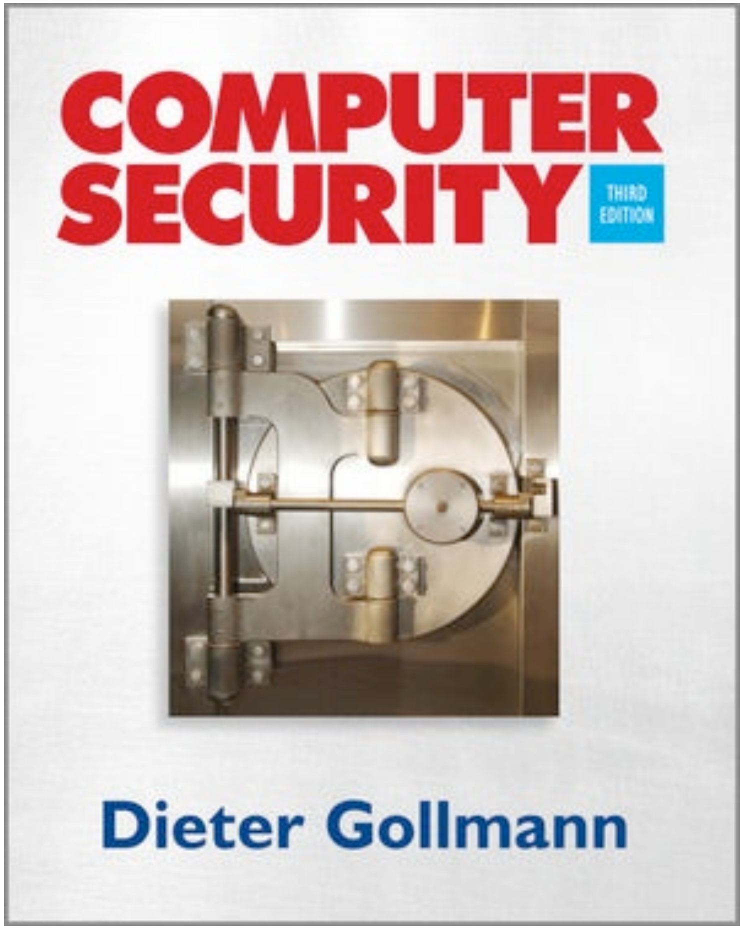
Computer Security 3e

Dieter Gollmann



Chapter 19:
Mobility
&
Lars Strand:
“Security Architecture for Mobile Telephony Systems”

Objectives

- Examine new security challenges and attacks specific to mobile services.
- Give an overview of the security solutions adopted for different mobile services.
- Show some novel ways of using of cryptographic mechanisms.
- Discuss the security aspects of location management in TCP/IP networks.

Agenda (slides 1-50)

- Security Architecture
- From PSTN to GSM
- GSM security
- UMTS authentication
  - What do we mean by “mutual authentication”
- LTE Security architecture
- ~~Mobile IPv6 security~~
  - ~~Secure binding updates~~
- ~~Cryptographically generated addresses~~
- ~~WLAN security~~
  - ~~WEP~~
  - ~~WPA~~
  - ~~Bluetooth~~

Security Architecture

- “The design artifacts that describe how the security controls (= security countermeasures) are positioned, and how they relate to the overall IT Architecture. These controls serve the purpose to maintain the system’s quality attributes, among them confidentiality, integrity, availability, accountability and assurance.”
- – Open Security Architecture (OSA)

[source: Lars Strand, 2011]

IETF Definition

- A plan and set of principles that describe
  - the security services that a system is required to provide to meet the needs of its users
  - the system components required to implement the services, and
  - the performance levels required in the components to deal with the threat environment

- – RFC4949

[source: Lars Strand, 2011]

Public Switched Telephone Networks

- The “plain old telephone system” (with additional functionality)
- Provided (worldwide) telephone service
  - Government owned telephone companies
- Main driver telco: Availability service (postulation)
  - Limited (none?) focus on security services
  - Results in practice: No security mechanisms at all
- Stable service: 99.999% uptime
- Main driver for early attacks: Get free calls!

[source: Lars Strand, 2011]

Attack: Blueboxing

- Signaling sent in-band
- Could be emulated and manipulated by user
- Bluebox: Dedicated devices did the work for you

[source: Lars Strand, 2011]

Attack: Clip-on

Physically attaching a phone to someone else's line to steal their service

Results:

- Customer billed incorrectly
- Hard to prove innocent

Telco incentives to follow up low:

- State owned (no competition)
- Increased usage = increased revenue (except international calls)

[source: Lars Strand, 2011]

Mobile systems

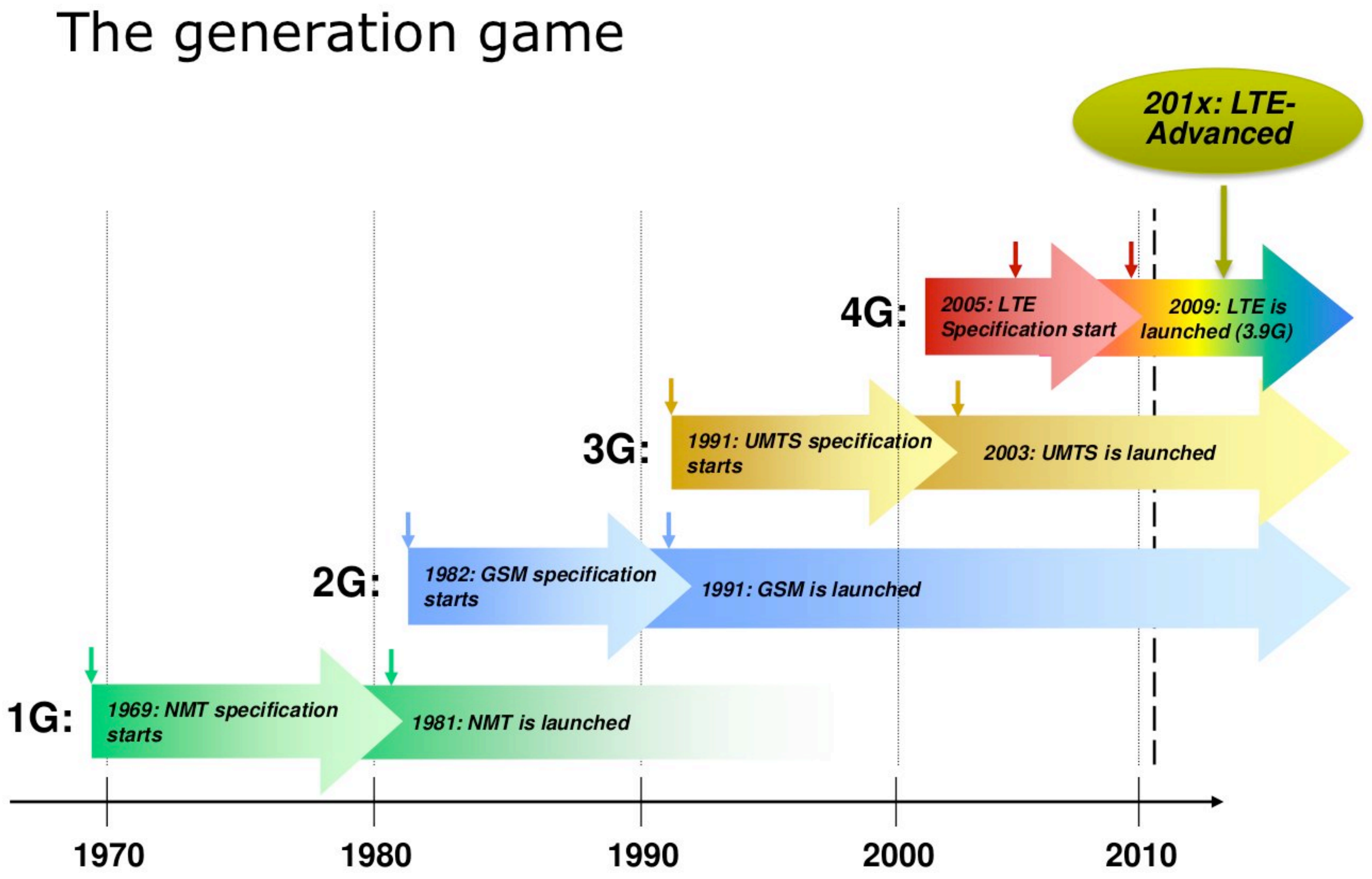

The generation game
201x: LTE-Advanced
4G:
2005: LTE Specification start
2009: LTE is launched (3.9G)
3G:
1991: UMTS specification starts
2003: UMTS is launched
2G:
1982: GSM specification starts
1991: GSM is launched
1G:
1969: NMT specification starts
1981: NMT is launched
1970
1980
1990
2000
2010

Figure from P. Lehne, Telenor

GSM & UMTS security

Mobile systems: GSM

- Developed in the late 1980s, deployed 1992.
  - Norway a key developer and inventor
- Today: Cover 80% of world population (5+ billion users!), gsmworld.com.
- GSM security goal: “as secure as the wire”
- GSM network consists of several network elements
  - Radio Subsystem (RSS)
    - Base station Subsystem (BSS)
    - Mobile Equipment (ME) (cell phone/handset)
  - Network and Switching Subsystem (NSS) – core network
  - Operation Subsystem (OSS)

[source: Lars Strand, 2011]

Threat environment

1. Vulnerability: Cloning
   - GSM security service: Authentication
   - GSM security mechanism: Authentication mechanism
2. Vulnerability: Content (voice) sent in clear
   - GSM security service: Call content confidentiality
   - GSM security mechanism: A5/1, A5/2, A5/3, A5/4
3. Vulnerability: Spying (subscriber location tracking)
   - GSM security service: Identity confidentiality
   - GSM security mechanism: Location security (TMSI)

[source: Lars Strand, 2011]

Security Goals

- Protect against interception of voice traffic on the radio channel:
  - Encryption of voice traffic.
- Protect signalling data on the radio channel:
  - Encryption of signalling data.
- Protections against unauthorised use (charging fraud):
  - Subscriber authentication (IMSI, TMSI).
- Theft of end device:
  - Identification of MS (IMEI), not always implemented.

GSM – Components

- MS (Mobile Station) = ME (Mobile Equipment) + SIM (Subscriber Identity Module);
  - SIM gives personal mobility (independent of ME)
- BSS (Base Station Subsystem) = BTS (Base Tranceiver Station) + BSC (Base Station Controller)
- Network Subsystem = MSC (Mobile Switching Center, central network component) + VLR, HLR, AUC, ...
- HLR (Home Location Register) + VLR (Visitor Location Register) manage Call Routing & Roaming Information
- AUC (Authentication Center) manages security relevant information
- ...

GSM: Problems

- Focus on *access security*
  - Confidentiality terminated at the base stations
  - Weak operator network protection
  - Example: Traffic to/from BS and AuC should be protected!
- *“Security through obscurity”* - A3/A5/A8 eventually leaked
- Algorithms not resistant to cryptanalysis attack
  - A5/1 can “easily” be broken – today gradually replaced by A5/3
  - No public scrutiny during development
- Lack of user visibility
  - User do not know if/what encryption is used
- Difficult to upgrade cryptographic algorithms
  - But not in theory? Resides on the SIM card
- Authentication: One-way authentication only
  - Only MS to BS and not BS to MS.
- + many more..

[source: Lars Strand, 2011]

SIM: Subscriber Identity Module

- Smart card (processor chip card) in MS:
  - Current encryption key Kc (64 bits)
  - Secret subscriber key Ki (128 bits)
  - Algorithms A3 and A8
  - IMSI
  - TMSI
  - PIN, PUK
  - Personal phone book
  - SIM Application Toolkit (SIM-AT) platform
  - ...

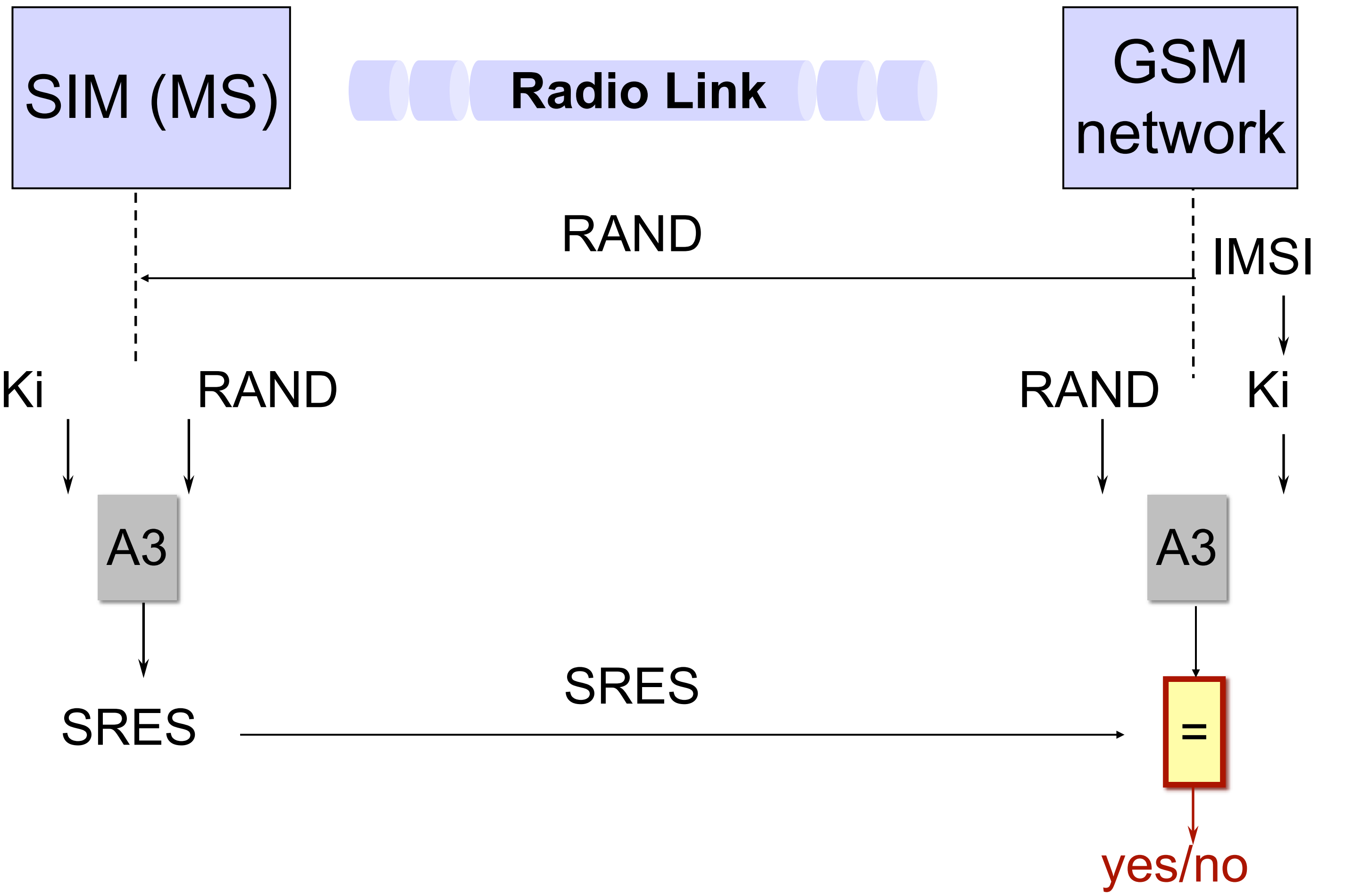
Cryptography in GSM

- A3 authentication algorithm
- A5 signalling data and user data encryption algorithm
- A8 ciphering key generating algorithm

- Symmetric key crypto algorithms (public key cryptography was considered at the time – 1980s – but not considered mature enough)

- *GSM/MoU: Memory of Understanding*
- *PLMN: Public Land Mobile Network*

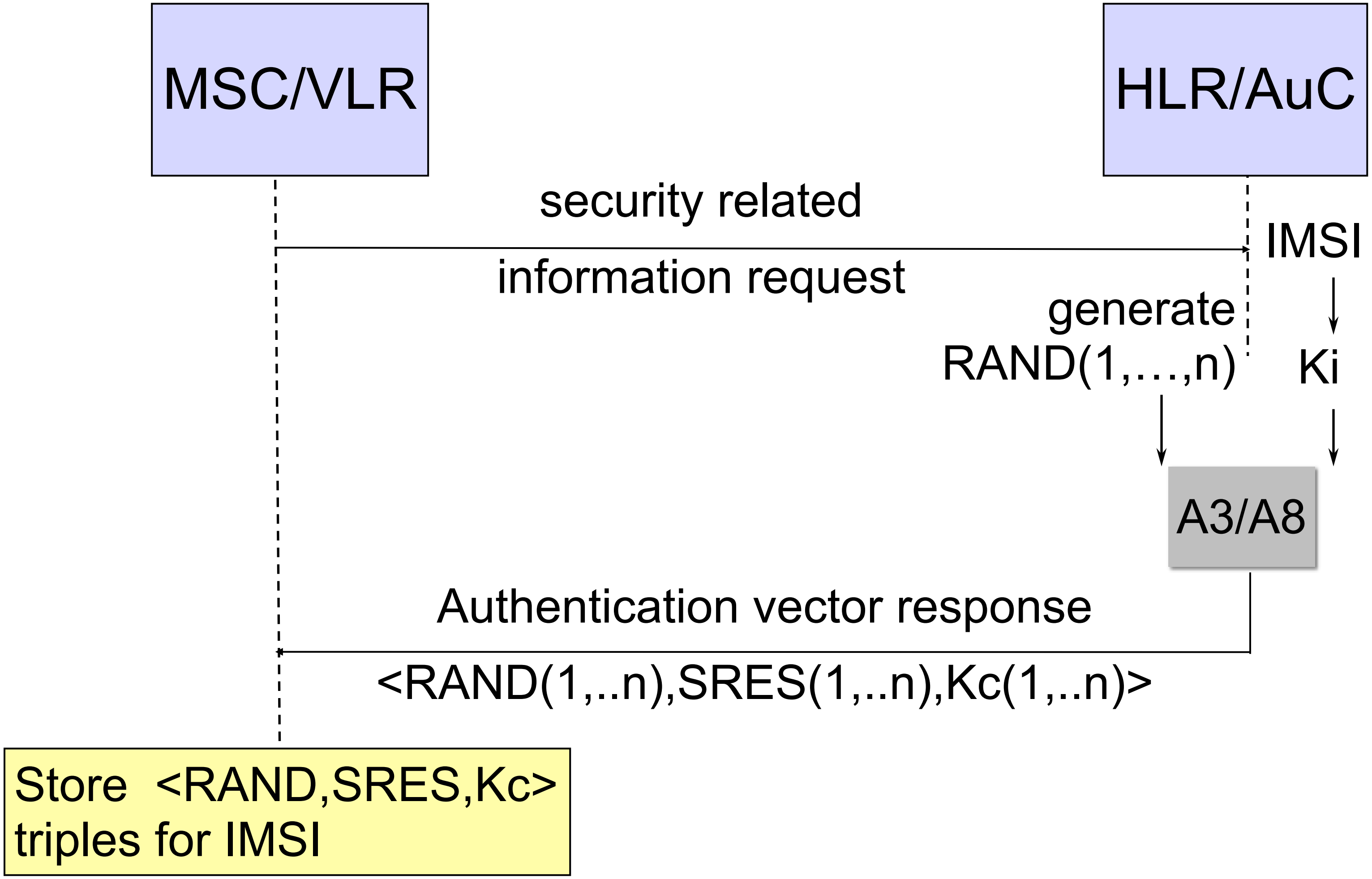
GSM Subscriber Authentication



Authentication in ME

- Fixed subsystem transmits a non-predictable number RAND (128 bits) to the MS.
  - RAND chosen from an array of values corresponding to MS.
- MS computes SRES, the ‘signature’ of RAND, using algorithm A3 and the secret : Individual Subscriber Authentication Key Ki.
- MS transmits SRES to the fixed subsystem.
- The fixed subsystem tests SRES for validity.
- Computations in ME performed in the SIM.
- Location update within the same VLR area follows the same pattern.

GSM Authentication: Fixed Network



GSM 02.09: Security Aspects

- The authentication of the GSM PLMN subscriber identity may be triggered by the network when the subscriber applies for:
  - change of subscriber−related information element in the VLR or HLR (including some or all of: location updating involving change of VLR, registration or erasure of a supplementary service); or
  - access to a service (including some or all of: set−up of mobile originating or terminated calls, activation or deactivation of a supplementary service); or
  - first network access after restart of MSC/VLR; or in the event of cipher key sequence number mismatch.

TMSI

- When a MS makes initial contact with the GSM network, an unencrypted subscriber identifier (IMSI) has to be transmitted.
- The IMSI is sent only once, then a temporary mobile subscriber identity (TMSI) is assigned (encrypted) and used in the entire range of the MSC.
- When the MS moves into the range of another MSC a new TMSI is assigned.

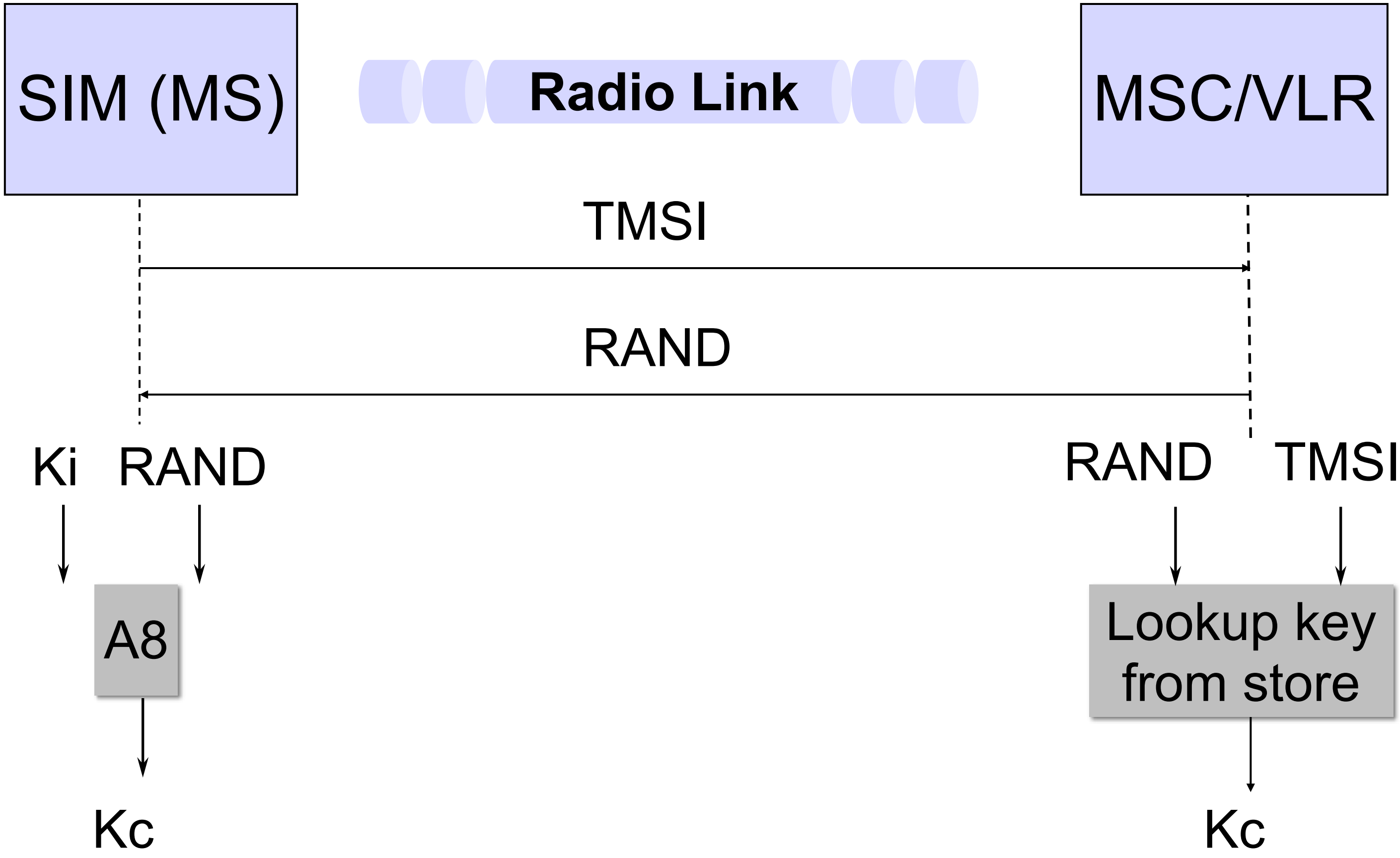
TMSI – GSM 03.20

- TMSI: temporary local ID:
  - protected identifying method is normally used instead of the IMSI on the radio path; and
  - IMSI is not normally used as addressing means on the radio path (see GSM 02.09);
  - when the signalling procedures permit it, signalling information elements that convey information about the mobile subscriber identity must be ciphered for transmission on the radio path.
- LAI = Local Area Information
- VLR keeps relation <(TIMSI, LAI), IMSI>

GSM 02.09: Encryption

- Encryption normally applied to all voice and non−voice communications.
  - The infrastructure is responsible for deciding which algorithm to use (including the possibility not to use encryption, in which case confidentiality is not applied).
  - When necessary, the MS shall signal to the network indicating which of up to seven ciphering algorithms it supports. The serving network then selects one of these that it can support (based on an order of priority preset in the network), and signals this to the MS.
  - The network shall not provide service to an MS which indicates that it does not support any of the ciphering algorithm(s) required by GSM 02.07.

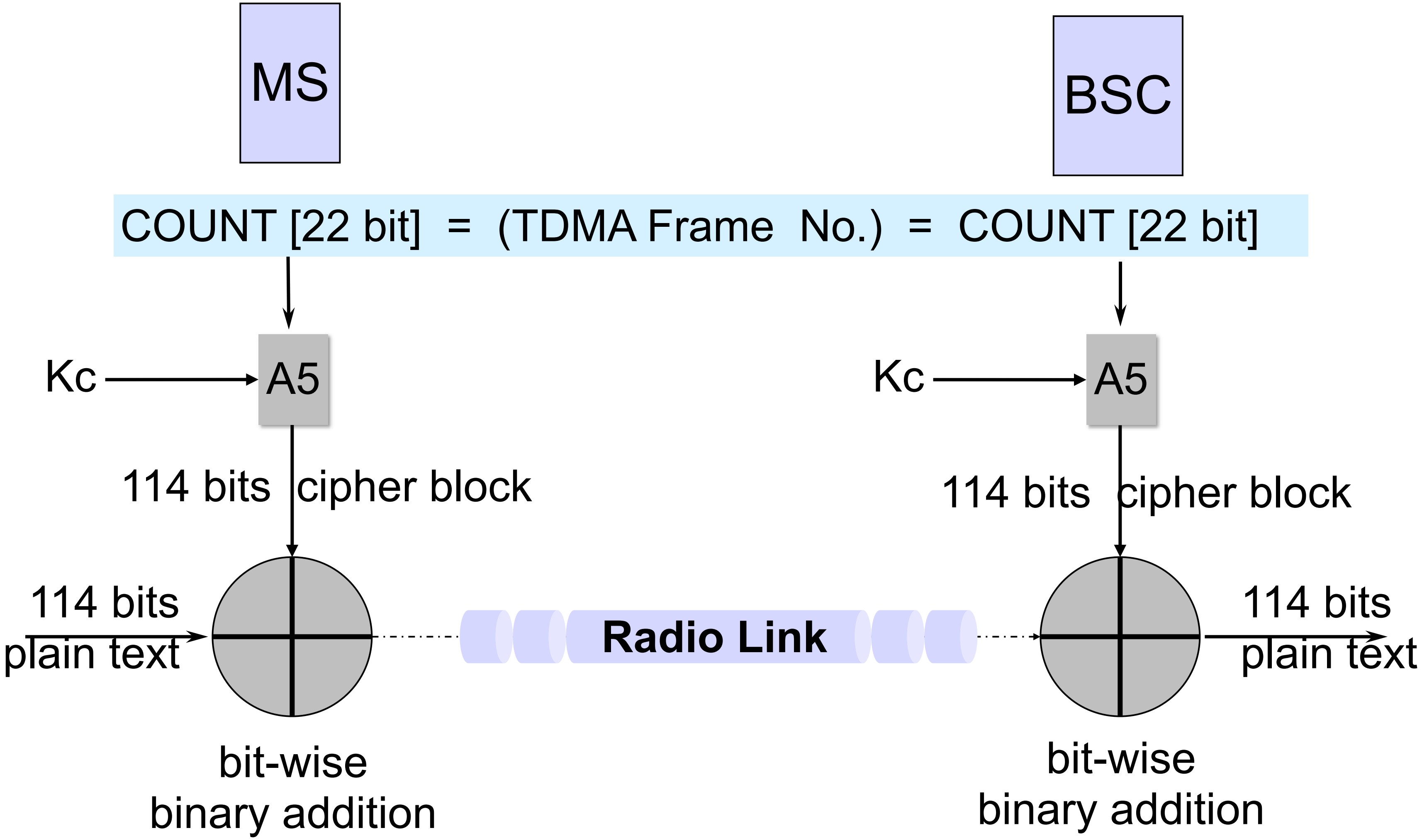
GSM Subscriber Authentication



Cryptographic Algorithms: A3/A8

- Algorithms A3 and A8 shared between subscriber and home network; thus each network could choose its own algorithms.
  - Algorithms A3 and A8 at each PLMN operator’s discretion.
  - GSM 03.20 specifies only the formats of their inputs and outputs; processing times should remain below a maximum value (A8: 500 msec).
- COMP128: one choice for A3/A8; attack to retrieve Ki from the SIM (→ cloning) possible; not used by many European providers.

MS/BSC Encryption



Cryptographic Algorithms: A5

- Algorithm A5 must be shared between all subscribers and all network operators; has to be standardized.
  - Specification of Algorithm A5 is managed under the responsibility of GSM/MoU.
- A5/1, A5/2 (simpler “export” version), A5/3.
  - Specifications of A5/1, A5/2 have not been (officially) published; A5/3 is public.
- Cryptanalytic attacks against all versions of A5 exist.
  - Elad Barkan, Eli Biham, Nathan Keller: Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication, Journal of Cryptology, Vol. 21, Nr. 3, July 2008
  - Orr Dunkelman, Nathan Keller, and Adi Shamir: A Practical-Time Attack on the A5/3 Cryptosystem Used in Third Generation GSM Telephony, 2009.

Stream Cipher: A5

- A5: Stream cipher that encrypts 114-bit frames; key for each frame derived from the secret key Kc and current frame number (22 bits).
- Why a stream cipher, not a block cipher (DES, AES)?
- Radio links are relatively noisy.
  - Block cipher: a single bit error in the cipher text affects an entire clear text frame;
  - Stream cipher: a single bit error in the cipher text affects a single clear text bit.

GSM Fraud

- Often attacks the revenue flow rather than the data flow and does not break the underlying technology.
- Roaming fraud: subscriptions taken out with a home network; SIM shipped abroad and used in visited network.
  - Fraudster never pays for the calls (soft currency fraud).
  - Home network has to pay the visited network for the services used by the fraudster (hard currency fraud).
  - Scope for fraudsters and rogue network operators to collude.
- Premium rate fraud: customers lured into calling back to premium rate numbers owned by the attacker.
  - GSM charging system (mis)used to get the victim's money.

GSM Fraud

- Business model attack: Criminals open a premium rate service, call their own number to generate revenue, collect their share of the revenue from the network operator, and disappear at the time the network operator realises the fraud.
- Countermeasures:
  - Human level: exercise caution before answering a call back request.
  - Legal system: clarify how user consent has to be sought for subscribers to be liable for charges to their account.
  - Business models of network operators.
- GSM operators have taken a lead in using advanced fraud detection techniques, based e.g. on neural networks, to detect fraud early and limit their losses.

GSM – Summary

- Voice traffic encrypted over the radio link (A5)
  - but calls are transmitted in the clear after the base station.
- Optional encryption of signaling data
  - but ME can be asked to switch off encryption.
- Subscriber identity separated from equipment identity.
- Some protection of location privacy (TMSI).
- Security concerns with GSM:
  - No authentication of network: IMSI catcher pretend to be BTS and request IMSI.
  - Undisclosed crypto algorithms.

Security architecture: GSM

Threats/attacks	Security services	Security mechanisms
Cloning	Authentication	Authentication mechanism (challenge-response with a shared secret)
Eavesdropping (voice sent in clear)	Confidentiality	Encryption of call content (A5/1, A5/2, A5/3)
Spying (identity tracking)	Confidentiality	Location security (TMSI)

Conclusion: GSM had a security architecture from the start

* Well defined threats and security services (at the time)
* Security mechanisms implemented poorly
  - missing public scrutiny
  - hard to replace components
  - not adaptive to future changes

[source: Lars Strand, 2011]

UMTS – Introduction

- Work on 3rd generation mobile communications systems started in the early 1990s; first release of specifications in 1999.
- Standards organization: 3G Partnership Project (3GPP).
  - ETSI (Europe)
  - ARIB (Japan)
  - TTC (Japan)
  - T1 (North America)
  - TTA (South Korea)
  - CCSA (China)
- Mission: Drive forward standardization of 3G systems.

UMTS (3G)

- Universal Mobile Telecommunications System (UMTS)
- Security mechanisms in GSM used as starting point for UMTS
- UMTS objectives, specified in *3G TS 33.120, 3G Security, Security Principles and Objectives*:
    - UTMS security will **build on** the security of 2G systems
    - UMTS security will **improve** on the security of 2G systems
    - UTMS security will **offer new** security features [services]
- Threat/risk analysis for 3G systems performed
    - *3G TS 21.133, 3G Security, Security Threats and Requirements*
- The objectives + threat environment became basis for
    - *3G TS 33.102, 3G Security, Security Architecture*

[source: Lars Strand, 2011]

Security architecture: UMTS

Main tasks of the security architecture (Køien, 2004):

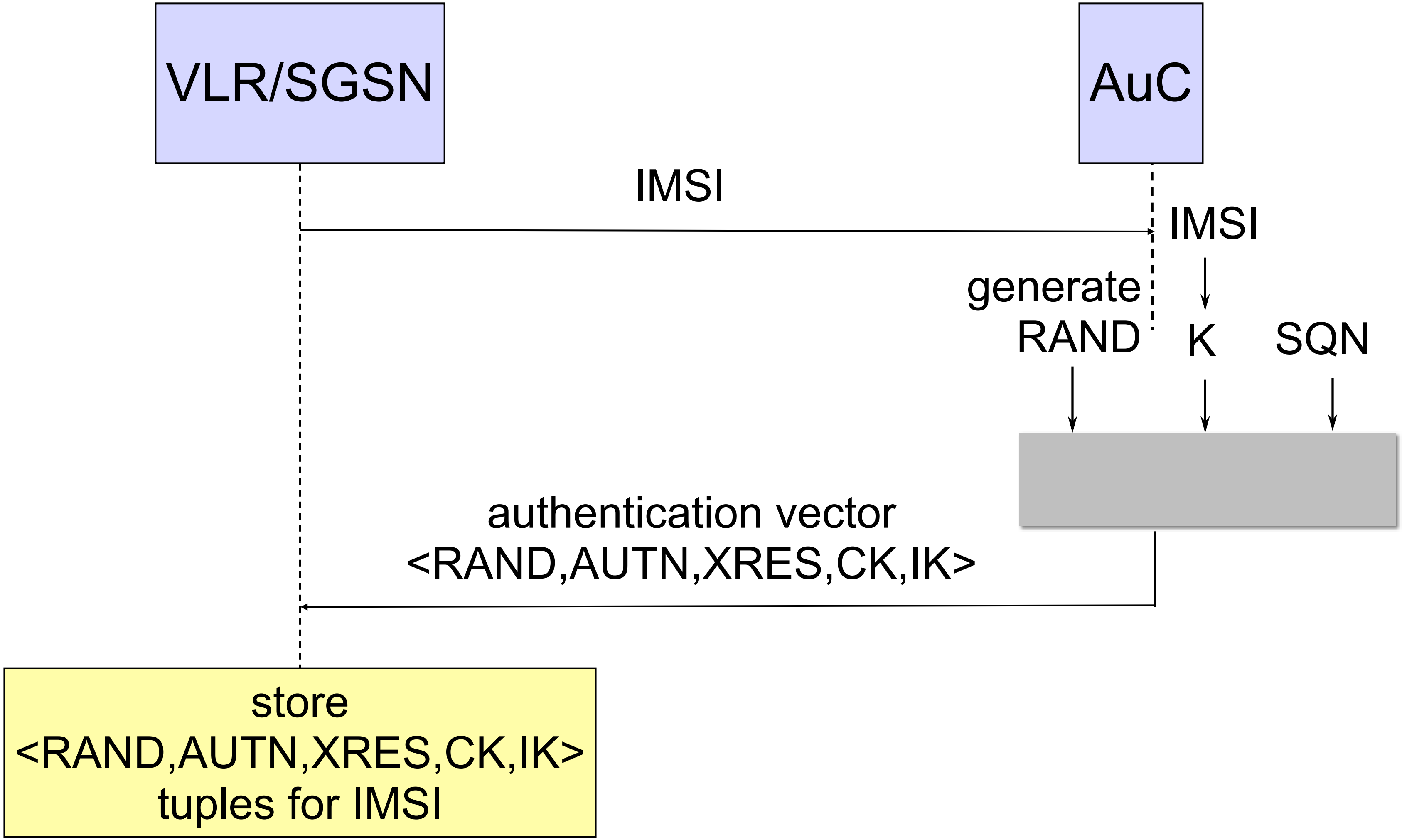
1) Authentication
   - GSM vulnerability: False BST
   - UMTS: Mutual authentication, new algorithm (MILENAGE)
2) Replace algorithms/New key generation
   - GSM vulnerability: Inadequate algorithm
   - UMTS: New algorithm (KASUMI)
3) Encryption/integrity protection
   - GSM vulnerability: Cipher keys and auth data sent in clear in operator network
   - UMTS: Extend confidentiality and integrity service to the operator network

[source: Lars Strand, 2011]

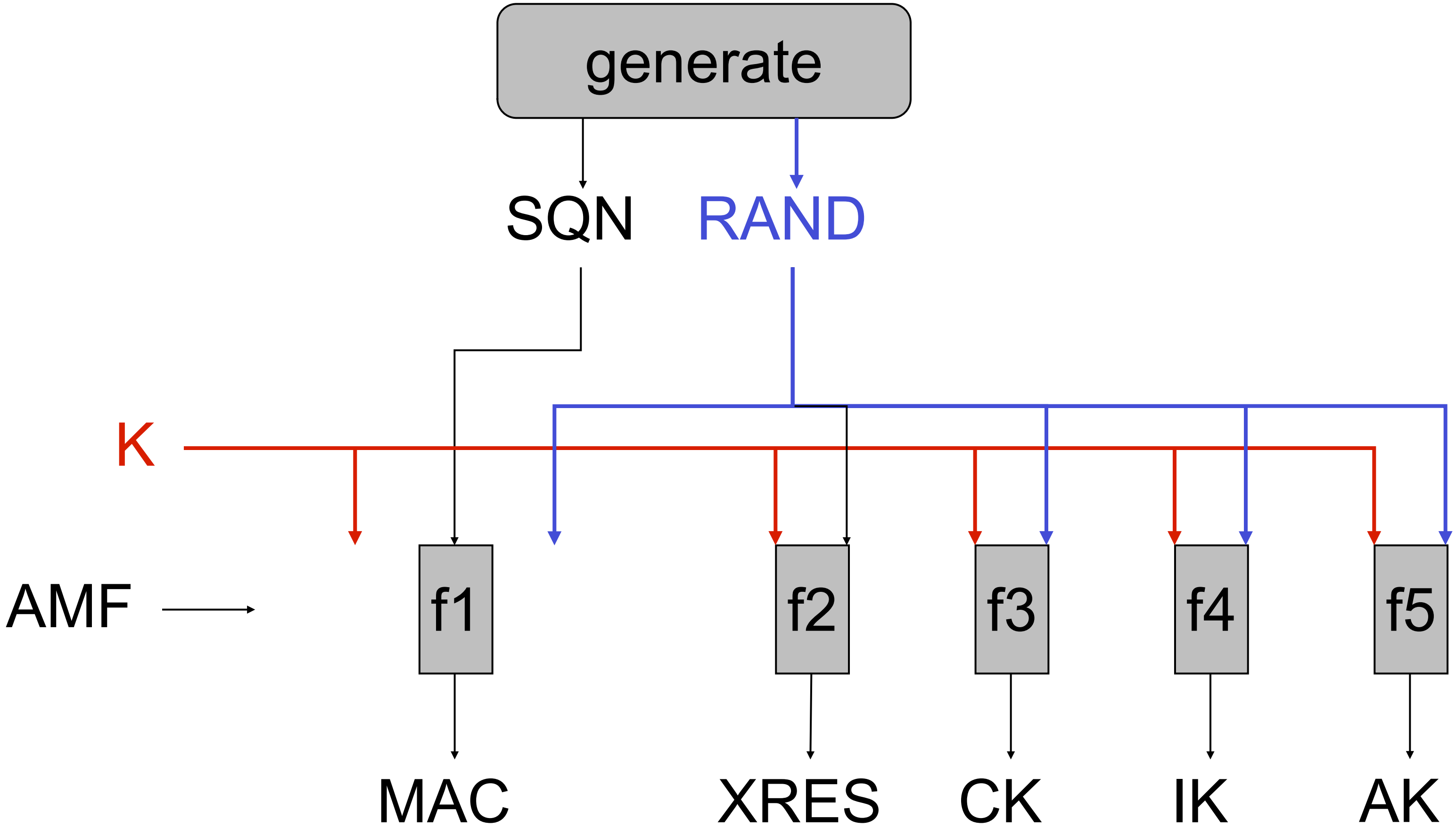
UMTS AKA
“Authentication and Key Agreement”

- Home network (AuC) and USIM (Universal Subscriber Identity Module) in user equipment (UE) share secret 128-bit key K.
- AuC can generate random challenges RAND.
- USIM and AuC have synchronized sequence numbers SQN available.
- Key agreement on 128-bit cipher key CK and 128-bit integrity key IK.
- AMF: Authentication Management Field.

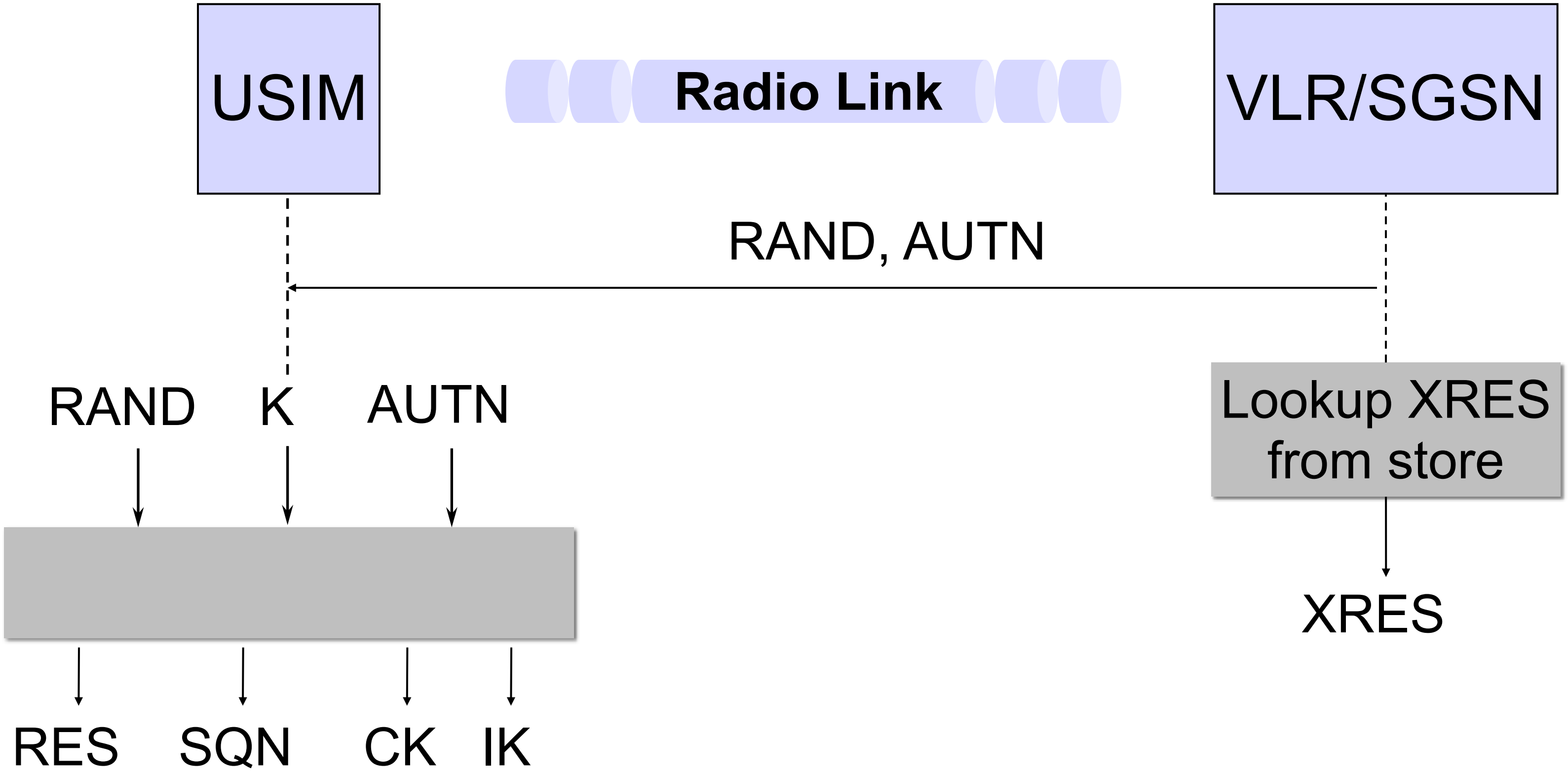
UMTS AKA: VLR ↔ AuC



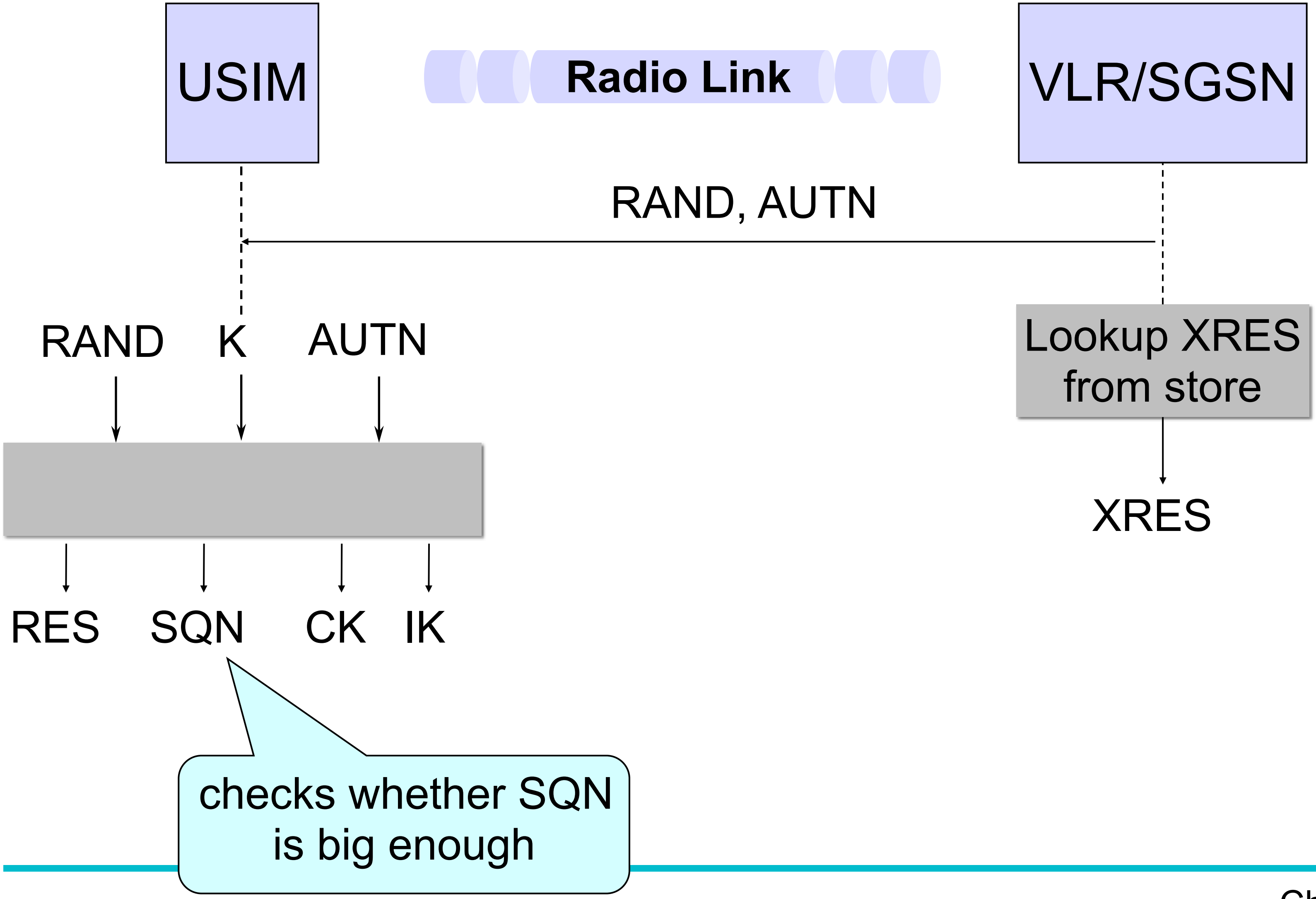
AV Generation at AuC



UMTS AKA: USIM ↔ VLR

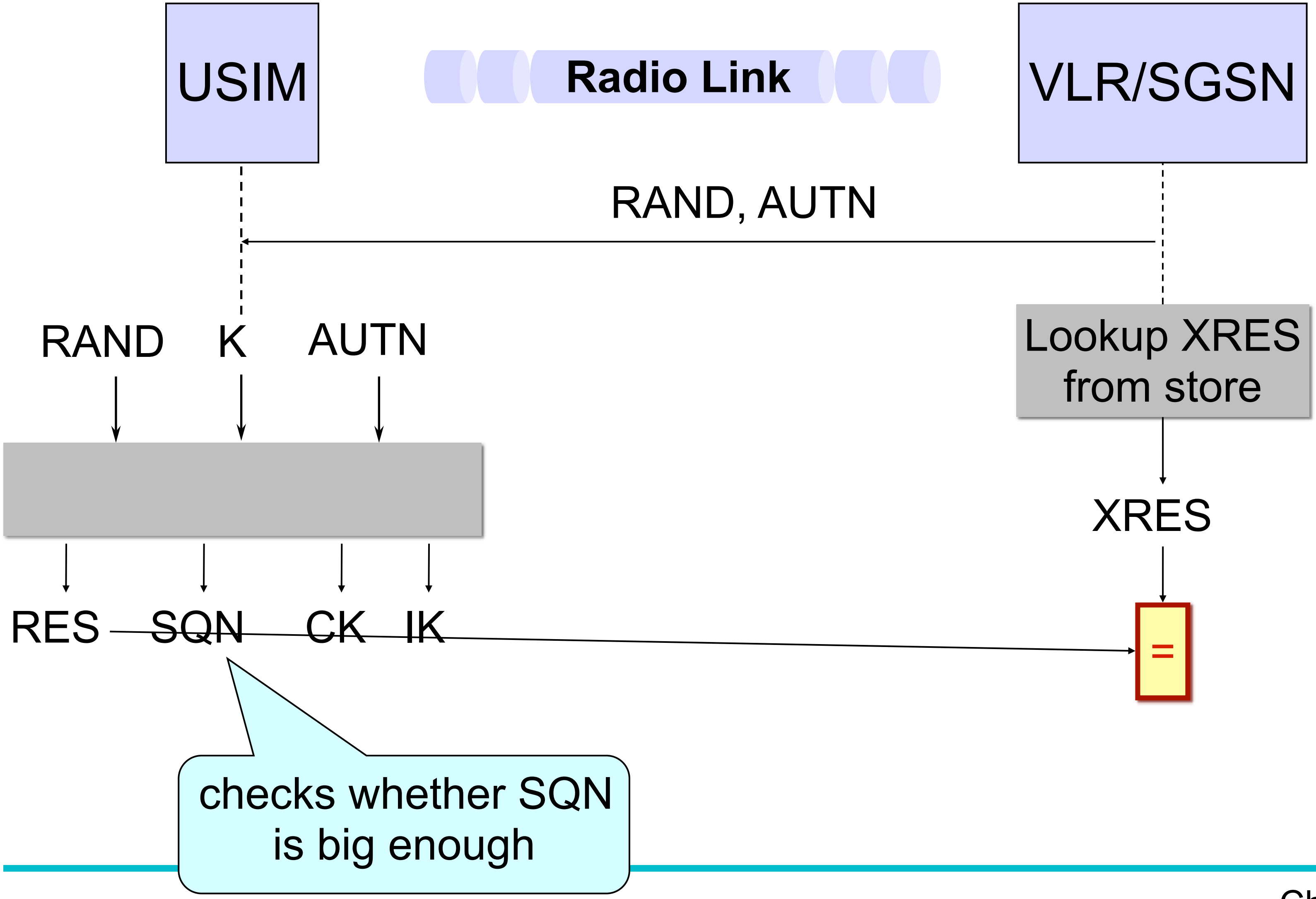


UMTS AKA: USIM ↔ VLR



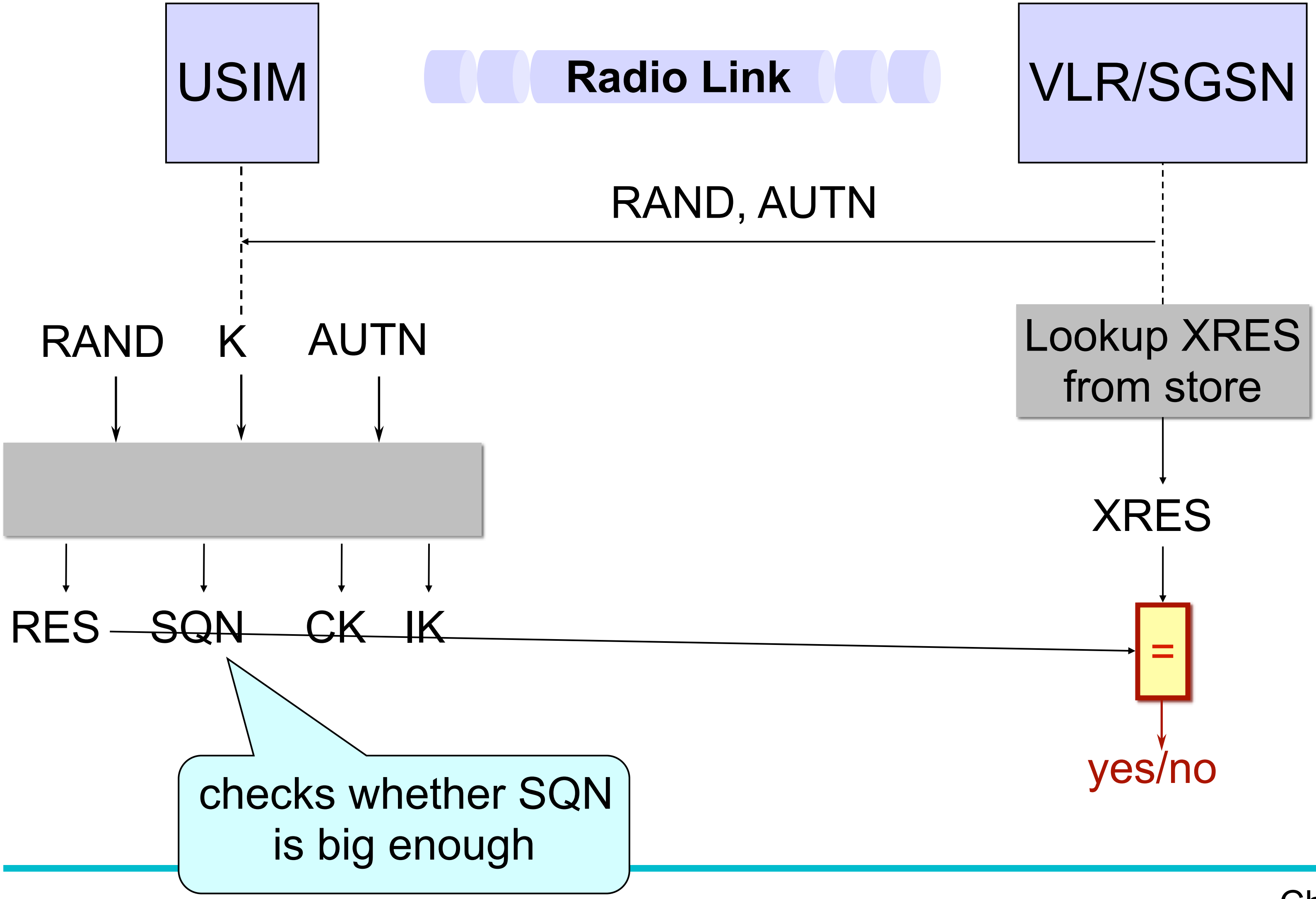
checks whether SQN is big enough

UMTS AKA: USIM ↔ VLR

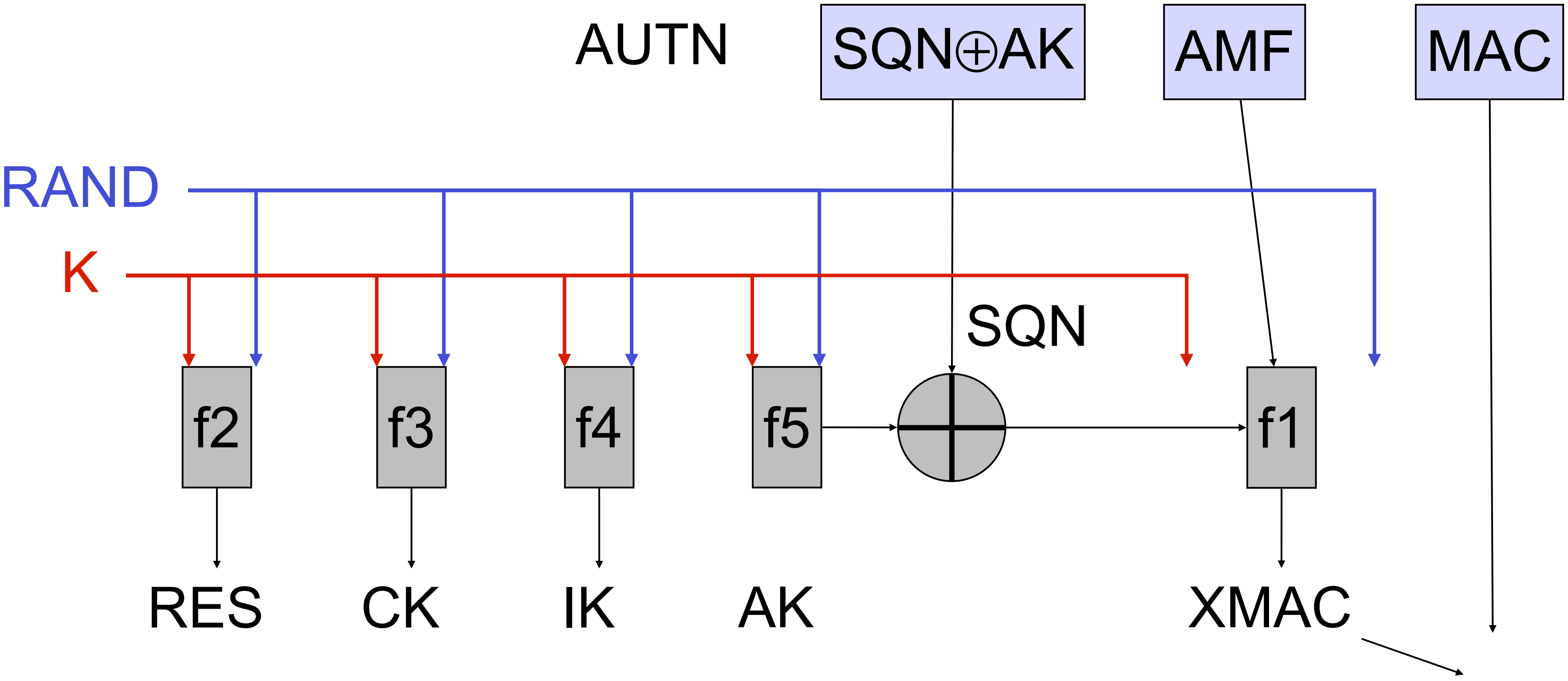


checks whether SQN is big enough

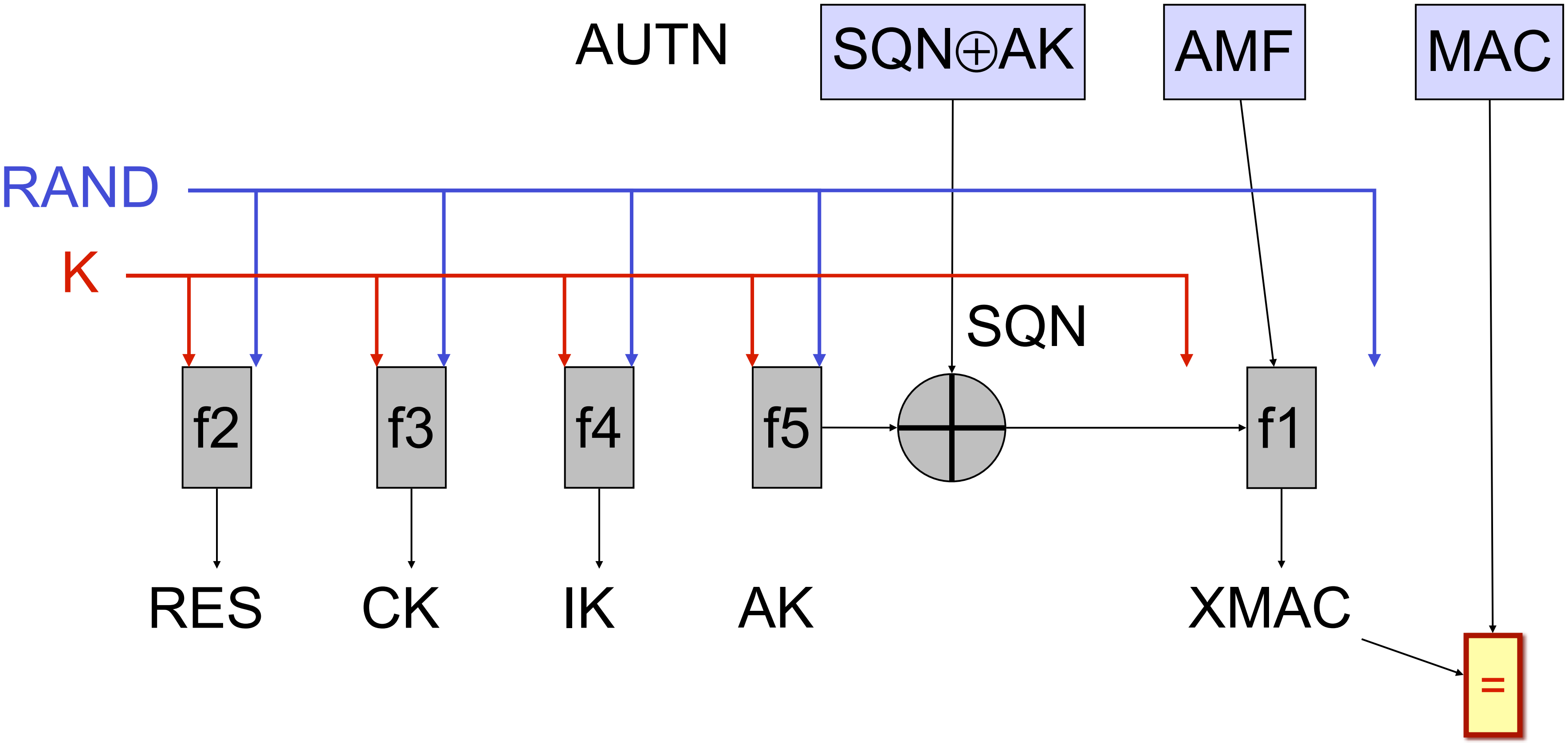
UMTS AKA: USIM ↔ VLR



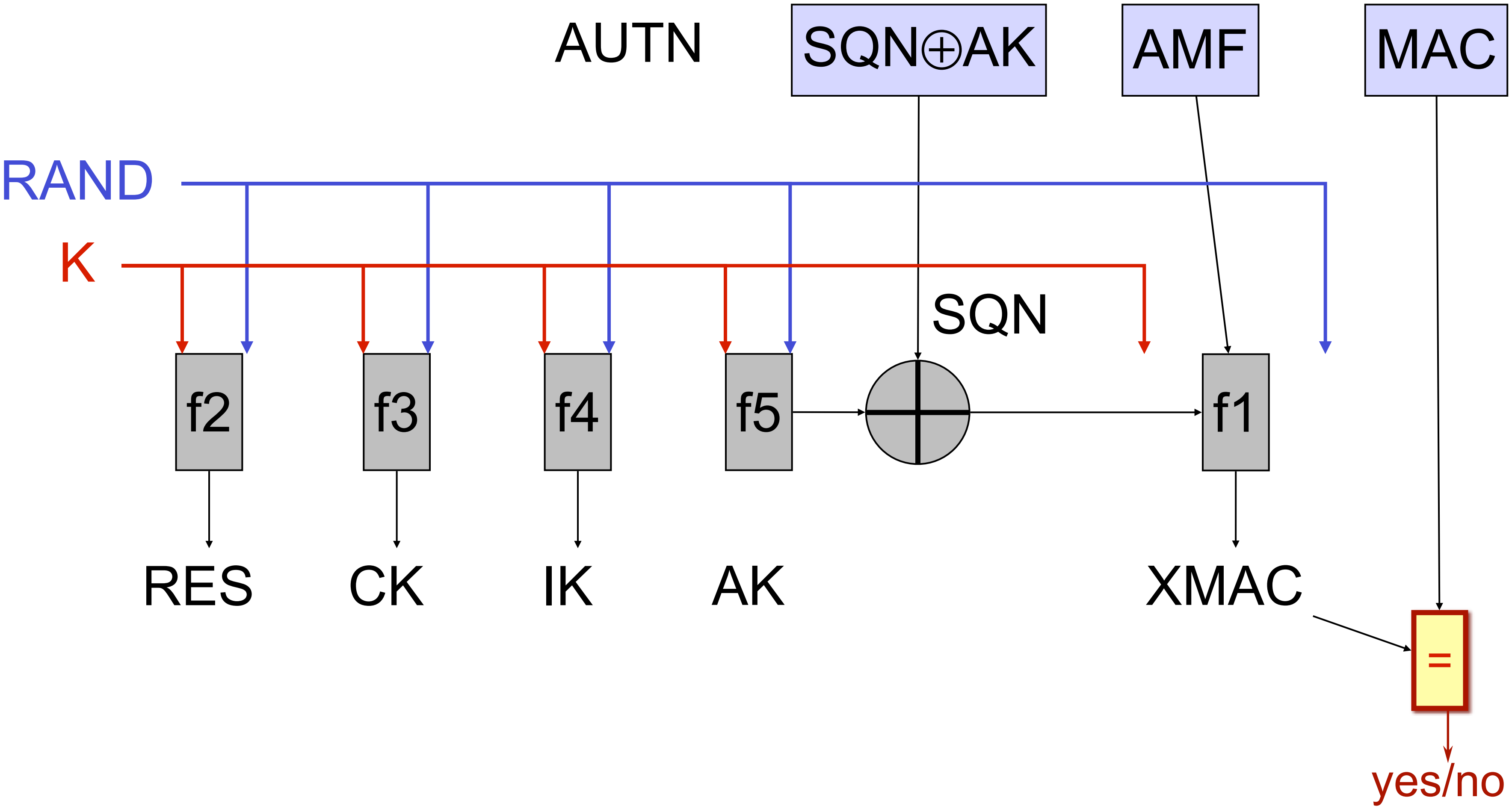
Authentication in USIM



Authentication in USIM



Authentication in USIM



UMTS AKA – Discussion

- Checks at USIM:
  - Compares MAC received as part of AUTN and XMAC computed to verify that RAND and AUTN had been generated by the home AuC.
  - Checks that SQN is fresh to detect replay attacks.
- Checks at VLR:
  - Compares RES and XRES to authenticate USIM.
- False base station attacks prevented by a combination of key freshness and integrity protection of signaling data, not by authenticating the serving network.

UMTS: Crypto Algorithms

- Confidentiality:
  - MISTY1: block cipher, designed to resist differential and linear cryptanalysis
  - KASUMI: eight round Feistel cipher, 64-bit blocks, 128-bit keys, builds on MISTY1
- Authentication and key agreement
  - MILENAGE: block cipher,128-bit blocks, 128-bit keys
- All proposals are published and have been subject to a fair degree of cryptanalysis.

Security architecture: UMTS

Threats/attacks	Security services	Security mechanisms
False BST	Authentication	Mutual authentication mechanism (challenge-response with a shared secret)
Eavesdropping (Poor GSM encryption)	Confidentiality	Encryption of signaling and call content
Data sent in clear in the operator network	Confidentiality	Encryption and integrity protection of data, to also cover operator network

Conclusion: UMTS has a decent security architecture

* Extensive threat and attack analysis
* Open development
* Modular (“flexible”) security mechanisms
    - “cryptographic core” can be replaced by operator
* Target: End-user, Operators and law enforcements

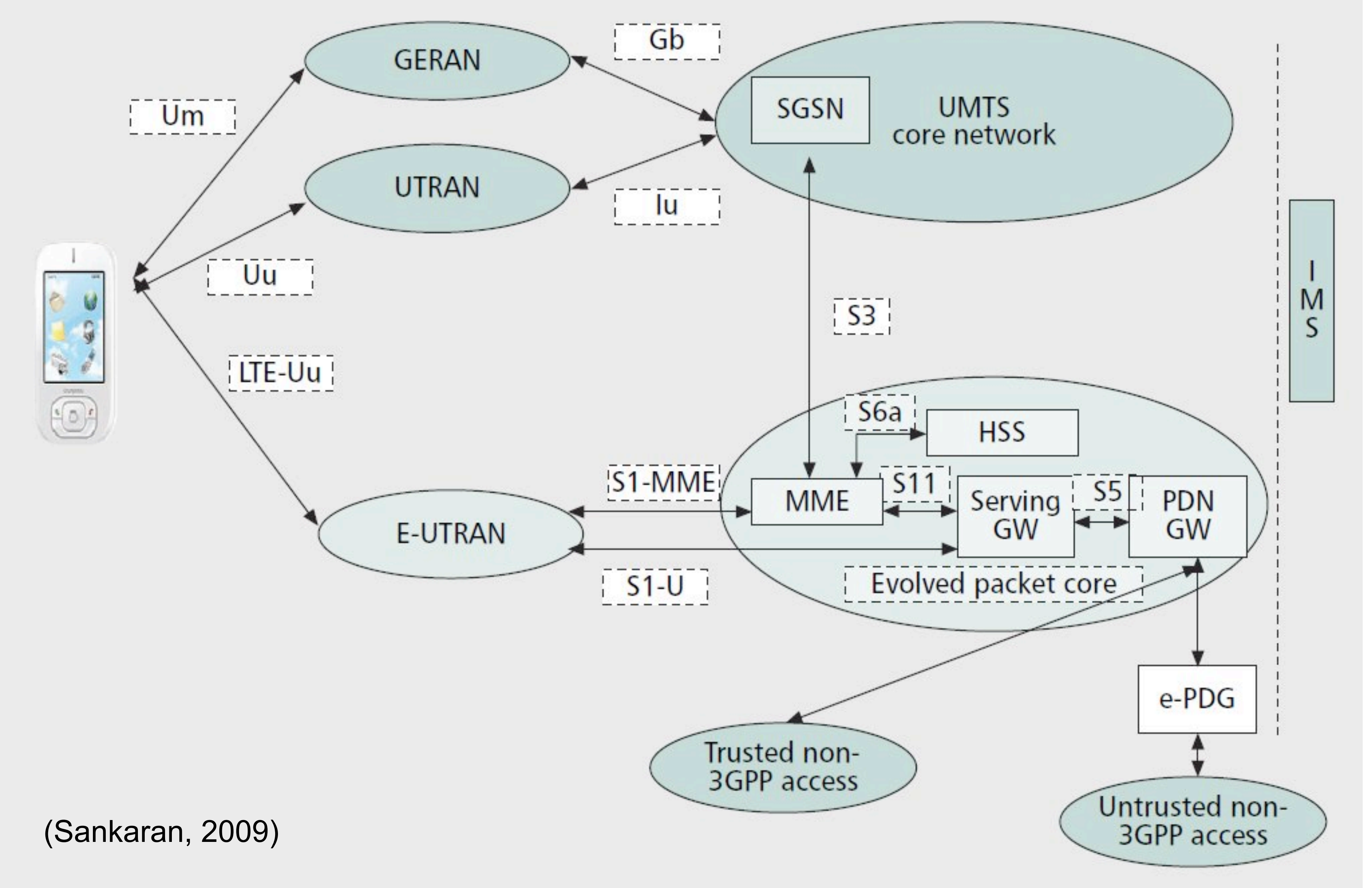
[source: Lars Strand, 2011]

LTE Advanced (4G)

- Long Term Evolution/System Architecture Evolution (LTE/SAE)
- Overall architecture of Evolved Packet System (EPS) consists of:
  1) Access network
  2) Evolved Packet Core (EPC) network
     - IP Multimedia Subsystem (IMS)
- *“Improved overall security robustness over UMTS”*
- Major changes from UMTS:
  - All IP network (AIPN)
  - Higher bandwidth
  - May use non-3GPP access networks

[source: Lars Strand, 2011]

LTE: EPS architecture



(Sankaran, 2009)

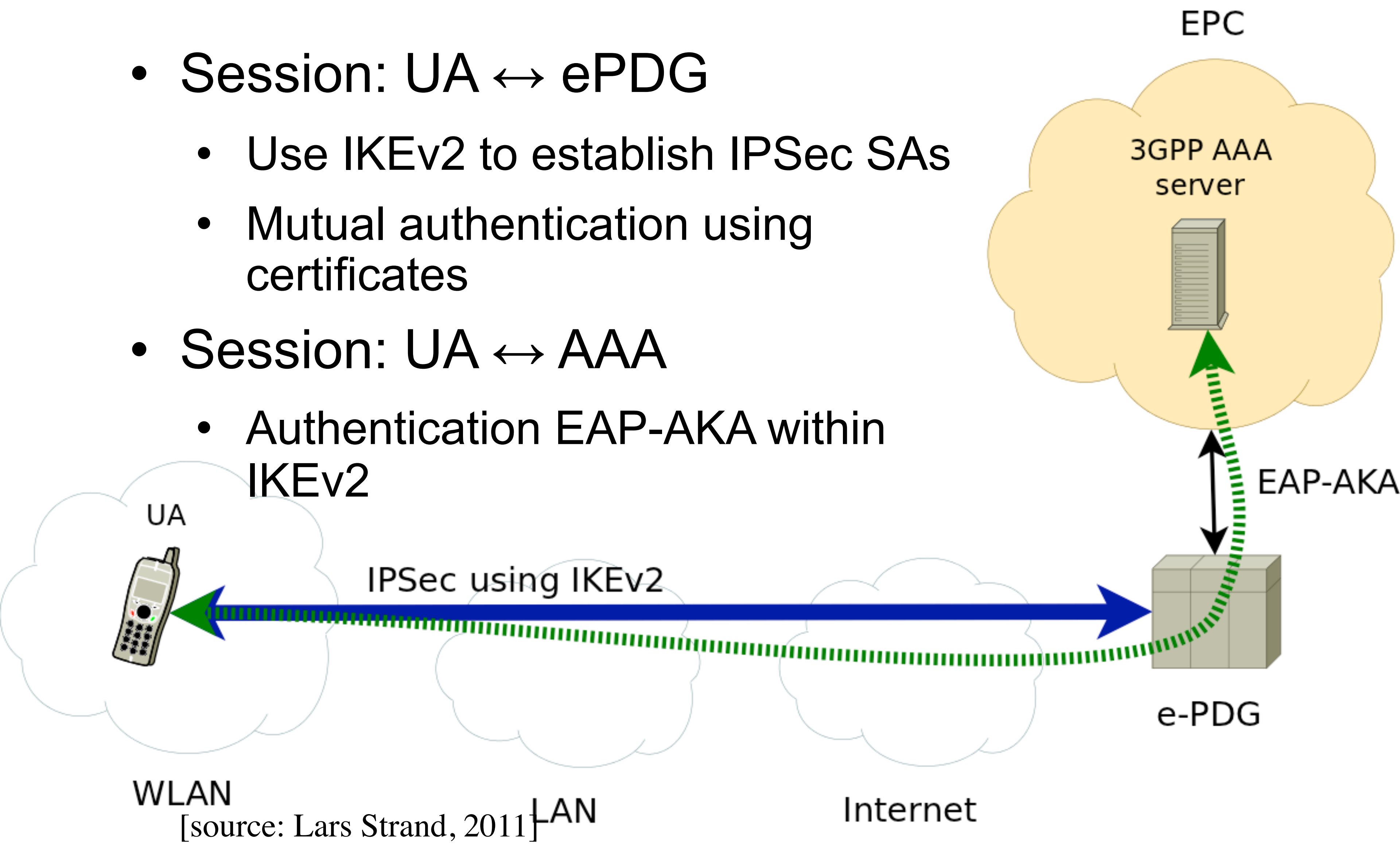
LTE: Heterogeneous networks

- Non-3GPP access network include:
  - cdm2000, WiFi (WLAN), fixed networks (Internet)
- Two classes of network access defined:
  1) Trusted access – has direct access to the operator network
     - Network operator decide which access technology is trusted
     - Can use EAP-AKA
  2) Untrusted access – everything else
     - Require IPSec with IKEv2 + EAP-AKA
     - Challenges: New threats (Internet), performance!

[source: Lars Strand, 2011]

LTE: Non-3GPP untrusted access

- Session: UA ↔ ePDG
  - Use IKEv2 to establish IPSec SAs
  - Mutual authentication using certificates
- Session: UA ↔ AAA
  - Authentication EAP-AKA within IKEv2



[source: Lars Strand, 2011]

Security architecture: LTE

Threats/attacks	Security services	Security mechanisms
Eavesdropping	Data confidentiality	IPSec
Modification of content	Data integrity	IPSec
Impersonation	Authentication	EAP-AKA
Denial of service, roaming, performance	Availability service	?, fast re-authentication? different access network?

Conclusion: LTE has a decent security architecture

* Built on and improved over UMTS
* All-IP architecture a challenge
* Untrusted non-3GPP access a challenge
* Performance might be an issue

[source: Lars Strand, 2011]

Additional slides
- Mobile IPv6 security

Mobility

- By definition, a mobile node can change its location (IP address!?) in the network.
- The ability to change location makes a node mobile.
- In the “old” setting (fixed network), a node could lie about its identity (spoofing).
- A mobile node can lie about its identity and about its location.

Attacks by a Mobile Node

- Alice could claim to be Bob to get messages intended for Bob (we have dealt with this issue in the fixed network).
- Alice could claim that Bob is at her location so that traffic intended for Bob is sent to her (hijacking, “old” attack in new disguise).
- Alice could claim that Bob is at a non-existing location so that traffic intended for Bob is lost.
- We could stop these attacks by checking that Bob gave the information about his location.

Bombing Attacks

- Alice could claim that she is at Bob's location so that traffic intended for her is sent to Bob.
- Alice could order a lot of traffic and thus mount a denial of service (bombing) attack.
- Verifying that the information about Alice's location came from Alice does not help; the information had come from her, but she had been lying about her location.

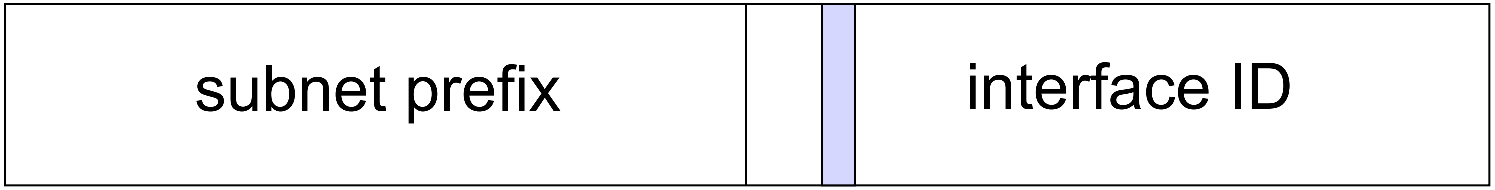
Mobility

- Mobility changes the rules of the (security) game.
- In a fixed network, nodes may use different identities in different sessions (e.g. NAT in IPv4), but in each session the current identity is the “location” messages are sent to.
- With mobile nodes, we should treat identity and location as separate concepts.

Mobile IPv6

- Mobile IPv6 (MIPv6) address (128-bit):
  subnet prefix + interface id
  (location) (identity in subnet)

- A MIPv6 address can specify a node and a location.
- Addresses of mobile nodes and stationary nodes are indistinguishable.



MIPv6 – Home Network

- In MIPv6, a mobile node is always expected to be addressable at its home address, whether it is currently attached to its home link or is away from home.
- Home address: IP address assigned to the mobile node within its home subnet prefix on its home link.
- While a mobile node is at home, packets addressed to its home address are routed to the mobile node's home link.

MIPv6 – Care-of Address

- While a mobile node is attached to some foreign link away from home, it is also addressable at a care-of address.
- This care-of address is an IP address with a subnet prefix from the visited foreign link.
- The association between a mobile node’s home address and care-of address is known as a binding for the mobile node.

MIPv6 – Binding Update

- Away from home, a mobile node registers its primary care-of address with a router on its home link, requesting this router to function as the home agent for the mobile node.
- Mobile node performs this binding registration by sending a Binding Update (BU) message to the home agent.
- Home agent replies to the mobile node by returning a Binding Acknowledgement.

MIPv6 – Binding Update

- Mobile node and home agent have a preconfigured IP security association (“trust relationship”).
- With this security association, mobile node and home agent can create a secure tunnel.
- Such a secure tunnel should also be used for binding updates.
- RFC 3776 specifies the use of ESP to protect MIPv6 signalling between mobile and home agent.

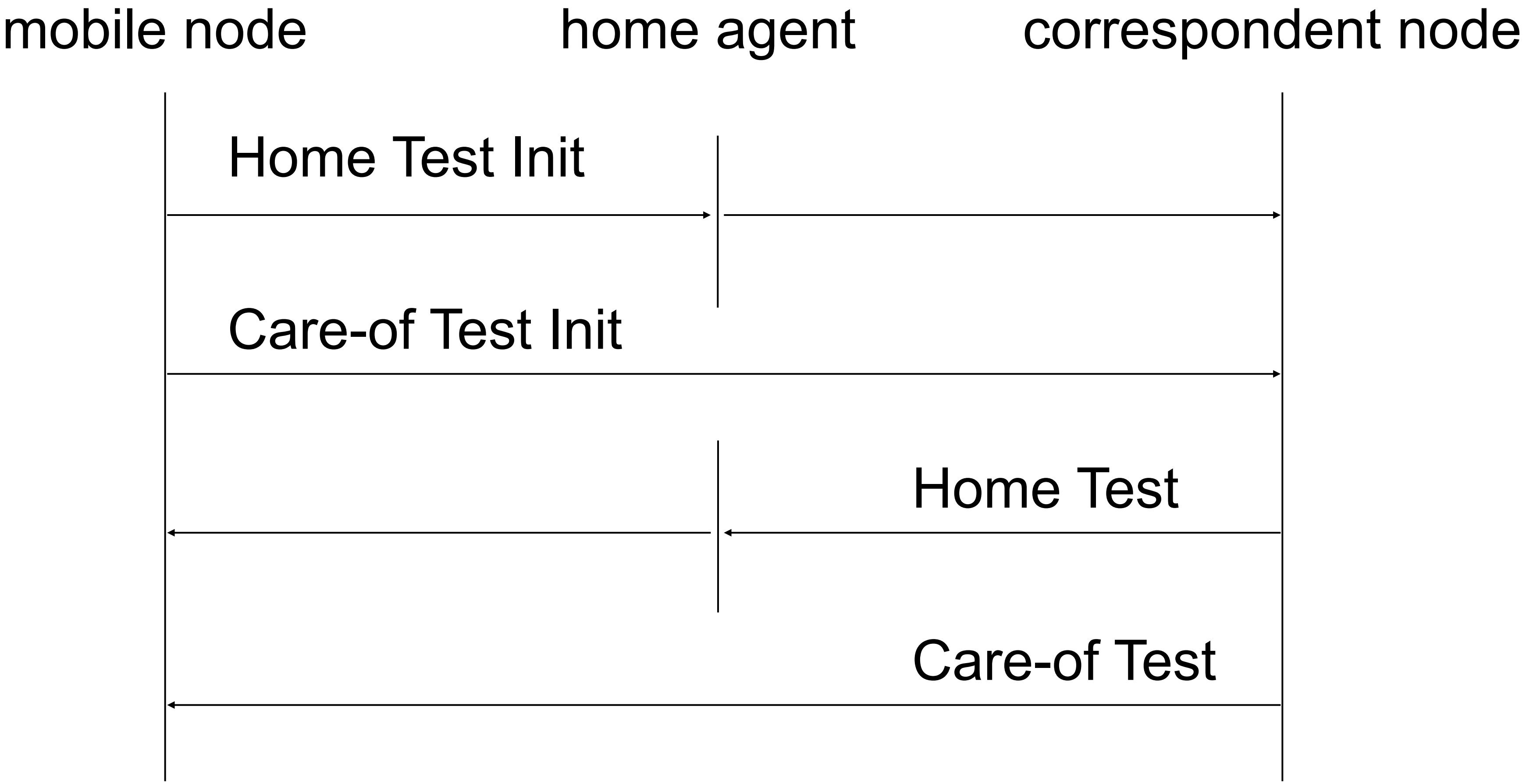
MIPv6 – Correspondent Nodes

- Any other node communicating with a mobile node is referred to as a correspondent node.
- Mobile nodes can information correspondent nodes about their current location using Binding Updates and Acknowledgements.
- The correspondent stores the location information in a binding cache; binding updates refresh the binding cache entries.
- Packets between mobile node and correspondent node are either tunnelled via the home agent, or sent directly if a binding exists in the correspondent node for the current location of the mobile node.

MIPv6 Security (RFC 3775)

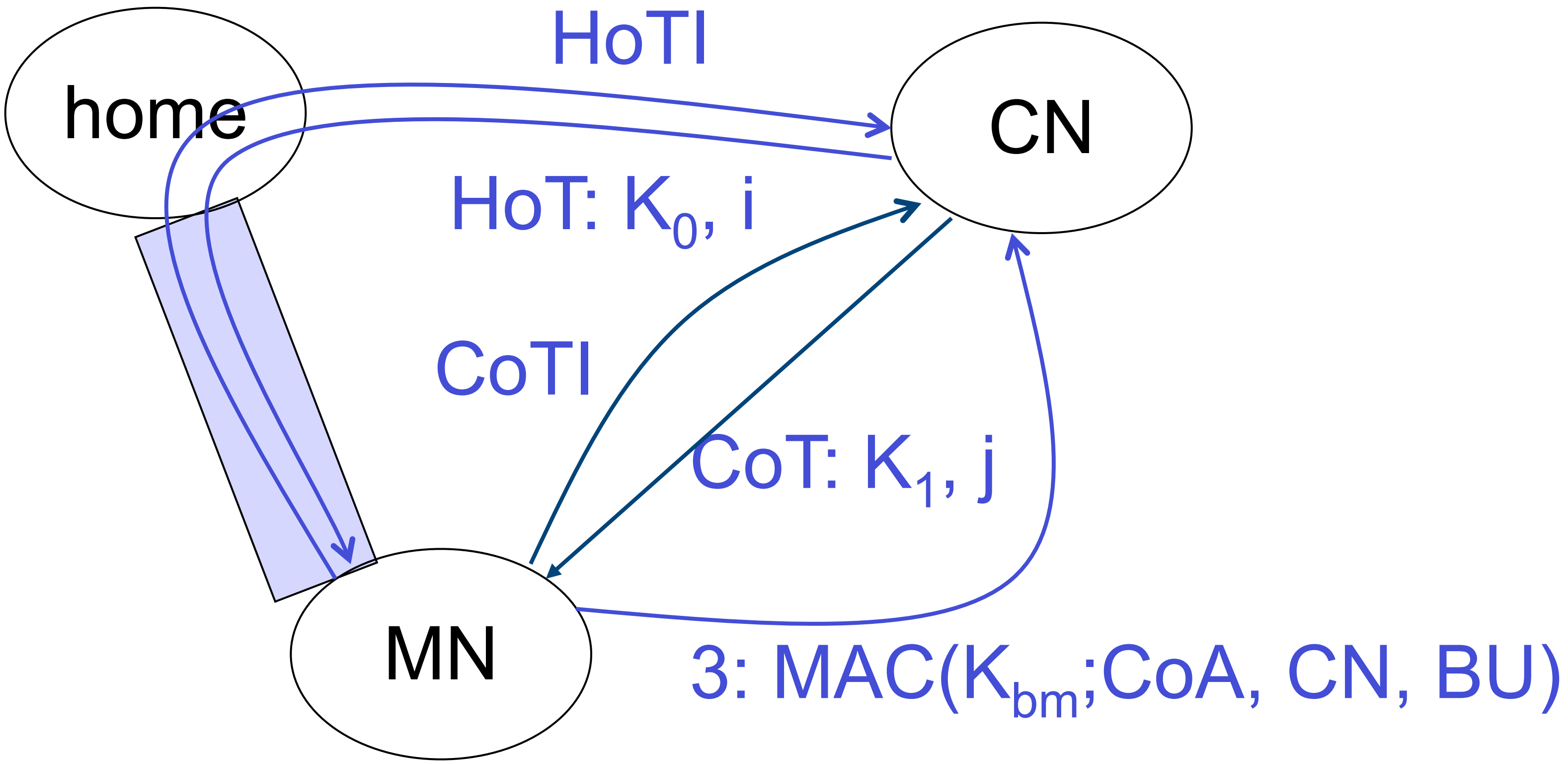
- Mobility must not weaken the security of IP
- Primary concern: protect nodes that are not involved in the exchange (e.g. nodes in the wired Internet)
- Resilience to denial-of-service attacks
- Security based on return routability: challenges are sent to identity and location, response binds identity to location.
- Cryptographic keys are sent in the clear! (You will see why.)

Return Routability Procedure



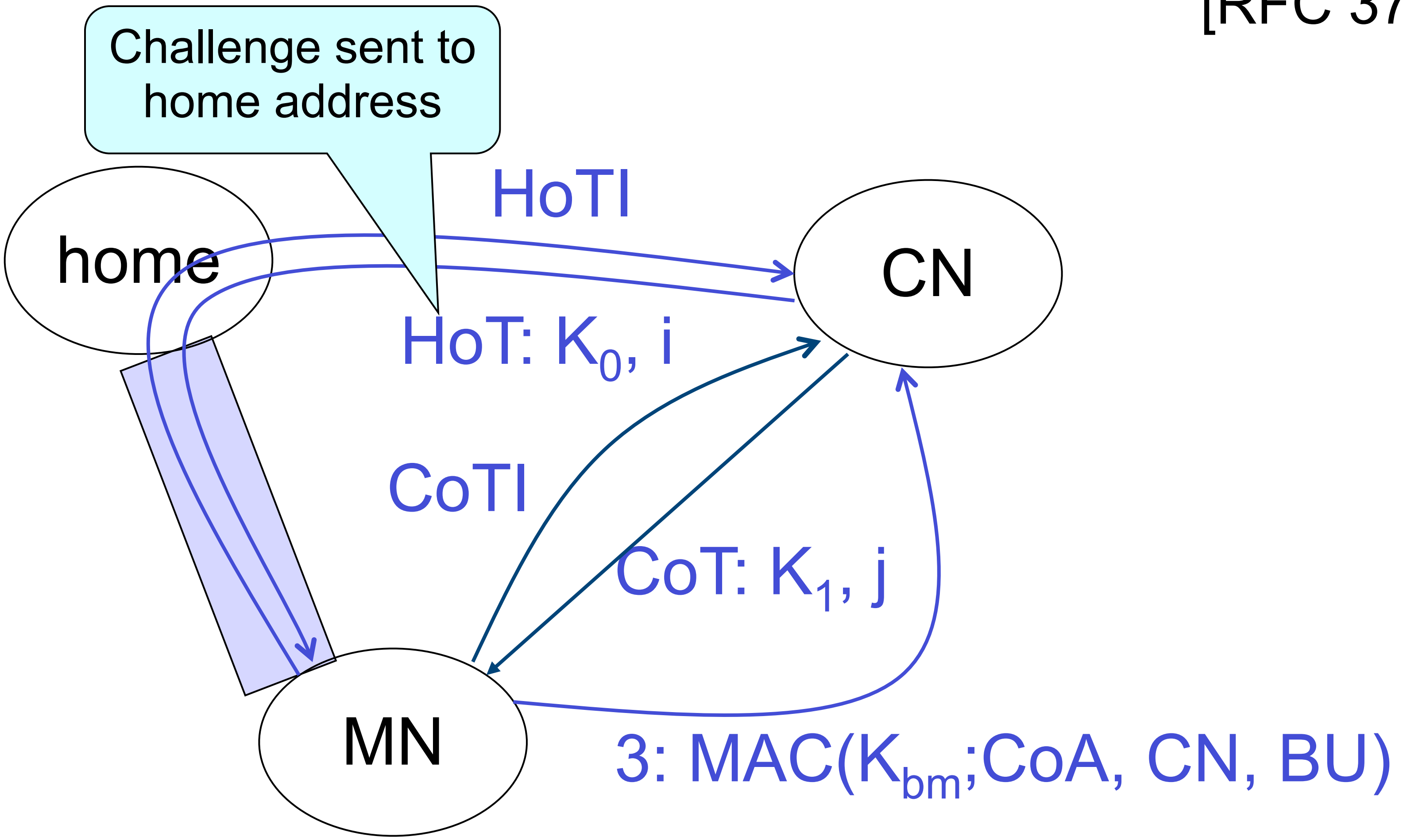
Binding Update Protocol

[RFC 3775]



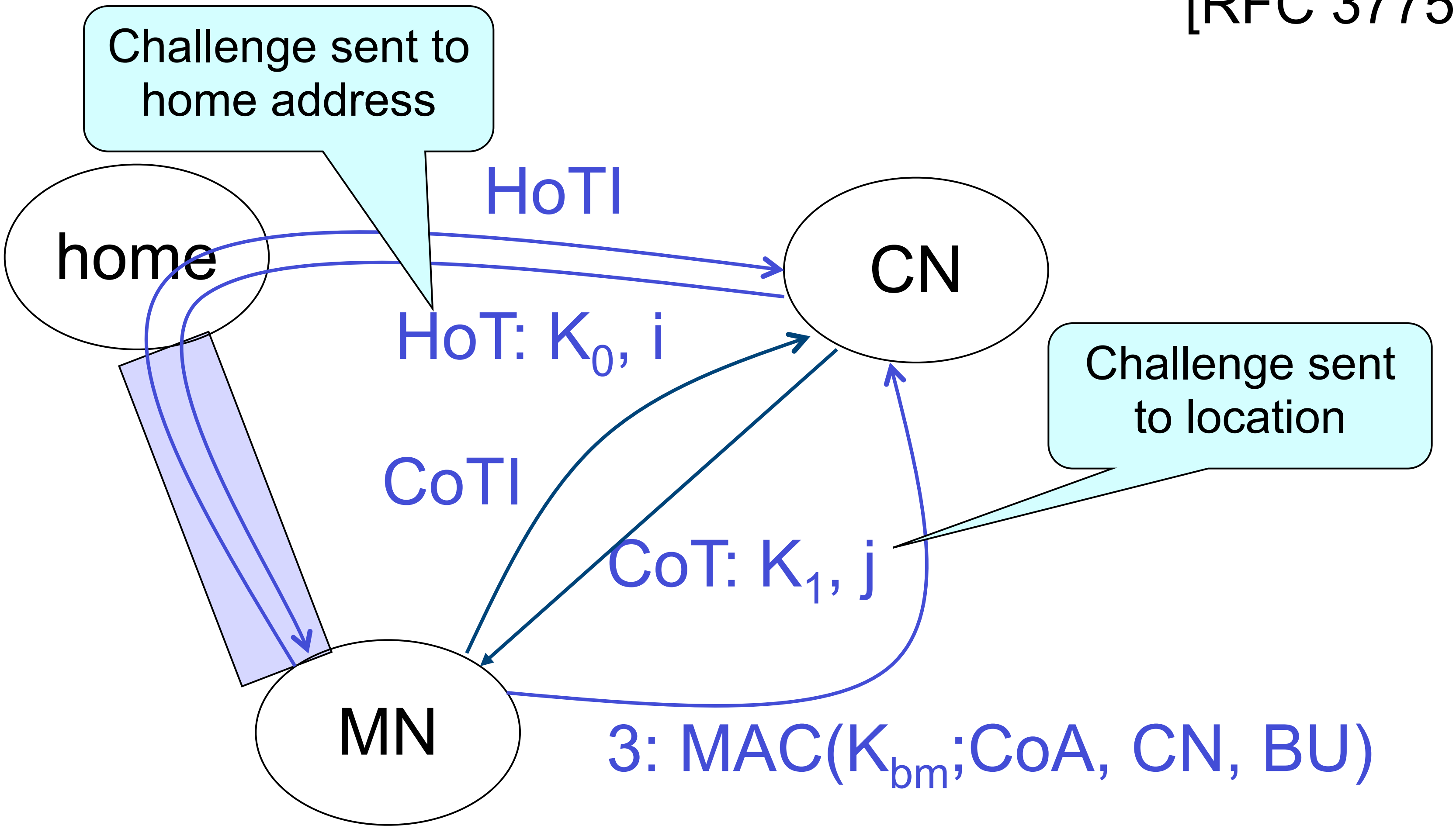
Binding Update Protocol

[RFC 3775]



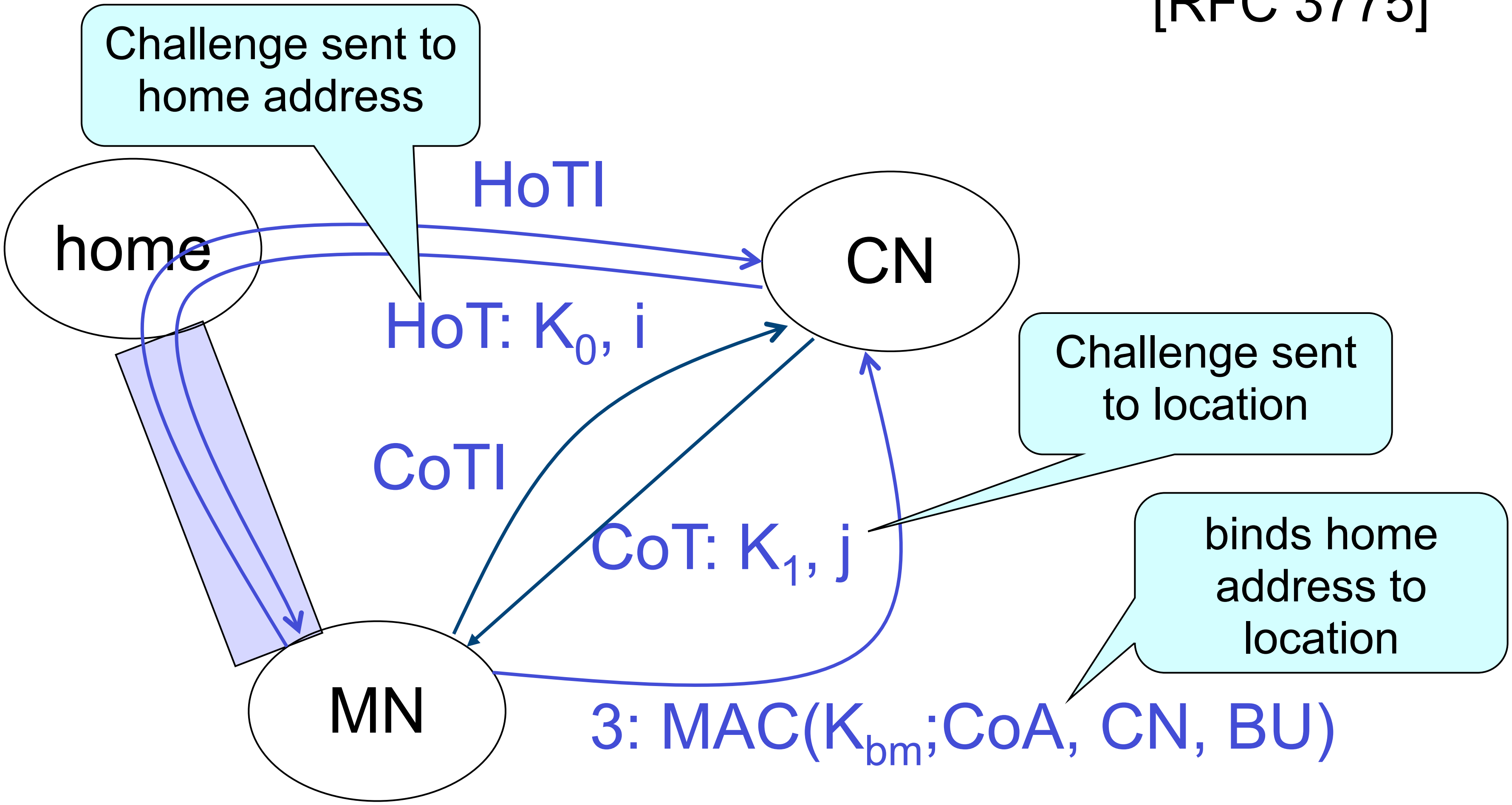
Binding Update Protocol

[RFC 3775]


Challenge sent to home address
HoTI
home
CN
HoT: K_0, i
Challenge sent to location
CoTI
CoT: K_1, j
MN
3: MAC(K_{bm};CoA, CN, BU)

Binding Update Protocol

[RFC 3775]


Challenge sent to home address
HoTI
home
CN
HoT: K_0, i
CoTI
Challenge sent to location
CoT: K_1, j
binds home address to location
MN
3: MAC(K_{bm};CoA, CN, BU)

BU Protocol

1. Mobile node sends two BU messages to the correspondent, one via the home agent, the other on the direct link.
2. Correspondent constructs a key for each of the two BU messages and returns these keys K_0 and K_1 independently to the mobile.
3. Mobile constructs a binding key K_{bm} = SHA-1(K_0,K_1) to authenticate the binding update.

Design Principles – 1

- Return routability: Correspondent checks that it receives a confirmation from the advertised location.
- Protocol creates a binding between home address (identity?) and current location.
- Protocol could be considered as a “location authentication” protocol.
- Keys are sent in the clear and could equally be interpreted as nonces.
- Protocol vulnerable to an attacker who can intercept both communications links, in particular the wired Internet.
- If we are concerned about the security of the wired Internet, we could use IPsec to protect traffic between the correspondent and the home agent.

Design Principles – 2

- Resilience against DoS attacks: protocol should be stateless for the correspondent.
- We do not want the correspondent to remember the keys K_0 and K_1.
- Each correspondent node has a secret node key, K_{cn}, which it uses to produce the keys sent to the mobiles.
- This key MUST NOT be shared with any other entity.

Key Generation

- Correspondent node generates nonces at regular intervals; each nonce is identified by a nonce index (indices *i* and *j* in the diagram).
- Key generation:

  K_0 := First (64, HMAC_SHA1 (K_{cn}, (home address | nonce | 0)))

  K_1 := First (64, HMAC_SHA1 (K_{cn}, (care-of address | nonce | 1)))
- After replying the correspondent can discard keys K_0 and K_1 because it is able to reconstruct the keys when it receives the final confirmation.
- The state the correspondent has to keep does not depend on the number of BU requests it receives.

Design Principle – 3

- Balancing message flows: A protocol where more than one message is sent in reply to one message received can be used to amplify DoS attacks.
- For this reason, the BU request is split in two; home address and care-of address could have been sent in one message but then the correspondent would have replied to one BU request with two BU acknowledgments.

Design Principle – 4

- Bombing attacks can be viewed as a flow control issue (data is sent to a victim who hadn't asked for it).
- Strictly speaking, flow control issues should be dealt with at the transport layer.
- "At which layer should we address security?"
- The decision was taken to address this issue at the IP layer because otherwise all transport protocols would have to be modified.

Active and Passive Attackers

- In communications security, it is traditionally assumed that passive attacks (intercepting communications) are easier to perform than active attacks.
- In mobile systems, the reverse may be true.
- To intercept traffic from a specific mobile, one has to be in its vicinity.
- Attempts to interfere with location management can be launched from anywhere.

Defence against Bombing

- Bombing is a flow control issue.
- Authenticating the origin of a BU does not prevent bombing; a node may lie about its location.
- It would be more accurate to check whether the receiver of a data stream is willing to accept the stream.
- Instead of origin authentication we require an authorisation to send from the destination.

Cryptographically Generated Addresses

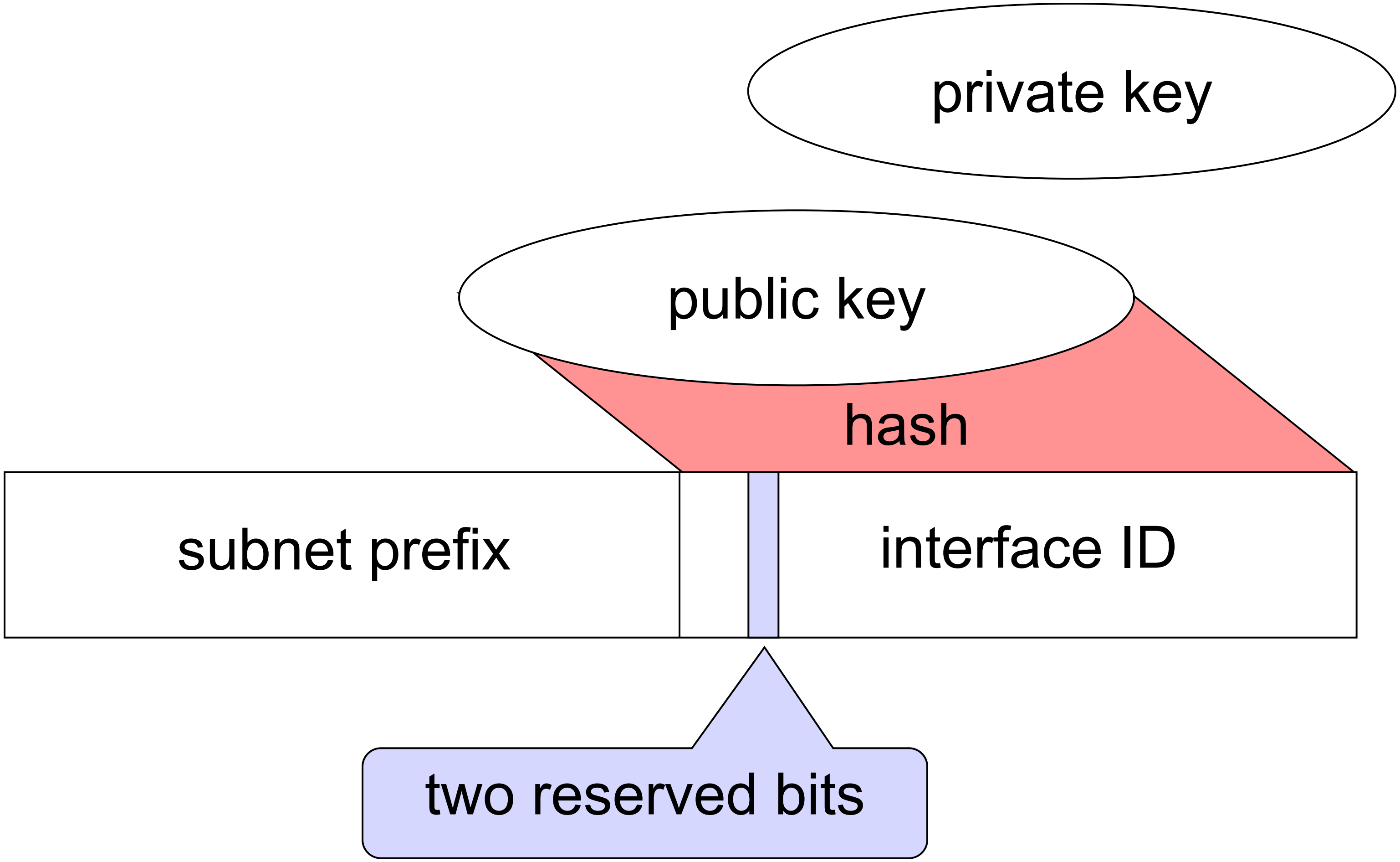
Ownership of Addresses

- Schemes that dynamically allocate addresses should check that a new address is still free.
- Broadcast a query asking whether there is any node on the network already using this address.
- Squatting attack: attacker falsely claims to have the address that should be allocated, preventing the victim from obtaining an address in the network.
- We describe a scheme whereby a node can prove that it “owns” an IP address without relying on any third party (home agent, certification authority).
- The scheme uses public key cryptography without using a PKI.

Cryptographically Generated Addresses (CGA)

- Address owner creates a public key/ private key pair and uses the hash of the public key as the interface ID in an IPv6 address.
- The mobile node can then sign BU information with its private key, and send the signed BU together with its public key to the correspondent.
- The correspondent can check that the public verification key is linked to the IP address.
- Address is “certificate” for its public key.
- CGA specified in RFC 3972

Cryptographically Generated Addresses (basic idea)



Hashing

- Hash function maps the public key to a 62-bit value.
- To forge binding updates for the given address, an attacker has to find a public key/ private key pair where the public key hashes to the address value.
- Attacker does not have to find the original key pair.
- Finding hashes for 62-bit values is too close for comfort.

Extending the Hash

- A CGA has a security parameter *Sec* (3 bit unsigned integer) encoded in the three leftmost bits of the interface ID.
- The security parameter increases the length of the hash in increments of 16 bits.
- Hash values *Hash1* and *Hash2* are computed for the public key.
- A CGA is an IPv6 address where the $16*Sec$ leftmost bits of *Hash2* are zero and the 64 leftmost bits of *Hash1* equal the interface ID (ignoring fixed bits).

Extending the Hash

- Resistance against collision attacks is now proportionate to a $59+16*Sec$ bit hash.
- Address owner is now required to do a brute force search to get a *Hash2* value of the required format.
- Effort for this search amounts to getting a hash with $16*Sec$ bits equal to a fixed value (zero).

Computing the Hashes

- *Hash1 = h(modifier, subnet prefix, collision count, public key)*
- *Hash2= h(modifier,* 0_{64}, 0_{8}*, public key)*
- Modifier (random 128-bit number) varied by the owner until a *Hash2* value of the required format is found.
- Collision count: incremented if a collision in the address space is reported (initialized to 0, error report after three failures).

CGA – Limitations

- CGA does not stop an attacker from creating bogus addresses to be used for DoS attacks.
- In particular, an attacker could launch a bombing attack against a network by creating a bogus CGA with the subnet prefix of this network.
- The correspondent has to do a signature verification when reacting to a BU request.

WLAN security

WLAN

- Wireless LAN (WLAN) specified in the IEEE 802.11 series of standards.
- Can be operated in infrastructure mode or in ad-hoc mode:
  - Infrastructure mode: mobile terminals connect to a local network via access points.
  - Ad-hoc mode: mobile terminals communicate directly.
- An open WLAN does not restrict who may connect to an access point.
- Public access points are known as hot spots.

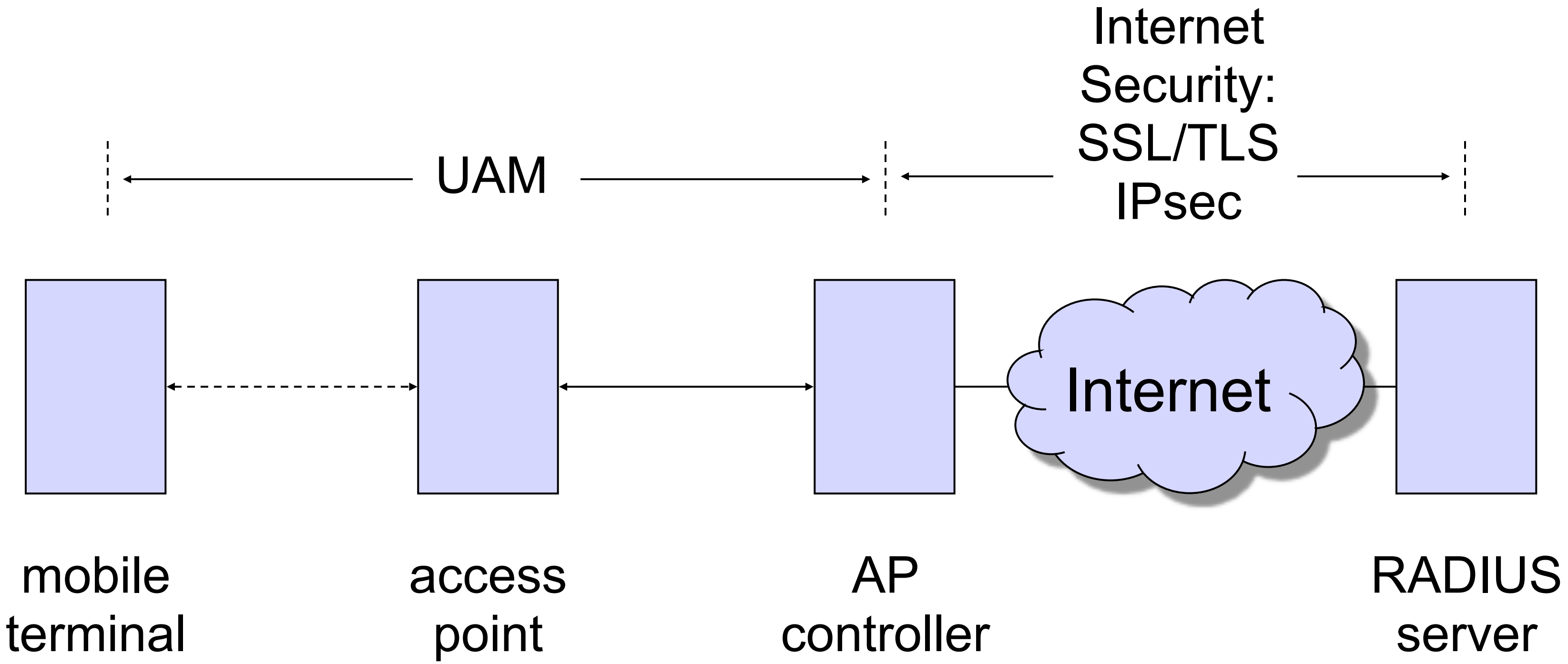
SSID & MAC

- Each access point has a Service Set Identifier (SSID).
- Access points can be configured not to broadcast their SSIDs so clients must know SSID to make a connection.
  - However, SSID is included in many signalling messages where it could be intercepted by an attacker.
- Access points can be configured to accept only mobile terminals with known MAC (medium access control).
  - Attacker can learn valid MAC address by listening to connections from legitimate device, then connect with spoofed MAC address.
- Do not base access control on information the network needs to manage connections; typically, this information must be transmitted when setting up a connection before security mechanisms can be started.

WLAN Access

- How to control access to WLAN?
- In most cases, AP does not have the resources to perform access control; there would also be the issue of managing policies on all access points in a WLAN.
- Thus, refer access control decisions to an AA (authentication & authorisation) server.
  - Also: AAA server: authentication, authorisation, and accounting.
- Example: UAM (Universal Access Mechanism)

Hot Spot Access with UAM



Universal Access Mechanism

- Client must have a web browser installed.
- Client connecting to AP gets dynamic IP address from DHCP server.
- When client's web browser starts, first DNS or http request is intercepted, redirected via an https session to a start page asking for user name and password.
- Web server at AP controller refers verification of user name and password entered to a RADIUS server.
- Once client has been authenticated, the AP can apply access control policies to the client's requests.
- Protection of subsequent traffic between client and AP is a separate issue.

WEP

- Wireless Equivalent Privacy (WEP) protocol specified in IEEE 802.11.
- First standard for protecting WLAN traffic (1997).
- Unfortunately, a case study in getting cryptographic protection seriously wrong.
- As in GSM/UMTS, stream cipher for secrecy.
- Unlike GSM/UMTS, WEP also tries to provide integrity protection of wireless traffic.

WEP – Cryptography

- Confidentiality: stream cipher (RC4), 24-bit Initialization Vector (IV) to randomize encryption.
  - Main problem: 24-bit IV is too short; weaknesses in RC4 identified after WEP was published.
- Integrity: Cyclic Redundancy Check.
  - Main problem: CRCs do not protect the integrity of messages against intentional modifications!
- Combination of stream cipher and CRC is particularly vulnerable.

WEP – Cryptography

- Authentication based on a shared secret: pre-shared secrets installed manually in all devices that should get access and in all access points of the network.
  - Suitable for small installations like home networks; most LANs use the same key for all terminals.
- Sender, receiver share secret 40-bit or 104-bit key K.
- Transmitting a message m: sender computes 32-bit checksum CRC-32(m); prepends 24-bit IV to key and generates a key stream with the 64-bit (128-bit) key $K' = \mathrm{IV}||K$ using RC4; IV sent in the clear.
- Ciphertext $c = (m||\text{CRC-32}(m)) \oplus \text{RC4}(K')$.
- Receiver computes $c \oplus \text{RC4}(K') = (m||\text{CRC-32}(m))$ and verifies checksum.

Problems with WEP

- CRC-32 is a linear function! An attacker who only has a ciphertext, but neither key nor plaintext, can modify the plaintext by a chosen difference Δ.
- Compute δ = CRC-32(Δ) and add $(\Delta||\delta)$ to c; this is a valid encryption of the plaintext $m \oplus \Delta$:

  $$(m||\text{CRC-32}(m)) \oplus \text{RC4}(K') \oplus (\Delta||\delta) = (m \oplus \Delta||\text{CRC-32}(m) \oplus \delta) \oplus \text{RC4}(K') = (m \oplus \Delta\ ||\text{CRC-32}(m \oplus \Delta)) \oplus \text{RC4}(K').$$

- Second problem: size of IV too small.
- Third problem: cryptanalytic attacks on RC4, e.g. exploiting weak keys; typically require attacker to collect a sufficient amount of encrypted packets.

Problem: Re-use of IVs

- Why is it a problem if the same IV is used for two different packets?
- Both packets are encrypted under the same key K'.

$$c_1 = (m_1 || \text{CRC-32}(m_1)) \oplus \text{RC4}(K')$$

$$c_2 = (m_2 || \text{CRC-32}(m_2)) \oplus \text{RC4}(K')$$

- Compute XOR of the two ciphertexts $c_1 \oplus c_2$:

$$(m_1 || \text{CRC-32}(m_1)) \oplus \text{RC4}(K') \oplus (m_2 || \text{CRC-32}(m_2)) \oplus \text{RC4}(K')$$

$$= (m_1 || \text{CRC-32}(m_1)) \oplus (m_2 || \text{CRC-32}(m_2))$$

$$= (m_1 \oplus m_2 || \text{CRC-32}(m_1 \oplus m_2))$$

- The result is the XOR of the two plaintexts.
- When the APs in a WLAN use the same secret it is particularly easy to collect traffic with reused IVs.

WPA – Wi-Fi Protected Access

- Developed by WiFi Alliance.
- Challenge: devices already deployed in the field but you have got the standard wrong.
  - Can’t ask users to throw away their devices; you must find a fix that works with current equipment.
  - Only software upgrades are feasible.
  - Changes to encryption must work with existing hardware architectures.
- Challenge: quick fix while new standard is being drafted that will be forward compatible.

WPA – Restrictions & Remedies

- Processor load: C implementation of 3DES needs about 180 instructions per byte.
- 802.11b data throughput: 7 Mbit/s, i.e. 875000 bytes/s.
- Processor must execute 157.5M instructions per second; way beyond a typical AP.
- First remedy: replace CRC with cryptographic integrity check function.
- Plus better key management, longer IV.

Michael

- CRC replaced by “Michael” a Message Integrity Code (MIC, Message Authentication Code).
- Constructed from shift, add, XOR operations; 3.5 cycles/byte on ARM, 5.5 cycles/byte on i486.
- 64-bit key, 32-bit blocks, returns 64-bit hash value.
- ‘Medium’ security: target security level equivalent to guessing 2^{20} messages; today best attack equivalent to guessing 2^{29} messages.
- Further countermeasure: base station switches off for a minute (opportunity for DoS attack) when receiving two bad packets within a second.

TKIP

- Temporal Key Integrity Protocol, specified in IEEE 802.11i.
- Combines encryption & integrity verification.
- Different ‘temporal’ key for each frame.
- Based on RC4 with 128-bit keys.
- 48-bit IV used as sequence number; sender and receiver obtain IV from sequence counter.
- MIC appended to data before encryption.
- Key update after 2^{16} IVs have been used.

TKIP – Key Hierarchy

- Pairwise Master Key (PMK): established when mobile station connects to network or derived from password (pre-shared key).
- Pairwise Transient Key (PTK): derived from PMK, MAC addresses of station and AP, nonces from station and AP; split into
  - Key Confirmation Key (KCK): for key authentication
  - Key Encryption Key (KEK): for distributing group keys
  - Temporal Key (TK): basis for data encryption
- Temporal session key: derived from TK and MAC address of AP.
- WEP key and IV (per packet): derived from temporal session key and sequence number.

Problem: Password Guessing

- WPA-PSK (pre-shared key) vulnerable to password guessing attacks.
- Attacker records traffic as victim connects to WLAN.
- Attacker guesses a passphrase, computes master key PMK' for the guess and the known (intercepted) values SSID and SSID length.
- Transient key PTK' is derived from PMK' and the intercepted MAC addresses and nonces.
- Recorded encrypted messages are decrypted with candidate key PTK'.
- If result is meaningful plaintext, the guess of the passphrase is correct with high probability.

WPA2 – New Standard

- IEEE 802.11i [June 2004]
  - Robust Security Network (RSN): dynamic negotiation of authentication and encryption algorithms.
- WPA2 from WiFi Alliance, based on IEEE 802.11i.
- IEEE 802.11i and WPA2 overlap and are sometimes used as synonyms; however, this is not completely correct.
- Two modes:
  - Backwards compatible with WEP (TSN).
  - Not backwards compatible (RSN).

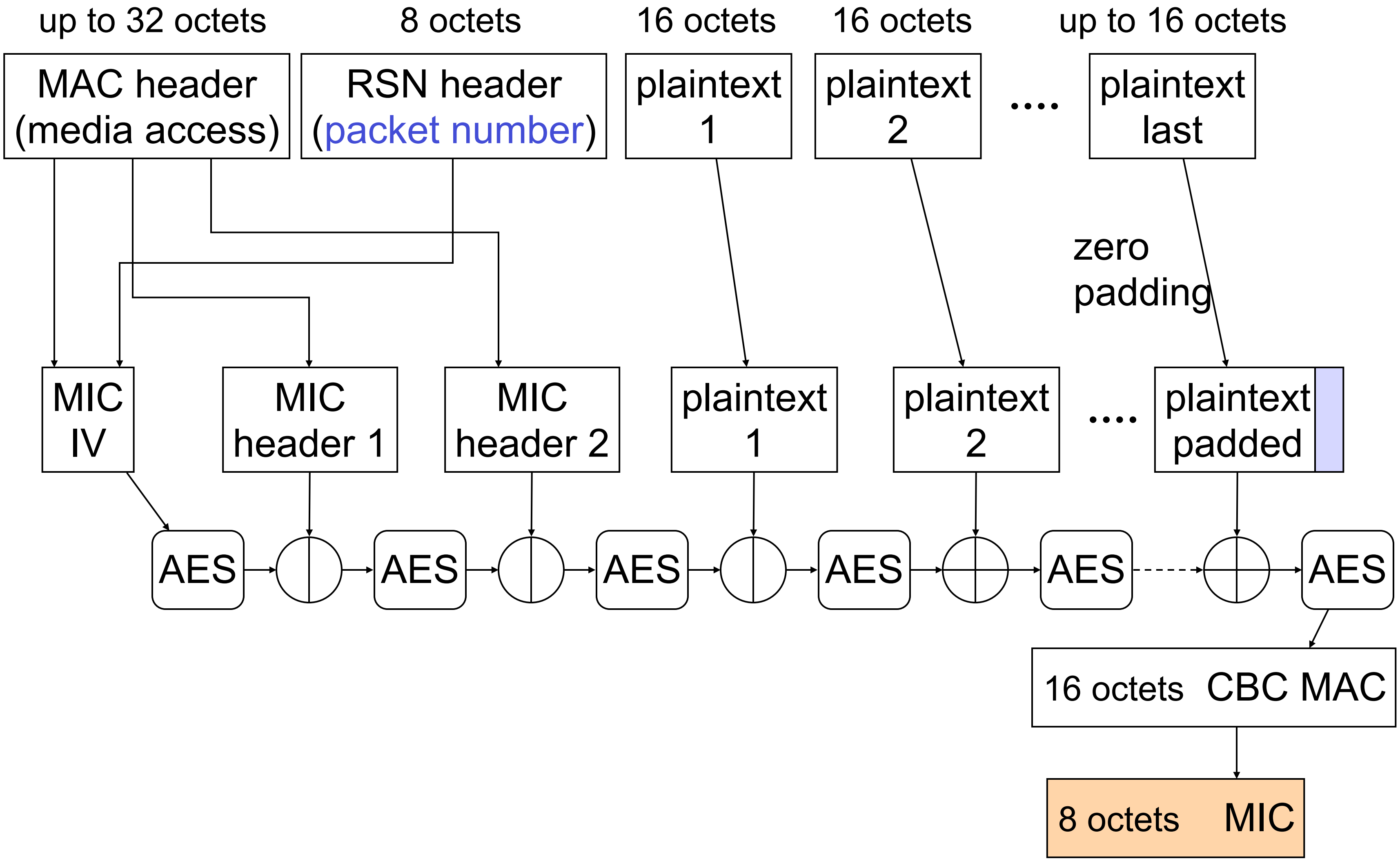
WPA2 – Cryptography

- Authentication:
  - For large networks with EAP.
  - For smaller networks with TKIP.
- Encryption: 128-bit AES (key & block size) in CCM mode: Counter mode CBC MAC Protocol (CCMP).
  - Counter with CBC-MAC (CCM) defined in RFC 3610.
  - 64-bit MIC derived from CBC-MAC.
- Not compatible with older hardware.
- Transitional Security Network (TSN) allows RSN and WEP to coexist on the same WLAN.
  - Devices using WEP can be a security risk.

CCMP

- Counter mode for encryption.
  - Input: MPDU: MAC header (media access), data; RSN header: KeyID, packet number (PN); key.
  - Counter initialized to 1 when establishing new temporal key.
  - Each 128-bit plaintext block XOR-ed with encrypted counter value; incremented for each block.
  - Output: MAC & RSN header (unencrypted), encrypted data, MIC.
- CBC-MAC for integrity.
  - CCM nonce block contains PN, MAC address field A2, priority field; encrypted to get the IV proper for CBC mode.
  - MIC: 8 least significant octets of CBC-MAC value.

MIC Calculation (simplified)



Bluetooth

- Technology for piconets (Personal Area Networks): wireless ad-hoc networks for short range communications between personal devices like a PC, keyboard, mouse, printer, headset, etc.
- Pairing: establishes security association between two devices manually; enter same PIN on both devices.
  - 128-bit link key derived from PIN; authentication uses a challenge-response protocol similar to GSM.
- Simple Secure Pairing protocol to establish link keys.
  - Uses elliptic curve Diffie-Hellman (ECDH); user decdes when to change public/private key pair of a device.
  - Physical proximity is the main protection against man-in-the-middle attacks.
- Bluetooth attacks that exploit flaws in the software configuration of the devices exist (e.g. Bluesnarf) .