Autenticazione nelle Reti Cellulari: Cellnet, GSM, UMTS e oltre

1 Introduzione

La sicurezza nelle reti cellulari wireless è un tema complesso che, in questa fase, si concentra primariamente sull'**autenticazione**. L'obiettivo è garantire che solo i dispositivi in possesso di credenziali valide (SIM/USIM) possano accedere ai servizi di rete, prevenendo frodi e accessi non autorizzati.

Questa lezione esamina i meccanismi con cui la rete verifica l'identità dell'utente, un processo che si è evoluto significativamente nel corso delle generazioni:

- Nelle prime generazioni (2G), l'autenticazione era spesso unidirezionale (la rete controlla l'utente).
- Nelle generazioni successive (3G, 4G, 5G), si è passati a una **mutua autenticazione**, dove anche l'utente verifica l'autenticità della rete per evitare attacchi di tipo *false base station* (IMSI catchers).

2 Architettura delle Reti Cellulari (Modello Astratto)

Come illustrato nello schema architetturale astratto, la struttura logica di sicurezza si basa sulla separazione tra la rete che serve fisicamente l'utente e la rete che detiene i dati dell'abbonato. L'architettura si compone dei seguenti blocchi logici:

2.1 1. User Equipment (UE)

È il dispositivo mobile dell'utente finale. Dal punto di vista della sicurezza, l'elemento critico non è solo il telefono, ma il modulo di identità (SIM per

2G, USIM per 3G/4G/5G) che custodisce la chiave segreta (spesso denotata come K o K_i). L'UE comunica con la rete attraverso l'interfaccia radio (U_u).

2.2 2. Serving Network (Rete Visitata)

È la rete a cui l'utente è fisicamente connesso in quel momento (può coincidere con l'operatore di casa o essere un operatore estero in roaming). Gestisce l'accesso radio e il controllo della mobilità. I nodi principali in questo segmento variano in base alla tecnologia:

- **2G/3G (Circuit Switched):** I nodi principali sono l'**MSC** (Mobile Switching Center) e il **VLR** (Visitor Location Register). Il VLR richiede le credenziali di autenticazione alla rete di casa per verificare l'utente.
- **4G/5G (Packet Switched):** La funzione di gestione della mobilità e autenticazione è svolta dall'**MME** (Mobility Management Entity), che interagisce con le stazioni base (**eNB** o eNodeB).

2.3 3. Home Network (Rete di Casa)

È la rete dell'operatore con cui l'utente ha sottoscritto l'abbonamento. È l'unica entità che possiede la copia master delle chiavi segrete dell'utente e il profilo completo.

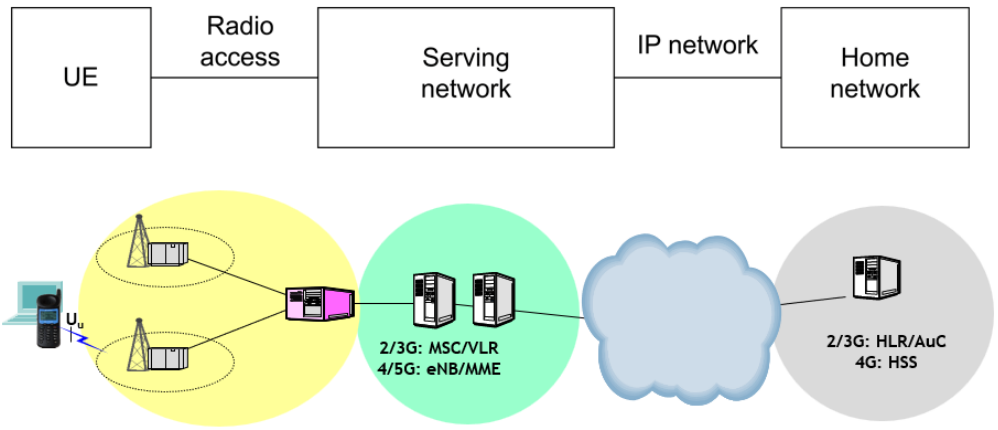
- **2G/3G:** I database principali sono l'**HLR** (Home Location Register) e l'**AuC** (Authentication Center). L'AuC genera i vettori di autenticazione (sfide crittografiche).
- **4G (LTE):** Queste funzioni sono consolidate nell'**HSS** (Home Subscriber Server), che funge da database centrale per le credenziali e le policy.

2.4 Interconnessione (IP Network)

Tra la *Serving Network* e la *Home Network* esiste una rete di trasporto (spesso basata su IP nelle generazioni moderne) che permette lo scambio di messaggi di segnalazione per l'autenticazione anche quando l'utente si trova dall'altra parte del mondo (Roaming).

Nota: Questa separazione è fondamentale per la sicurezza: la chiave segreta master non lascia mai la Home Network (o la USIM dell'utente); alla Serving

Network vengono inviati solo dei "vettori di autenticazione" temporanei.



3 Sicurezza nelle Reti di Prima Generazione (1G)

Le reti 1G erano caratterizzate da sicurezza quasi nulla:

- Mancanza di autenticazione reciproca: la rete autenticava l'utente, ma non viceversa.
- Assenza di cifratura o cifratura molto debole.
- Vulnerabilità a attacchi di spoofing e intercettazione.

Queste limitazioni hanno stimolato lo sviluppo delle reti successive con livelli crescenti di sicurezza.

4 Sicurezza nelle Reti 2G GSM

Nel sistema GSM 2G, l'autenticazione si basa su un protocollo *challenge-response*:

- Al centro della sicurezza c'è la **SIM**, una smart card che contiene una chiave segreta Ki.
- Quando un dispositivo si collega, la rete invia una sfida casuale (RAND).
- La SIM usa la chiave Ki e un algoritmo segreto (denominato A3) per calcolare una risposta (SRES).

- La rete confronta il valore ricevuto e, se corrispondente, autorizza l'accesso.
- Inoltre, viene derivata una chiave di cifratura Kc usata per proteggere la comunicazione radio.

Il sistema funziona con **triplette** di valori $(Ki, RAND, SRES)$ pre-calcolate per sessioni multiple. Tuttavia, la sicurezza di questi algoritmi è stata spesso affidata all'*obscurity* (segretezza degli algoritmi), che è risultata insufficiente.

5 Vulnerabilità di GSM

Sistemi come COMP128 sono stati reverse engineered e violati, esponendo la chiave segreta Ki attraverso attacchi che richiedono molte interrogazioni (150.000 circa). Questo permette la clonazione della SIM, compromettendo la sicurezza.

In più, GSM prevede solo autenticazione unilaterale: il dispositivo si autentica verso la rete, ma non viceversa. Ciò apre la possibilità di falsi "rogue base stations" per intercettare comunicazioni.

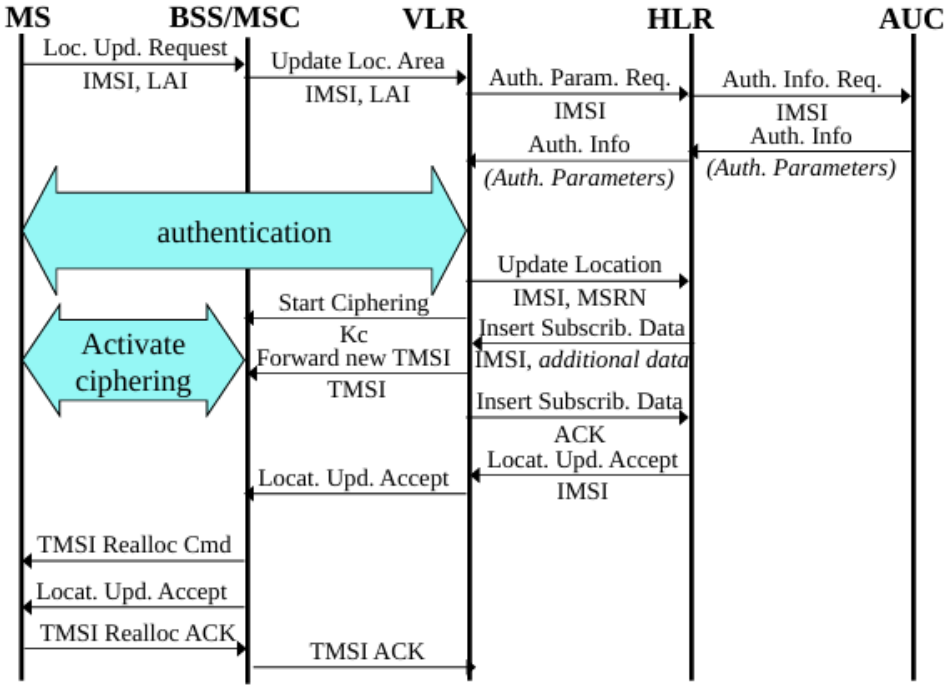
6 Evoluzione della Sicurezza nelle Reti 3G, 4G e 5G

Le reti successive (UMTS, LTE, 5G) introducono:

- **Autenticazione mutua**: sia l'utente che la rete si autenticano reciprocamente, riducendo il rischio di attacchi MITM.
- **Algoritmi crittografici pubblici e analizzati dalla comunità di ricerca**, non più sicurezza per obscurity.
- **Gestione centralizzata delle credenziali** con componenti come UDM (Unified Data Management) e AUSF (Authentication Server Function).
- **Protezione della privacy** tramite l'uso di identificatori temporanei (TMSI) e mascheramento nel trasporto di informazioni sensibili.

7 Dettagli dell'Autenticazione GSM (2G)

Il processo di sicurezza nelle reti GSM (2G) si basa su un meccanismo di tipo *Challenge-Response*. Questo approccio è progettato per verificare l'identità dell'abbonato senza mai trasmettere la chiave segreta master sulla rete radio. Di seguito vengono analizzati i componenti crittografici, il protocollo di scambio e le criticità di sicurezza emerse nel tempo.



7.1 Primitive Crittografiche e Algoritmi

L'autenticazione si fonda su tre elementi dati e due algoritmi principali:

- K_i **(Subscriber Authentication Key)**: È una chiave segreta a 128 bit. È memorizzata unicamente in due luoghi sicuri: all'interno della SIM (lato utente) e nell'Authentication Center (AuC) dell'operatore (lato rete). Non lascia mai questi dispositivi.
- **RAND (Random Challenge)**: È un numero casuale a 128 bit generato dalla rete per sfidare l'utente.
- **Algoritmo A3**: È la funzione di autenticazione. Prende in input K_i e $RAND$ e produce una risposta firmata chiamata **SRES** (Signed

Response) a 32 bit.

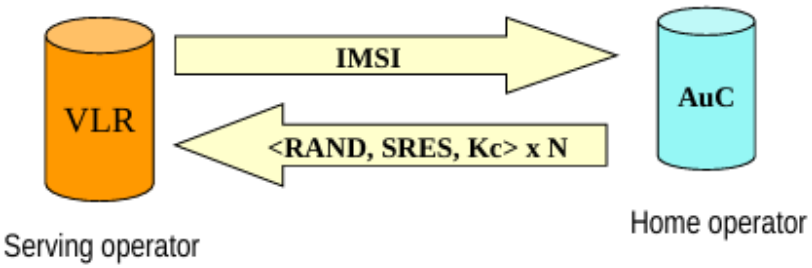
$$SRES = A3(K_i, RAND)$$

- **Algoritmo A8**: È la funzione di generazione della chiave di sessione. Utilizza gli stessi input (K_i e $RAND$) per generare la chiave di cifratura K_c a 64 bit.

$$K_c = A8(K_i, RAND)$$

Spesso, nelle implementazioni reali, gli algoritmi A3 e A8 sono combinati in un'unica esecuzione logica denominata **A38**.

7.2 Vettori di Autenticazione (Triplets)



➔ **Idea: once in a VLR area, autentication will need to be performed MANY times**

➔ **Hence deliver N triplets, to be used for N distinct authentications**

➔ **IMPORTANT: VLR does NOT need to know authentication algo used (A3, A8)**
- ⇨ Triplet contains computed result by AuC
- ⇨ A3, A8 run inside the SIM (given by operator)

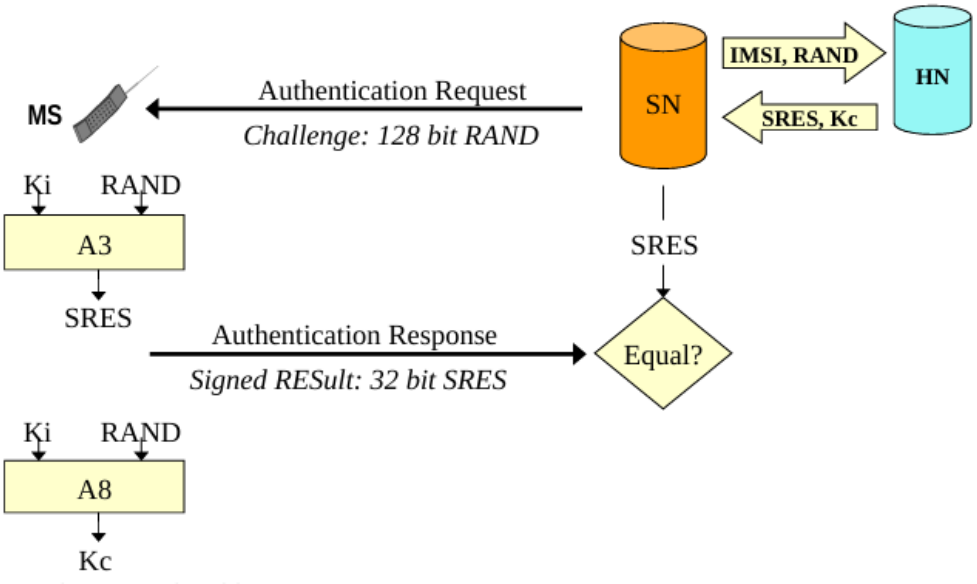
Per motivi di efficienza e per ridurre il carico di segnalazione verso la rete di casa (Home Network - HN), l'autenticazione non coinvolge l'AuC in tempo reale per ogni singola chiamata. L'AuC genera dei pacchetti pre-calcolati chiamati **Triplette** (Authentication Vectors) e li invia al VLR (Visitor Location Register) della rete ospitante (Serving Network - SN).

Una tripletta è composta da:

$$< RAND, SRES, K_c >$$

Nota Importante: Il VLR/MSC (la rete che serve l'utente) **non** conosce la chiave segreta K_i né gli algoritmi A3/A8. Riceve semplicemente il risultato del calcolo dall'AuC. Questo permette all'operatore di mantenere segreti i propri algoritmi proprietari all'interno della SIM e dell'AuC.

7.3 Protocollo di Autenticazione Unilaterale



La procedura di autenticazione avviene secondo i seguenti passaggi (visualizzati nel diagramma di sequenza):

1. La rete (MSC/VLR) seleziona una tripletta non ancora utilizzata e invia la sfida **RAND** alla Mobile Station (MS).
2. La MS passa il RAND alla SIM. La SIM, usando la sua K_i interna, esegue gli algoritmi A3 e A8.
3. La SIM restituisce il risultato **SRES** al terminale, che lo invia alla rete.
4. La rete confronta l'SRES ricevuto con quello memorizzato nella tripletta. Se coincidono ($SRES_{MS} == SRES_{Net}$), l'utente è autenticato.
5. Contemporaneamente, la SIM calcola la chiave di sessione K_c, che verrà usata per cifrare le comunicazioni successive.

7.4 Vulnerabilità e Sicurezza

Il sistema 2G presenta diverse debolezze strutturali e implementative che sono state oggetto di attacchi storici.

7.4.1 Autenticazione Unilaterale

Il difetto architetturale più grave è la mancanza di mutua autenticazione. Mentre la rete autentica l'utente (verificando l'SRES), l'utente non ha modo di verificare l'autenticità della rete.

- **Attacco Rogue BTS:** Una stazione base falsa può inviare un RAND qualsiasi a un cellulare, completare la procedura di "attach" e intercettare il traffico o l'identità dell'utente (IMSI catcher).

7.4.2 Debolezza degli Algoritmi (Security by Obscurity)

Lo standard GSM non ha reso pubblici inizialmente gli algoritmi A3/A8, affidandosi alla "sicurezza tramite oscurità". Gli operatori potevano scegliere il proprio algoritmo, ma molti hanno adottato un'implementazione standard chiamata **COMP128**.

- **COMP128 Broken:** Nel 1998, ricercatori (Briceno, Goldberg, Wagner) hanno dimostrato che COMP128 era vulnerabile a un attacco a testo scelto (Chosen Challenge Attack). Con circa 150.000 query alla SIM (circa 8 ore), era possibile estrarre la chiave master K_i, permettendo la clonazione della SIM.
- Nel 2002, un attacco migliorato (Rao et al.) ha ridotto il tempo necessario a meno di 1 minuto.

7.4.3 Debolezza della Chiave K_c

La chiave di cifratura K_c dovrebbe essere a 64 bit. Tuttavia, in molte implementazioni (incluso COMP128), gli ultimi 10 bit sono forzati a zero. Questo riduce l'entropia effettiva a soli **54 bit**, rendendo la cifratura deliberatamente debole e suscettibile ad attacchi di forza bruta.

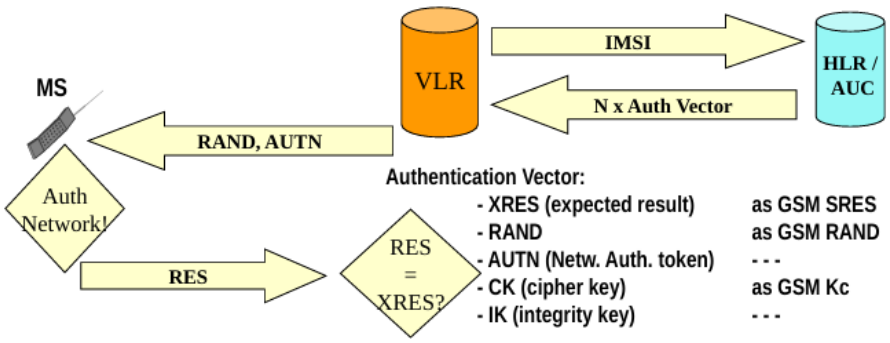
8 3G/4G/5G Authentication: Protocollo di Autenticazione AKA (Authentication and Key Agreement)

9 3G/4G/5G Authentication: Protocollo AKA (Authentication and Key Agreement)

Il protocollo **AKA** (Authentication and Key Agreement) rappresenta il cuore della sicurezza nelle reti mobili moderne (UMTS, LTE, 5G), sostituendo il vecchio modello del GSM (2G). A differenza del 2G, dove solo la rete autenticava l'utente, AKA introduce l'**autenticazione mutua**: non solo la rete verifica l'identità dell'utente (MS - Mobile Station), ma l'utente verifica l'autenticità della rete, proteggendosi da stazioni base false (IMSI Catchers).

Inoltre, gli algoritmi crittografici non sono più basati sulla "security by obscurity", ma sono stati scrutinati dalla comunità di ricerca prima di essere selezionati.

9.1 Il Vettore di Autenticazione (Authentication Vector)



La procedura inizia quando il VLR (Visitor Location Register) richiede i dati di autenticazione all'HLR/AuC (Home Location Register / Authentication Center). L'AuC genera un **Vettore di Autenticazione** (spesso chiamato "quintupla" in 3G, a differenza della "tripla" del 2G), composto da 5 elementi:

- **RAND**: Un numero casuale generato dalla rete (la "sfida").

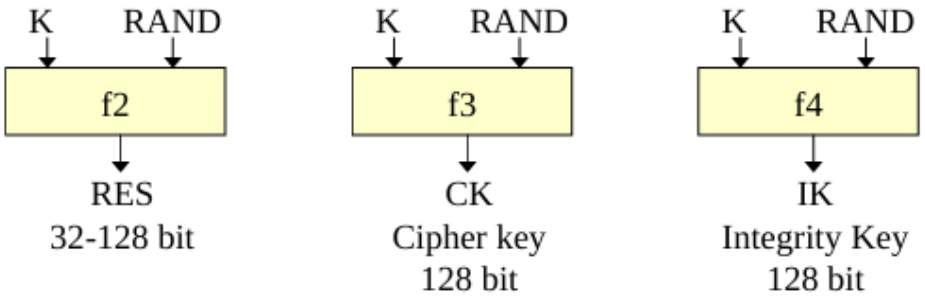
- **XRES** (Expected Response): La risposta attesa che l'utente deve calcolare per dimostrare la sua identità (equivalente a SRES in GSM).
- **CK** (Cipher Key): Chiave a 128 bit utilizzata per cifrare il traffico dati.
- **IK** (Integrity Key): Chiave a 128 bit (nuova rispetto al 2G) utilizzata per garantire l'integrità dei messaggi di segnalazione e impedire manomissioni.
- **AUTN** (Authentication Token): Il "passaporto" della rete. È un token che permette all'utente di verificare che la richiesta provenga da una rete legittima.

Il VLR inoltra alla MS solo **RAND** e **AUTN**.

10 Fasi dell'Autenticazione e Algoritmi

Il processo si basa su una chiave segreta condivisa K (memorizzata nella SIM/USIM e nell'AuC) e su una famiglia di algoritmi pubblici (f1, f2, f3, f4, f5).

10.1 Autenticazione dell'Utente (MS Authentication)



La MS deve dimostrare la propria identità rispondendo alla sfida $RAND$.

- La MS utilizza l'algoritmo **f2** con input K e $RAND$ per calcolare la risposta RES.
- La MS invia RES alla rete.
- La rete confronta RES con $XRES$ (contenuto nel vettore). Se $RES = XRES$, l'utente è autenticato.

Contestualmente, la MS usa gli algoritmi **f3** e **f4** per generare localmente le chiavi di sessione CK e IK.

10.2 Autenticazione della Rete (Network Authentication)

Questa è la grande novità rispetto al 2G. La MS deve essere sicura che il $RAND$ non sia stato inviato da un attaccante o che non sia una riproduzione di una vecchia comunicazione (Replay Attack). Per fare ciò, la rete invia il token **AUTN**, che ha il seguente formato:

$$AUTN = (SQN \oplus AK) \,||\, AMF \,||\, MAC\text{-}A$$

1. **MAC-A (Message Authentication Code):** Generato dall'algoritmo **f1**. Garantisce l'integrità. La MS ricalcola il MAC localmente; se corrisponde a quello ricevuto, sa che il messaggio viene da chi possiede la chiave K (la rete HLR/AuC).
2. **SQN (Sequence Number):** È un contatore che funge da "nonce implicito". Invece di richiedere un messaggio extra alla MS per generare un nonce, si usa un numero di sequenza sincronizzato tra MS e AuC.

10.2.1 Il meccanismo anti-replay (SQN)

La MS memorizza l'ultimo SQN valido ricevuto (SQN_{MS}). Quando riceve un nuovo SQN dalla rete:

- Verifica che $SQN > SQN_{MS}$ (cioè che sia "fresco" e non vecchio).
- Se la verifica passa, aggiorna il proprio SQN_{MS}.
- Se SQN è inferiore o già visto, la MS scarta la richiesta (protezione da Replay Attack).

Questo richiede che MS e AuC siano approssimativamente sincronizzati; esistono procedure specifiche per la risincronizzazione in caso di disallineamento.

11 Protezione della Privacy e Anonymity Key

C'è un problema di privacy nell'inviare il SQN in chiaro: essendo un contatore incrementale, un attaccante passivo potrebbe osservare i valori SQN (es. 100, 101, 102...) e correlarli per tracciare gli spostamenti o le attività di uno specifico utente.

11.1 Soluzione: Mascheramento del SQN

Per risolvere il problema, il SQN non viene inviato in chiaro, ma viene mascherato tramite un'operazione XOR con una **Anonymity Key (AK)**.

$$SQN_{trasmesso} = SQN \oplus AK$$

- **Generazione AK:** La chiave di anonimato AK viene generata dall'algoritmo **f5** prendendo in input la chiave segreta K e il numero casuale $RAND$.
- **Recupero SQN:** Poiché la MS possiede K e riceve $RAND$, può calcolare localmente AK. Facendo l'XOR del primo campo dell'AUTN con la AK calcolata, ottiene il SQN pulito:

$$(SQN \oplus AK) \oplus AK = SQN$$

In questo modo, solo l'utente legittimo può leggere il numero di sequenza, proteggendo la propria privacy dagli eavesdropper.

12 Conclusioni

La sicurezza nelle reti cellulari è un processo evolutivo. Il protocollo AKA del 3G/4G/5G risolve le vulnerabilità del 2G attraverso:

1. **Autenticazione Mutua:** Impedisce attacchi con false stazioni base.
2. **Chiavi di Integrità (IK):** Protegge la segnalazione da manomissioni.
3. **Sequence Number (SQN):** Previene i replay attack senza messaggi extra.
4. **Anonymity Key (AK):** Protegge la privacy dell'utente nascondendo il contatore di sequenza.