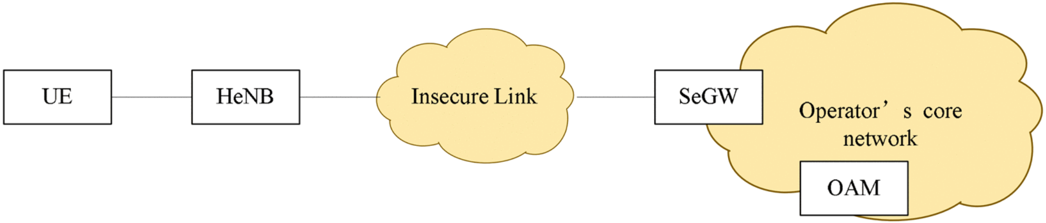


key	period	bits	use
k_A	lifetime	128	master
CK	session	128	encryption
IK	session	128	integrity
k_{ASME}	session	256	master
$k_{NAS,enc}$	session	256	NAS encrypt
$k_{NAS,int}$	session	256	NAS integrity
k_{eNB}	handover	256	master
$k_{RRC,enc}$	handover	256	AS C-plane encryption
$k_{RRC,int}$	handover	256	AS C-plane integrity
$k_{UP,enc}$	handover	256	AS U-plane encryption

LTE encryption and integrity protection mechanisms

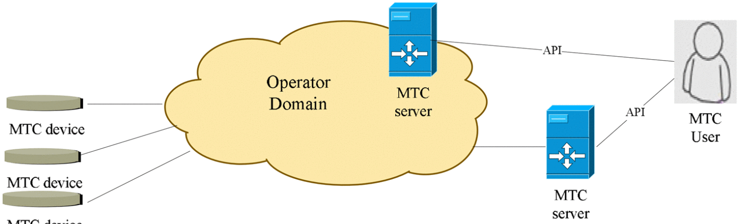
type	EPS Encryption Algorithm (EEA)	EPS Integrity Algorithm (EIA)
0	none	none
1	SNOW 3G	SNOW 3G
2	AES	AES CBC-MAC
3	ZUC (stream cipher)	ZUC

Security at HeNB

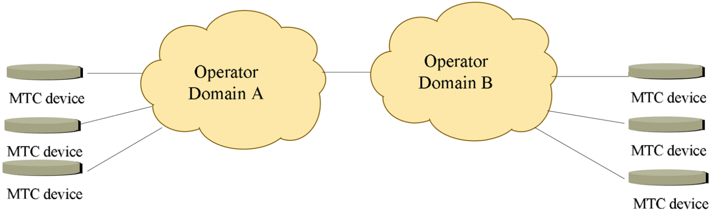


A HeNB is a low-power access point (femtocell)
HeNB connects to the EPC over Internet (possibly throug an insecure link)
The security gateway (SeGW) performs mutual authentication with HeNB

Security in MTC



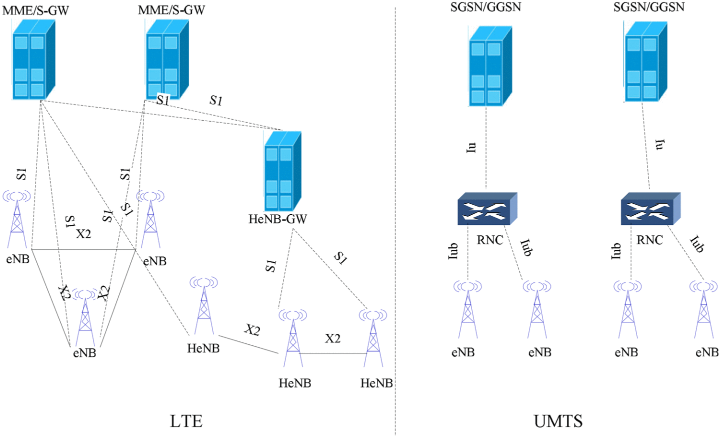
(a) MTC server is located in or outside the operator domain



(b) MTC Devices communicating directly with each other without intermediate MTC server

- security between MTC device and EPC
- security between MTC server / user and EPC
- security between MTC device and MTC server/user

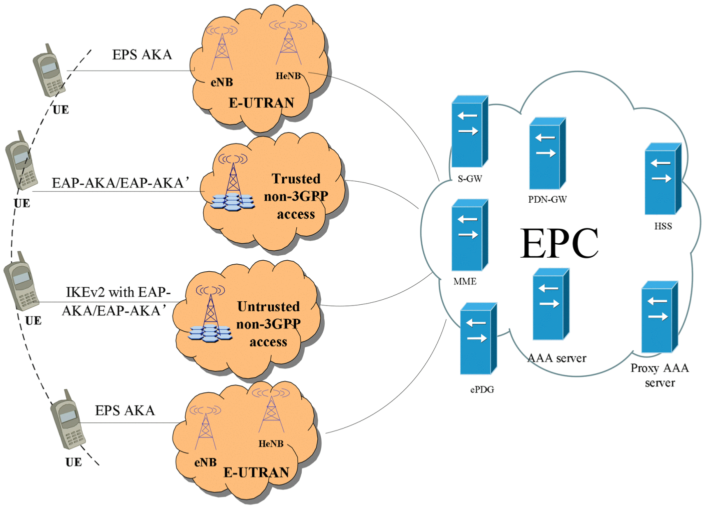
LTE vs UMTS network access



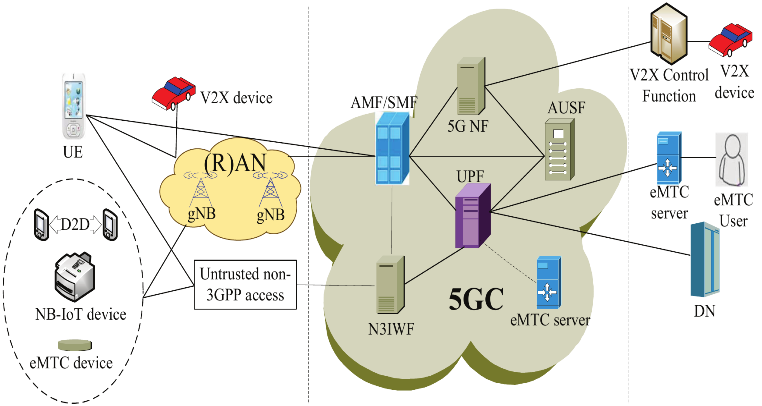
flat, IP-based ⇒ more risks

hierarchical, closed, less risky

Handover to non 3-GPP access



5G reference architecture



Main blocks

- 5G Core (5GC)
- Radio Access Network (RAN)
- 5G Network functions (5G NF)

New entities

- Vehicular to everything (V2X)
- Internet of Things (IoT)
- Device-to-device (D2D)

5G security architecture

5G security extends its domain beyond the UE-eNB radio link

Security domains

network access protection of 3GPP and non-3GPP radio link between UE and EPC

user domain protection of internal connection between USIM and UE

network domain protection of wired network aong nodes

application domain protection at the application layer

service based architecture protection of service based interfaces

visibility and configurability enabling the user to be informed whether a security service is in operation

Security for massive MIMO

Challenges and threats

- passive eavesdropping
- pilot contamination / spoofing

Proposed solutions

- cooperation between base stations
- physical layer authentication
- physical layer secrecy

Security for software defined networking (SDN)

Challenges and threats

- network functions as appications (what about malicious apps?)
- centralized control plane
- forwarding devices with limited capacity

Proposed solutions

- access control to network configuration for applications
- access control to controller
- authentication and authorization for applications that change flow rules

Security for network function virtualization (NFV)

Challenges and threats

- coexistence of different systems on the same physical device
- incresaed configuration complexity

Proposed solutions

- consistent security policies for vistrtualized environments
- slicing and distributed VNFs

Summary

In this lecture we have:

- introduced the security design principles in cellular networks, evolving from 2G to 5G
- described the mobile to network authentication and key agreement protocols, evolving from 2G to 4G
- discussed the choice of cryptographic mechanisms, evolving from 2G to 4G
- presented the security issues and landscape for 5G networks

Assignment

- class notes

End of lecture

Phone security, reproduced from xkcd URL: xkcd.com/1934