Cryptography for Mobile security

Valtteri Niemi
University of Helsinki
Fall 2018
• The secret key of user i exists (and stays) only in two places:
  - in her own SIM card
  - in the Authentication Center
Trust model

- Each operator shares long term security association with its subscriber
  - Security association credentials stored in tamper-resistant identity module issued to subscriber (called the SIM or UICC)

- Operators may enter roaming agreements with other operators → a certain level of trust exists between the respective domains
Original design decisions for GSM security

• GSM aimed to be *as secure as the fixed networks* to which it would be connected

• *Active attacks* which involve impersonating a network element were intentionally *not* addressed
Authentication of user i

• Authentication Center chooses a random number RAND and computes

\[
\text{RAND} \quad K_i
\]

one-way function

\[
\text{SRES} \quad Kc
\]

• The triple (RAND, SRES, Kc) is sent to the MSC/VLR.
• MSC/VLR sends RAND to the phone.
• The one-way function of computing SRES/Kc is called A3/A8. These are *operator-specific*. 
Authentication cont’d

• The SIM card computes

\[
\text{RAND} \quad \text{Ki}
\]

\[
\downarrow \quad \downarrow
\]

\[
\text{one-way function}
\]

\[
\downarrow \quad \downarrow
\]

\[
\text{SRES’} \quad \text{Kc’}
\]

and sends the output SRES’ to the MSC/VLR.

• If SRES = SRES’, then the call is accepted.
Encryption of the call

• During the authentication a secret key is exchanged: $$K_c = K_c'$$

   by which all calls/signalling are encrypted between the phone and the base station until the next authentication occurs.

• The encryption algorithm is called A5. The first two versions A5/1 and A5/2 were standardized but the specs are confidential and managed by GSM Association. The third version A5/3 is publicly available. All make use of 64-bit keys Kc.

• There is also a 128-bit key algorithm A5/4.
  – Deployment of this is more difficult than in A5/3 case because longer keys require changes in many parts of the system
Structure of A5 stream cipher

Kc (64 bits) \rightarrow \text{core of A5} \rightarrow \text{pseudorandom bit stream (114)} \rightarrow \text{encrypted message (114)}

frame number (22) \rightarrow \text{core of A5} \rightarrow \text{pseudorandom bit stream (114)} \rightarrow \text{plain message (114)}

\text{XOR}
GSM security protocol

MS (SIM)
IMSI, $Ki$

MSC/VLR
(IMSI, $Ki$)

HLR

{IMSI, $Ki$}

IMSI / TMSI

RAND

$Kc$

SRES

encrypted TMSI

IMSI

RAND, XRES, $Kc$

SRES=XRES ?
3G security
3G security background

• Leading *design principles* were:
  – Move useful 2G security features to 3G
  – Add countermeasures against real weaknesses in 2G

• Main *security characteristics* in GSM ( = 2G ) :
  • User authentication & radio interface encryption
  • SIM used as security module
  • Operates without user assistance
  • Requires minimal trust in serving network

• Main *weaknesses* in GSM:
  • Active attacks are possible (false BS etc.)
  • Authentication data (e.g. cipher keys) sent in clear inside one network and between networks
  • Cipher keys too short (if 64 bits)
  • Secret algorithms do not create trust
Active attack

• A false element masquerades
  – as a base station towards terminal
  – as a terminal towards network

• Objectives of the attacker:
  – eavesdropping
  – stealing of connection
  – manipulating data
3G system architecture

based on GSM/GPRS architecture

Encryption & integrity

Execution of authentication

Transport of auth data
Mutual authentication

• There are three entities involved:
  – Home network HN (AuC)
  – Serving network SN (VLR/SGSN)
  – Mobile station MS (USIM)
• Executed whenever SN decides

• The idea: SN checks MS’s identity (as in GSM) and MS checks that SN has authorization from HN
• A master key $K$ is shared between MS and HN
• GSM-like challenge-response in user-to-network authentication
• Network proves its authorization by giving a token AUTN which is protected by $K$ and contains a sequence number SQN

• Each operator may use its own algorithms for authentication
• At the same time keys for ciphering and integrity checking are derived
• Ciphering and integrity checking are performed in MS and in RNC and these are independent of the authentication mechanism
Generation of security parameters

SN

IMSI

RAND

K

SQN

XRES

AUTN

CK

IK

RAND, AUTN, XRES, CK, IK
3G Authentication & key agreement

RAND     K    AUTN
RES     SQN     CK    IK

checks whether SQN is big enough

RAND, AUTN

RES

cHECKS RES = XRES?
3G ciphering mechanism

- Between UE and RNC
- **Stream cipher** like in GSM and GPRS
- Key length **128** bits
- Key lifetime could be limited.

- Begins with RNC sending “*Security mode command*”
3G Ciphering algorithm

COUNT-C/32

DIRECTION/1

BEARER/8

LENGTH

CK/128

KEYSTREAM BLOCK

Plaintext MAC SDU or RLC PDU (data part)

Ciphered MAC SDU or RLC PDU (data part)
UEA1 (based on KASUMI block cipher)

\[
\text{COUNT} \parallel \text{BEARER} \parallel \text{DIRECTION} \parallel 0\ldots0
\]

\[
\text{CK'} \rightarrow \text{KASUMI}
\]

\[
\text{BLKCTR} = 0
\]

\[
\text{CK} \rightarrow \text{KASUMI}
\]

\[
\text{BLKCTR} = 1
\]

\[
\text{CK} \rightarrow \text{KASUMI}
\]

\[
\text{BLKCTR} = 2
\]

\[
\text{CK} \rightarrow \text{KASUMI}
\]

\[
\text{BLKCTR} = n
\]

\[
\text{KS}[0] \ldots \text{KS}[63]
\]

\[
\text{KS}[64] \ldots \text{KS}[127]
\]

\[
\text{KS}[128] \ldots \text{KS}[191]
\]

\[
\text{CT}[i] = \text{PT}[i] \oplus \text{KS}[i]
\]
KASUMI block cipher

Fig. 1: KASUMI

Fig. 2: FO Function

Fig. 3: FI Function

Fig. 4: FL Function
S7 substitution box

int S7[128] = {
  54, 50, 62, 56, 22, 34, 94, 96, 38, 6, 63, 93, 2, 18, 123, 33,
  55, 113, 39, 114, 21, 67, 65, 12, 47, 73, 46, 27, 25, 111, 124, 81,
  53, 9, 121, 79, 52, 60, 58, 48, 101, 127, 40, 120, 104, 70, 71, 43,
  20, 122, 72, 61, 23, 109, 13, 100, 77, 1, 16, 7, 82, 10, 105, 98,
  117, 116, 76, 11, 89, 106, 0, 125, 118, 99, 86, 69, 30, 57, 126, 87,
  112, 51, 17, 5, 95, 14, 90, 84, 91, 8, 35, 103, 32, 97, 28, 66,
  102, 31, 26, 45, 75, 4, 85, 92, 37, 74, 80, 49, 68, 29, 115, 44,
  64, 107, 108, 24, 110, 83, 36, 78, 42, 19, 15, 41, 88, 119, 59, 3
};
Integrity mechanism

For UIA1: the one-way function is based on KASUMI block cipher
Second set of algorithms based on SNOW3G

- These are called UEA2 and UIA2
- Added in 3GPP in year 2006
- SNOW3G is a stream cipher
  - based on SNOW 2.0 (Nordic origin)
  - structure of UEA2 is straight-forward
SNOW 3G: structure

LFSR

R1

FSM

S1

S2

+ +

R1

R1

+ +

R1

Key stream
Network domain security (based on IPsec)

IKE "connection"

ESP Security Association
Status on 3G security today

- 3G security resilient against security analyses
- No significant attacks known on cryptographic algorithms
- No false base station attacks seem possible
- 3G security seems still sufficient for 3G networks
Brief introduction to LTE (= 4G)
SAE / LTE: What and why?

SAE = System Architecture Evolution
LTE = Long Term Evolution (of radio networks)

• LTE offers high data rates, up to 100 Mb/sec
  – Multi-antenna technologies
  – New transmission schema based on OFDM
  – Signaling/scheduling optimizations

• SAE offers optimized (flat) IP-based architecture
  – Two network nodes for user plane
  – Simplified protocol stack
  – Optimized inter-working with legacy cellular, incl. CDMA
  – Inter-working with non-3GPP accesses, incl. WiMAX
E-UTRAN architecture

From 3GPP TS 36.300
LTE Security
Implications of LTE/SAE architecture on security

• **Flat** architecture:
  – All radio access protocols terminate in one node: eNodeB
  – IP protocols also visible in eNB

• Security implications due to
  – Architectural design decisions
  – Interworking with legacy and non-3GPP networks
  – Allowing eNB placement in untrusted locations
  – New business environments with less trusted networks involved
  – Trying to keep security breaches as local as possible

• As a result (when compared to UTRAN/GERAN):
  – Extended Authentication and Key Agreement
  – More complex key hierarchy
  – More complex interworking security
  – Additional security for eNB (compared to NodeB/BTS/RNC)
Major design decisions for EPS security (1/2)

- Permanent security association
  - Inherited from GSM and 3G
- Interfaces in UE and HSS/HLR
  - ME-USIM interface is fully standardized but HSS-AuC is not
- Reuse of 3G USIMs
- **No** reuse of 2G SIMs in EPS
- Delegated authentication
  - Inherited from GSM and 3G
- Reuse of 3G AKA
- Cryptographic network separation
- Serving network authentication
Major design decisions for EPS security (2/2)

• Termination point for encryption and integrity protection
  – Flat architecture required moving to base station site
• New key hierarchy in EPS
• Key separation in handovers
• Homogeneous security for heterogeneous access networks
• User identity confidentiality *not* protected against active attackers

• Other „NOT“ – decisions:
  – No integrity protection for user plane on radio interface
  – No (cryptographic) non-repudiation of charging
Authentication and key agreement
Authentication and key agreement

• HSS generates authentication data and provides it to MME
• Challenge-response authentication and key agreement procedure between MME and UE
From “LTE security”
Generation of UMTS and EPS AV’s

$\text{EPS AV} := \text{RAND} \ || \ XRES \ || \ K_{\text{ASME}} \ || \ \text{AUTN}$

$\text{UMTS AV} := \text{RAND} \ || \ XRES \ || \ \text{CK} \ || \ \text{IK} \ || \ \text{AUTN}$

$\text{AUTN} := \text{SQN} \boxtimes \text{AK} \ || \ \text{AMF} \ || \ \text{MAC}$

From “LTE security”
Verification in USIM

Verify that SQN is in the correct range

Verify MAC = XMAC

From "LTE security"
LTE Data protection
Confidentiality and integrity of signalling

- RRC signalling between UE and E-UTRAN
- NAS signalling between UE and MME
- S1 interface signalling
  - protection is not UE-specific
  - optional to use
EPS signalling protection

From “LTE security”
User plane confidentiality

- S1-U protection is not UE-specific
  - (Enhanced) network domain security mechanisms (based on IPsec)
  - Optional to use
- Integrity is not protected for various reasons, e.g.:
  - performance
  - limited protection for application layer
EPS user plane protection

From “LTE security”
Ciphering mechanism

Extract from 3GPP TS 33.401
Integrity protection
LTE Key hierarchy

USIM / AuC

UE / HSS

UE / MME

UE / eNB

K

CK, IK

K_{ASME}

K_{NASenc}  K_{NASint}

K_{eNB} / NH

K_{UPenc}  K_{RRCint}  K_{RRCenc}
Cryptographic network separation

(1/2)

USIM / AuC

UE / MME

UE / HSS

USIM / AuC

UE / HSS

UE / MME

UE / eNB

K

CK, IK

K_{ASME}

K_{NASenc} K_{NASint}

K_{eNB} / NH

K_{UPenc} K_{RRCint} K_{RRCenc}

Network id
LTE crypto-algorithms
Crypto-algorithms

• Two sets of algorithms from Day One
  – If one breaks, we still have one standing
  – Should be as different from each other as possible
  – AES and SNOW 3G chosen as basis → ETSI SAGE has specified/chosen modes

• A third algorithm set was added for Release 11
  – The base algorithm ZUC is of Chinese origin and usable in China

• Rel-99 USIM is sufficient → master key 128 bits
  – All keys used for crypto-algorithms are 128 bits but included possibility to add 256-bit keys later (if needed)

• Deeper key hierarchy → (one-way) key derivation function needed
  – HMAC-SHA-256 chosen as basis
SNOW 3G

- The only algorithm that was inherited from 3G
- Discussed earlier
Structure of ZUC
Need for algorithm agility: example

- Theory break of algo 2
- Spec work for algo 3
- Practical break of algo 2
- Algo 3 implemented
- Majority of terminal base supports algo 3

(time)
Need for algorithm agility: example

Theory break of algo 2

Spec work for algo 3

Practical break of algo 2

Algo 3 implemented

Majority of terminal base supports algo 3

Dependent on one algo only
Caveat: Security of algorithm capability negotiation

- Algorithm capabilities exchanged first without protection
- Re-exchanged and verified once integrity protection is turned on → all integrity algorithms should resist real-time attacks in the beginning of the connection

- If this is not the case anymore, broken algorithm has to be withdrawn completely from the system (takes a long time)
Introduction to 5G security
5G service dimensions (3GPP)

- Massive MTC
- Enhanced Mobile Broadband
- eV2X
- Network Slicing / Reconfiguration
- Connectivity / Routing
- Migration / Interworking

Applications:
- eHealth / Wearable
- Subway / Stadium
- eCity / eFarm / Inventory
- AR / VR
- Train / Airplane
- UHD / Hologram
- Industry Robot / Drone
- Game / Sports

Features:
- Vehicle / autonomous driving
5G service requirements (3GPP)

- User experienced **data rate** up to Gbps.
- User peak data rate at tens of Gbps;
- The whole **traffic volume** at Tbps/ km².
- Very **low latency** for user experienced data exchange (~1 ms).
## Selected services

<table>
<thead>
<tr>
<th>Application</th>
<th>Average End User Throughput</th>
<th>Latency (end-to-end)</th>
<th>Latency (over the air)</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Definition Video 8K (streaming)</td>
<td>&lt; 100 Mbps (DL) [7]</td>
<td>&lt; 1 s [8]</td>
<td>&lt; 200 ms</td>
</tr>
<tr>
<td>High Definition Video (conversational)</td>
<td>&lt; 10 Mbps [7] (DL/UL)</td>
<td>&lt; 150 ms [8]</td>
<td>&lt; 30 ms</td>
</tr>
<tr>
<td>Cloud Computer Games with 4K 3D graphics – Low Latency Applications</td>
<td>&lt; 50 Mbps (DL/UL) [9] (UL is needed for multiplayer game computation in user device)</td>
<td>&lt; 7.5 ms (10 times less than in [8] for real time games)</td>
<td>&lt; 1.5 ms</td>
</tr>
</tbody>
</table>
5G key technologies

- Cloud computing
- Software-defined networking (SDN)
- Network function virtualization (NFV)
- (massive) Internet of Things
- Machine-to-machine communications
- Critical communications
- Network slicing
5G key technologies

• Cloud computing
• Software-defined networking (SDN)
• Network function virtualization (NFV)
• (massive) Internet of Things
• Machine-to-machine communications
• Critical communications
• Network slicing

• All have implications on security!
Cloud security

• Generic cloud security issues
  – Isolation
  – Platform security
  – etc.
5G has service-based architecture

**NSSF** = Network Slice Selection Function  
**NEF** = Network Exposure Function  
**NRF** = Network Repository Function  
**PCF** = Policy Control Function  
**AF** = Application Function  
**AMF** = Access and Mobility Management Function  
**SMF** = Session Management Function  
**UPF** = User Plane Function  
**DN** = Data Network  
**SEPP** = Security Edge Protection Proxy  
**UDM** = Unified Data Management  
**AUSF** = Authentication Server Function
Network slices

- Smartphone Slice 1 (e.g. for the network operator’s subscribers)
- Smartphone Slice 2 (e.g. for a virtual operator’s subscribers)
- Vehicle Services Slice 1 (e.g. for a truck manufacturer’s fleet assistance)
- M2M Service Slice 1 (e.g. for a goods or container tracking system)

Overall operator network (PLMN) domain

UE domain | (Radio) Access Network domain | Core Network domain | Data Network / applications

Figure from 3gpp.org
3GPP deployments using network slicing

From 3gpp.org
Service-based architecture

• TLS between the two SEPPs
• In addition, HTTP messages between network elements are protected using JSON Object Signing and Encryption (JOSE):
  – JSON Web Signature (JWS)
  – JSON Web Encryption (JWE)
  – JSON Web Key (JWK)
  – JSON Web Token (JWT)

JSON = Javascript Object Notation
Authentication and key agreement
Authentication in cellular systems

- **GSM:** *only* client authentication
  - Active attack by fake base stations
- **3G:** *mutual* authentication
  - Network *authorization* is verified (not identity)
- **LTE:** network *identity* is also verified
- **5G:**
  - Increased *home* control (for roaming)
  - Service authentication for *3rd party*
Trust model in LTE

![Diagram of LTE network components]

- **AN (Access Network)**
- **CN (Core Network)**
- **PDN (Packet Data Network)**

Key components:
- MME (Mobility Management Entity)
- HSS (Home Subscriber Server)
- S-GW (Serving Gateway)
- PDN-GW (Packet Data Network Gateway)

**Trusted domain**

**Exposed interface**
Trust model in 5G

AN

CN

PDN

Service A

Service B

Trusted domain

Exposed interface
Authentication types

• Three types of (UE related) authentication specified in 3GPP for 5G purposes:
  – **Network access** authentication over 3GPP radio
  – **Network access** authentication over non-3GPP access (such as WiFi)
  – **Service** authentication towards 3rd party Data Network (secondary authentication)
About authentication mechanism

- **Network access authentication:**
  - The 5G UE and 5G serving network shall support EAP-AKA’ for primary authentication, for both 3GPP access and untrusted non-3GPP access in 5G phase 1.
  - The 5G UE and the 5G serving network shall support **5G AKA** for primary authentication for 3GPP access in 5G phase 1.
  - The 5G UE and 5G serving network shall support the **EAP framework** for primary authentication in 5G phase 1, for both 3GPP and non-3GPP accesses.
  - 5G AKA over 3GPP access is the **only** supported authentication method in 5G phase 1 that is **not** an EAP method.
5G AKA

Device side

PLMN id | "5G"

HMAC-SHA-256 truncated to i bits, where i = 128

RES*

K

RAND

f1

RES

f2

CK

f3

IK
RAND \xrightarrow{K} \{f_1, f_2, f_3\} \xrightarrow{XRES} \text{PRNG} \xrightarrow{XRES*} \text{HMAC-SHA-256 truncated to i bits, where i = 128} \xrightarrow{PLMN id|"5G"} \text{HXRES*} \xrightarrow{XRES*} \text{(Home) Network side}
UE -> AMF
Auth. Req. (RAND|AUTN)
-> Auth-Response (RES*)

AMF -> AUSF
Auth. Info. Req.
<- Auth. Info. Answer (RAND, AUTN, HXRES*,...)

AUSF -> AMF
Auth. Confirmation (RES*)
->
Key hierarchy
LTE Key hierarchy

USIM / AuC

K

CK, IK

UE / HSS

K_{ASME}

UE / MME

K_{NASenc}  K_{NASint}

UE / eNB

K_{eNB} / NH

K_{UPenc}  K_{RRCint}  K_{RRCenc}
5G key hierarchy
Main additions:
Identity and location privacy

• Key feature in mobile systems since GSM
• Protection against passive adversaries
Active attack

• A *false* element masquerades
  – as a base station towards terminal
  – as a terminal towards network

• Objectives of the attacker:
  – eavesdropping
  – stealing of connection
  – manipulating data
Active attack

• A *false* element masquerades
  – as a base station towards terminal
  – as a terminal towards network

• Objectives of the attacker:
  – eavesdropping
  – stealing of connection
  – manipulating data

This part sufficient for IMSI catcher
# Identity protection in 2G/3G/4G/5G

<table>
<thead>
<tr>
<th>Attacker type</th>
<th>2G</th>
<th>3G</th>
<th>4G</th>
<th>5G</th>
</tr>
</thead>
<tbody>
<tr>
<td>Passive</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>IMSI catcher</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>YES</td>
</tr>
<tr>
<td>MitM</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Method to prevent IMSI catchers

- User identity is encrypted by network **public key** in the connection set-up
  - Only **one** public/private key pair in the system
  - The key is **owned by** the **HN**. UEs encrypt IMSI using the public key of the HN. UE sends the encrypted identity together with HN identity to SN.
Root-key based solution

Only one public/private key pair in the system. The key is owned by the HN. UEs encrypt IMSI using the public key of the HN. UE sends the encrypted identity together with HN identity to SN.
ECIES = Elliptic Curve Integrated Encryption Scheme

Diagram:

1. Eph. key pair generation
2. Key agreement
3. Key derivation
4. MSBs
5. LSBs
6. Symmetric encryption
7. MAC function

Final output = Eph. public key || Ciphertext || MAC tag || any other parameter
More information

www.3gpp.org