Sicurezza nelle Reti Wireless GSM e UMTS

William Wolfowicz

Autenticazione (e sicurezza) nelle reti wireless

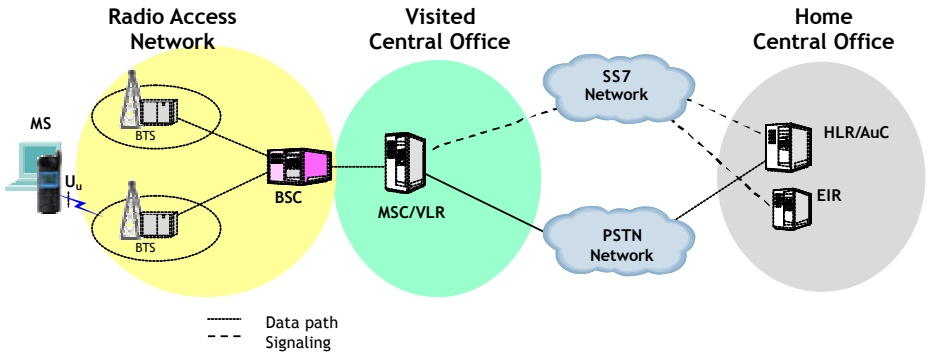
- **Diverse peculiarità delle reti wireless che richiedono particolare attenzione agli aspetti di sicurezza**
  - ***Il mezzo trasmissivo radio***
    - L'interfaccia permette, per definizione, attacchi passivi e attivi direttamente sul mezzo trasmissivo
    - Attacchi attivi di solito più difficili, ma comunque possibili
    - Banda disponibile ridotta rispetto al caso wired: necessità di meccanismi leggeri, sia dal punto di vista del numero di scambi richiesti dai protocolli che della dimensione dei dati scambiati
  - ***Mobilità***
    - La mobilità degli utenti richiede che i meccanismi di sicurezza impiegati siano sufficientemente rapidi ed efficienti in modo da gestire *hand-off* veloci
  - ***Tipologia dei dispositivi***
    - Ridotte capacità di calcolo e di memoria
- **Cosa vedremo**
  - Autenticazione nelle reti GSM (cenni)
  - Autenticazione (e sicurezza) nelle reti UMTS

William Wolfowicz

Autenticazione (e sicurezza) nelle reti GSM

William Wolfowicz

GSM: architettura di riferimento semplificata



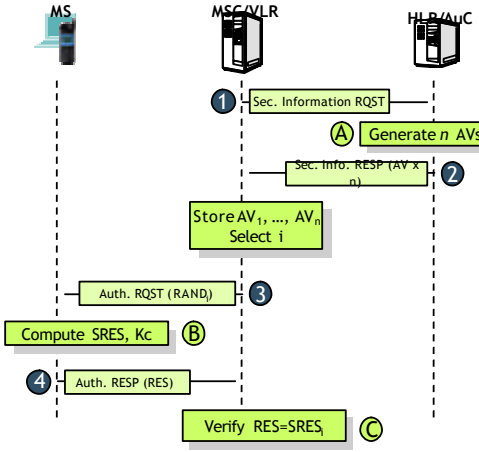
- MS: **Mobile System**
- HLR: **Home Location Register**
- VLR: **Visiting Location Register**
- AuC: **Authentication Center**
- BTS: **Base Transceiver Station**
- BSC: **Base Station Controller**
- SIM: **Subscriber Identity Module**
- MSC: **Mobile Switching Center**
- EIR: **Equipment Identity Register**

William Wolfowicz

GSM: il protocollo di autenticazione

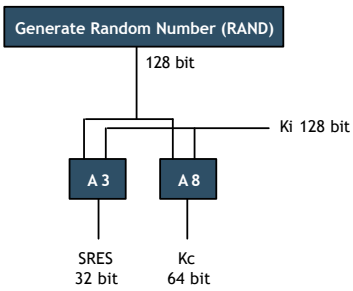
- **Obiettivi**
  - Autenticazione ***non*** mutua: la rete autentica MS, non viceversa
  - Generazione di chiavi effimere per proteggere la confidenzialità del traffico sul canale radio
  - Confidenzialità dell'identità di MS (quando possibile): per quest'ultimo obiettivo, si faccia riferimento alla spiegazione nel caso UMTS
- **Credenziali di autenticazione:**
  - IMSI, Ki: memorizzate nella SIM, impossibile "leggere" Ki
  - IMEI (International Mobile Equipment Identity): codice numerico associato al terminale, non alla SIM
- **Altri parametri di autenticazione memorizzati permanentemente nella SIM: algoritmi crittografici**
  - A3: autenticazione
  - A5: confidenzialità
  - A8: key-generation
- **In parallelo al protocollo di autenticazione crittografico, il GSM prevede che sia possibile effettuare il controllo dello stato di MS basandosi sul valore IMEI**
  - L'EIR può classificare un IMEI come *white* (MS OK), *grey* (MS è "sotto osservazione"), *black* (MS rubato, o comunque non autorizzato)

GSM: il protocollo di autenticazione (semplificato)



- **L'*Authentication Vector* (AV) nel messaggio (2) contiene *n* vettori di codici utili al VLR per effettuare *n* procedure di autenticazione diverse con lo stesso MS, senza dover ri-consultare l'HLR**
  - Ciascun vettore i-esimo include, tra gli altri parametri
    - RAND: la challenge
    - SRES: la risposta attesa
    - Kc: la chiave effimera, da utilizzarsi nell'algoritmo A5 per proteggere la confidenzialità sulla tratta radio
- ***RAND* nel messaggio (3) serve da challenge dalla rete per MS**
- **Al passo (C) la rete autentica MS**

GSM: ruolo di AuC e MS - passi A e B



- **L'AuC possiede il database delle credenziali degli utenti, indicizzato per IMSI**
- **Il VLR, nella richiesta di informazioni di sicurezza (messaggio (1)) invia l'IMSI dell'MS in questione**
- **A3-A8: algoritmi MAC, con parametro K**
  - ⇨ Gli algoritmi non sono stati mai ufficialmente pubblicati, e non sono stati direttamente basati su algoritmi già noti
- **L'AuC genera *n* vettori $[RAND,SRES,Kc]_i$, 1=i=n, e li invia al VLR nel messaggio (2)**
- **MS calcola RES e Kc con lo stesso meccanismo, e invia la risposta al VLR nel messaggio (4)**

GSM: il ruolo di VLR - passo C

- **Il VLR, ricevuto l'Authentication Vector da AuC, ne sceglie uno, e invia il corrispondente $RAND_i$ a MS nel messaggio (3)**
- **Il VLR controlla che il valore RES inviato da MS nel messaggio (4) corrisponda a $SRES_i$, autenticando quindi MS**
- **Il fatto che il VLR abbia a disposizione *n* AV gli permette di ri-autenticare, in seguito, MS, senza consultare AuC**
  - ⇨ Questo può anche essere usato quando MS si sposta tra un VLR e l'altro
- **Per evitare replay attack, i valori $RAND_i$ non possono essere riutilizzati**

GSM: gli algoritmi crittografici

- **A3: autenticazione**
  - Può essere scelto dall'operatore *home* indipendentemente dagli altri operatori
  - Basato, almeno inizialmente, su un algoritmo oggi noto con il nome di COMP128
  - Crittanalizzato (almeno in pubblico) nel 1998 con successo: vulnerabile ad attacchi chosen-text (chosen-challenge), che permettono all'attaccante di ricavare con successo Ki
    - Una volta ricavata Ki, è semplice ricavare Kc, e quindi violare anche la confidenzialità delle chiamate
  - Attacchi possibili sia se si è in possesso della SIM (è possibile che un rivenditore di SIM cloni telefoni), sia *over the air* ("basta" avere una BTS GSM, grazie al fatto che l'autenticazione non è mutua)
    - Nota: è comunque illegale, nella maggior parte dei paesi, attivare una BTS GSM senza autorizzazione governativa
- **A5: confidenzialità**
  - Deve essere scelto di comune accordo tra tutti gli operatori, per garantire la possibilità di roaming
  - Stream cipher
  - Anche la sua variante più forte (A5/1) è stata crittanalizzata con successo nel 1998/1999, ed è suscettibile ad attacchi over-the-air (è possibile ricavare Kc crittanalizzando per un tempo sufficiente un canale radio GSM). Questo tipo di attacchi è però relativamente poco pratico, a causa delle ipotesi raramente realizzabili
- **A8: key-generation**
  - Valgono le stesse considerazioni fatte per A3

Breve analisi sulla sicurezza del GSM

- **Dal punto di vista crittografico, il GSM si è rivelato un notevole fallimento**
  - Problema fondamentale: la progettazione degli algoritmi, e del loro uso all'interno di protocolli crittografici, è stato fatto "a porte chiuse"
- **La crittografia dei dati scambiati tra rete e MS copre solo la tratta radio, tra MS e BSC**
  - Se non vengono prese adeguate contromisure, è sempre possibile portare attacchi alla parte terrestre della rete
- **Oltre alla debolezza crittografica degli algoritmi A3/A5/A8, anche la scelta di chiavi di lunghezza relativamente piccola può essere causa di problemi di sicurezza**
  - Per esempio, Kc è lunga soli 64 bit
  - Problema mitigato dal fatto che Kc è effimera
- **Infine, problema serio dovuto all'autenticazione *non* mutua**
  - Può essere un problema relativamente poco rilevante nel caso di reti GSM "pure", mentre può diventare un problema serio se si cerca di riutilizzare la SIM GSM per altri tipi di autenticazione (per esempio, per le reti 802.11)

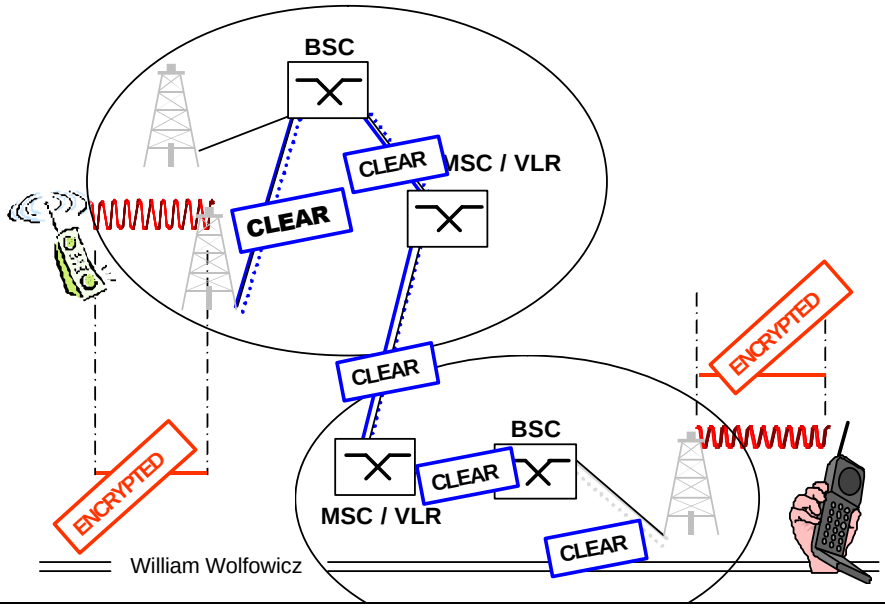
Limitations of GSM Security (1)

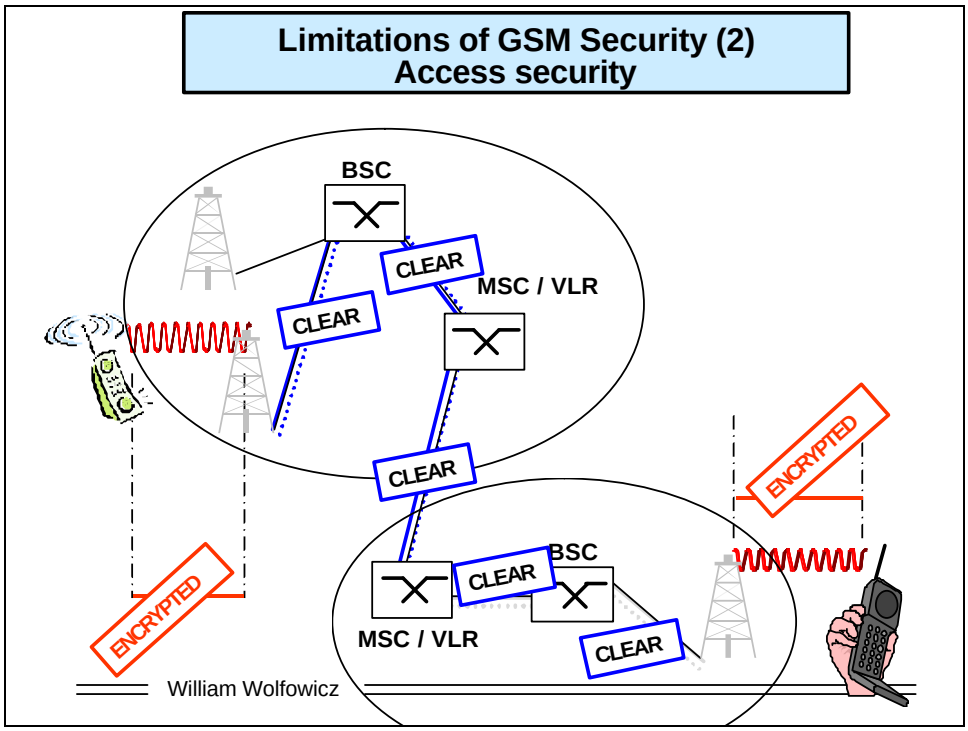
1 GSM was **designed to be "only" as secure as the wired networks** it interconnects to;

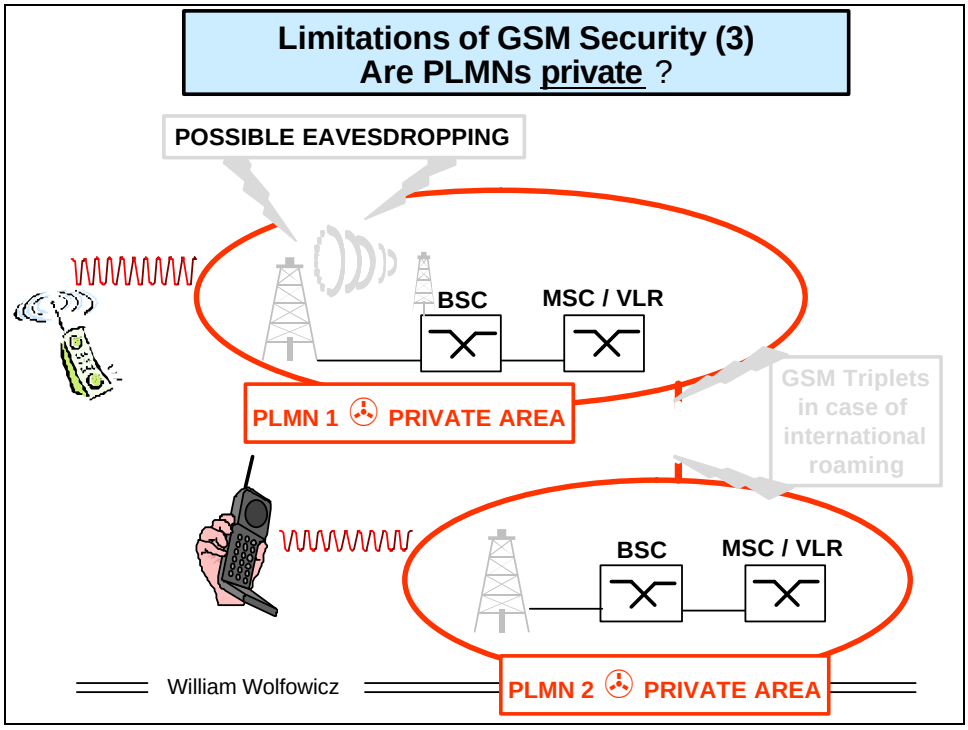
GSM only provides **access security**

(in the wired portion of the network, neither user data nor signalling traffic are protected. "Protection" either refers to **integrity** or to **confidentiality**).

Limitations of GSM Security (2) Access security




Limitations of GSM Security (2)
Access security
BSC
CLEAR
MSC / VLR
CLEAR
CLEAR
ENCRYPTED
ENCRYPTED
BSC
CLEAR
MSC / VLR
CLEAR
William Wolfowicz


Limitations of GSM Security (3)
Are PLMNs private ?
POSSIBLE EAVESDROPPING
BSC
MSC / VLR
PLMN 1 PRIVATE AREA
GSM Triplets in case of international roaming
BSC
MSC / VLR
PLMN 2 PRIVATE AREA
William Wolfowicz

Limitations of GSM Security (4)

2 No **openness** in algorithms design (A5, COMP128);

Suspicion around their real strength

-o- attack by Wagner on what was presented as COMP128 (practical) ;

-o- “attack” by Shamir on A52 (unpractical under the assumption that there exists a large amount of known plaintext);

William Wolfowicz

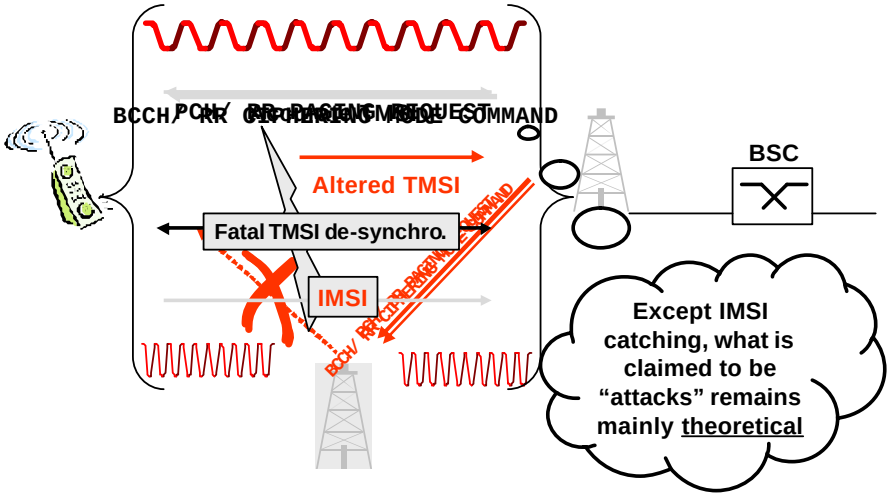
Limitations of GSM Security (5)

3 GSM **does not address active attacks**

It is a widely shared feeling that network elements may be impersonated (“ **false base station** “ acting as a **repeater**)

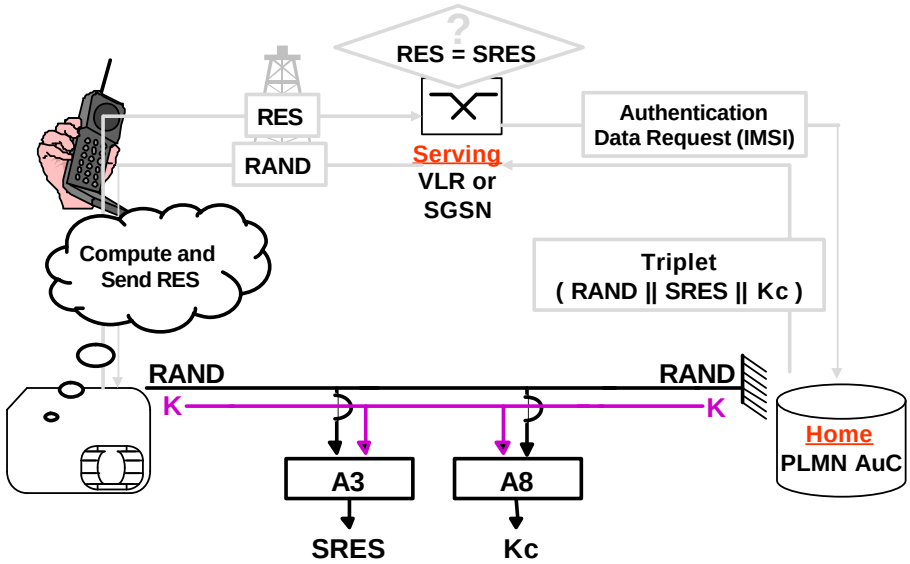
William Wolfowicz

Limitations of GSM Security (6)



William Wolfowicz

Limitations of GSM Security (7)
One way authentication



William Wolfowicz

Limitations of GSM Security (8) Miscellaneous

4 **Lack of flexibility in security administration**

- upgrading a BTS-hard-coded key length is difficult;
- codec designed for voice but not for data;
- OSI layers independence model not fulfilled;

5 **Mobile handsets are tampered with : IMEI alteration**

GSM SIM cards

- Principle of a smart card as a **privileged tool to bear a user profile** ;

- Smart card **tamper resistance** has not been questioned (GEMPLUS policy is transparency) ; so far, it has been a smart card specific property ;

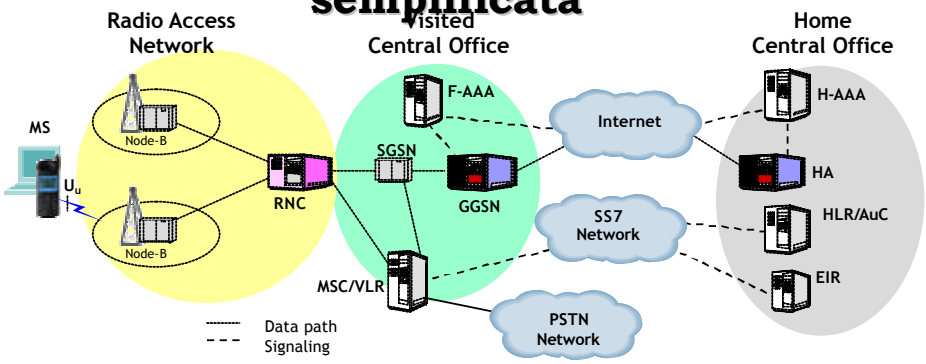
- SIM cards provide a **secure operator-user link for OTA administration purposes** ;

- Security is often hindered by its cost ; **smart cards achieve one of highest ratio security/cost**.

Autenticazione (e sicurezza) nelle reti UMTS

William Wolfowicz

UMTS: architettura di riferimento semplificata

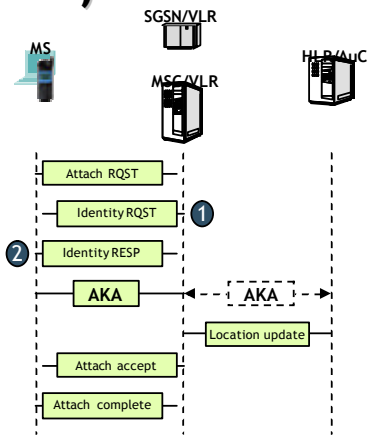


- MS: **Mobile System**
- HLR: **Home Location Register**
- VLR: **Visiting Location Register**
- AuC: **Authentication Center**
- H-AAA: **Home AAA**
- F-AAA: **Foreign AAA**
- SGSN: **Serving GPRS Support Node**
- GGSN: **Gateway GPRS Support Node**
- RNC: **Radio Network Controller**
- HA (FA): **Home (Foreign) Agent**
- PS/CS: **Packet Switched (service), Circuit Switched (service)**
- USIM: **User Services Identity Module**

William Wolfowicz

UMTS: *Authentication and Key Agreement* (AKA)

- **Il meccanismo di autenticazione in UMTS è mutuo, tra rete e MS**
  - Generalizzazione di uno degli algoritmi ISO/IEC 9798-4
- **Le entità che partecipano allo scambio sono MS, VLR (SGSN per *Packet Switched* mode, MSC per *Circuit Switched* mode), e HLR/AuC**
- **Obiettivi**
  - Autenticazione mutua (MS a Rete e Rete a MS)
  - Instaurazione di chiavi effimere sia per proteggere la confidenzialità che l'integrità dei dati
  - Protezione della confidenzialità, nel caso di attacchi passivi sul canale di comunicazione, di
    - Identità utente (IMSI), non sempre: i messaggi (1) e (2) vengono inviati solo quando l'IMSI dell'utente non esiste già nel database del VLR
    - Posizione dell'utente all'interno della rete
    - Servizi di rete che utente sta usando

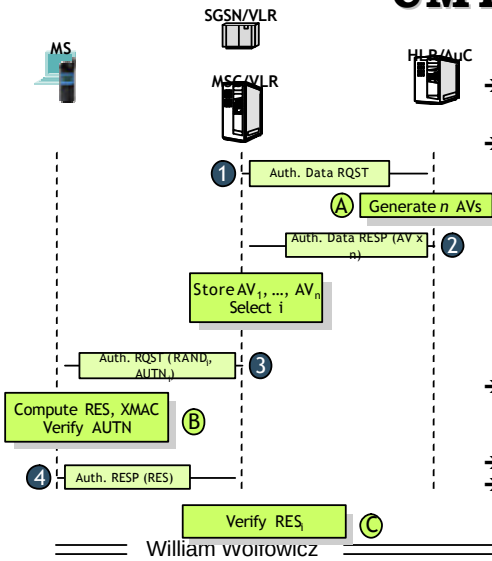


La procedura di *attach* ad una rete UMTS (semplificata)

Autenticazione in UMTS: i parametri principali

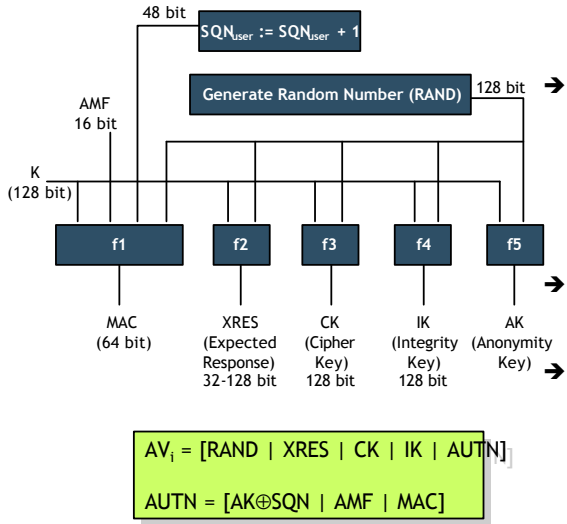
- **Credenziali di MS, memorizzate sulla USIM**
  - Identificazione (principali)
    - International Mobile Subscriber Identity **(IMSI)**
    - Temporary Mobile Subscriber Identity **(TMSI)**
    - Packet Temporary Mobile Subscriber Identity **(P-TMSI)**
  - Autenticazione
    - K: la chiave (simmetrica) condivisa tra l'AuC dell'utente e il MS (USIM)
- **Credenziali di HLR/AuC**
  - K
- **Gli algoritmi crittografici f1-f5, f8-f9**
  - Approccio ortogonale rispetto a quello seguito dal GSM: questi algoritmi sono stati pubblicati e analizzati prima di essere standardizzati

Autenticazione con AKA in UMTS



- **Il messaggio (1) contiene l'IMSI di MS, permettendo quindi a AuC di identificare l'utente**
- **L'*Authentication Vector* (AV) nel messaggio (2) contiene *n* vettori di codici utili al VLR per effettuare *n* procedure di autenticazione diverse con lo stesso MS, senza dover ri-consultare l'HLR**
  - Ciascun vettore i-esimo include, tra gli altri parametri
    - XRES (Expected Response)
    - AUTN, il parametro con cui MS può autenticare la rete
    - Chiavi effimere
- ***RAND* nel messaggio (3) serve da challenge dalla rete per MS, mentre *AUTN* serve come dato di autenticazione dalla rete a MS**
- **Al passo (B) MS autentica la rete**
- **Al passo (C) la rete autentica MS**

AKA: ruolo di AuC al passo (A)



- **AuC deve recuperare nel proprio database, indicizzato per IMSI, i seguenti parametri**
  - K: la chiave associata all'IMSI di MS
  - SQN: numero di sequenza corrente associato all'IMSI di MS
- **f1-f5: algoritmi MAC (e generazione di chiavi temporanee), con parametro *K***
- **AMF: Authentication and key Management Field**
  - Gestione di "casi particolari" (selezione di algoritmi diversi, ecc…)

AV_i = [RAND | XRES | CK | IK | AUTN]

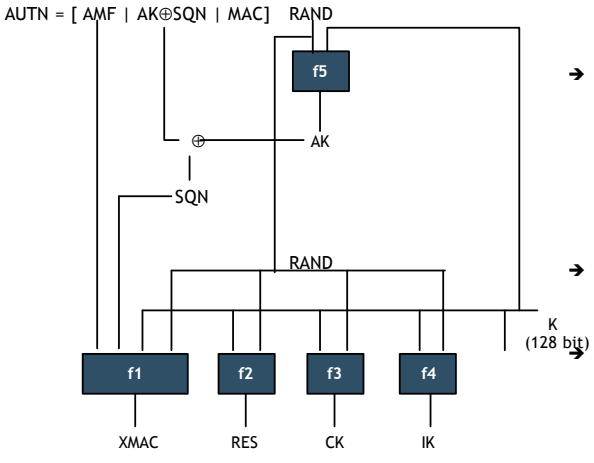
AUTN = [AK⊕SQN | AMF | MAC]

AKA: ruolo di AuC al passo (A)

➔ **SQN: numero di sequenza**
- ⇨ Rappresenta un'alternativa ai protocolli di autenticazione con nonce: è una nonce implicita da MS a AuC
  - →MS accetterà AUTN solo se è relativo ad un numero di sequenza valido (non ancora usato)
- ⇨ Permette di garantire la freschezza dei parametri, e proteggere da replay attack, minimizzando il numero di messaggi richiesti per farlo (rispetto ad una soluzione con nonce)
- ⇨ Necessita di sincronizzazione tra MS e AuC
  - →Sia MS che AuC devono memorizzare gli ultimi valori usati per SQN
- ⇨ Procedura di ri-sincronizzazione "costosa", in termini di numero di messaggi

➔ **AK protegge SQN da attacchi passivi**
- ⇨ Osservando l'andamento di SQN potrebbe essere possibile capire la posizione e/o l'identità dell'utente

AKA: ruolo di MS al passo (B)



➔ **Oltre a verificare il codice di autenticazione della rete (XMAC), MS deve anche verificare che SQN sia valido**
- ⇨ USIM memorizza l'ultimo valore utilizzato dalla rete
- ⇨ Si ammettono piccole discrepanze per superare eventuali problemi di perdite di messaggi senza necessariamente iniziare la procedura di sincronizzazione (costosa)

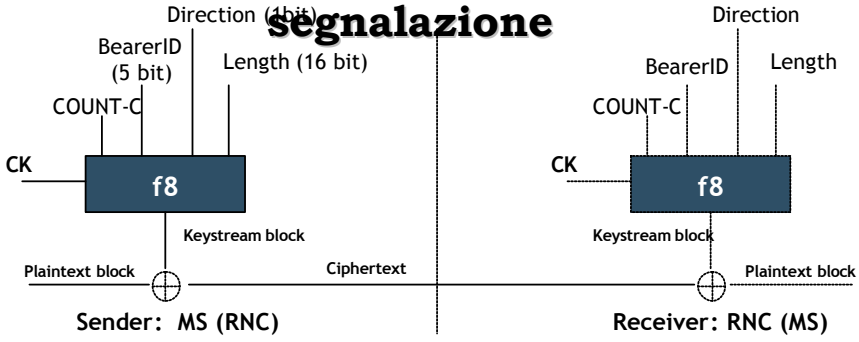
➔ **Se la verifica di MAC fallisce, MS** *non invia RES*
- ⇨ Risoluzione di potenziali problemi dovuti ad attacchi known-text, come nel caso GSM

➔ **Tutti questi algoritmi sono eseguiti all'interno della USIM, non nel dispositivo MS**

AKA: ruolo di VLR al passo (C)

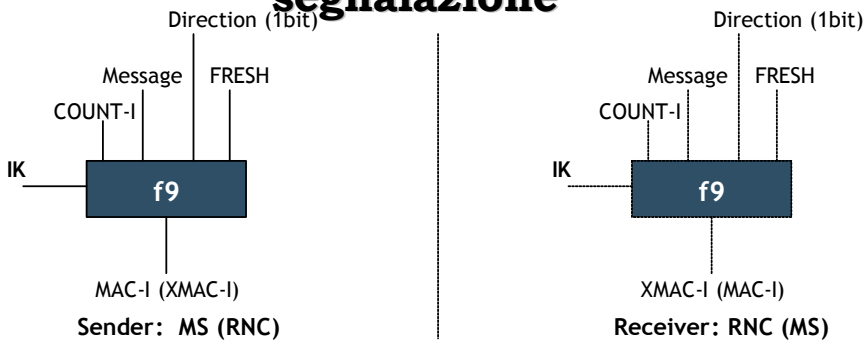
- ➔ **Al VLR resta il compito di verificare che il valore RES ricevuto da MS sia corretto (RES = $XRES_i$)**
- ➔ **Il fatto che VLR riceva e memorizzi un Authentication Vector (più vettori di autenticazione) permette, come per il GSM, di effettuare altri run di AKA senza necessariamente interrogare AuC**
- ➔ **Anche in questo caso, come nel GSM, ciascun valore $RAND_i$ può essere usato una sola volta**
  - ⇨Esauriti gli *n* valori disponibili, il VLR dovrà interagire ancora con l'HLR per richiedere un nuovo AV

UMTS: confidenzialità, sia per dati utente che per messaggi di segnalazione



- ➔ *COUNT-C* - **Semplice metodo per aggiungere un'ulteriore variabile allo stream cipher (evitare che lo stesso keystream sia generato più volte): il suo valore dipende dal valore di vari parametri trasmissivi**
- ➔ *BearerID* - **Identifica il particolare canale trasmissivo in uso: permette di evitare che si usi lo stesso keystream per diversi canali trasmissivi tra MS e RNC**
- ➔ *Direction* - **Permette di evitare che lo stesso keystream venga utilizzato in entrambe le direzioni trasmissive**
- ➔ *Length* - **Permette di specificare la lunghezza di ciascun blocco del keystream**

UMTS: integrità, sia per dati utente che per messaggi di segnalazione



- *COUNT-I* - **Cfr. COUNT-C**
- *Message* - **Il messaggio la cui integrità si vuole proteggere**
- *Direction* - **Cfr. lucido precedente**
- *FRESH* - **Nonce inviata dalla rete a MS prima dell'inizio delle operazioni di cifratura. È un valore che cambia ogni volta che MS effettua un attach. Permette di evitare che MS possa riutilizzare codici di integrità usati in precedenza (replay attack)**

UMTS: l'algoritmo Kasumi

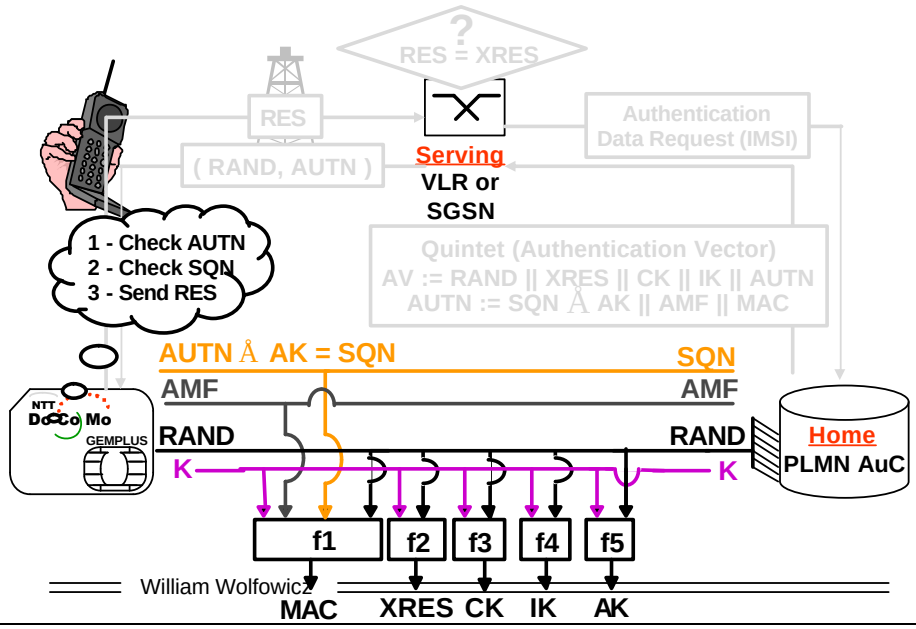
- **Kasumi è un algoritmo crittografico simmetrico a blocchi, con *b* = 64 bit, basato su uno schema di tipo Feistel, con 8 round**
- **Sia f8 che f9 sono basate su Kasumi**
- **Brevettato da Mitsubishi**
- **Altro vantaggio di UMTS rispetto a GSM: ad oggi è stato crittanalizzato relativamente a lungo, senza scoprire particolari problemi crittografici**

2 - What 3G improves

3G Security Principles

- **Build on GSM security as much as possible**
- **Ensure backward compatibility**
- **Correct known GSM security weaknesses**
- **Add new security features as necessary (new services or new network architecture choices)**

AKA message flow



What is new in AKA ?

- Different CK for PS and CS (important : PS formatting usually leaves a large amount of known plaintext) ;
- User visibility over his effective underlying security (PIN, non-ciphered calls, use of algorithms) ;
- Authentication vectors are marked with a SQN : prevents authentication replay scenarios ;
- IK protects the signalling traffic integrity ;
- Secure messaging between the USIM and the network (based on GSM 03.48)
- Authentication reject Notification from the USIM to the SN;

3 - New potential weaknesses in 3G networks

"Security-Universal" advises

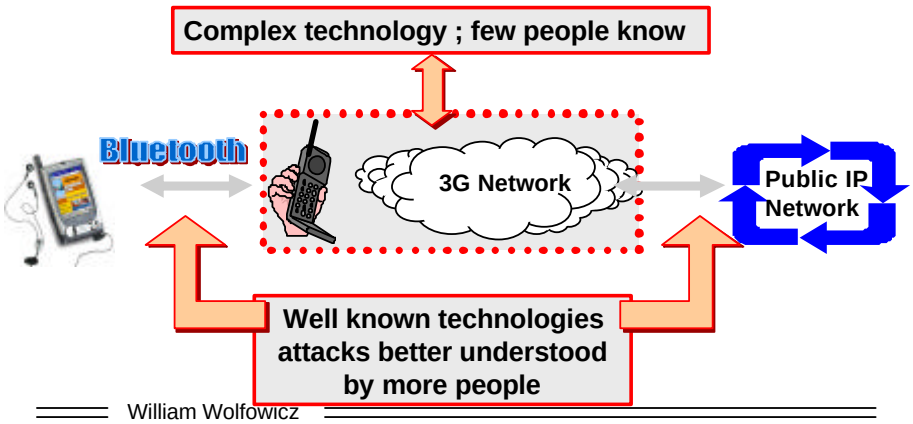
1. **The MAPSec specification only mandates a security framework; effective implementations are up to operators.**

2. **No way to get rid of "Denial of Service" oriented attacks on the radio link.**

3. **More flexible security ➡ increased needs for fine grained configuration of the network entities. Take care in configuring, take care in remote access management.**

“3G specific” security threats

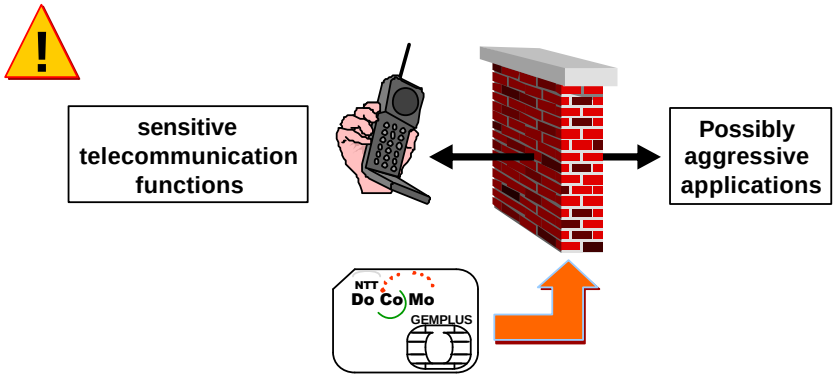
4 **3G networks are to be widely interconnected.**



William Wolfowicz

Mixing pure telephony and applications !

5 **Handsets are about to become execution platforms for many applications (see MExE, Mobile Execution Environment). We can expect viruses and Trojan horses to spread throughout.**



William Wolfowicz