SIEMENS

- 3GPP Security/AKA - Requirements and development

Bart Vinck

Siemens Atea

bart.vinck@siemens.atea.be

3GPP Security/AKA development time schedule

Requirements and objectives (until Dec 98)

- TD on attacks/insufficiencies on the protocol level
- TS 33.120 “Security objectives”
- TS 21.133 “Security Threats and Requirements”

Selection of features and mechanisms (until Apr 99)

- TS 33.102 “Security Architecture”
- TS 33.105 “Cryptographic algorithm requirements”

Evolution and integration of mechanisms (until Dec 99)

- TS 33.102 “Security Architecture” (many CRs)
- TR 33.902 “Formal analysis of 3GPP AKA”
- Specs of other groups

3GPP Security - Requirements and objectives
Some objectives

Enhance GSM security (2G security)

- Encryption terminates at the base station
- Cipher key length of 64 bits
- In-call authentication relies on ciphering
- Cipher mode negotiation open to attack
- False base station attacks (more generally)
- Compromised “triplet” can be re-used indefinitely

Build on GSM security (2G security)

- No standardised authentication algorithm
- Delegation of authentication to serving network
- Symmetric key techniques for authentication (Nov ‘98)

3GPP Security - Requirements and Features Release 99 - Results

Data integrity of signalling data

- Secure cipher mode negotiation
- In-call authentication independent of ciphering
- Prevents false base station attacks

Key freshness assurance to the user at key agreement

- Prevents (unlimited) re-use of (compromised) key sets

Cipher/integrity key lengths up to 128 bits

- Provides margin for future advances in computing power

Encryption terminates at the radio network controller

- Ensures that all radio-links are ciphered

Reviewed and public algorithms

3GPP Security - Requirements and features Requirements on AKA

GSM AKA security services

- authentication of the user
- agreement of a cipher key (64 bits)

Additional or enhanced security services for 3GPP

- agreement of an integrity key (128 bits)
- agreement of a longer cipher key (64 bits ®128 bits)
- assurance of cipher/integrity key freshness to the user
- authenticated signalling field

Retain GSM AKA aspects

- symmetric key authentication
- runs between UIM and VLR/SGSN on behalf of HLR/AuC

3GPP Security - Selection of the mechanisms
3GPP AKA - How to achieve key freshness assurance

Sequence numbers

- Challenge contains sequence number so that the user can verify that the challenge is fresh such that cipher/integrity keys derived from the challenge are fresh

Advantages

- Compatibility with GSM AKA
- No standardised algorithms
- Two-way message exchange
- No online home network involvement

Preferred (April ‘99 onwards)

Mutual challenge/response

- The user contributes with a nonce to the derivation of the cipher and integrity keys, such that he is assured of the freshness of the cipher/integrity keys

Advantages

- Higher degree of mutual authentication
- Cipher/integrity refreshment without the need to involve the home network

Back-up (April ‘99-Dec. ‘99)

3GPP Security/AKA - Evolution and integration Enhanced sequence number management

… shall not compromise user identity confidentiality

- either through concealment of the SQN with a mask
- either through derivation from (partially) time-based counter

… shall recover from data loss in the home network

- re-synchronisation procedure: if the counter in the home network is corrupted, interaction the UIM ensures that the counter is securely reset

… shall allow out-of-order use of quintets

- the UIM stores in addition to a counter additional information on the sequence numbers it has accepted (e.g. list)

… shall protect against lock-out

- the UIM limits the maximum increment of its counter

3GPP Security/AKA - Evolution and integration
Secure connection establishment / key re-use

Secure connection establishment without AKA

- re-uses cipher/integrity keys for several connections
- security through mandatory data integrity on signalling
- secure cipher mode negotiation

User control of cipher/integrity key usage

- user keeps track of the amount of data ciphered using a particular cipher key
- user can trigger new authentication (at connection set-up) when amount of data ciphered exceeds a threshold

Network control of cipher/integrity key lifetime

- Serving network should refresh the cipher/integrity keys on a regular basis (at least once every 24 hours)

3GPP Security/AKA - Evolution and integration Interoperation between GERAN and UTRAN

Authentication

- 3GPP AKA Þ "UMTS security context" (= CK/IK)
  - Over UTRAN if UIM is Release 99 (ME and VLR are Release 99)
  - Over GERAN if UIM, ME and VLR (SGSN) are Release 99
- GSM AKA Þ "GSM security context" (= Kc)
  - When UIM, ME or VLR/SGSN not Release 99

Access link key agreement

- Conversion functions
  - c3: (CK, IK) → Kc
  - c4: Kc → CK; c5: Kc → IK
- Used for intersystem registration
- Use for intersystem handover/ intersystem change

3GPP Security/AKA - Evolution and integration Interoperation between 3GPP and 3GPP2 networks

3GPP AKA+ as proposed for ESA

- A common AKA mechanism to establish secret “roaming” keys between the MS and the VLR, based on a subscriber authentication key shared between the MS and the HLR/AuC
- A local authentication mechanism between MS and VLR (similar to secure connection establishment in 3GPP)

Advantages

- Facilitation of global roaming through a single protocol on the Network-to-Network Interface (NNI)

3GPP Security/AKA - Evolution and integration
Additional AKA features/mechanisms

Authentication management field

- Home network ® UIM
- Authentication management field
- Example uses: subscriber key identifier, threshold value for key refreshment

Authentication failure reporting

- Serving network ® Home network
- Includes the cause of the failure

3GPP AKA
Conclusion

Protocol - stage 1 & stage 2

- Meets the requirements that were set out
- Evolution meets the concerns that were raised
- Stable description in TS 33.102 (6.3, B)

Protocol - stage 3

- Integration & review by SA-3 well under way

Algorithms

- No standardisation required
- SAGE has been tasked to develop an example
- Funding not resolved / work not started