**eSIM**

**Cos’è una eSIM?**È detta anche **embedded-SIM** o **SIM virtuale** e rappresenta un servizio virtuale che sostituisce la scheda SIM fisica e, in particolare, è un software embeddato in un chip eUICC1. GSMA2 la definisce come la SIM per la prossima generazione di dispositivi connessi in rete. Con lei è possibile attivare virtualmente il proprio numero di telefono in pochi passaggi a partire semplicemente da un QR code. Una volta che la eSIM viene installata nell’eUICC, opererà esattamente come una SIM fisica e avrà un **ICCID** (**integrated circuit card identifier**) unico e una **network authentication key**.  
La eSIM consente a un dispositivo di supportare più profili di operatori di rete contemporaneamente, il che significa che l’utente può cambiare operatore senza dover sostituire fisicamente la scheda SIM.

*1 Un chip eUICC (embedded Universal Integrated Circuit Card) è un tipo di chip SIM utilizzato nei dispositivi mobili che, a differenza delle tradizionali SIM card, sono integrate direttamente nei dispositivi (i.e. non sono rimovibili) e sono progettate per essere programmate a distanza.*

*2 GSMA (GSM Association) è un’organizzazione industriale che rappresenta gli interessi degli operatori delle reti virtuali in tutto il mondo.*

**5G**

**Definizione**Il termine **5G** (acronimo di **5th Generation**) indica l’insieme di tecnologie di telefonia mobile e cellulare, i cui standard definiscono la quinta generazione della telefonia mobile.

**Caratteristiche generali**  
- Ottimizzazione dell’uso delle risorse di rete mediante la definizione di sottoreti virtuali indipendenti per ogni tipologia del servizio (**network slicing**).  
- Virtualizzazione di gran parte dei dispositivi di rete.  
- Capacità di gestire una maggiore quantità di dispositivi per unità di superficie.  
- Supporto di caratteristiche più spinte in termini di latenza per garantire tempi di risposta in “tempo reale”.  
- Maggiore velocità di trasmissione dei dati (teoricamente fino a 10 Gbit/s).  
- Riduzione significativa del consumo energetico (90% in meno rispetto alla 4G per ogni bit trasmesso).

Come le generazioni precedenti, la rete 5G è una rete cellulare di tipo digitale, in cui la zona coperta dal servizio è suddivisa in piccole aree geografiche denominate **celle**. Tutti i dispositivi 5G all’interno di una cella ricevono e trasmettono il segnale via radio all’antenna locale, che a sua volta è collegata alla rete telefonica e a Internet tramite fibra ottica o via ponte radio. Come in tutte le reti cellulari, i dispositivi mobili che si spostano da una cella all’altra vengono presi in carico automaticamente e in modo trasparente dalla nuova cella senza perdere il collegamento.

L’aumento della velocità di trasferimento dei dati si ottiene in parte utilizzando frequenze radio più elevate. Tuttavia, a frequenze radio più elevate corrisponde anche un raggio di portata ridotto, il che comporta celle più piccole. Per assicurare un servizio ampio, le reti 5G utilizzano tre bande di frequenza: bassa, media e alta. Di conseguenza, una rete 5G è composta da tre tipi di celle differenti a seconda della banda di frequenza associata, ognuna con un proprio tipo di antenna:  
-> Le celle in banda bassa trasmettono sulla gamma di frequenze compresa tra 694 e 790 MHz. Qui la portata e l’area di copertura delle celle radio è simile a quelle 4G operanti a 800 MHz.  
-> Le celle in banda media impiegano microonde a 2,5-3,7 GHz, che consentono una dimensione della cella del raggio di alcuni chilometri.  
-> Le celle in banda alta utilizzano frequenze a 25-39 GHz, prossime alla banda delle onde millimetriche, che però richiedono molte celle di piccole dimensioni. A causa dei loro costi elevati, queste celle vengono attualmente distribuite solo in ambienti urbani densamente popolati e nelle aree in cui si riuniscono folle di persone (e.g. stadi).

Network slicing:  
È un’architettura di rete che consente di definire sulla medesima infrastruttura fisica un insieme di reti virtuali indipendenti tra loro e in grado di funzionare contemporaneamente e senza interferenze, come se ognuna di loro avesse una rete fisica dedicata. Ogni fetta di rete è a tutti gli effetti una rete completa appositamente ritagliata per soddisfare tutti i requisiti di livello di servizio di una particolare applicazione (**Service Level Requirement**, **SLR**). La realizzazione della visione di rete come orientata ai servizi si basa sui concetti di **software-defined networking** (**SDN**) e di virtualizzazione delle funzioni di rete (**Network Functions Virtualization**, **NFV**).  
Da un punto di vista del modello di business, ogni partizionamento di rete è amministrato da un operatore virtuale di rete mobile (**Mobile Virtual Network Operator**, **MVNO**). Il gestore dell’infrastruttura affitta le sue risorse fisiche agli operatori virtuali che condividono la stessa rete fisica e, a seconda della disponibilità delle risorse assegnate, ogni MVNO può a sua volta realizzare le sue *network slice* adattate alle applicazioni offerte ai suoi utenti. Ciò consente alla rete 5G di poter essere utilizzata a tutti gli effetti come Internet Service Provider su infrastruttura di tipo mobile.

**Tecnologie**  
Nuove frequenze radio:  
Il consorzio industriale che definisce gli standard per la tecnologia 5G è il **Third Generation Partnership Project** (**3GPP**), che prevede due bande di frequenza:  
-> **FR1**: banda media o bassa (sotto ai 6 GHz).  
-> **FR2**: banda alta (sopra i 24 GHz). Sappiamo che è una banda di frequenza che richiede celle di piccole dimensioni con stazioni radio base ravvicinate; inoltre, a causa delle caratteristiche fisiche delle onde millimetriche, la trasmissione a queste frequenze è ostacolata o attenuata da oggetti solidi come automobili, alberi e alcuni tipi di muri. Per questo motivo, le celle 5G sono volutamente progettate e posizionate in modo da coprire aree il più possibile prive di tali ostacoli, come ad esempio l’interno dei ristoranti o dei centri commerciali.

Dimensionamento delle celle:



MIMO massivo:  
È una tecnologia di tipo **MIMO** (**multiple-input multiple-output**) che sfrutta la disponibilità di più terminali radio indipendenti al fine di migliorare le capacità di trasferimento e la capacità di comunicazione di ogni singolo terminale.

Edge computing:  
Viene fornito da server dedicati vicini all’utente finale e il suo scopo è ridurre la latenza e la congestione sul traffico dei dati.

Small cell:  
Dette anche *piccole celle*, sono nodi di accesso radio cellulare a basso consumo e hanno una copertura che varia dai dieci metri fino a qualche chilometro. Come abbiamo già detto, sono cruciali nel momento in cui le onde radio con frequenze elevate non sono in grado di coprire lunghe distanze.

Filtraggio spaziale:  
Detto anche **beamforming**, viene usato per dirigere le onde radio verso un destinatario preciso. È una tecnica che si basa sull’utilizzo di antenne in fase e consiste nel modulare la potenza dei singoli elementi di antenna in modo tale da generare interferenza costruttiva sui segnali diretti verso un determinato angolo e distruttiva sui segnali diretti verso angolazioni differenti.

NOMA (Non-Orthogonal Multiple Access):  
È una tecnica di accesso multiplo in cui più utenti vengono serviti usando la stessa risorsa in termini di frequenza, spazio e tempo. L’accesso multiplo viene garantito assegnando a ogni utente un livello di potenza differente in funzione della sua distanza dalla stazione base. Questa tecnica tuttavia presenta una serie di problemi legati all’aumento di interferenza dovuta alla condivisione della risorsa e alla sicurezza e privacy dei dati.

SDN/NFV:  
Il software-defined networking (SDN) consente di realizzare in tempo reale il partizionamento della rete alla base del network slicing, di gestire ogni slice come se fosse una rete indipendente e di coordinare in modo dimanico e automatizzato la distribuzione complessiva delle risorse tra gli slice (e.g. allocando banda dove e quando serve sulla base delle caratteristiche e delle richieste momentanee del servizio).  
La virtualizzazione delle funzioni di rete (NFV) è anch’essa funzionale a questo modello di gestione sia per abbattere i costi di infrastruttura, sia per integrare servizi più sofisticati sfruttando soluzioni basate più sul software che sull’hardware.

**Sicurezza informatica**  
Nell’ottobre 2018, un team di ricercatori appartenenti al Politecnico federale di Zurigo, all’università della Lorena e all’università di Dundee ha pubblicato il documento ***A Formal Analysis of 5G Authentication*** in cui avvisava che la tecnologia 5G potrebbe aprire la strada a una nuova serie di minacce alla sicurezza, definendo il 5G come una tecnologia “immatura e non sufficientemente testata”.  
In parallelo, aziende specializzate nella sicurezza informatica come Fortinet, Arbor Networks, A10 Networks e Voxility hanno annunciato la realizzazione di soluzioni di sicurezza personalizzate e miste contro attacchi massicci di tipo DoS previsti come conseguenza dello sviluppo delle reti 5G.  
Nel gennaio 2020, il gruppo di cooperazione NIS dell’Unione europea ha adottato il ***pacchetto di strumenti dell’UE sulla cibersicurezza del 5G***, che specifica una serie di misure volte ad affrontare le minacce alla sicurezza delle reti 5G.

**5G SA**

**Introduzione**Attualmente è ancora in vigore la tecnologia **5G Non-Standalone** (**5G NSA**), che è nota come *non autonoma* poiché si appoggia alla rete sottostante 4G sia per gestire la connessione radio che per la commutazione dei servizi (core network). Di conseguenza, un terminale 5G NSA dev’essere sempre collegato alla rete 4G, anche quando sta scambiando dati attraverso la rete 5G.  
L’architettura **5G Standalone** (**5G SA**) prevede invece che la rete 5G sia del tutto autonoma, ovvero che ci sia un terminale 5G connesso a una rete radio 5G, a sua volta collegata a una core network 5G senza altri intermediari.

**Vantaggi**  
- Migliore connettività alle reti.  
- Riduzione della latenza.  
- Incremento della copertura.  
- Maggiore sicurezza: sono implementate non solo tutte le funzionalità incluse nella 4G ma anche protocolli di sicurezza aggiornati a livello core network.  
- Riduzione dei consumi delle batterie dei dispositivi mobili.

**SDR**

**Introduzione  
Software-defined radio** (**SDR**) è un sistema di comunicazione radio dove i componenti che tradizionalmente sono stati implementati nell’hardware analogico (e.g. mixer, filtri, amplificatori, modulatori/demodulatori, detector) vengono qui implementati mediante porzioni di software su un PC o un sistema embedded. In particolare, un sistema SDR di base può consistere in un PC equipaggiato con una scheda audio (o un qualunque altro convertitore analogico-digitale3) preceduta da una qualche forma di RF front-end4. Tale tipo di design dà luogo a una vera e propria radio che può ricevere e trasmettere protocolli radio ampiamente diversi e basati unicamente sull’uso di software.  
SDR ha un’utilità molto significativa sia per i servizi nell’ambito militare che per i servizi per i dispositivi mobili.

**Vantaggi**- Maggiore flessibilità.  
- Maggiore efficienza spettrale.  
- Possibilità di configurare un sistema SDR in modo da elaborare simultaneamente più segnali audio, aumentando così la capacità di elaborazione dei segnali.  
- Possibilità di aggiornare il software per supportare nuove funzionalità.  
- Possibilità di modificare determinati parametri del segnale (e.g. frequenza di lavoro, larghezza di banda, modulazione) mediante il software, senza dover toccare l’hardware del sistema.

*3 Un convertitore analogico-digitale è un sistema che converte un segnale analogico (e.g. un suono preso da un microfono) in un segnale digitale.*

*4 L’RF front-end (front-end di radiofrequenza) è una parte di un sistema elettronico che gestisce (elaborando e manipolando) i segnali radio e le onde elettromagnetiche all’ingresso del sistema.*

**LTE**

**Introduzione**Il **Long Term Evolution** (**LTE**) è una tecnologia di accesso radio utilizzata nelle reti cellulari per fornire servizi di comunicazione wireless ad alta velocità e alta affidabilità. Nasce come nuova generazione per i sistemi di accesso mobile a banda larga (Broadband Wireless Access). In particolare, si pone come obiettivo migliorare le prestazioni e la copertura offerte dalla tecnologia 4G (utilizzando comunque quest’ultima).  
La standardizzazione di LTE è stata completata dal 3GPP nel 2008.

**Descrizione**  
LTE è parte integrante dello standard UMTS5 ma prevede diverse modifiche e migliorie6 fra cui:  
- Efficienza spettrale7 tre volte superiore alla versione più evoluta dell’UMTS, ovvero l’HSPA (High Speed Packet Access).  
- Velocità di trasferimento dati in scaricamento fino a 326,4 Mbit/s.  
- Velocità di trasferimento dati in caricamento fino a 86,4 Mbit/s.  
- Velocità di trasferimento dati al bordo della cella da due a tre volte superiore all’UMTS / HSPA.  
- RTT inferiore ai 10 ms (contro i 70 ms dell’HSPA e i 200 ms dell’UMTS).  
- Ottimo supporto in mobilità: sono state registrate prestazioni elevate fino a 350 km/h, o addirittura fino a 500 km/h, a seconda della banda di frequenza usata.

Tecnologie introdotte da LTE:  
-> **OFDM (Orthogonal Frequency-Division Multiplexing)**: è una tecnologia che permette di ottenere un elevato rate di dati trasmessi pur mantenendo un alto livello di robustezza nei confronti delle interferenze. Il suo funzionamento consiste nel suddividere la banda in molteplici sotto-portanti, ciascuna delle quali trasporta uno stream di dati separato ed è ortogonale alle altre sotto-portanti: ciò implica che le varie sotto-portanti sono matematicamente indipendenti e non si interferiscono tra loro.  
-> **MIMO (Multiple-Input Multiple-Output)**: uno dei problemi principali dei sistemi di telecomunicazione precedenti è relativo ai cammini multipli ed è dovuto alla presenza di palazzi o oggetti che provocano la riflessione dei segnali (multipath fading). Il MIMO permette di trarre giovamento da tale situazione, andando a combinare tra loro i vari segnali ricevuti. Quando si usa il MIMO è necessario utilizzare più antenne per permettere di distinguere i segnali che provengono da percorsi diversi; mentre è facile aggiungere antenne dal lato delle stazioni radio base, lo stesso non si può dire dal lato del terminale dove le dimensioni limitano il numero di antenne che è possibile installare.  
-> **SAE (System Architecture Evolution)**: molte funzioni, precedentemente gestite dalla core network, sono state trasferite verso la periferia della rete. Questo conferisce alla rete una forma “piatta“ che consente di ridurre notevolmente i tempi di latenza.

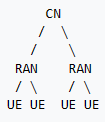
*5 UMTS (Universal Mobile Telecommunications System) è un sistema di telecomunicazioni wireless di terza generazione (3G) utilizzato per fornire servizi di comunicazione vocale e dati su reti mobili.*

*6 Come accennato in precedenza, molte delle migliorie sono anche rispetto alla tecnologia 4G tradizionale.*

*7 L’efficienza spettrale è pari al numero di bit al secondo trasmessi per ogni hertz dell’onda portante.*

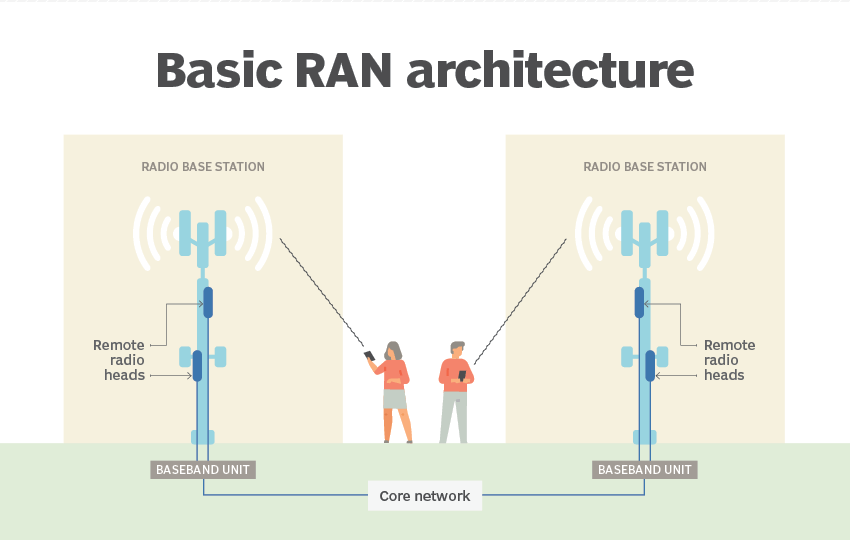
**RAN**

**Introduzione**Una **radio access network** (**RAN**) è una parte fondamentale dell’architettura delle reti cellulari. Concettualmente, risiede tra un dispositivo (e.g. un dispositivo mobile o un computer) e la core network (CN), che gestisce le informazioni e la locazione degli utenti finali. In particolare, connette i dispositivi alla core network tramite un collegamento radio. Dipendentemente dallo standard, i dispositivi sono nominati user equipment (UE), terminal equipment (TE), mobile station (MS) e così via.  
Le funzionalità di RAN sono tipicamente fornite da un circuito integrato che risiede sia nella core network che nello user equipment.



**Vantaggi**  
- Richiede meno componenti hardware e sistemi meno costosi.  
- Aumenta la flessibilità.  
- Offre la possibilità di attivare e disattivare i carichi di lavoro col minimo intervento.  
- Consente di aumentare e ridurre le risorse in modo flessibile per rispondere a esigenze di rete in continua evoluzione.

**Componenti di una RAN**  
-> Antenne: convertono i segnali elettrici in onde radio.  
-> Radio: trasformano le informazioni digitali in segnali che possono essere inviati in modalità wireless e assicurano che le trasmissioni avvengano con la frequenza e la potenza corrette.  
-> Baseband unit (BBU): forniscono un insieme di funzioni di processamento dei segnali che rendono possibile la comunicazione wireless; in particolare, rilevano gli errori e rendono sicuro il segnale wireless.



**eNodeB / gNodeB**

**Cos’è un eNodeB (Evolved Node B)?**È una stazione base della rete mobile LTE che fornisce la connessione wireless tra i dispositivi mobili e la rete di trasporto centrale. Tra le funzioni dell’eNodeB ci sono la gestione delle risorse di frequenza, il controllo dell’accesso al canale radio, la modulazione / demodulazione dei dati e la gestione delle informazioni di controllo per la comunicazione tra il dispositivo mobile e la rete centrale.

**Cos’è un gNodeB (Next Generation Node B)?**È una stazione radio base che trasmette e riceve segnali radio nella rete 5G e fornisce la connessione tra i dispositivi utente e la rete di comunicazione. Si occupa di funzioni come la modulazione / demodulazione dei segnali radio, il controllo del flusso di dati e la gestione delle risorse radio. È anche progettato per supportare nuove funzionalità che non erano disponibili nelle generazioni precedenti di stazioni radio base, come ad esempio la tecnologia beamforming, che permette di indirizzare il segnale radio verso un dispositivo utente specifico per aumentare la qualità e la velocità della connessione.

**SMDP**

**Introduzione**Il protocollo Subscription Manager Data Preparation (SMDP) è una tecnica di provisioning che viene utilizzata per configurare le schede SIM dei dispositivi mobili in modo automatico e remoto, senza la necessità di interventi manuali da parte degli utenti finali. In sostanza, il protocollo SMDP fornisce alle reti mobili un modo per gestire e configurare in modo centralizzato le schede SIM dei dispositivi mobili.

**Funzionamento**  
Di seguito sono riportati alcuni dettagli tecnici del funzionamento del protocollo SMDP:  
-> Il protocollo SMDP è basato su HTTPS per fornire una comunicazione sicura e crittografata tra i dispositivi mobili e il server SMDP.  
-> Il protocollo SMDP utilizza il protocollo di autenticazione SIM (SIM Authentication Protocol) per verificare l'identità della scheda SIM del dispositivo mobile che richiede la configurazione.  
-> Il protocollo SMDP utilizza il protocollo Remote SIM Provisioning (RSP) per gestire la comunicazione tra il server SMDP e la scheda SIM del dispositivo mobile. Il protocollo RSP definisce le operazioni di provisioning specifiche per la configurazione della scheda SIM.  
-> Il protocollo SMDP utilizza il protocollo Over-the-Air (OTA) per trasferire le informazioni di configurazione alla scheda SIM del dispositivo mobile. Il protocollo OTA è un metodo di trasferimento dati wireless utilizzato per la configurazione remota di dispositivi mobili.

Il processo di provisioning delle schede SIM utilizzando il protocollo SMDP si svolge in diverse fasi. In primo luogo, il dispositivo mobile richiede al server SMDP di registrare la scheda SIM con la rete mobile. Il server SMDP risponde fornendo una serie di parametri di configurazione che la scheda SIM utilizzerà per la configurazione del dispositivo mobile. Successivamente, la scheda SIM del dispositivo mobile utilizza il protocollo RSP per comunicare con il server SMDP e ottenere le informazioni di configurazione necessarie. La scheda SIM utilizza poi il protocollo OTA per scaricare le informazioni di configurazione dal server SMDP e configurare il dispositivo mobile per l'utilizzo con la rete mobile.

**DEPLOYMENT eSIM**

**Introduzione**Il protocollo di deployment di una eSIM è il processo mediante il quale le informazioni di identità dell'utente e le credenziali di autenticazione sono trasferite dalla rete mobile al dispositivo mobile attraverso una connessione sicura e crittografata. Il protocollo è stato sviluppato per consentire alle reti mobili di configurare le eSIM dei dispositivi mobili in modo automatico e remoto, senza la necessità di interventi manuali da parte degli utenti finali.

**Funzionamento**  
Ecco una descrizione tecnica del funzionamento del protocollo di deployment di una eSIM:  
1) Inizializzazione della connessione: il dispositivo mobile si connette al server della rete mobile utilizzando una connessione sicura. La connessione può essere stabilita tramite la rete mobile o attraverso una connessione Wi-Fi / Ethernet.  
2) Autenticazione: il server della rete mobile verifica l'identità del dispositivo mobile e della sua eSIM utilizzando la crittografia a chiave pubblica. Questo processo avviene attraverso lo scambio di certificati digitali.  
3) Creazione del profilo utente: il server della rete mobile crea un profilo utente per l'eSIM, includendo le informazioni di identità dell'utente e le credenziali di autenticazione. Il profilo utente viene quindi memorizzato nel database della rete mobile.  
4) Provisioning: il profilo utente viene trasferito dall'operatore di rete mobile al dispositivo mobile attraverso una connessione sicura, utilizzando il protocollo Over-the-Air (OTA). Il processo di provisioning è crittografato per garantire la sicurezza delle informazioni di identità dell'utente e delle credenziali di autenticazione.  
5) Attivazione: il dispositivo mobile attiva l'eSIM utilizzando le informazioni di profilazione e le credenziali di autenticazione ricevute dalla rete mobile. L'eSIM viene quindi utilizzata per l'accesso alla rete mobile.

Inoltre, il protocollo di deployment di una eSIM supporta la personalizzazione delle eSIM, consentendo agli operatori di rete mobile di configurare le eSIM per soddisfare le esigenze specifiche di ogni utente. La personalizzazione può includere l'installazione di applicazioni e la configurazione di servizi specifici.

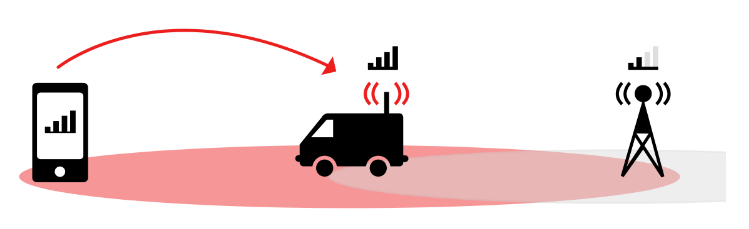
**Protocollo di deployment di una eSIM vs SMDP**Il protocollo di deployment di una eSIM e il protocollo SMDP sono strettamente correlati tra loro e si integrano per garantire la gestione sicura e affidabile delle eSIM nel contesto delle reti mobili.

**IMSI-CATCHER**

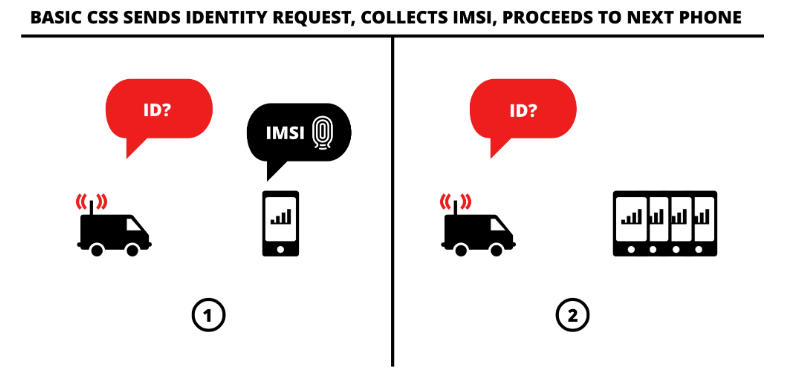
**Introduzione**I **Cell Site Simulator** (**CSS**), noti anche come **Stingray** o **IMSI-catcher**, sono dispositivi utilizzati per intercettare e raccogliere informazioni sul traffico delle comunicazioni cellulari. Simulano una torre di cella legittima e attirano i dispositivi mobili nella loro area di copertura, intercettando le comunicazioni tra il telefono e la rete.

**Terminologia**  
-> IMSI (International Mobile Subscriber Identity): è un identificatore univoco collegato a una SIM, che rappresenta un elemento utilizzato per autenticare l’utente finale alla rete mobile. È pensato per essere privato anche perché potrebbe rivelare la posizione fisica e delle informazioni sensibili del dispositivo mobile (come le telefonate e i messaggi).

**Attacco IMSI-catcher di base**  
Nelle reti GSM (2G), gli IMSI-catcher classici catturano semplicemente gli IMSI degli utenti vicini fingendo di essere delle stazioni radio base reali, ma non hanno altre interazioni significative coi dispositivi target.  
Entrando più nel dettaglio, i dispositivi tipicamente provano a connettersi a una qualunque stazione radio base che stia trasmettendo alla massima potenza del segnale.



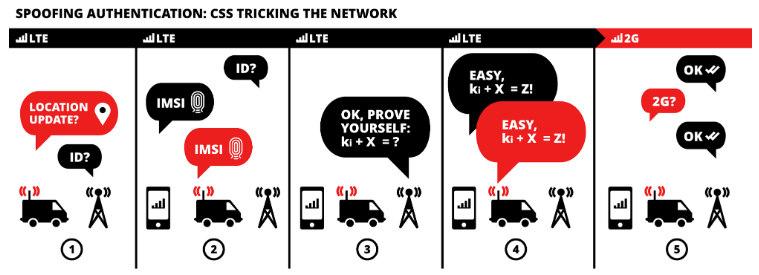
Stabilita la connessione, la stazione radio base chiede al dispositivo quali sono gli algoritmi di encryption che supporta: se si tratta di un CSS anziché di una torre di cella legittima, può anche fare in modo che non venga stabilito alcun algoritmo di encryption.  
Dopodiché, la stazione radio base invia un’Identity Request, a cui il dispositivo risponde col proprio IMSI. Questa è un’azione necessaria poiché l’IMSI è memorizzata nella SIM (che è stata rilasciata da un particolare operatore telefonico) e la rete telefonica ha bisogno di identificare che l’utente sia effettivamente un customer (che paga) associato all’operatore telefonico.  
Dopo aver ricevuto l’IMSI, il CSS rilascia il dispositivo mobile alla rete mobile e prova a connettersi ad altri telefoni, sempre con lo scopo di catturarne l’IMSI.



**Intercettazione della comunicazione**  
L’intercettazione della comunicazione tra un dispositivo mobile e una torre di cella legittima è possibile solo in GSM, poiché:  
- La comunicazione su GSM non richiede sempre l’encryption.  
- Anche quando l’encryption è abilitata, molti algoritmi crittografici utilizzati possono essere bucati in real time.

Un CSS che vuole effettuare un attacco attivo dove intercetta le comunicazioni di un dispositivo deve essere in grado di performare un **MITM**, piazzandosi tra il dispositivo mobile e la torre di cella. Per far questo, si seguono due step:  
1) **Spoofing authentication**: il CSS deve convincere la rete mobile che lui è effettivamente un dispositivo mobile.  
2) **Breaking encryption**: il CSS deve provare a disabilitare o bucare gli algoritmi di encryption che la rete mobile prova a impostare.

Spoofing authentication:  
Avviene secondo i seguenti step:  
1) Il CSS performa un attacco IMSI-catcher di base per ottenere l’IMSI di un qualche dispositivo mobile.  
2) Il CSS invia a una torre di cella legittima una **Location Update Request**, che è una richiesta usata dai dispositivi per aggiornare la rete mobile sulla loro locazione (specificatamente il LAC – Location Area Code).  
3) La torre di cella risponde con una challenge cifrata che richiede la chiave segreta Ki per essere risolta (che è la chiave installata all’interno della SIM). Poiché il CSS non ha accesso a Ki, passa la challenge cifrata al dispositivo mobile, il quale decifra la challenge e la restituisce al CSS; quest’ultimo, infine, inoltra la challenge decriptata alla torre di cella.  
4) A questo punto viene stabilita la connessione tra la rete mobile e il CSS (che risulta essere autenticato).



Breaking encryption:  
Esistono diversi algoritmi di encryption usati in GSM e hanno nomi come A5/1, A5/2, ecc. D’altra parte, A5/0 indica l’assenza di un algoritmo di cifratura.  
Se la rete mobile specifica di voler comunicare usando l’encryption, il CSS può semplicemente rispondere di non avere alcuna capability di encryption e si imposta a A5/0. A questo punto, il CSS ha completato l’attacco MITM e può leggere i messaggi plaintext tra la rete e il dispositivo mobile.  
In alternativa, è possibile negoziare un algoritmo di encryption debole (come A5/1) e bucarlo in real time durante la comunicazione tra la rete e il dispositivo mobile.

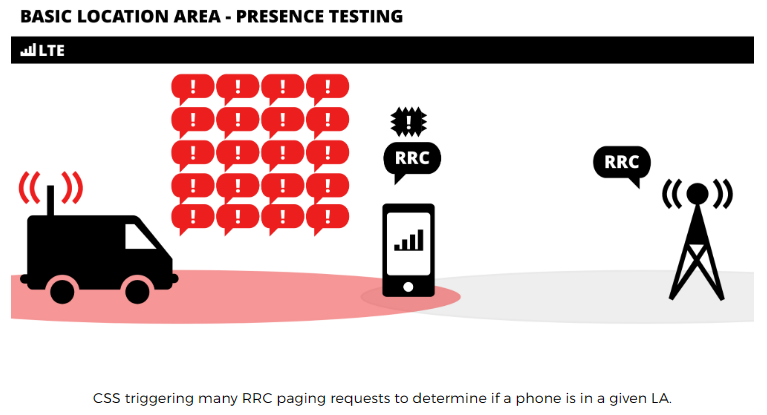
**Tecniche di connessione del CSS in LTE**  
Sappiamo che in GSM è facile per un CSS connettersi ai dispositivi mobili spacciandosi per torre di cella legittima poiché i dispositivi si connettono a una qualunque stazione radio base che stia trasmettendo alla massima potenza del segnale.  
Ciò non vale ad esempio in LTE, dove i dispositivi mantengono una lista delle stazioni più vicine ottenuta da parte della torre di cella a cui sono connessi. Qui, se per qualche motivo un dispositivo perde la connessione con la torre, proverà a connettersi con un’altra torre riportata nella lista, prima di effettuare uno scan completo delle stazioni radio base presenti nelle vicinanze.  
Un CSS può dunque effettuare due tipi di attacchi:  
-> Spacciarsi per una torre presente nella lista delle stazioni più vicine (utilizzando la stessa frequenza, lo stesso ID di cella, ecc.) e trasmettere a una potenza superiore.  
-> Sfruttare il fatto che le frequenze in LTE sono associate a priorità diverse: se un dispositivo mobile vede che esiste una stazione radio base che opera a una frequenza a priorità maggiore rispetto a quella a cui è attualmente connesso, dovrà switchare a tale stazione più prioritaria indipendentemente dalla potenza del segnale. Per scoprire quali sono le frequenze a priorità più elevate in una determinata zona, basta recuperarle da messaggi di configurazione non cifrati provenienti dalle stazioni radio base.

**Location tracking attack**  
È un tipo di attacco che può avvenire in due modi:  
-> **Presence testing**: il CSS verifica se un dispositivo mobile è presente o meno in una Location Area (i.e. in un determinato gruppo di celle).  
-> **Fine-grained location**: il CSS scopre le coordinate GPS di un dispositivo mobile attraverso la trilaterazione (e facendo in modo che sia il telefono a comunicare all’attaccante le proprie coordinate GPS).

Presence testing:  
Il presence testing può a sua volta avvenire secondo modalità differenti. Analizziamole una per volta.

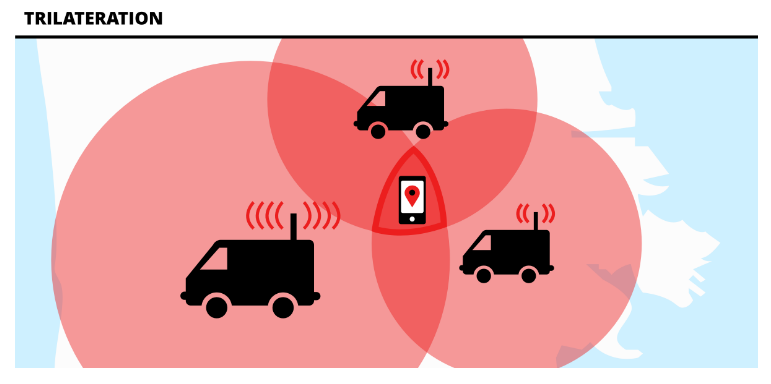
1) **Passive presence testing**: qui per l’attaccante è sufficiente scansionare i segnali disponibili all’interno della rete.  
Da una parte si ha il modello di paging: quando la rete ha una chiamata o un messaggio da instradare verso un dispositivo mobile, invia un messaggio “RRC paging” (dove RRC sta per Radio Resource Control) ai vari telefoni, chiedendo a questi ultimi di contattare la stazione radio base per negoziare il completamento di una connessione (in modo da stabilire se si deve ricevere una particolare chiamata o messaggio). Pertanto, i telefoni sono sempre in ascolto in attesa di messaggi “RRC paging” e scartano quelli che non sono direttamente rivolti a loro.  
D’altra parte, i dispositivi mobili trasmettono periodicamente messaggi non cifrati che spesso specificano la loro locazione GPS esatta ma, in ogni caso, contengono anche informazioni sulla potenza del segnale delle torri di cella vicine: queste ultime informazioni sono sufficienti per calcolare la posizione del dispositivo mobile.

2) **Basic Location Area test**: qui l’attaccante triggera l’invio di messaggi “RRC paging” effettuando delle telefonate verso il dispositivo target. Per non allertare l’utente vittima, l’attaccante può riattaccare subito dopo aver inizializzato la chiamata in modo tale che l’utente non riceva alcuna notifica di chiamata (seppur l’invio di messaggi “RRC paging” sia sempre triggerato). Si tratta di una tecnica che funziona in modo semplice perché in genere le telefonate sono considerate delle richieste ad alta priorità (per cui vengono notificate *tutte* le torri di cella appartenenti alla Location Area in cui si trova correntemente il dispositivo target).  
Nella pagina seguente è riportato uno schema riassuntivo che descrive l’esecuzione del basic Location Area test.

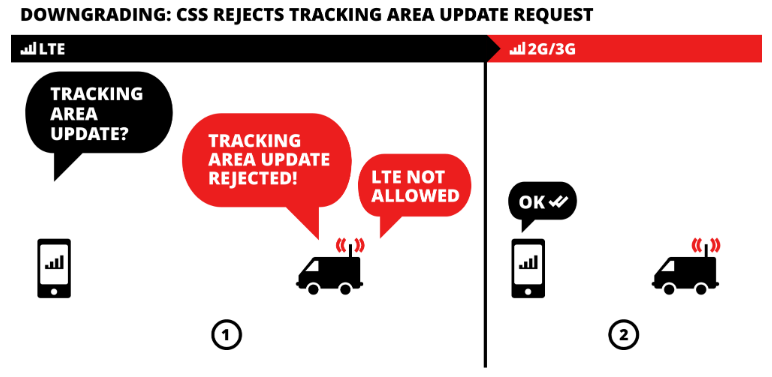


3) **Smart paging test**: qui l’attaccante triggera l’invio di messaggi “RRC paging” inviando dei messaggi (e.g. Whatsapp o Messenger) verso il dispositivo target. Stavolta, poiché i messaggi sono considerati come delle richieste a bassa priorità, viene notificata solo l’ultima torre di cella a cui il dispositivo target è / era connesso. Di conseguenza, affinché l’attacco abbia successo, l’attaccante dovrebbe avere un equipaggiamento per ogni singola cella (il che è molto costoso) oppure dovrebbe ripetere la procedura per tutte le celle finché non ottiene un match.

Fine-grained location:  
Supponiamo che il CSS attaccante abbia stabilito una connessione con un dispositivo mobile con le tecniche spiegate in precedenza. A questo punto invia al dispositivo mobile il comando “RRC Connection Reconfiguration”, che contiene il cell ID di almeno tre torri di cella vicini e le relative frequenze di connessione. La risposta del dispositivo a questo comando contiene la potenza del segnale proveniente dalle tre torri di cella; tale potenza è funzione della distanza tra il telefono e le torri stesse (chiaramente, più il segnale è forte, più la distanza è ridotta). Con queste informazioni, è possibile disegnare tre circonferenze, ciascuna delle quali ha come centro la relativa torre di cella e come raggio una lunghezza che è funzione della potenza del segnale. La tecnica della trilaterazione prevede che il dispositivo mobile si trovi in un punto appartenente all’intersezione tra le tre circonferenze.



**Protocol downgrade attack**  
Supponiamo anche qui che il CSS attaccante abbia stabilito una connessione con un dispositivo mobile con le tecniche spiegate in precedenza. Dopo la procedura di connessione iniziale, il telefono invia una richiesta **TAU** (**Tracking Area Update**), che serve a mantenere la rete mobile aggiornata sulla locazione più recente del telefono stesso, in modo tale che la rete possa instradare le chiamate più velocemente. Il CSS risponde con un messaggio “TAU reject” in cui viene specificato il codice errore 7 (che significa “LTE services not allowed”). A questo punto, il dispositivo considera la sua SIM come invalida per LTE, per cui inizia a cercare reti 3G o GSM per connettersi e non proverà più a negoziare una connessione LTE finché non verrà riavviato.



**Denial of Service (DoS)**È un attacco che avviene con le stesse identiche modalità descritte per il protocol downgrade attack, con l’unica differenza che il messaggio “TAU reject” inviato dal CSS non ha 7 più come codice di errore, bensì 8 (che significa “LTE and non-LTE services not allowed”).

**ASN.1**

**Cos’è ASN.1?**È uno standard di codifica per rappresentare dati strutturati in forma binaria ed è stato sviluppato per supportare la trasmissione di dati tra sistemi e dispositivi diversi. Viene utilizzato in molti protocolli di rete (come TLS) nonché in svariati ambiti come la sicurezza informatica, la crittografia e l’e-commerce.

Esempio:  
Person ::= SEQUENCE {  
 name VisibleString,  
 age INTEGER  
}

Qui l'oggetto ASN.1 è definito come una sequenza di due elementi: il nome e l'età della persona. Il nome è rappresentato come una stringa visibile (VisibleString), mentre l'età è rappresentata come un numero intero (INTEGER).