Case Study: security in GSM and UMTS

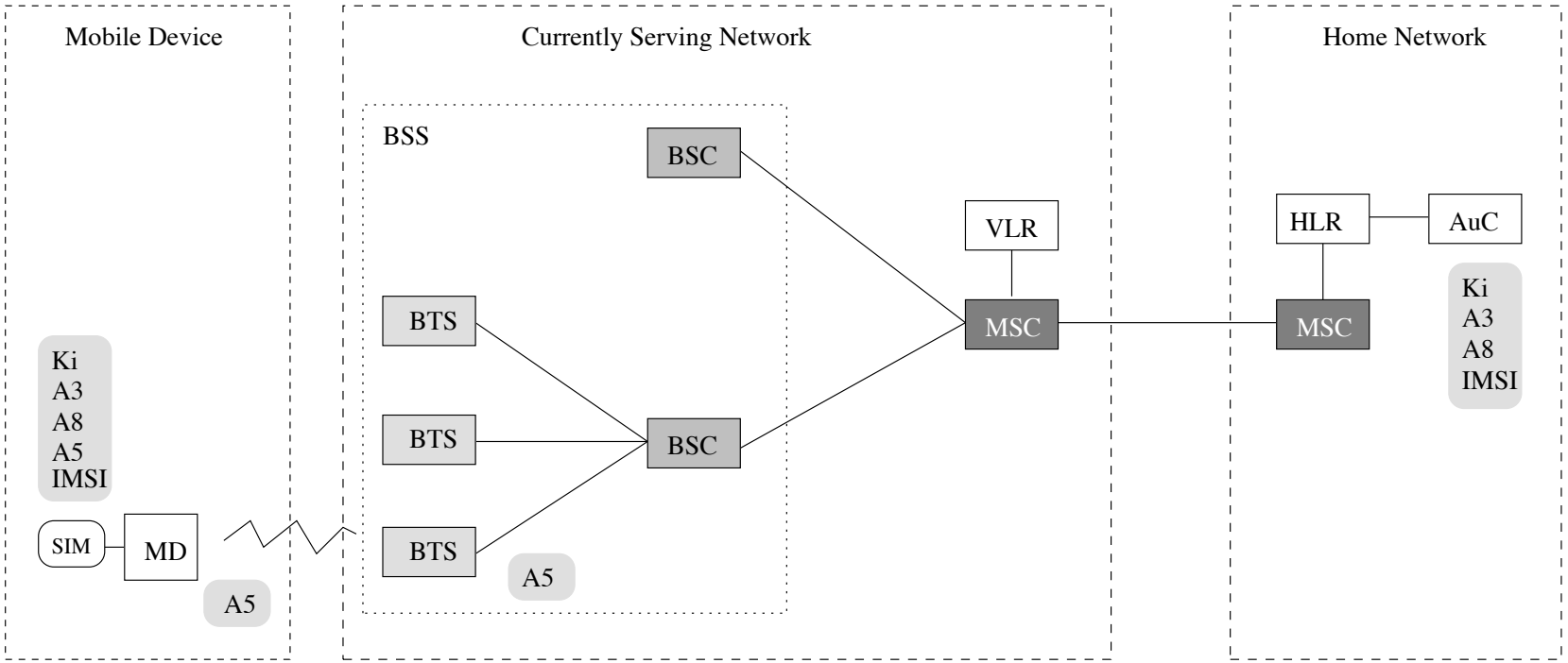
Security in Networked Computing Systems

GSM and UMTS security

GSM

System model

UNIVERSITÀ DI PISA



MD: Mobile Device
BTS: Base Transeiver Station
BSC: Base Station Controler
MSC: Mobile Switching Center
BSS: Base Station System

VLR: Visitor Location Register
HLR: Home Location Register
AuC: Authentication Center
Ki: Secret per subscriber key
IMSI: International Mobile Subscriber Identity

A3: Authentication algorithm
A8: Key generation algorithm
A5: Encryption algorithm
SIM: Subscriber Identity Module

Security model

- What is supported
  - Mobile device authentication
  - Encryption of the air interface between MD and BTS
- What it is NOT supported
  - Network authentication
  - Integrity

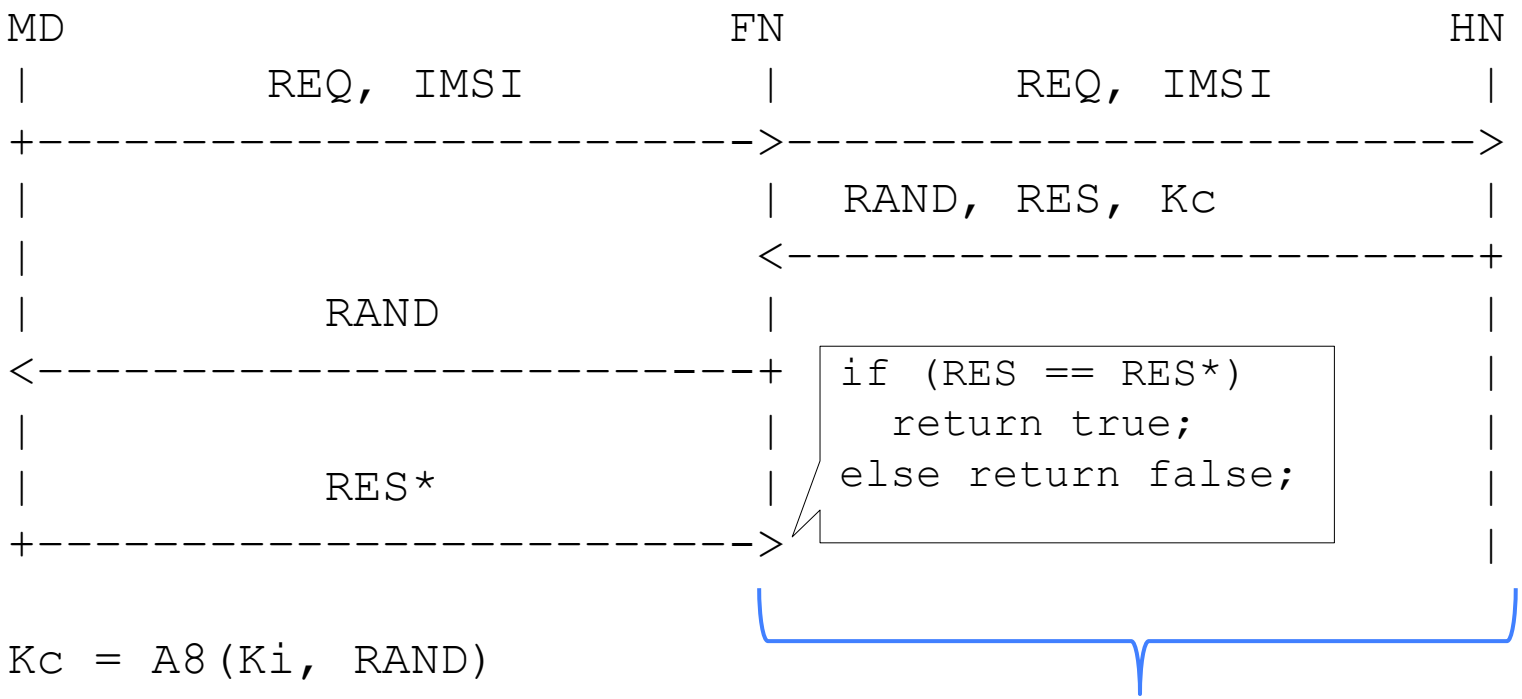
Registration

- Each user (subscriber) registers for a Home Provider (Network)
- HP associates the user with IMSI and Ki (128 bit)
  - IMSI: International Mobile Subscriber Identity
- IMSI and Ki are stored on HN's AuC and SIM
  - SIM: Subscriber Identity Module

Security algorithms

- Authentication and Key agreement
  - A3: Authentication algorithm
  - A8: Key generation algorithm
  - Provider specific
- Encryption algorithms
  - A5/0 (no encr), A5/1 (standard), A5/2 (weaker that A5/1), A5/3 (similar to KASUMI)
  - A5/0, A5/1 and A5/2 are mandatory
  - Standardized, no provider-specific
- Implemented by MD and BTS

GSM authentication: simplified



Kc = A8(Ki, RAND)
RES = A3(Kc, RAND)

HN: Home Network; FN: Foreign Network

Analysis

UNIVERSITÀ DI PISA

$$MD, HN \mid\equiv MD \overset{Ki}{\rightleftharpoons} HN$$ Registration

$$FN \mid\equiv FN \overset{Kc}{\leftrightarrow} MD$$

$$FN \mid\equiv \#(RAND)$$

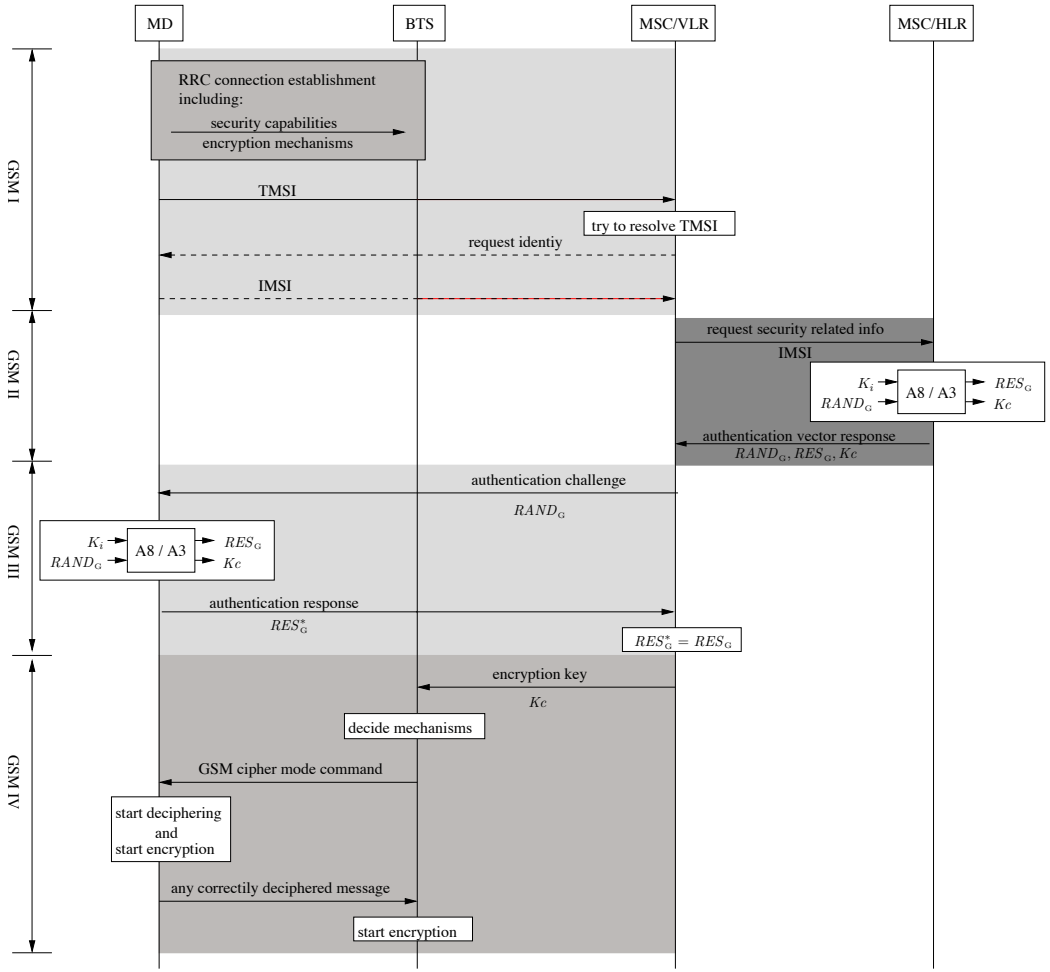
$$FN \mid\equiv \#(FN \overset{Kc}{\leftrightarrow} MD)$$

By virtue of the secure channel between FN and HN

$$FN \mid\equiv MD \mid\equiv (FN \overset{Kc}{\leftrightarrow} MD)$$ Final belief

MN achieves no beliefs

GSM authentication



Negotiation and policies

UNIVERSITÀ DI PISA

- Negotiation
  - MD sends its security (encryption capabilities)
    - FN drops connection if MD does not enforce mandatory algorithms
  - FN chooses one of the encryption algorithms and acknowledges its choice to MD
    - Even A5/0 or A5/2
    - HN has non influence
    - MD cannot enforce the use of A5/1 or A5/3

Anonimity

- In order to protect anonymity, IMSI is sent in the clear over the ai interface as rarely as possible
- Upon first connection FN associates a TIMSI to MD
  - Upon next connection, MD presents its TIMSI to the FN
  - If FN is not able to resolve the TIMSI, it requests MD its IMSI and a new TIMSI is allocated

Intra-provider roaming

- Inter-provider roaming always causes roaming authentication
- This is not the case if MD is in idle-mode and moves within the same network
- Kc is moved to the next BTS or MSC, as needed
- If encryption between MD and BTS was disabled, it is not re-enabled after roaming to the next BTS
- Standard say nothing if the next BTS does not support the A5 alg chosen by the previous one

Impersonation attack

UNIVERSITÀ DI PISA

- **One-dide MiM** An attacker impersonates a fake base station to MD
  - The attacker makes MD to connect to the fake base station
  - The attacker requests MD to turn encryption off
  - The attacker can eavesdrop on all mobile traffic
  - Unless the attacker cannot impersonate MD to a real network as well, MD will be unreachable for incoming traffic
    - The attacker need Kc!

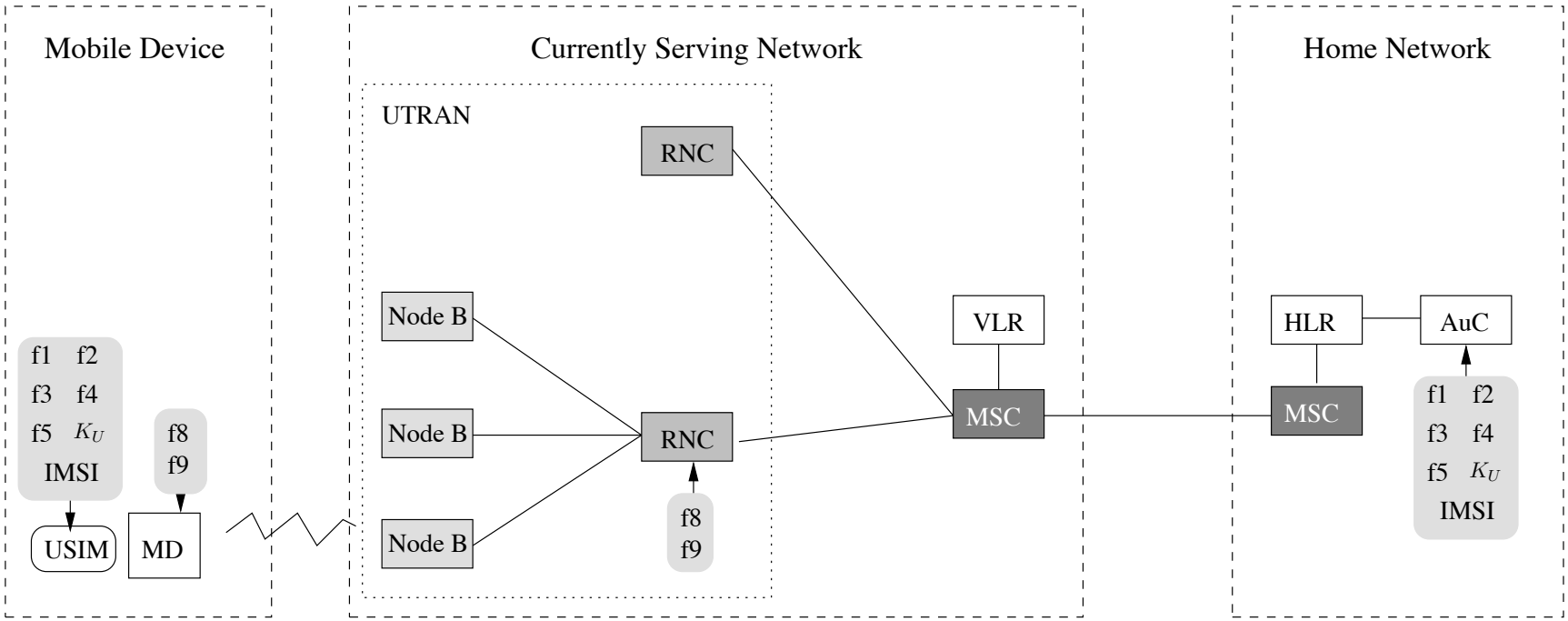
Impersonation attack

- **Two-sided MiM** An attacker can impersonate a MD during authentication by simply forwarding the authentication traffic
  - It's not easy for the adversary to turn encryption off because of mandatory algorithms
- The attacker succeeds if (s)he knows that a network always uses A5/0
  - Actually the attacker can make MD to connect to a network that disables encyption

GSM and UMTS security

UMTS

System model



MD: Mobile Device
Node B: Base Transceiver Station
RNC: Radio Network Controller
VLR: Visitor Location Register
UTRAN: UMTS Terrestrial Radio Access Network

MSC: Mobile Switching Center
HLR: Home Location Register
AuC: Authentication Center

K_U Secret per subscriber key
f1–f5: key generation functions
f8: encryption mechansim
f9: integrity protection mechansim

Security model

- Mobile device and visited network mutual authentication
- Integrity
- Encryption of the air interface between MD and BTS

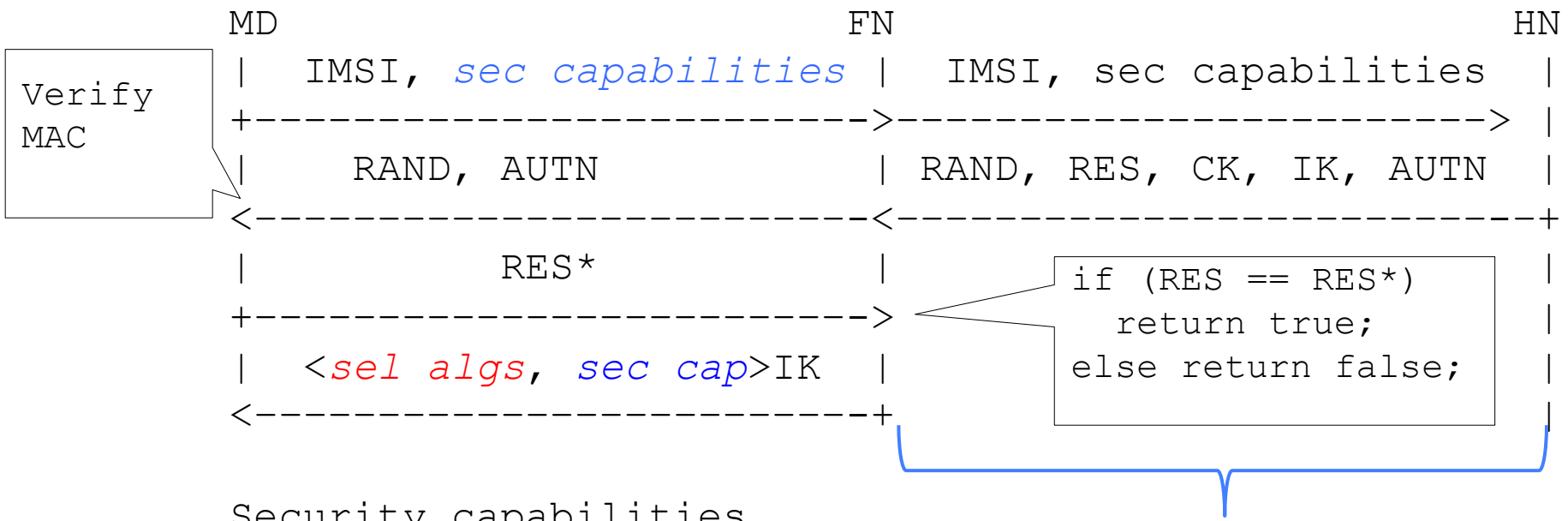
Registration

- Each user (subscriber) registers for a Home Provider (Network)
- HP associates the user with IMSI and Ku (128 bit)
  - IMSI: International Mobile Subscriber Identity
- IMSI and Ki are stored on HN's AuC and SIM
  - USIM: Universal Subscriber Identity Module
  - USIM implements crypto-functions f1, f2, f3, f4, f5 (MILENAGE)
  - These functions are provider-dependent

Confidentiality and integrity

- End-to-end confidentiality and integrity between MD and RNC
  - Encryption and integrity algorithms are implemented on the MD
- No mechanism to restrict Kc lifetime
- Encryption
  - Up to 16 encryption algs
  - Currently UEA0 (no encryption) and UEA1 (stream cipher built on KASUMI)
- Integrity
  - Up to 16 integrity algs
  - Currently UIA0 built on KASUMI

UMTS authentication: simplified



Pre-defined secure channel

Security capabilities
Selected algorithms
RES = f2(Ku, RAND)
CK = f3(Ku, RAND)
IK = f4(Ku, RAND)
AUTN = SQN xor f5(Ku, RAND) || AMF || f1(Ku, SQN||AMF)

AK

MAC

Analysis

UNIVERSITÀ DI PISA

Assumptions

$$MD, HN \mid\equiv MD \overset{Ku}{\rightleftharpoons} HN$$

$$HN \mid\equiv (MD \overset{CK}{\leftrightarrow} HN, MD \overset{IK}{\leftrightarrow} HN)$$

Goals

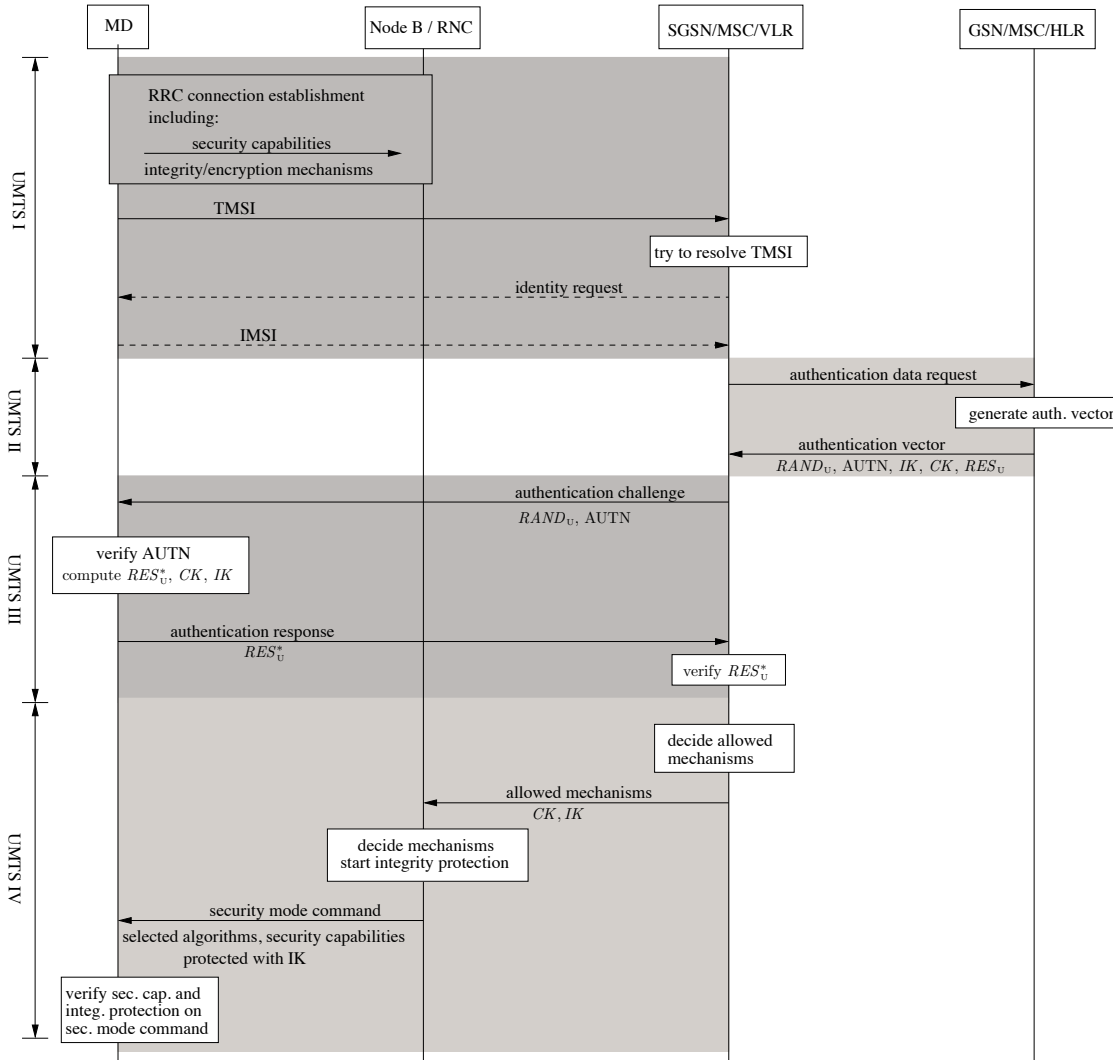
$$FN \mid\equiv MN \mid\equiv (FN \overset{CK}{\leftrightarrow} MD)$$

$$MD \mid\equiv HN \mid\equiv (MD \overset{IK}{\leftrightarrow} HN)$$

Mutual authentication

$$MD \mid\equiv HN \mid\equiv (\text{security capabilities})$$

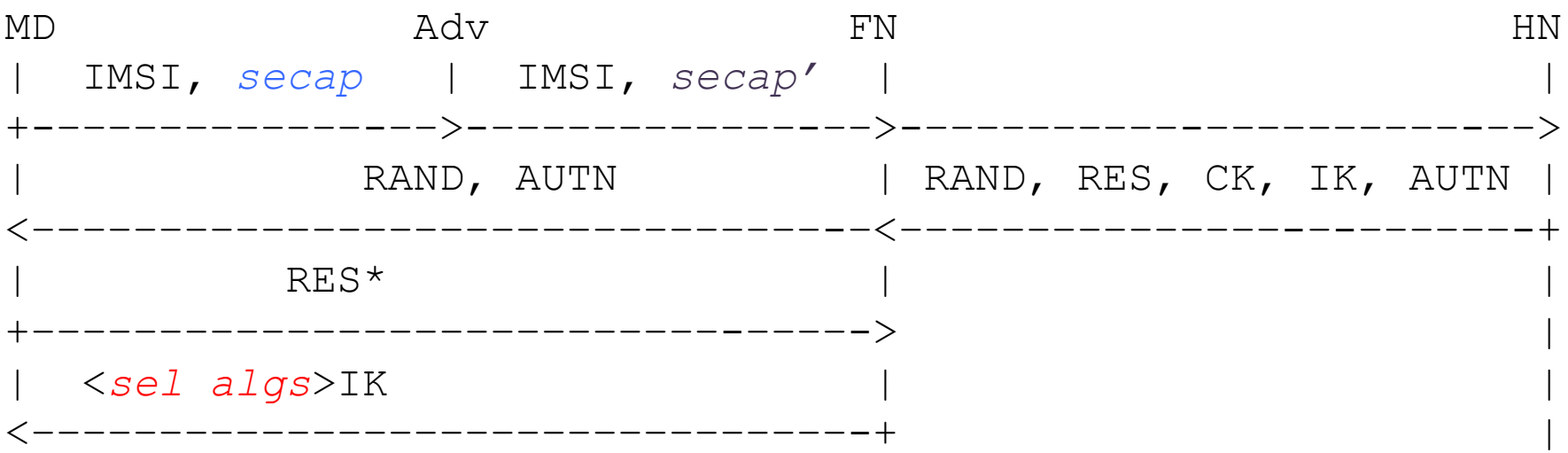
UMTS Authentication



Negotiation and policies

- MD and FN negotiate encryption-/integrity-algs
- After authentication of MD, FN selects a pair of algs
  - MD is mandated to implement *no-encryption* (UEA0)
  - Neither MD nor HN can enforce encryption to be enabled
- UMTS uses the same TIMSI mechanism as GSM
- Intra-provider roaming is similar to GSM

Impersonation attack



By means of ***secap'*** the adversary could claim to support only the mandatory encryption algorithms (security capabilities)