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

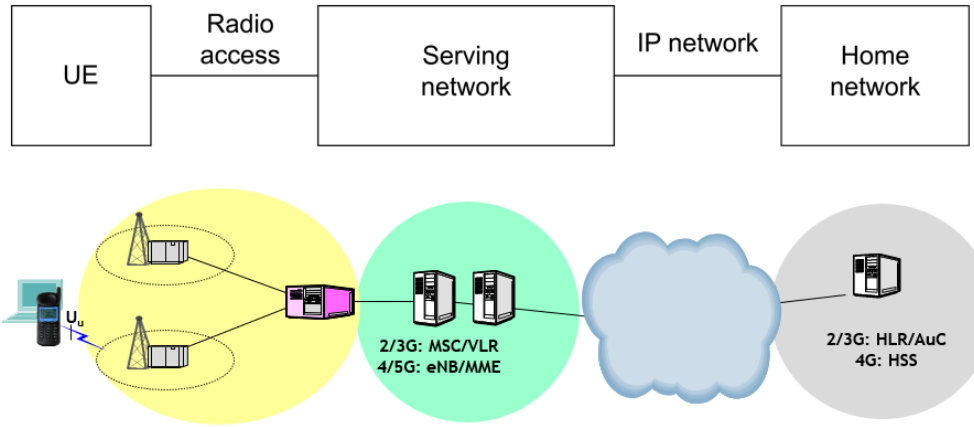
Introduzione

La sicurezza nelle reti cellulari wireless è un tema complesso che si concentra primariamente sull'autenticazione degli utenti per garantire che solo i dispositivi autorizzati possano accedere alla rete. Questa lezione esamina i metodi di autenticazione utilizzati nelle diverse generazioni di reti mobili, evidenziandone le evoluzioni e le vulnerabilità storiche.

Architettura Generale delle Reti Cellulari Wireless

Le reti cellulari sono strutturate in diversi componenti fondamentali:

- **Utente (UE - User Equipment)**, ovvero il dispositivo mobile.
- **Rete di accesso radio (RAN)**, presente ad esempio nell'UMTS e 4G con nodi come eNodeB.
- **Core network**, che gestisce autenticazione, mobilità, e instradamento.
- **Sistemi di gestione**, come HSS/UDM che conservano le credenziali e gestiscono le policy di autenticazione.



Questa architettura assicura funzioni di sicurezza distribuite, dalla verifica delle identità fino al mantenimento della confidenzialità e integrità delle comunicazioni.

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.

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.

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.

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.

Protocollo di Autenticazione AKA (Authentication and Key Agreement)

Il protocollo AKA è il cuore della sicurezza nelle reti mobili moderne:

- Basato su vettori di autenticazione che comprendono:
  - Un valore casuale $RAND$ inviato come sfida.
  - Un valore atteso $XRES$ calcolato dal server.
  - Una chiave di cifratura CK e chiave di integrità IK.
  - Un token di autenticazione $AUTN$ che permette all'utente di verificare la rete.
- L'utente risponde con una risposta RES, anch'essa calcolata usando $RAND$ e la chiave segreta.
- Il protocollo garantisce freschezza e prevenzione da replay attack utilizzando numeri di sequenza (SQN).
- Supporta l'autenticazione mutua e garantisce l'integrità dei messaggi grazie a meccanismi crittografici.

Protezione della Privacy e Contro gli Attacchi

Gli attacchi di localizzazione e tracciamento sono contrastati mascherando valori sensibili come SQN tramite chiavi di anonimato AK. La sincronizzazione tra il dispositivo e la rete viene gestita per evitare problemi di autenticazione fallita.

Conclusioni

La sicurezza nelle reti cellulari è un processo evolutivo, nato con solide basi di autenticazione 2G che si sono rafforzate e rese più complesse nelle tecnologie successive. L'autenticazione mutua, l'uso di chiavi temporanee e l'adozione di algoritmi pubblici e verificati rappresentano i pilastri della protezione degli utenti nelle moderne reti mobili.