3GPP LTE
Security Aspects

Dionisio Zumerle
Technical Officer, 3GPP
ETSI
Contents

- LTE security architecture
- Security algorithms
- Lawful Interception
- Backhaul Security
- Relay Node Security
LTE Security Architecture
LTE Security: UMTS Security and LTE Architectural impact

UMTS security enhancements:
- Mutual authentication
- Integrity keys
- Public algorithms
- “Deeper” encryption
- Longer key length

LTE Architecture:
- Flat architecture
- Separation of control plane and user plane
- eNodeB instead of NodeB/RNC
- All-IP network
- Interworking with legacy and non-3GPP networks

Characteristics of LTE Security:
- Re-use of UMTS Authentication and Key Agreement (AKA)
- Use of USIM required (GSM SIM excluded)
- Extended key hierarchy
- Possibility for longer keys
- Greater protection for backhaul
- Integrated interworking security for legacy and non-3GPP networks
AKA and signalling protection

Confidentiality and integrity for signalling and confidentiality for user plane (RRC & NAS)
Confidentiality and integrity for signalling only (NAS)
Optional user plane protection (IPsec)
Authentication and Key Agreement

**UE**
- NAS attach request (IMSI)

**eNB**
- NAS auth request (AUTN, RAND, KSIasme)
- NAS auth response (RES)
- NAS SMC (confidentiality and integrity algo)
- NAS Security Mode Complete

**MME**
- S1AP Initial Context Setup
- RRC SMC (confidentiality and integrity algo)
- RRC Security Mode Complete

**AuC**
- AUTH data request (IMSI, SN_id)
- AUTH data response (AV={AUTN, XRES, RAND, Kasme})
- S1AP Initial Context Setup
Security Algorithms
LTE Security Algorithms

- Currently two separate algorithms specified
  - In addition to one NULL algorithm
- Current keylength 128 bits
  - Possibility to extend to 256 in the future
- Confidentiality protection of NAS/AS signalling recommended
- Integrity protection of NAS/AS signalling mandatory
- User data confidentiality protection recommended
- Ciphering/Deciphering applied on PDCP and NAS
LTE Ciphering and Integrity mechanisms

ciphering

integrity
128-EEA1/EIA1

Based on SNOW 3G

- stream cipher
- keystream produced by Linear Feedback Shift Register (LFSR) and a Finite State Machine (FSM)

Different from KASUMI as possible

- selected during UMTS security design

Allows for:

- low power consumption
- low gate count implementation in hardware
128-EEA2/EIA2

AES block cipher
- Counter (CTM) Mode for ciphering
- CMAC Mode for MAC-I creation (integrity)

Different from SNOW 3G as possible
- Cracking one would not affect the other

Reasons why KASUMI was not re-used:
- eNB already supports AES
  - needs to support AES for NDS/IP
- Similarity with other non-3GPP accesses (e.g. 802.11i)
- Other
128-EEA3/EIA3

Based on Chinese ZUC

• stream cipher

Three-phase evaluation ongoing

• Public evaluation ongoing! http://zucalg.forumotion.net/

• 2\textsuperscript{nd} International Workshop on ZUC: June 5-6 in Beijing http://www.3gpp.org/Call-for-Papers-Beijing-ZUC

Network-mandatory/network-optional to be decided
Deeper Key hierarchy in LTE

- Faster handovers and key changes, independent of AKA
- Added complexity in handling of security contexts
- Security breaches local
Key Derivation

Key distribution and key derivation scheme for EPS (network side), found in 33.401
Key Derivation Function (KDF) specification can be found in 33.220
Lawful Interception
Lawful Interception in 3GPP
Lawful Interception in EPS

Context and mechanisms similar to case of UMTS PS

- Different core entities (ICE, Intercepting Control Elements)
- ADMF handles requests from Law Enforcement Authorities
  - target identity: IMSI, MSISDN and IMEI
- X1 interface provisions ICEs and Delivery Functions
- X2 delivers IRI (Intercept Related Information)
- X3 delivers CC (Content of Communication)
- HI1,2,3: Handover Interfaces with law enforcement
  - Convey requests for interception of targets (HI1)
  - Deliver IRI (HI2) and CC (HI3) to LEAs
EPS LI Architecture

EPS LI Architecture diagram including nodes and interfaces such as S1, S3, S4, S6a, Gx, S1-MME, MME, HSS, PCRF, S12, S3, S1-U, X1_1, X1_2, X1_3, X2, X3, HI1, HI2, HI3, LEMF, and connections between these elements.
Backhaul Security
Backhaul Security

- Base stations becoming more powerful
  - LTE eNode B includes functions of NodeB and RNC
- Coverage needs grow constantly
- Infrastructure sharing

- Not always possible to trust physical security of eNB
- Greater backhaul link protection necessary
Certificate Enrollment for Base Stations

RA/CA

Vendor root certificate pre-installed.

CMPv2

base station obtains operator-signed certificate on its own public key from RA/CA using CMPv2.

SEG

Enrolled base station certificate is used in IKE/IPsec.

IPsec

Enrolled base station certificate is used in IKE/IPsec.

base station

Vendor-signed certificate of base station public key pre-installed.

Operator root certificate pre-installed.
Relay Node Security
Relay Node Authentication

- Mutual authentication between Relay Node and network
  - AKA used (RN attach)
  - credentials stored on UICC
- Binding of Relay Node and USIM:
  - Based on symmetric pre-shared keys, or
  - Based on certificates
Relay Node Security

- Control plane traffic integrity protected
- User plane traffic optionally integrity protected
- Relay Node and network connection confidentiality protected
- Device integrity check
- Secure environment for storing and processing sensitive data
Conclusions

LTE Security: building on GSM and UMTS Security
Newer security algorithms, longer keys
Extended key hierarchy
New features, addressing new scenarios
  • Backhaul Security
  • Relay Node Security
Thank You!

dionisio.zumerle@etsi.org

More Information about 3GPP:

www.3gpp.org
contact@3gpp.org
Backup: Selection of 3GPP Security Standards

LTE Security:
- **33.401** System Architecture Evolution (SAE); Security architecture
- **33.402** System Architecture Evolution (SAE); Security aspects of non-3GPP

Lawful Interception:
- **33.106** Lawful interception requirements
- **33.107** Lawful interception architecture and functions
- **33.108** Handover interface for Lawful Interception

Key Derivation Function:
- **33.220** GAA: Generic Bootstrapping Architecture (GBA)

Backhaul Security:
- **33.310** Network Domain Security (NDS); Authentication Framework (AF)

Relay Node Security
- **33.816** Feasibility study on LTE relay node security (also **33.401**)

Home (e) Node B Security:
- **33.320** Home (evolved) Node B Security