# Mobility

# 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

GSM security

UMTS authentication

- What do we mean by “mutual authentication”

Mobile IPv6 security

- Secure binding updates

Cryptographically generated addresses

WLAN security

- WEP
- WPA
- Bluetooth

# GSM & UMTS security

# GSM – History

Study group Groupe Spéciale Mobile (GSM) of the Conference of European Posts and Telegraphs (CEPT) founded in 1982 to specify new mobile network.

Goals: good subjective voice quality, cheap end systems, low running costs, international roaming, handheld mobile devices, new services (e.g. SMS), ISDN-Compatibility.

Responsibility for GSM transferred to European Telecommunication Standards Institute (ETSI) in 1989, Phase I of GSM specification published 1990.

Renamed: Global System for Mobile Communications

# 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

...

# 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

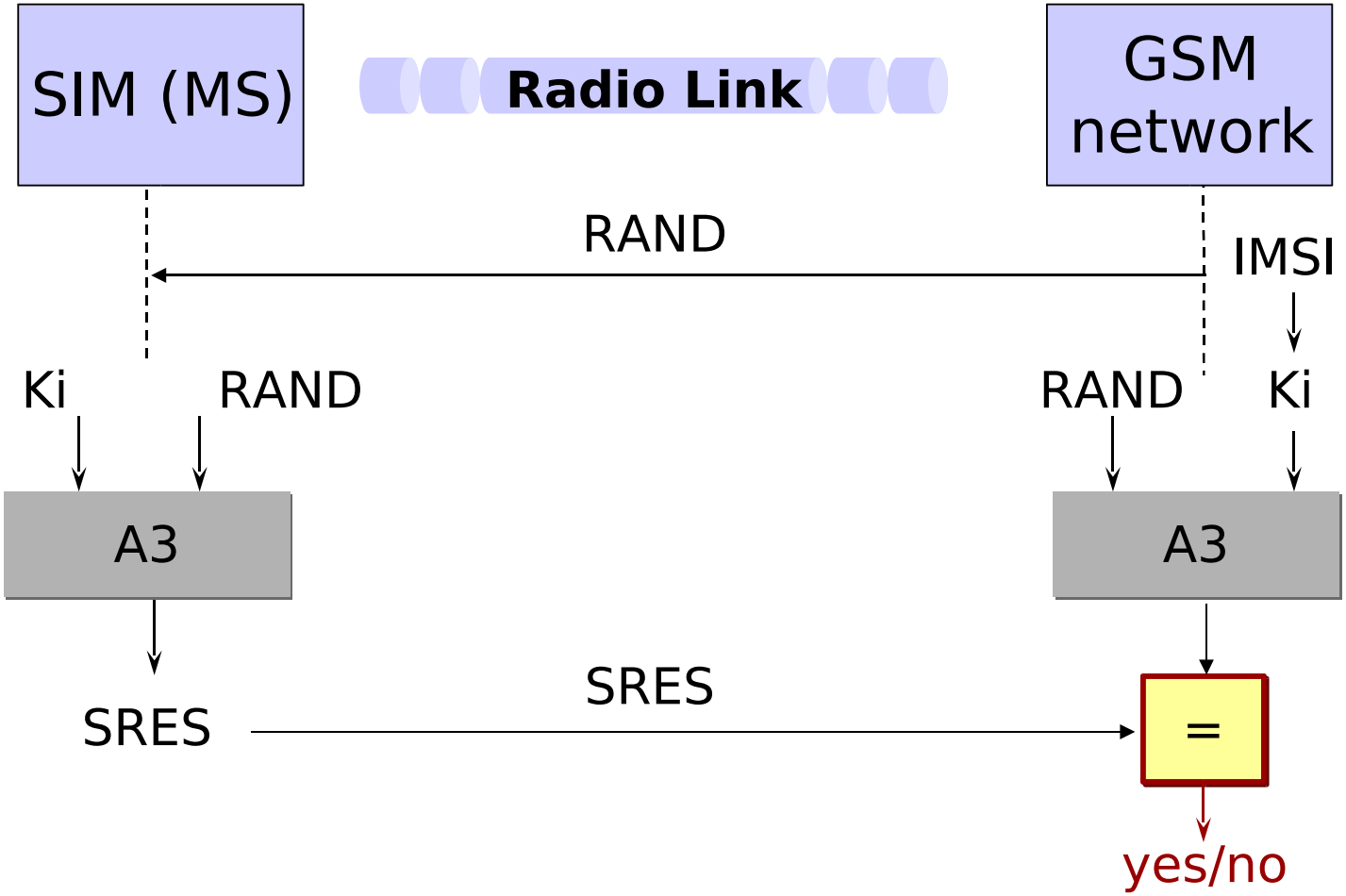
A8 ciphering key generating algorithm

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 the MS.

MS computes SRES, the ‘signature’ of RAND, using algorithm A3 and the secret : Individual Subscriber Authentication Key Ki.

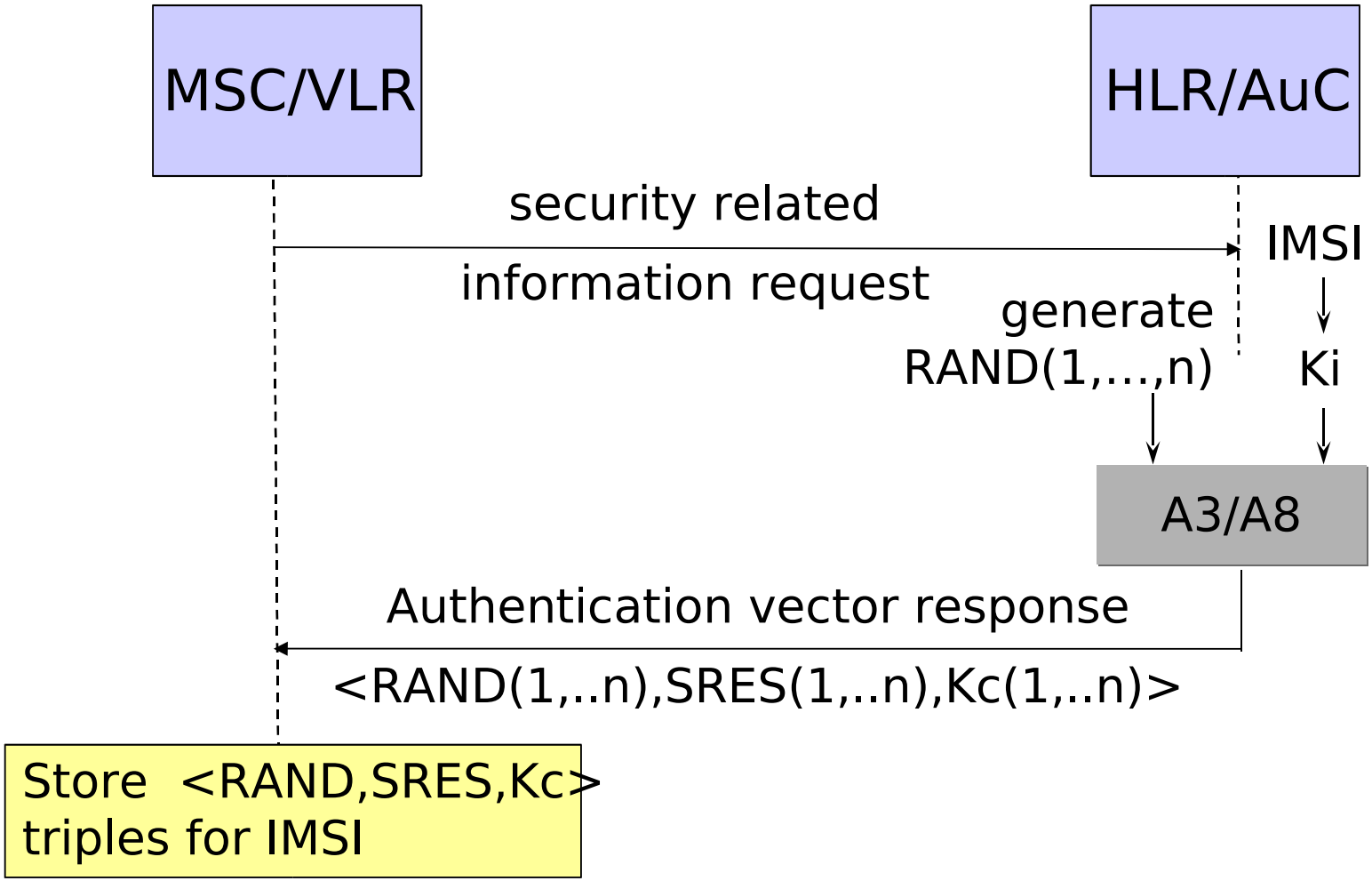
MS transmits SRES to the fixed subsystem.

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

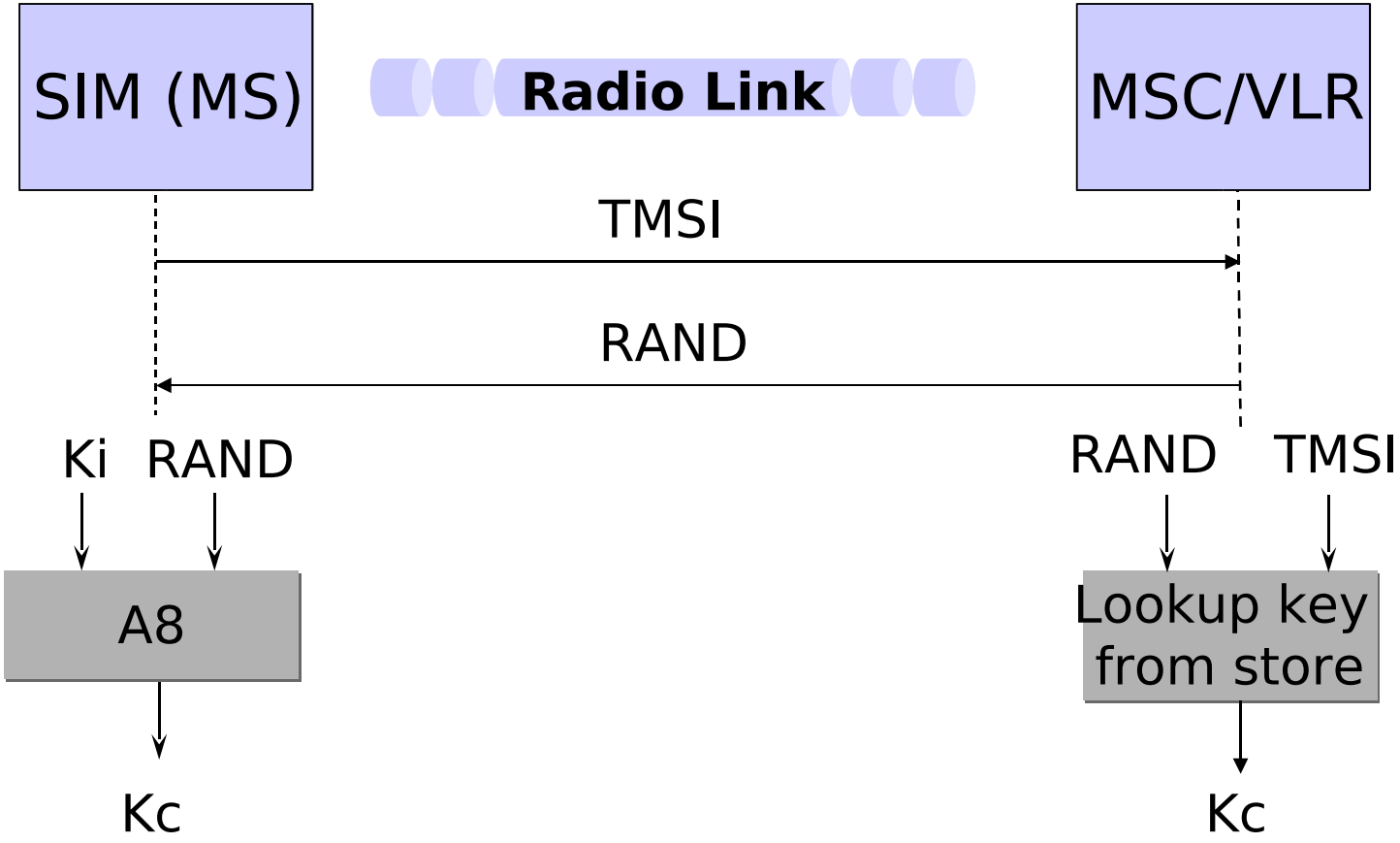
VLR keeps relation <(TIMSI, LAI), IMSI>

# 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



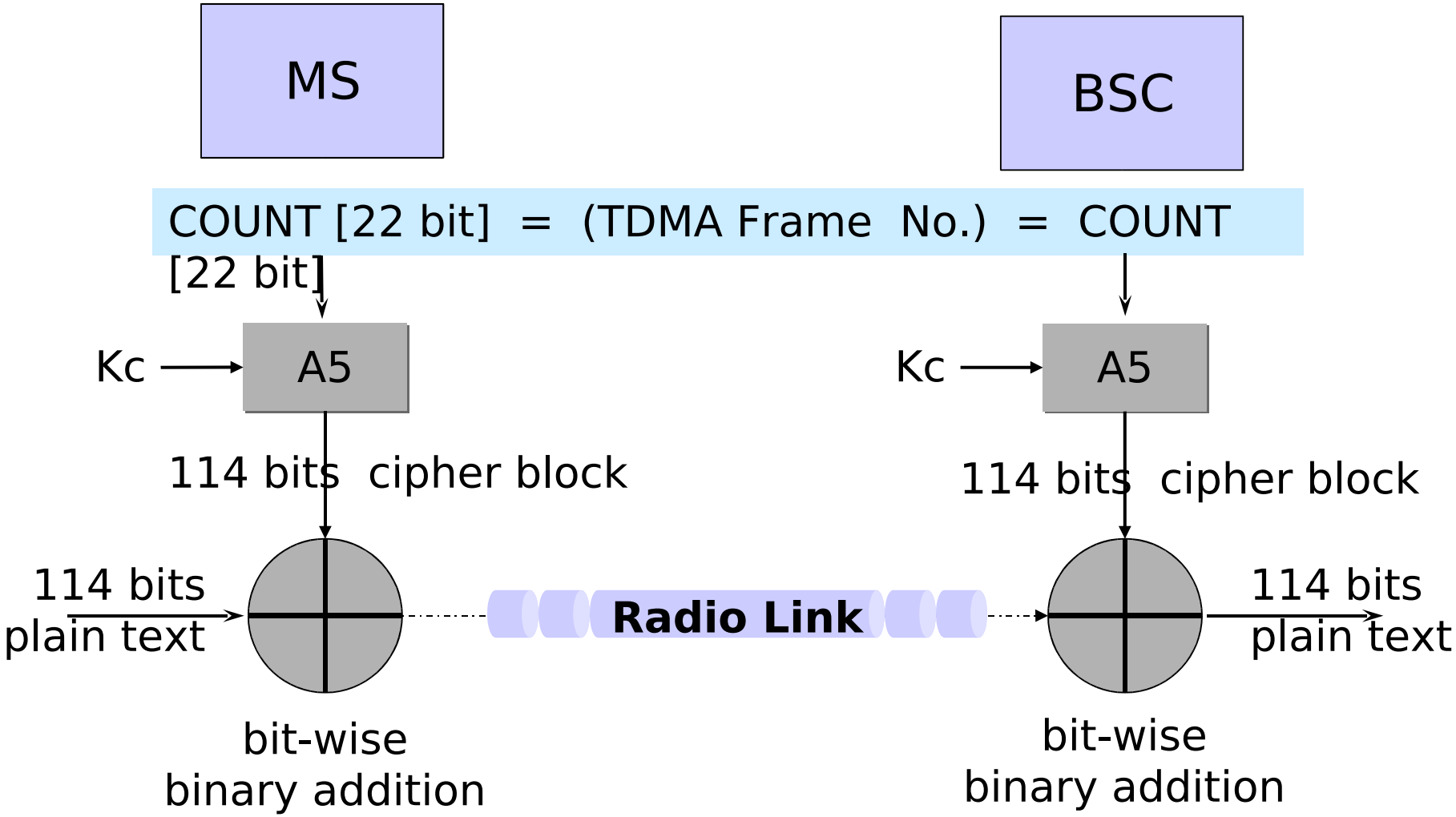
# Cryptographic algorithms: A3/A8

Algorithms A3 and A8 are shared between subscriber and home network; thus each network could choose its own algorithms.

- Algorithms A3 and A8 are 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 has to be shared between all subscribers and all network operators.

This algorithm has to be standardized.

- The specification of Algorithm A5 is managed under the responsibility of GSM/MoU.

A5/1, A5/2 (simpler “export” version).

The specification of these algorithms has not been (officially) published.

Cryptanalytic attacks against both algorithms have been published.

# Stream Cipher: A5

A5: stream cipher that encrypts 114-bit frames; key for each frame derived from the secret key Kc and the current frame number (22 bits).

Why a stream cipher, not a block cipher (DES)?

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

Separation of subscriber identity from equipment identity

Some protection of location privacy (TMSI)

No authentication of network.

- IMSI catcher pretend to be BTS and request IMSI.

# UMTS

Universal Mobile Telecommunications System

Work on 3rd generation mobile communications systems started in the early 1990s.

Security concerns with GSM:

- No authentication of network.
- Undisclosed crypto algorithms.

The UMTS security architecture is similar to GSM, but adds mutual authentication; the crypto algorithms are published.

Main standards organization: 3GPP.

# 3GPP

The 3G Partnership Project:

- ETSI (Europe)
- ARIB (Japan)
- TTC (Japan)
- T1 (North America)
- TTA (South Korea)
- CCSA (China)

Mission: Drive forward the standardization of 3G systems.

First release of specifications in 1999.

# 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.

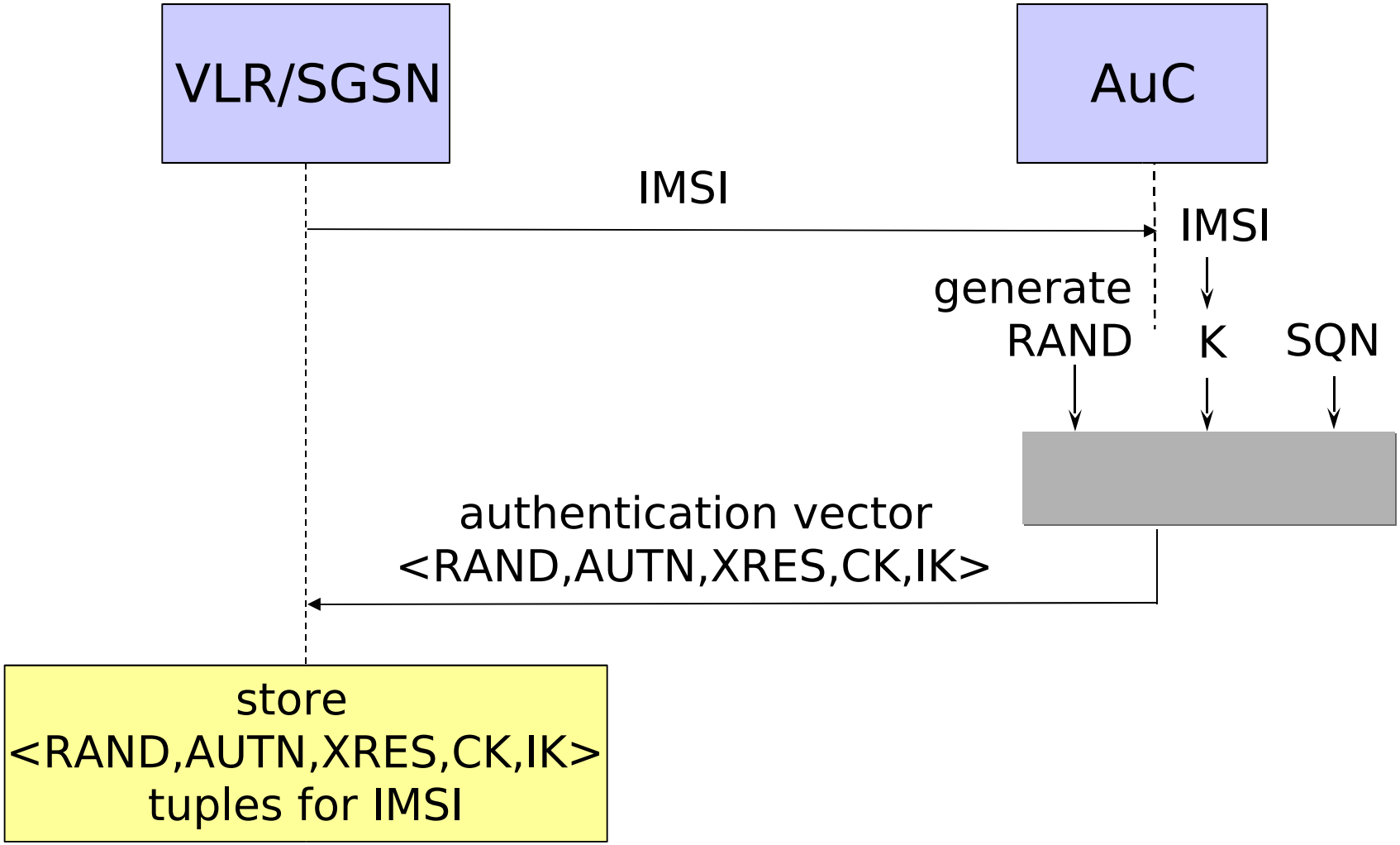
AuC can generate random challenges RAND.

USIM and AuC have synchronized sequence numbers SQN available.

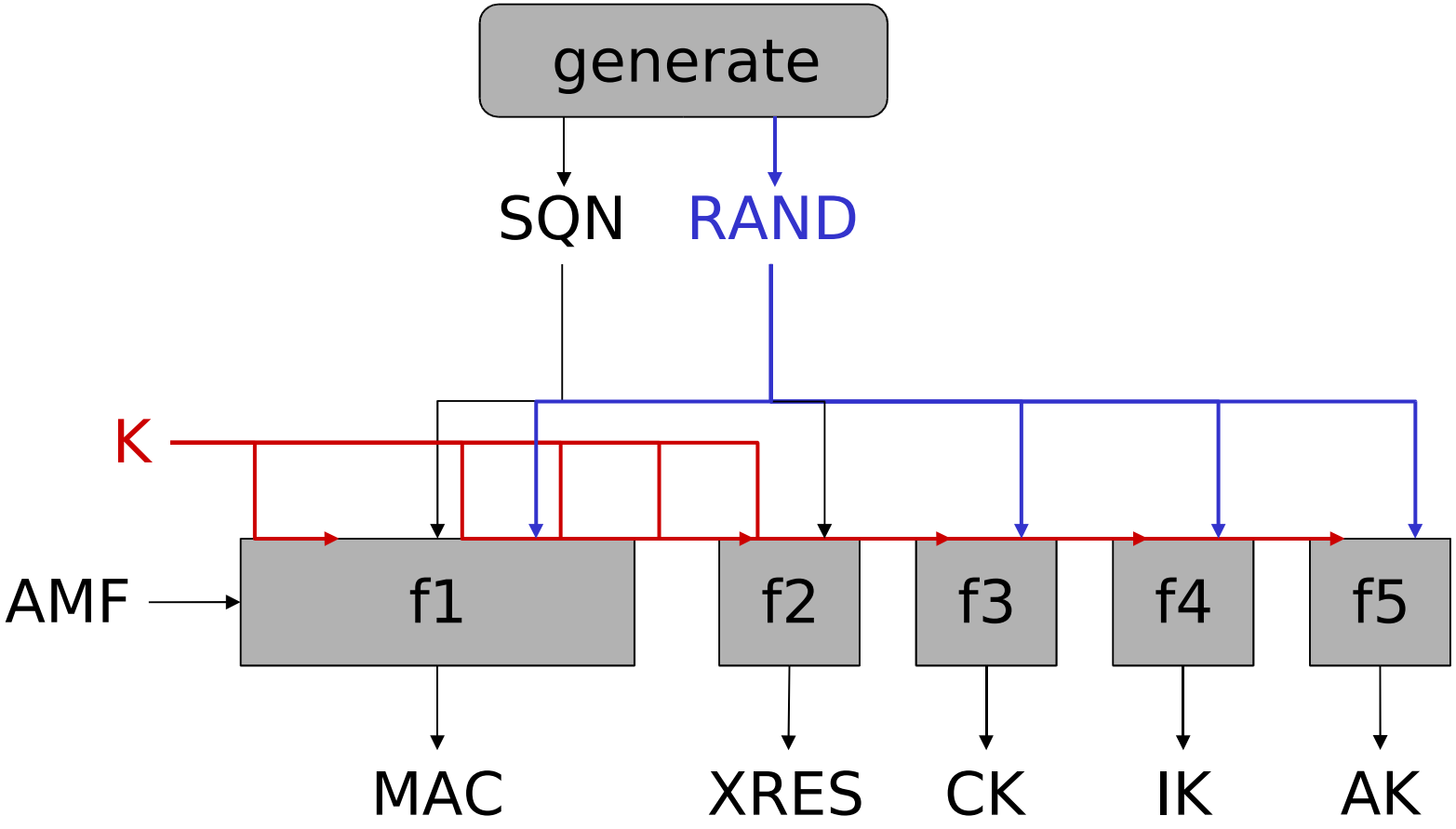
Key agreement on 128-bit cipher key CK and 128-bit integrity key IK.

AMF: Authentication Management Field.

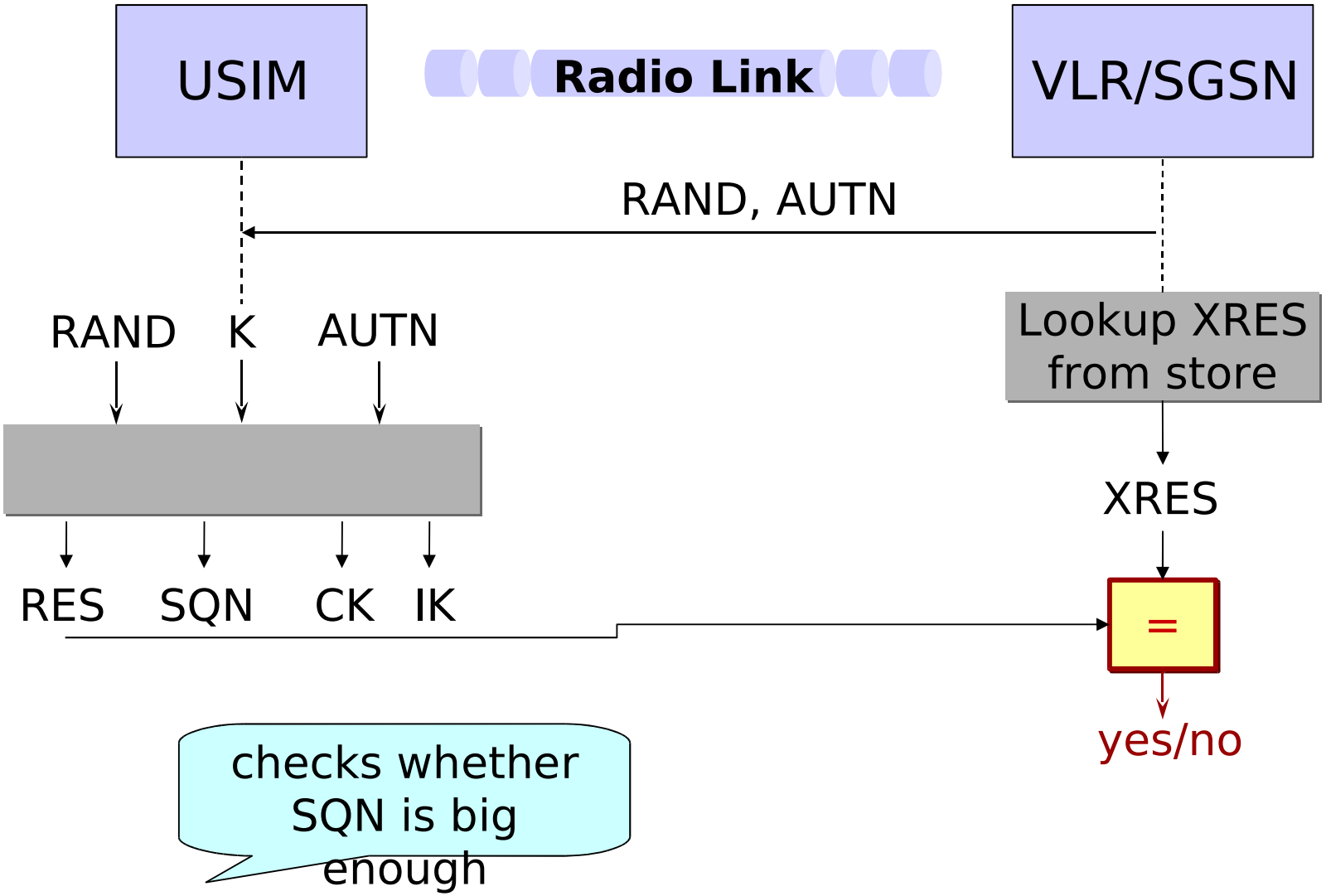
# UMTS AKA: VLR ↔ AuC



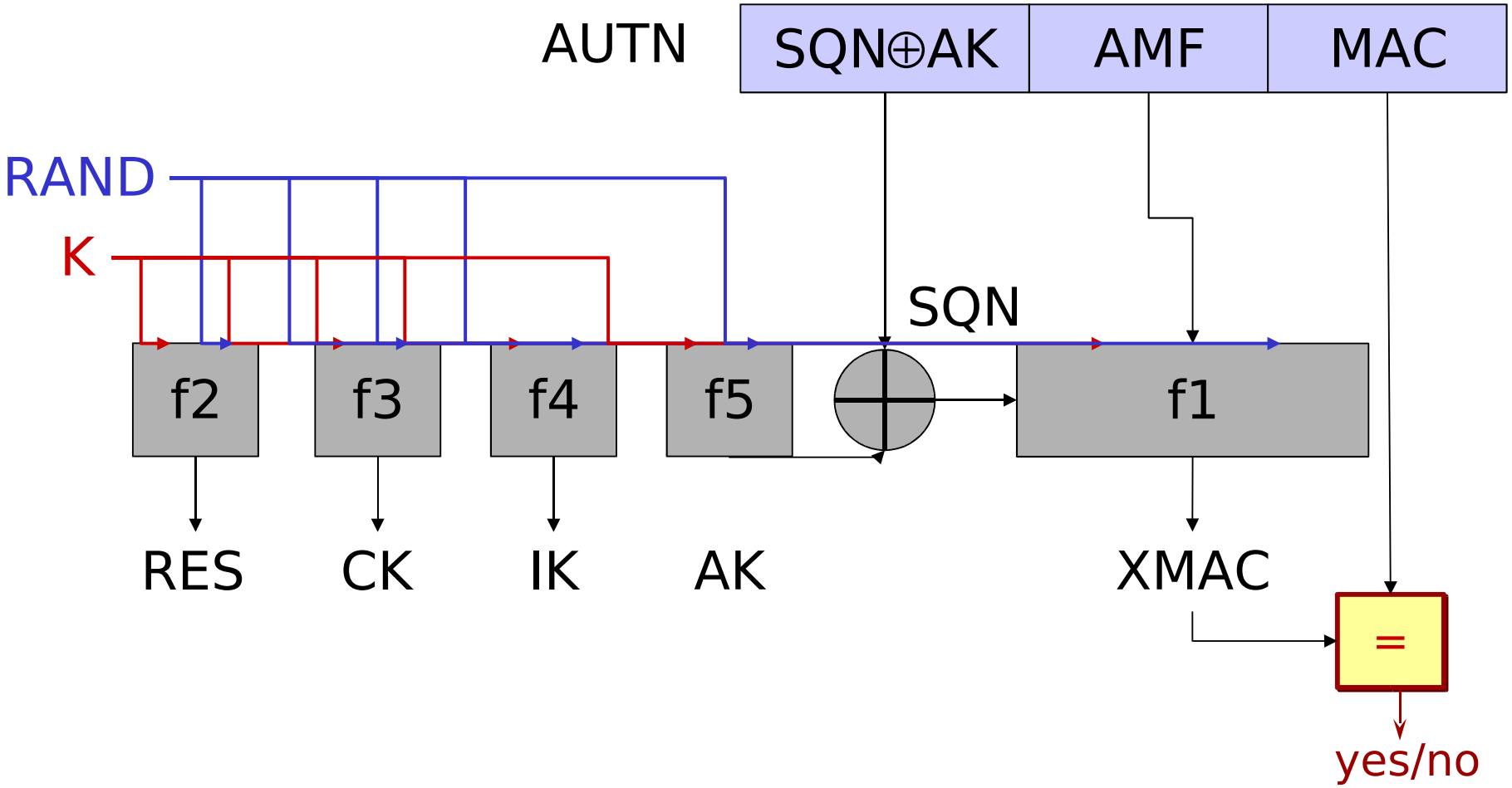
# AV Generation at AuC



# UMTS AKA: USIM ↔ VLR



# 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

# 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

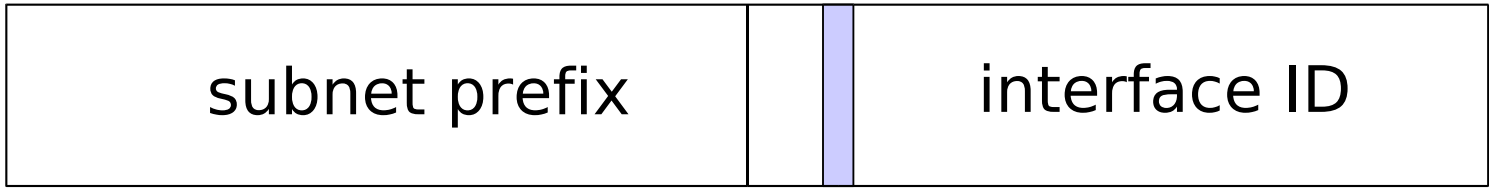
Mobile IPv6 (MIPv6) address (128-bit):

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.

The home address is an 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.

The mobile node performs this binding registration by sending a Binding Update (BU) message to the home agent.

The home agent replies to the mobile node by returning a Binding Acknowledgement.

# MIPv6 – Binding Update

The mobile node and its 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

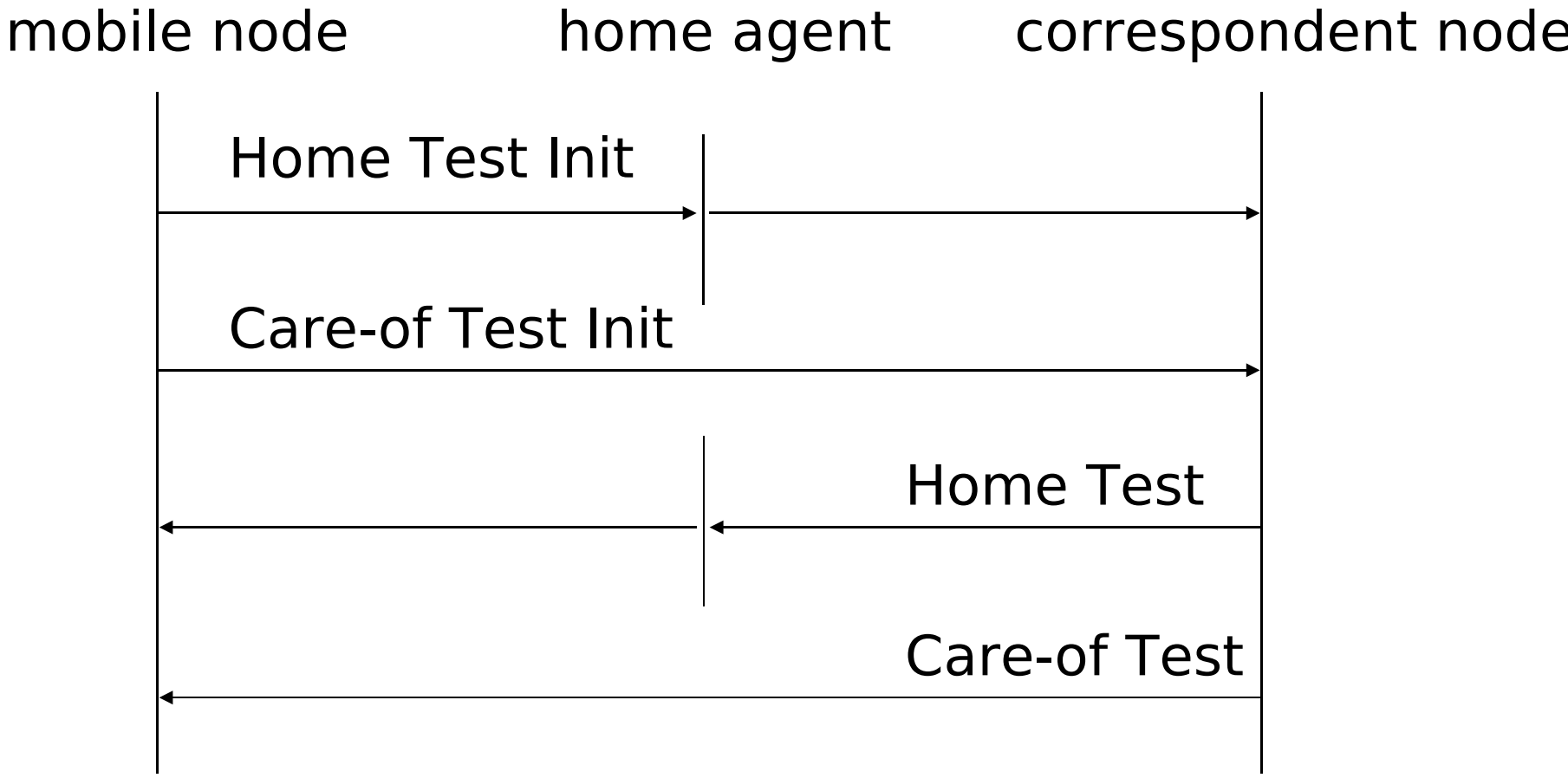
Primary concern: protect nodes that are not involved in the exchange (e.g. nodes in the wired Internet)

Resilience to denial-of-service attacks

Security based on return routability: challenges are sent to identity and location, response binds identity to location.

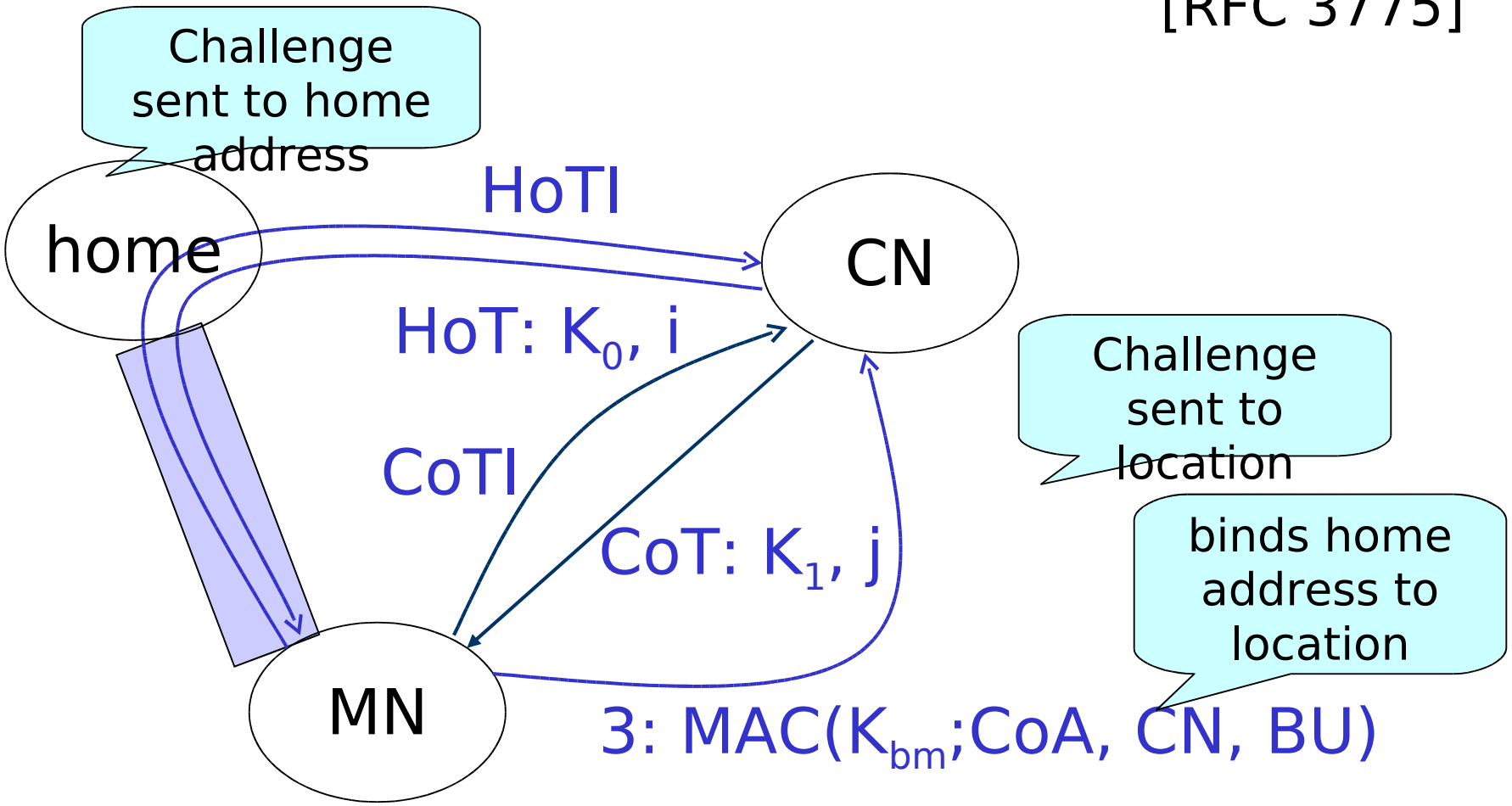
Cryptographic keys are sent in the clear! (You will see why.)

# Return Routability Procedure



# Binding Update Protocol

[RFC 3775]



# BU Protocol

1. The mobile sends two BU messages to the correspondent, one via the home agent, the other on the direct link.
2. The 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. The mobile constructs a binding key $K_{bm} = \text{SHA-1}(K_0, K_1)$ to authenticate the binding update.

# Design Principles – 1

Return routability: Correspondent checks that it receives a confirmation from the advertised location.

The protocol creates a binding between home address (identity?) and current location.

The protocol could be considered as a “location authentication” protocol.

Keys are sent in the clear and could equally be interpreted as nonces.

# Design Principles – 1 (ctd)

The protocol is 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: The 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 the 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 could be viewed as a flow control issue (data is sent to a victim who had not 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: an 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)

The 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.

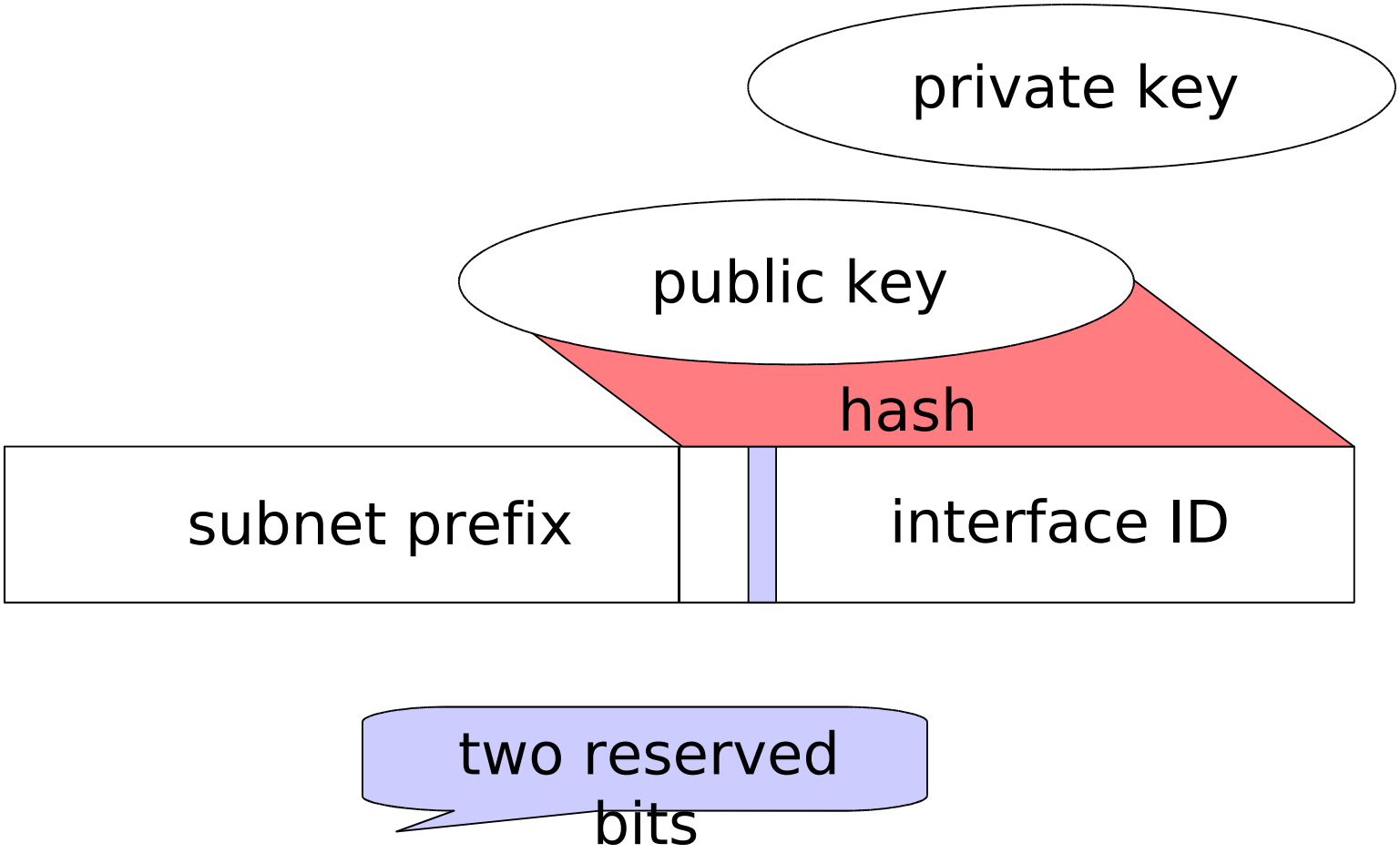
The mobile node can then sign BU information with its private key, and send the signed BU together with its public key to the correspondent.

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.

The 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.

The address owner is now required to do a brute force search to get a *Hash2* value of the required format.

The 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)*

The modifier (random 128-bit number) is 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, the 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).

- An attacker can learn valid MAC addresses by listening to connections from legitimate devices and then connect with a spoofed MAC address.

Do not base access control on information needed by the network to manage connections; typically, this information has to be transmitted when setting up a connection before security mechanisms can be started.

# WEP

Wireless Equivalent Privacy (WEP) protocol specified in IEEE 802.11.

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.

Stream cipher for encryption, with a 24-bit Initialization Vector (IV) to randomize encryption.

Sender and receiver have a shared secret 40-bit or 104-bit key $K$. To transmit a message $m$, the sender computes a 32-bit checksum CRC-32($m$), takes the 24-bit IV, and generates a key stream with the 64-bit (128-bit) key $K' = \mathrm{IV}||K$ using the stream cipher RC4.

# Problems with WEP

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 the checksum.

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 $\Delta$.

Compute $\delta = \text{CRC-32}(\Delta)$ 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 the IV is too small.

Third problem: cryptanalytic attacks on RC4.

# WPA

WiFi Protected Access (WPA) designed as a quick preliminary solution to remove the major flaws of WEP; required to run on existing WLAN hardware.

Improved procedures for authenticating client to network and for establishing temporary encryption keys dynamically: IEEE 802.1X, Extensible Authentication Protocol (EAP) ,

CRC-32 replaced by a message integrity code (MIC) Michael; 48-bit IVs.

Temporal Key Integrity Protocol (TKIP) for creating a key hierarchy.

WPA2: complete redesign of WLAN security mechanisms specified in IEEE 802.11i.

# Bluetooth

Technology for Personal Area Networks: wireless ad-hoc networks, initially envisaged for short range communications between personal devices like a PC, keyboard, mouse, printer, headset, or other peripherals.

Security association between two devices established manually by pairing: user enters a common PIN on both devices.

128-bit link key derived from PIN; authentication uses in a challenge-response protocol similar to GSM.

Bluetooth attacks that exploit flaws in the software configuration of the devices exist (e.g. Bluesnarf) .