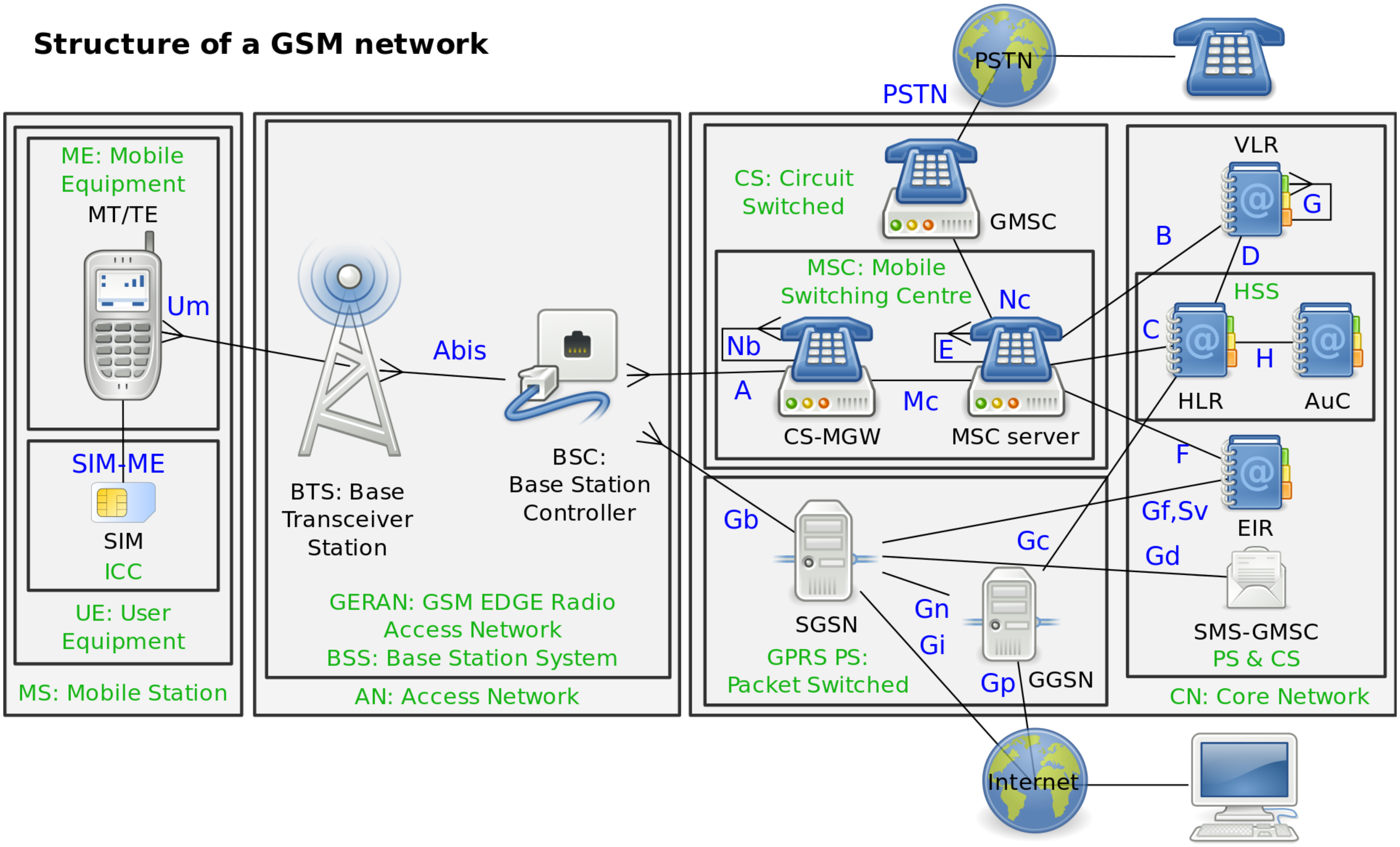
Bezpečnost mobilních sítí (téměř) všech generací

This talk focuses on vulnerabilities that stem from standard itself, not on vulnerabilities introduced by faulty implementation.

2nd Generation: GSM

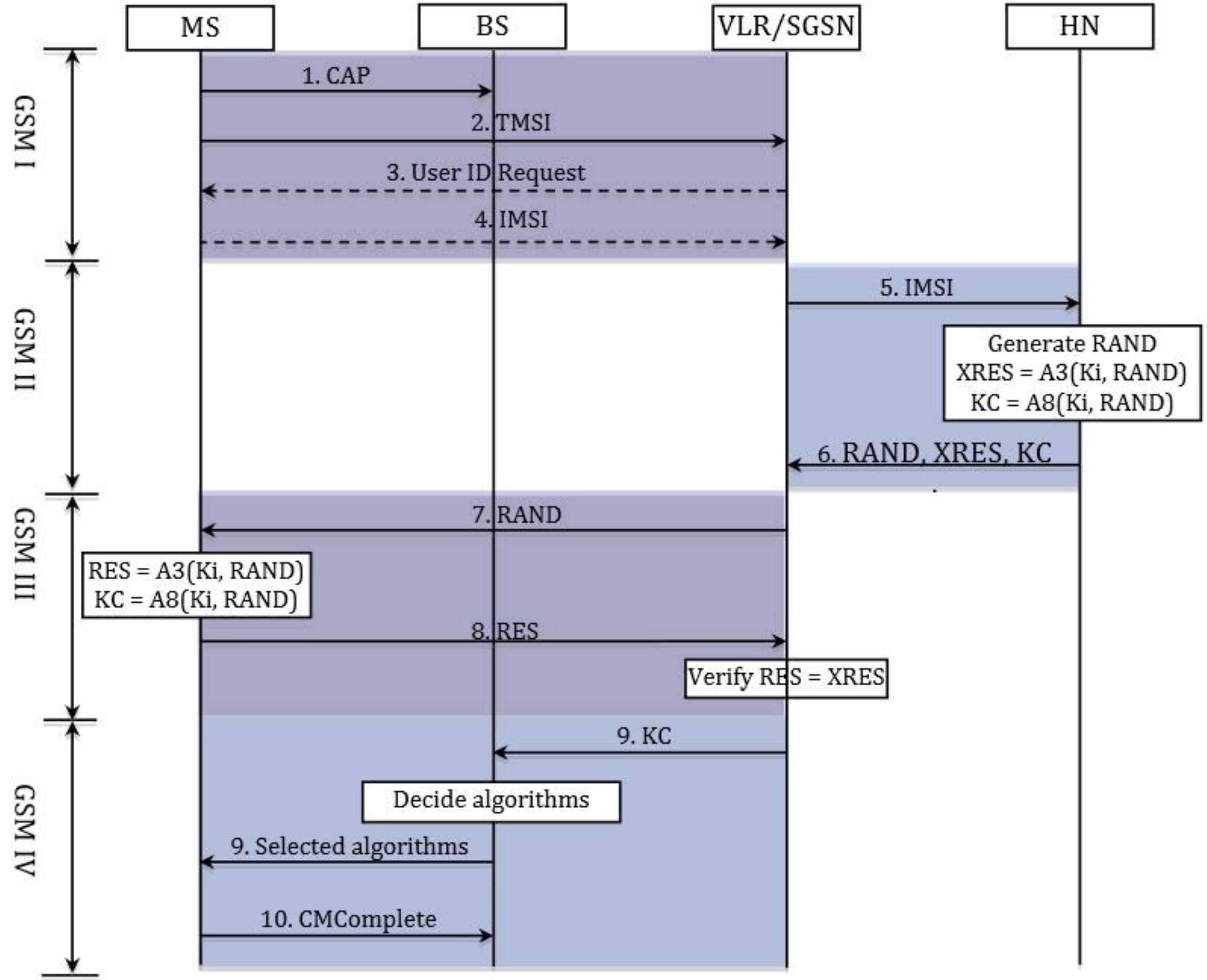
Structure of a GSM network



Source: https://en.wikipedia.org/wiki/GSM

GSM security goals

- Accountability to enable billing
- Confidentiality of user data
- User privacy – not possible to track and locate individual user



- Ki – 128-bit key, pre-shared secret between SIM and Network
- A3 – Authentication function
- A8 – Key derivation function
- A3/8 usually implemented together
  - available in SIM
  - network provider dependent

- Authentication triplet
  - RAND – 128-bit random challenge
  - XRES – 32-bit signed response
  - Kc – 64-bit ciphering key

Source: C. Tang, D.A. Naumann, S. Wetzel, “Analysis of Authentication and Key Establishment in Inter-generational Mobile Telephony”, IEEE HPCC & IEEE EUC 2013

Vulnerabilities and attacks

Weak encryption

- Encryption takes place on air interface between MS and BTS
  - No integrity protection, ECC used before encryption -> dependencies between plaintext bits
- A5/0 - no encryption
  - Banned by most networks today -> still lot of content not encrypted at all
- A5/1 - 64-bit stream cipher, LSFR based
  - Primary encryption algorithm of GSM
  - Broken using TMTO attacks, revealing key in seconds (open source tools available – see Kraken and Deka)
  - Known-plaintext attack, predictable plaintext available
  - Ciphertext-only possible, but not necessary

Weak encryption cont.

- A5/2 – intentionally weakened variant of A5/1
  - Intended for export, used mostly outside western countries
  - Now deprecated and not implemented in modern phones
  - Broken using Linear cryptanalysis, revealing key in milliseconds
  - Ciphertext-only attack
- A5/3 – stream cipher based on KASUMI block cipher, 64-bit block, 64-bit key
  - Transition to A5/3 from A5/1 in recent years
  - 64-bit key, revealing keys in days
- A5/4 – added later, similar to A5/3 but requires 128-bit key
  - Not used in the wild
- Packet domain uses different set of algorithms

Passive attacks

- Off-air interception
  - Passive interception using dedicated radios or SDRs
  - Breaking weak encryption algorithms
- Infrastructure interception
  - Encryption takes place on Air interface between phone and BTS
  - Traffic beyond BTS used to be unprotected
  - Tapping backhaul links

Weak key derivation

- A3/8 – Key derivation and authentication function
- Standardized interface, implementation may be proprietary
- Example function COMP-128 adopted by most network operators
- Fully leaked in 1998
  - Butterfly structure of compression function
  - Multiple attacks that reveal Ki and enable SIM cloning appeared, narrow-pipe
- 10 rightmost bits are zeroed, which yields keys with only 54-bits of entropy
  - Passive attacks and encryption breaking even easier

- COMP-128v2 introduced – still only 54-bits
- COMP-128v3 – same as v2 but with full 64-bit length

Attacks on COMP-128v1

- 1998 – Goldberg, Wagner, ”GSM Cloning”, http://www.isaac.cs.berkeley.edu/isaac/gsm.html
  - 6 hours to clone SIM
- 2002 – Rao, Rohatgi, Scherzer, Tinguely, ”Partitioning Attacks: Or How to Rapidly Clone Some GSM Cards”, S&P 2002
  - Side-channel attack, 8 chosen queries
- 2004 – Hulton, David, ”Smart Card Security”, DEFCON 2004
  - 15 minutes to clone SIM

As of now, problem fixed by most of network operators

- Use of proprietary algorithms or new GSM-MILENAGE set of algorithms
- 3G and 4G has own set of algorithms that are secure

Missing integrity protection

- No integrity protection of messages
- Everybody can modify messages that are sent in plaintext

- Mobile phone declares its classmark – set of supported algorithms
- Network selects suitable algorithm from this set
- Attacker can present weak options such as A5/0 or A5/2 on behalf of its victim

Missing authentication of network side

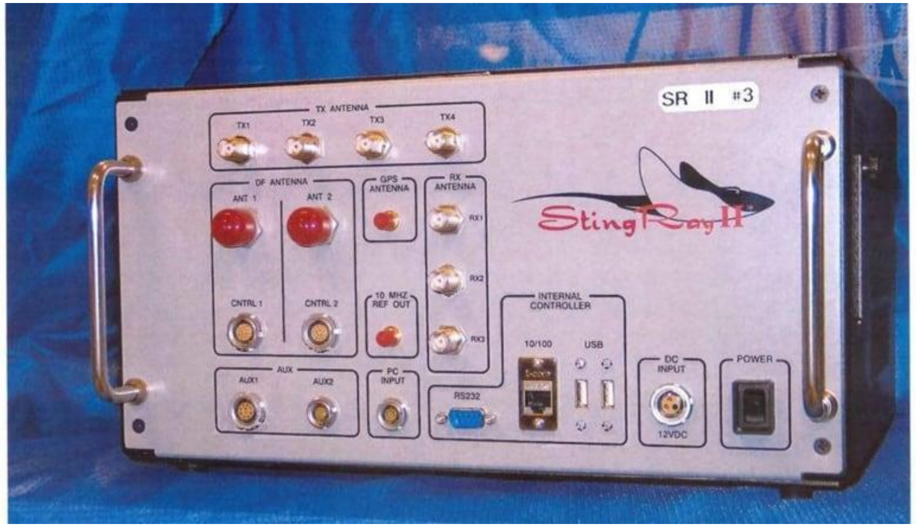
- Phone selects and connects to a BTS with most suitable parameters – signal strength, cell capacity, Cell Reselection Offset, …
- There is no guarantee that the selected BTS is a genuine one
- Originally it was not assumed that an attacker could have technical possibilities to create a fake BTS or fake phone

- Today, anybody with $20 SDR and a laptop can create his own BTS!

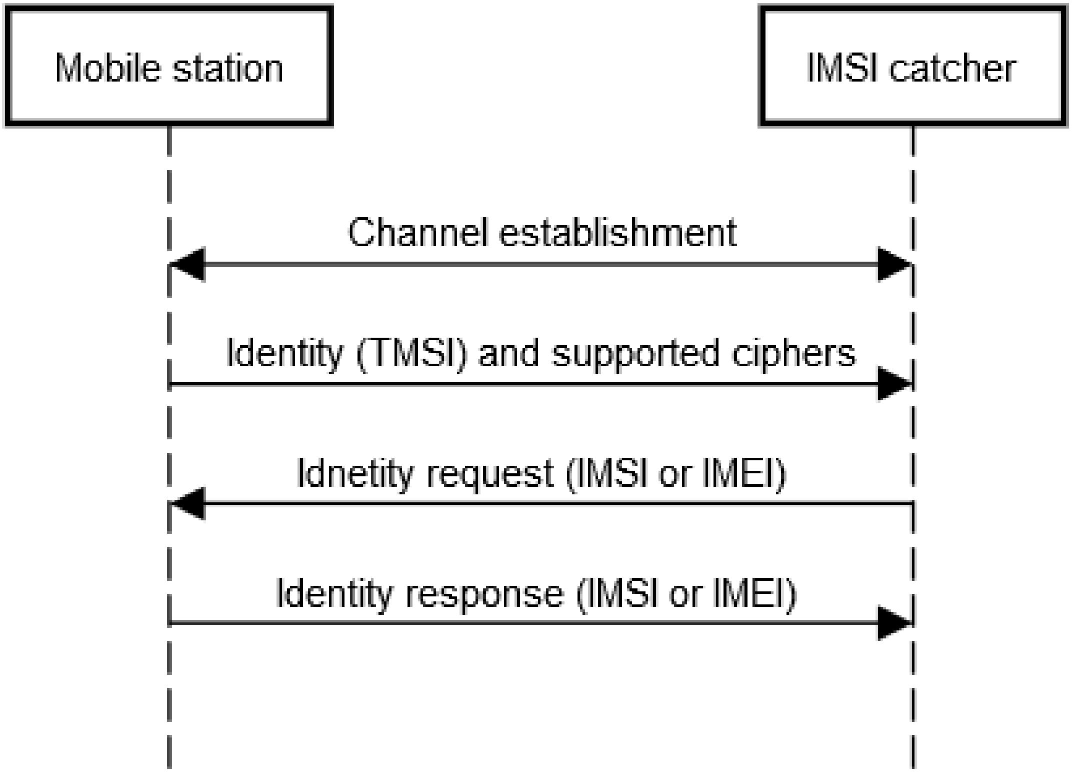
- Attacker can create a fake BTS and achieve a position between a phone and a network
- Large set of Man-In-The-Middle attacks is possible!

Active attacks – IMSI catcher

- aka Stingray, aka Cell Site Simulator, aka Agata, …
- Collection of identities



Source: https://www.cbc.ca/news/technology/imsi-catcher-stingray-device-use-report-1.3760675



Mobile station

IMSI catcher

Channel establishment

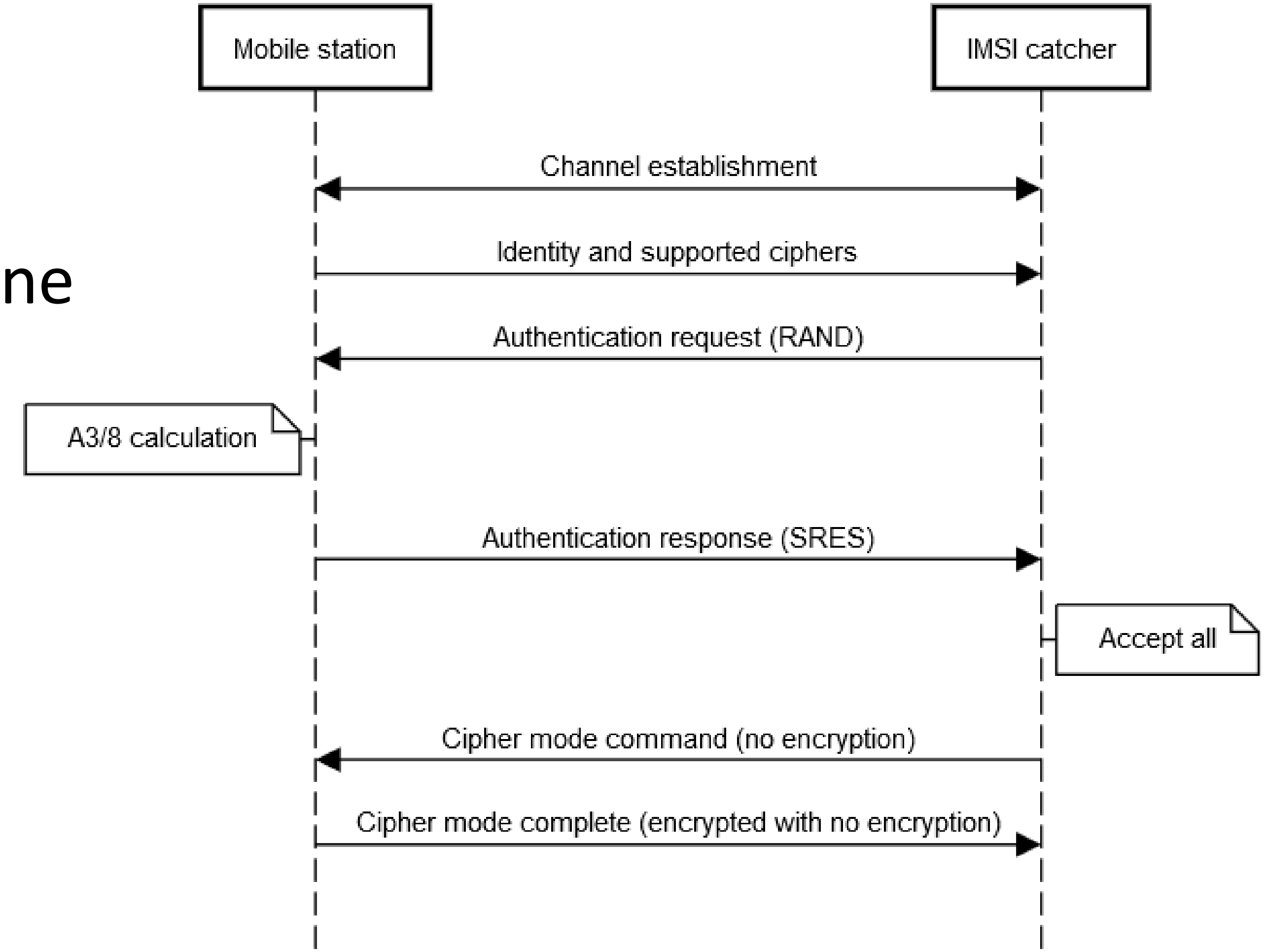
Identity (TMSI) and supported ciphers

Idnetity request (IMSI or IMEI)

Identity response (IMSI or IMEI)

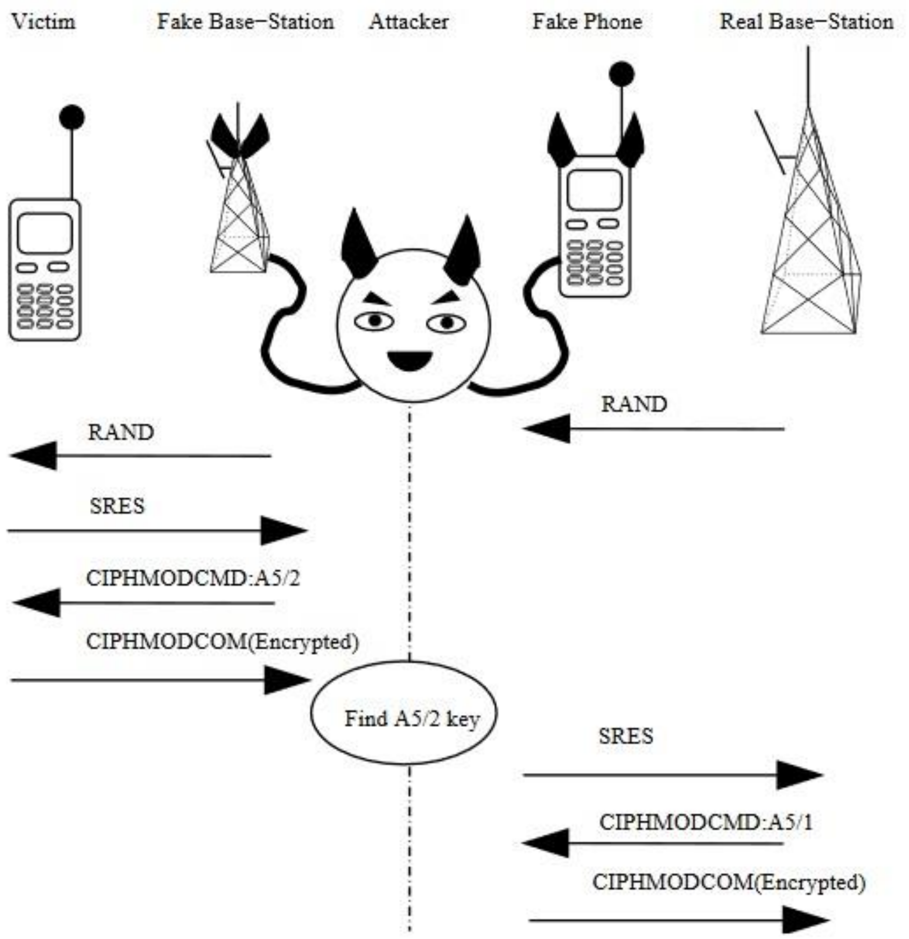
Active attacks – IMSI catcher cont.

- Encryption can be turned off or weakened
- IMSI catcher controls a victim phone

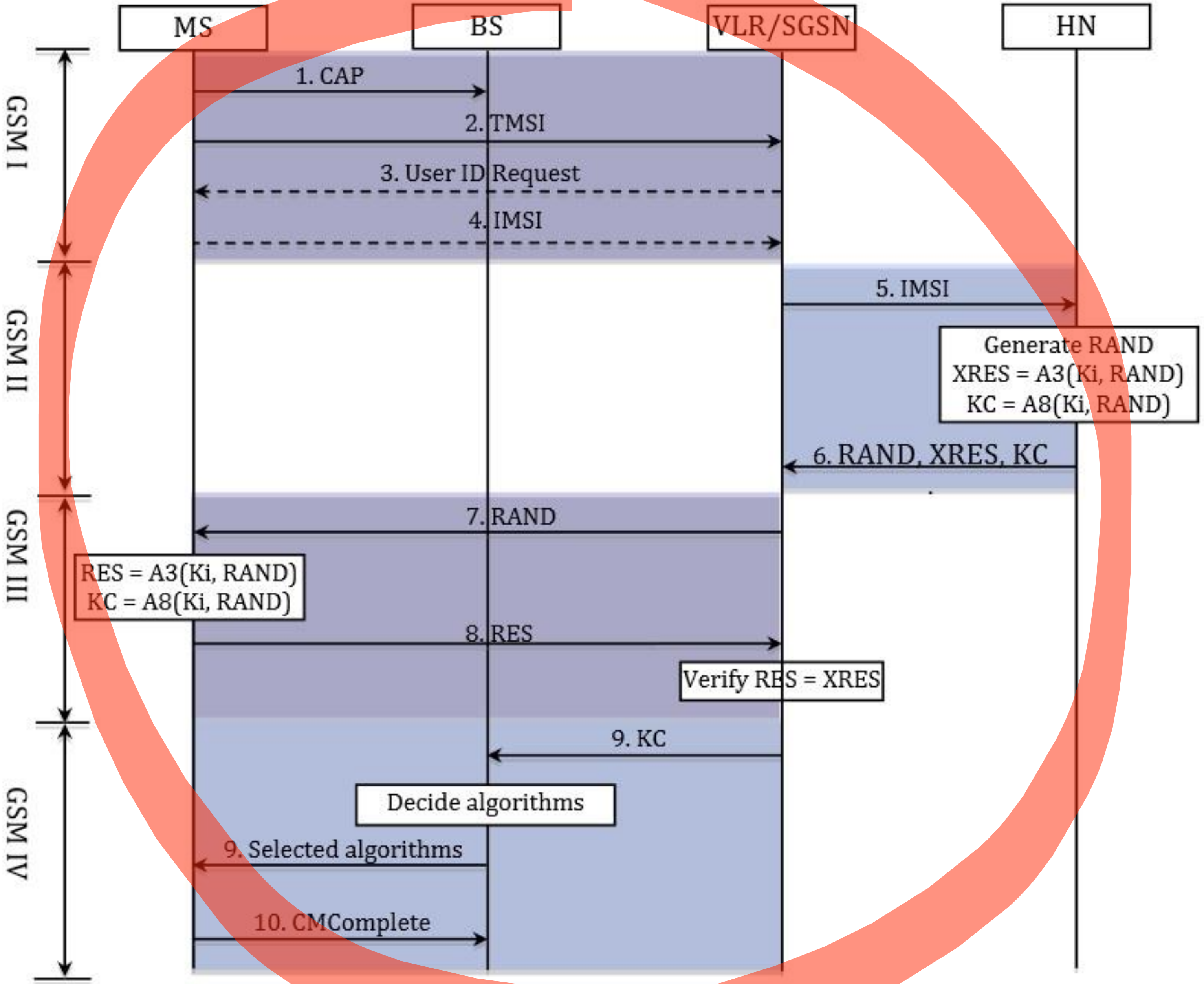

Mobile station
IMSI catcher
Channel establishment
Identity and supported ciphers
Authentication request (RAND)
A3/8 calculation
Authentication response (SRES)
Accept all
Cipher mode command (no encryption)
Cipher mode complete (encrypted with no encryption)

Active attacks – IMSI catcher – MITM attack

- Key not bound to cipher, can be used in different contexts
- MITM attack practically doable also by breaking A5/1



Source: Barkan, Biham, Keller, "Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication", Technion - Computer Science Department - Technical Report CS-2006-07 - 2006



- Ki – 128-bit key, pre-shared secret between SIM and Network
- A3 – Authentication function
- A8 – Key derivation function
- A3/8 usually implemented together
  - available in SIM
  - network provider dependent

- Authentication triplet
  - RAND – 128-bit random challenge
  - XRES – 32-bit signed response
  - Kc – 64-bit ciphering key

Source: C. Tang, D.A. Naumann, S. Wetzel, "Analysis of Authentication and Key Establishment in Inter-generational Mobile Telephony", IEEE HPCC & IEEE EUC 2013

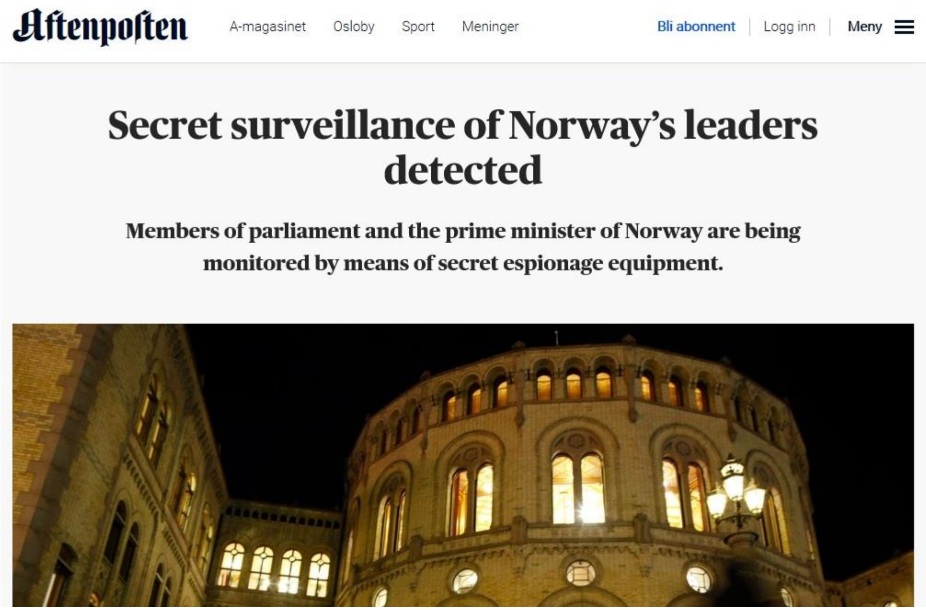
IMSI catcher capabilities

- Collection of identities and tracking of victims
- Interception and manipulation of calls and SMSs
- Making fake calls to and on behalf a victim phone

Security goals
❌ Accountability to enable billing
❌ Confidentiality of user data
❌ User privacy – not possible to track and locate individual user

Detection of IMSI catchers

- IMSI catchers are out there



Secret surveillance of Norway's leaders detected

Members of parliament and the prime minister of Norway are being monitored by means of secret espionage equipment.

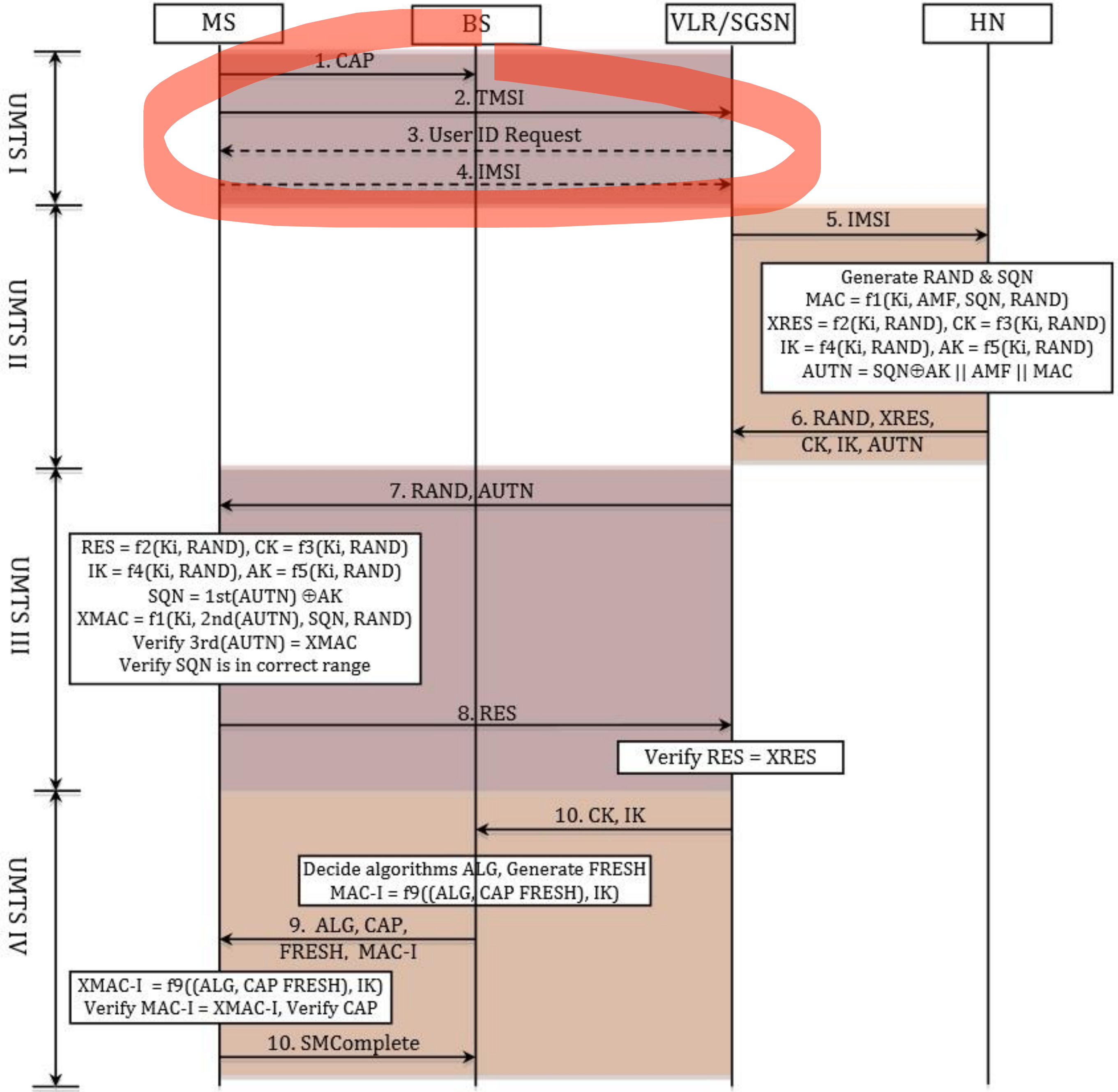
https://www.aftenposten.no

- Many commercial and open source solutions available to detect them
- Focusing on several indicators (high CRO, suspicious LAC, identity req., …)
- Problem of false positives and limited data to analyze
- Snoop Snitch by SRLabs
  - https://opensource.srlabs.de/projects/snoopsnitch

3rd Generation: UMTS

Changes

- SIM becomes USIM
  - New algorithms introduced (MILENAGE set), but old remained
- New encryption algorithms (KASUMI based, SNOW 3G)
- Increased key lengths – 128-bits
- Added authentication of network
- Added integrity protection of signaling messages



MS

BS

VLR/SGSN

HN

UMTS I

1. CAP

2. TMSI

3. User ID Request

4. IMSI

UMTS II

5. IMSI

Generate RAND & SQN
MAC = f1(Ki, AMF, SQN, RAND)
XRES = f2(Ki, RAND), CK = f3(Ki, RAND)
IK = f4(Ki, RAND), AK = f5(Ki, RAND)
AUTN = SQN⊕AK || AMF || MAC

6. RAND, XRES,
CK, IK, AUTN

UMTS III

7. RAND, AUTN

RES = f2(Ki, RAND), CK = f3(Ki, RAND)
IK = f4(Ki, RAND), AK = f5(Ki, RAND)
SQN = 1st(AUTN) ⊕AK
XMAC = f1(Ki, 2nd(AUTN), SQN, RAND)
Verify 3rd(AUTN) = XMAC
Verify SQN is in correct range

8. RES

Verify RES = XRES

UMTS IV

10. CK, IK

Decide algorithms ALG, Generate FRESH
MAC-I = f9((ALG, CAP FRESH), IK)

9. ALG, CAP,
FRESH, MAC-I

XMAC-I = f9((ALG, CAP FRESH), IK)
Verify MAC-I = XMAC-I, Verify CAP

10. SMComplete

Source: C. Tang, D.A. Naumann, S. Wetzel, “Analysis of Authentication and Key Establishment in Inter-generational Mobile Telephony”, IEEE HPCC & IEEE EUC 2013

Vulnerabilities and attacks

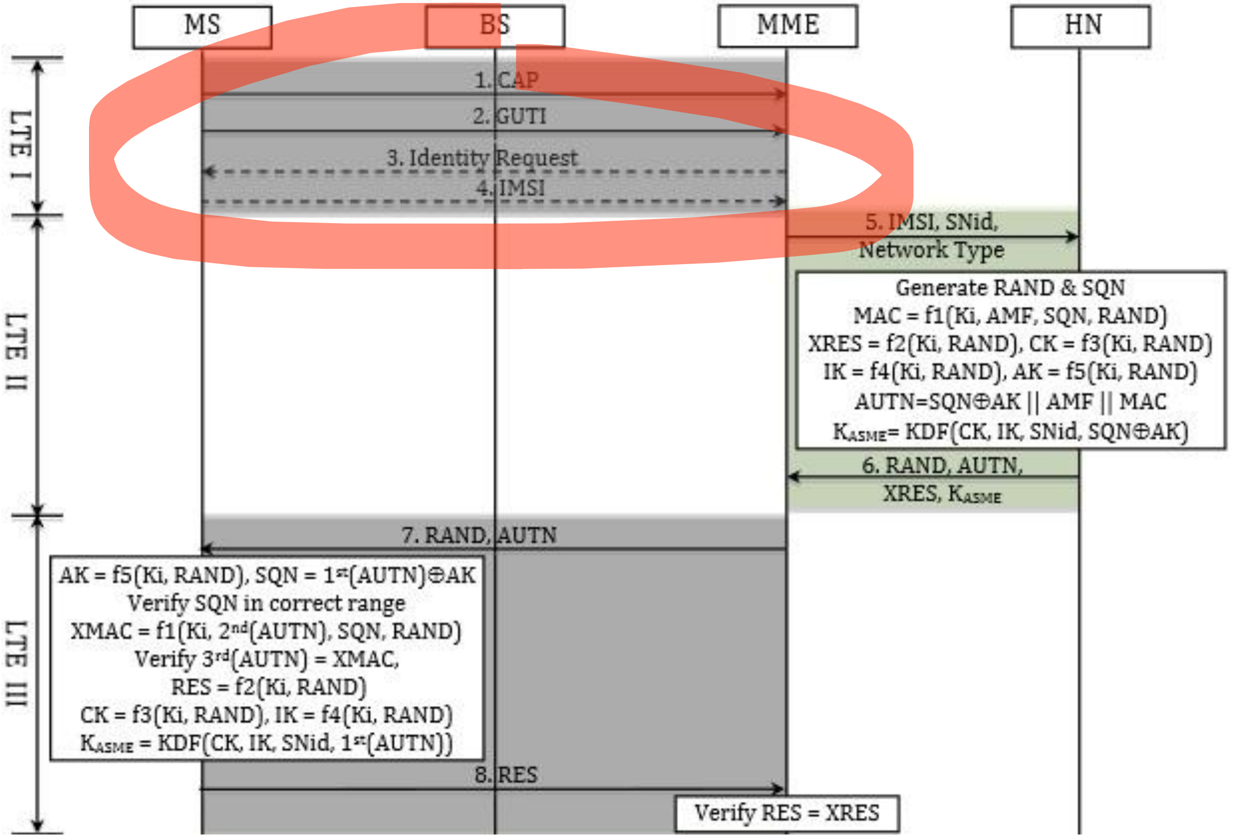
- Lot of commands available prior to AKA handshake
- Collection of IMSI and IMEI still possible
    - IMSI catcher can still ask for identities
- Extraction of GPS coordinates
    - RRLP protocol
- Downgrading to 2G
    - Jamming 3G signal
        - Phone roams to 2G BTS
    - Fake 3G BTS can redirect the victim phone to 2G BTS
        - Routing Area Update Reject, …
    - Once on the 2G, all the 2G attacks are possible

4rd Generation: LTE

Changes

- Access stratum protection (was in 2G and 3G)
  - Protects signaling and user data exchanged between phone and eNodeB (4G name for BTS)
- Introduced Non-access stratum protection
  - Provides integrity and confidentiality of signaling between phone and MME
- DIAMETER protocol replaces SS7 in the core network
- New encryption algorithms (but some algs from 3G remained)

LTE Authentication and Key Agreement



1. CAP

2. GUTI

3. Identity Request

4. IMSI

5. IMSI, SNid, Network Type

Generate RAND & SQN
MAC = f1(Ki, AMF, SQN, RAND)
XRES = f2(Ki, RAND), CK = f3(Ki, RAND)
IK = f4(Ki, RAND), AK = f5(Ki, RAND)
AUTN=SQN⊕AK || AMF || MAC
K_{ASME}= KDF(CK, IK, SNid, SQN⊕AK)

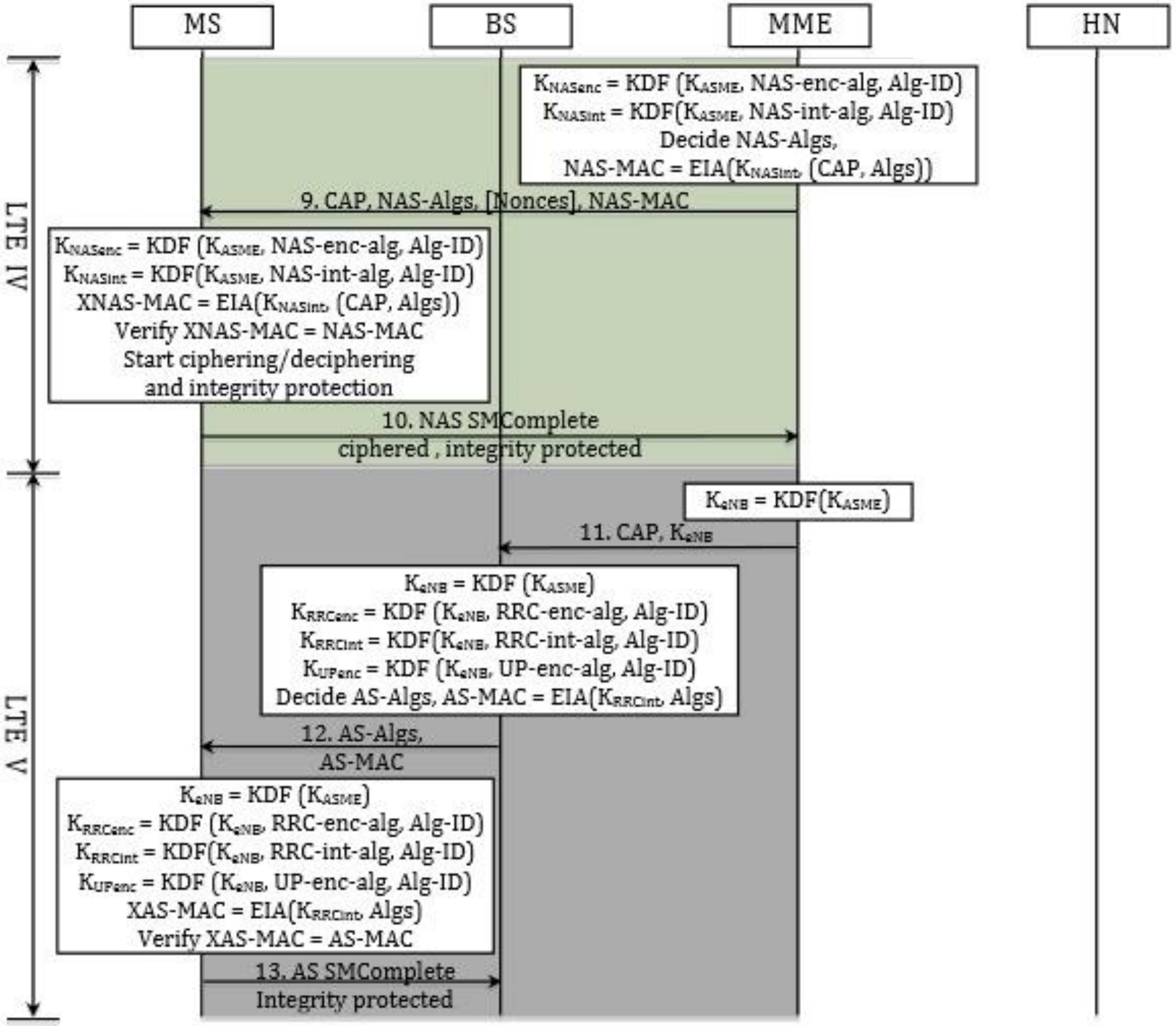
6. RAND, AUTN, XRES, K_{ASME}

7. RAND, AUTN

AK = f5(Ki, RAND), SQN = 1st(AUTN)⊕AK
Verify SQN in correct range
XMAC = f1(Ki, 2nd(AUTN), SQN, RAND)
Verify 3rd(AUTN) = XMAC,
RES = f2(Ki, RAND)
CK = f3(Ki, RAND), IK = f4(Ki, RAND)
K_{ASME} = KDF(CK, IK, SNid, 1st(AUTN))

8. RES

Verify RES = XRES



K_{NASenc} = KDF (K_{ASME}, NAS-enc-alg, Alg-ID)
K_{NASint} = KDF(K_{ASME}, NAS-int-alg, Alg-ID)
Decide NAS-Algs,
NAS-MAC = EIA(K_{NASint}, (CAP, Algs))

9. CAP, NAS-Algs, [Nonces], NAS-MAC

K_{NASenc} = KDF (K_{ASME}, NAS-enc-alg, Alg-ID)
K_{NASint} = KDF(K_{ASME}, NAS-int-alg, Alg-ID)
XNAS-MAC = EIA(K_{NASint}, (CAP, Algs))
Verify XNAS-MAC = NAS-MAC
Start ciphering/deciphering
and integrity protection

10. NAS SMComplete
ciphered , integrity protected

K_{eNB} = KDF(K_{ASME})

11. CAP, K_{eNB}

K_{eNB} = KDF (K_{ASME})
K_{RRCenc} = KDF (K_{eNB}, RRC-enc-alg, Alg-ID)
K_{RRCint} = KDF(K_{eNB}, RRC-int-alg, Alg-ID)
K_{UPenc} = KDF (K_{eNB}, UP-enc-alg, Alg-ID)
Decide AS-Algs, AS-MAC = EIA(K_{RRCint}, Algs)

12. AS-Algs,
AS-MAC

K_{eNB} = KDF (K_{ASME})
K_{RRCenc} = KDF (K_{eNB}, RRC-enc-alg, Alg-ID)
K_{RRCint} = KDF(K_{eNB}, RRC-int-alg, Alg-ID)
K_{UPenc} = KDF (K_{eNB}, UP-enc-alg, Alg-ID)
XAS-MAC = EIA(K_{RRCint}, Algs)
Verify XAS-MAC = AS-MAC

13. AS SMComplete
Integrity protected

Source: C. Tang, D.A. Naumann, S. Wetzel, “Analysis of Authentication and Key Establishment in Inter-generational Mobile Telephony”, IEEE HPCC & IEEE EUC 2013

Vulnerabilities and attacks

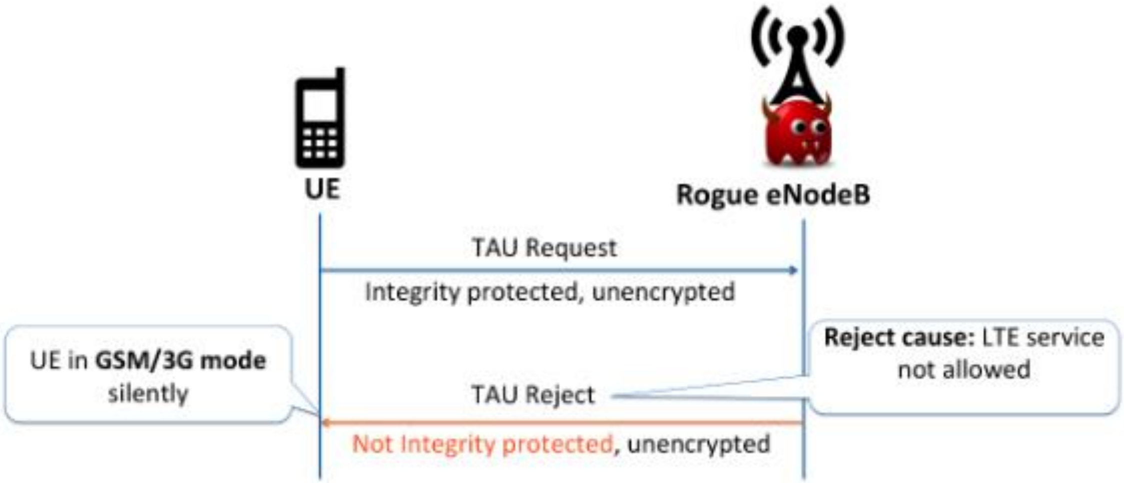
- Similarly to 3G lot of commands available prior to AKA handshake
- Collection of IMSI still possible
  - IMSI catcher can ask for IMSI not IMEI
  - IMEI possible to extract due to implementation bug in certain baseband chips

- Extraction of GPS coordinates
  - RRC Connection Reconfiguration specifying 3 or more neighboring cells
  - Phone responses with Measurement Report indicating received signal strength for the cells
    - New phones may include also GPS coordinates

Source: R. Borgaonkar, A. Shaik, N. Asokan, V. Niemi, J.-P. Seifert: LTE and IMSI catcher myths, BlackHat EU, 2015

Vulnerabilities and attacks

- Downgrading to 2/3G
  - Jamming 4G signal
    - Phone roams to 3G or 2G BTS
  - Fake 4G BTS can redirect the victim phone to lower technology
    - Tracking Area Update Reject, …
  - Once on the 2G, all the 2G attacks are possible


UE
Rogue eNodeB
TAU Request
Integrity protected, unencrypted
Reject cause: LTE service not allowed
UE in GSM/3G mode silently
TAU Reject
Not Integrity protected, unencrypted

Source: A. Shaik, R. Borgaonkar, N. Asokan, V. Niemi, J.-P. Seifert, “Practical attacks against privacy and availability in 4G/LTE mobile communication systems”, NDSS Symposium 2015

Passive attack on Data Link Layer

- Communication on data link layer is encrypted, but communication pattern still visible – when and how often data are transmitted
- Fingerprinting of popular websites traffic pattern and correlation against observed traffic possible
- 50 most popular websites fingerprinted
  - 89% +-10 success rate
- https://alter-attack.net/

Source: D. Rupprecht, K. Kohls, T. Holz, Ch. Pöpper, “Breaking LTE on Layer Two”, S&P 2019

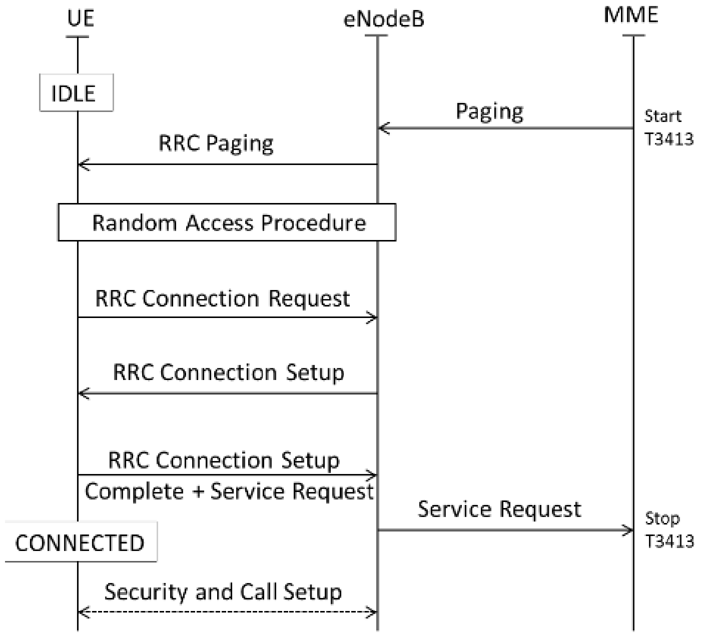
Active attack on Data Link Layer

- Mutual authentication happens on the layers above DLL
- Attacker can establish a relay between phone and network and forward higher layer messages
- Only signaling traffic is integrity protected
  - User traffic only encrypted using cipher in counter mode
- Knowing the plaintext, attacker can do predictable changes to ciphertext
  - Malleable encryption
- Attacker can spoof DNS responses and redirect victim to IP of his choice
- https://alter-attack.net/

Source: D. Rupprecht, K. Kohls, T. Holz, Ch. Pöpper, “Breaking LTE on Layer Two”, S&P 2019

Linking of identities

- Network searches for phones in Tracking area using paging
- Sending message over Facebook triggers paging
- Calling the phone triggers Paging
- Attacker can learn GUTI identity
  - LTE equivalent of TMSI, should change often
- Attacker can link various IDs
  - GUTI, IMSI, MSISDN, facebook account , …



Source: A. Shaik, R. Borgaonkar, N. Asokan, V. Niemi, J.-P. Seifert, "Practical attacks against privacy and availability in 4G/LTE mobile communication systems", NDSS Symposium 2015

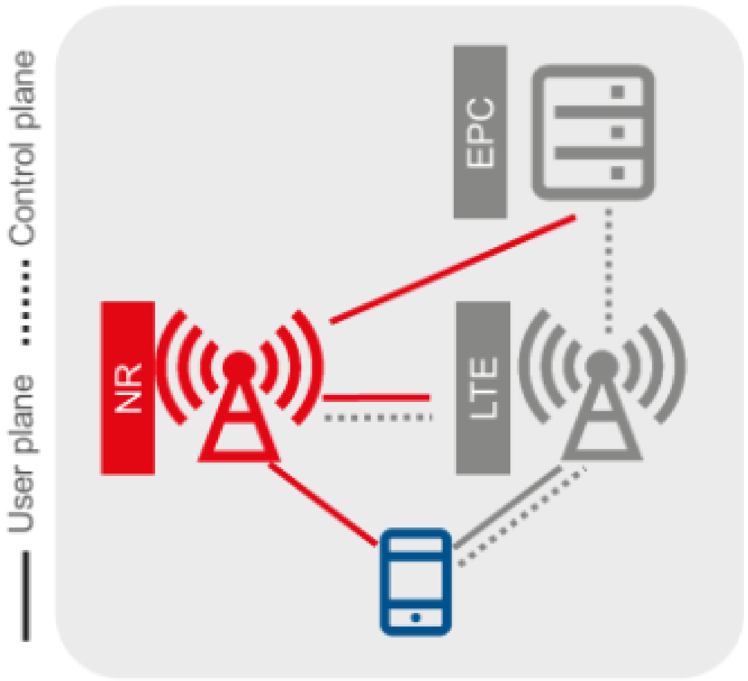
5rd Generation

4G TDD vs NSA vs SA

- 4G TDD (Time Division Duplex)
    - sometimes wrongly referred to as 5G
- 5G NSA (Non-Stand Alone)
    - 4G core network for mobility management + 5G cells with 5G physical layer for wider bandwidth
    - Inherits most of the security issues from 4G
- 5G SA (Stand Alone)
    - 5G core network + 5G cells

5G around us

- As of May 2022, vast majority of 5G installations are 5G NSA (Option 3)
- Inherits vulnerabilities from 4G



Source: GSMA

5G SA - Changes

- Introduced unified authentication framework
  - Access network agnostic – cellular network, Wifi, cable, …
  - 3 authentication methods
    - 5G-AKA, EAP-AKA’, EAP-TLS
  - Establishes multiple security contexts – for different network types
- SUPI replaces IMSI, never sent in plain
  - Encrypted with home network’s public key becomes SUCI
- Home network makes the final decision on authentication
  - Before home network only used to send authentication vectors
- Algorithms remain the same

Build your own testing tool

- SDR – Ettus Research USRP B210 or similar
- GSM stacks
  - OpenBTS
  - OsmoBTS + OsmoBSC
- UMTS stack - OpenBTS-UMTS
- LTE stacks
  - OpenLTE
  - srsLTE (srsRAN)
  - OpenAirInterface4G
- 5G
  - srsRAN
  - OpenAirInterface5G

Resources

- Project Kraken, https://opensource.srlabs.de/projects/a51-decrypt
- K. Nohl, L. Melette, “GPRS Intercept: Wardriving your country”, CCC 2011
- Barkan, Biham, Keller, “Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication”, Technion - Computer Science Department - Technical Report CS-2006-07 – 2006
- SRLabs, “Snoop Snitch”, https://opensource.srlabs.de/projects/snoopsnitch
- 3GPP TS 33.102, “3G Security; Security architecture”
- C. Tang, D.A. Naumann, S. Wetzel, “Analysis of Authentication and Key Establishment in Inter-generational Mobile Telephony”, IEEE HPCC & IEEE EUC 2013
- D. Rupprecht, K. Kohls, T. Holz, Ch. Pöpper, “Breaking LTE on Layer Two”, S&P 2019
- R. Borgaonkar, A. Shaik, N. Asokan, V. Niemi, J.-P. Seifert, “LTE and IMSI catcher myths”, BlackHat EU 2015
- A. Shaik, R. Borgaonkar, N. Asokan, V. Niemi, J.-P. Seifert, “Practical attacks against privacy and availability in 4G/LTE mobile communication systems”, NDSS Symposium 2015
- Tobias Engel, “SS7: Locate. Track. Manipulate.”, 31c3, CCC 2014