UNIVERSITÀ
DEGLI STUDI
DI PADOVA

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

CORSO DI LAUREA IN INGEGNERIA INFORMATICA

ATTACCO DI TIPO DENIAL OF SERVICE ALLE RETI CELLULARI

Relatore: Prof. Mauro Migliardi

Laureando: Stefano Leggio

ANNO ACCADEMICO: 2020-2021

Data di laurea: 20/09/2021

Sommario

In un mondo sempre più interconnesso, l'attacco di tipo *denial of service* alle reti cellulari assume sempre più pericolosità. In questa tesi verranno illustrate le più comuni vulnerabilità che vengono sfruttate, in particolare al sistema di autenticazione degli utenti. Verrà inoltre condotta una comparazione sulla sicurezza delle reti di quinta generazione e quelle precedenti.

Indice

Elenco delle figure

Elenco delle abbreviazioni

BS *Base Station.*

DOS *Denial Of Service.*

IOT *Internet Of Things.*

MS *Mobile system.*

RAN *Radio Access Network.*

SIM *Subscriber Identity Module.*

UE *User Equipment.*

Capitolo 1

Introduzione

Le reti cellulari rappresentano un punto nevralgico per le nostre comunicazioni. Per questo, la loro sicurezza è fondamentale per garantire un normale funzionamento di tutti i servizi a cui ormai ci siamo abituati.
La nuova tecnologia di quinta generazione è ormai vicina ad essere implementata su larga scala per permettere lo sviuluppo del mondo dell'*Internet Of Things* (IOT). Questa nuova tecnologia stravolge numerosi paradigmi strutturali che sono stati utilizzati fin'ora nelle generazioni precedenti, introducendo nuove sfide nell'ambito della loro sicurezza.

1.1 Struttura del documento

Il documento è strutturato in modo da fornire al lettore le competenze e terminologie adeguate per comprendere tutti i dettagli delle vulnerabilità trattate.
L'elaborato inizia con una breve panoramica sulla rete cellulare, descrivendo genericamente la sua struttura e architettura.
Dato che le specifiche dell'architettura di una rete cellulare sono molto diverse a seconda della generazione, è stato necessario illustrare l'evoluzione delle varie tecnologie: da 1G a 5G. Per ogni generazione verranno illustratate prevalentemente le sue propietà architetturali oltre che le principali novità introdotte.
Successivamente, verrà introdotta la tipologia dell'attacco trattato, ossia il *Denial Of Service* (DOS), spiegando in cosa consiste e come si applica alle reti cellulari. Inoltre, verranno illustrate le misurazioni necessarie per valutare l'efficienza di un attacco.
Tra le tante vulnerabilità che possono essere sfruttate per generare un DOS, questo documento si vuole soffermare sull'analisi dell'attacco all'autenticazione. Per comprendere le vulnerabilità in questo ambito verranno analizzati nel dettaglio i sistemi di autenticazione per le varie generazioni cellulari.
Nel capitolo seguente verranno introdotti gli attacchi all'autenticazione delle reti 2G-4G, spiegando il loro funzionamento di base e citando vari studi che hanno permesso di quantificare la pericolosità di questi attacchi.
Infine, verranno analizzati gli attacchi DOS alle reti 5G, specificando quali miglioramenti o peggioramenti sono stati introdotti dalla sua nuova architettura.

1.2 Scopo della tesi

Questo elaborato vuole descrivere il funzionamento degli attacchi di tipo DOS alle reti cellulari, in particolare al meccanismo di autenticazione degli utenti.
Infine, si vuole scoprire se le vulnerabilità delle generazioni 2G-4G sono state risolte nel 5G.

Capitolo 2

La rete cellulare

La rete cellulare è la struttura *hardware* e *software* che consente il corretto funzionamento delle comunicazioni tramite i dispositivi cellulari, dalle normali comunicazioni vocali alle *smart cities* nel 5G.
Grazie ad una fitta rete di antenne, i gestori telefonici riescono a garantire il servizio per la gran parte del territorio mondiale.

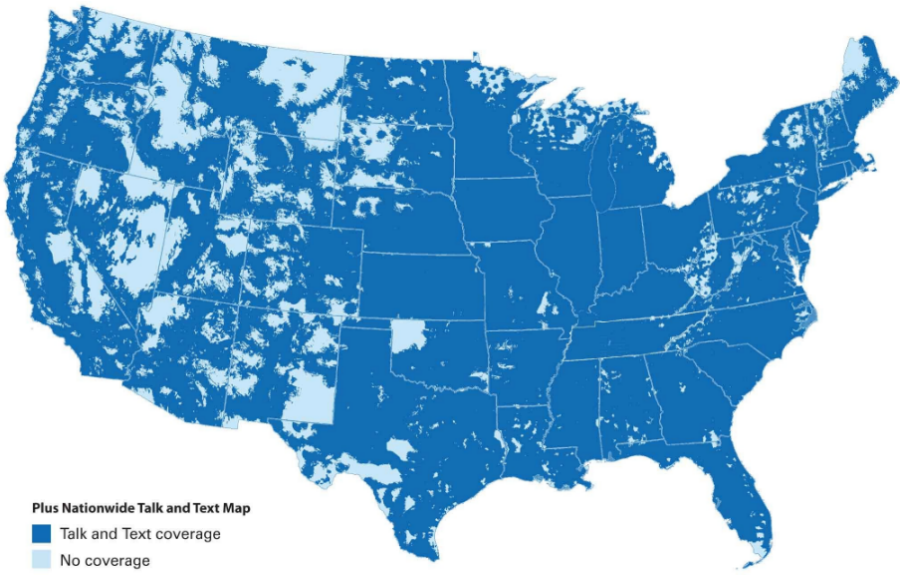

Figura 2.1: Mappa compertura AT&T negli USA

2.1 Struttura

La loro struttura e architectura hanno subito numerosi cambiamenti nel corso delle generazioni, in particolare con la rete 5G.
Si possono comunque identificare degli elementi chiave che sono presenti in tutte le generazioni:

- *Mobile system* (MS) ovvero il dispositivo cellulare, in alcune generazioni questo acronimo è leggermente diverso, come per esempio dal 3G è lo *User Equipment* (UE).
- *Radio Access Network* (RAN) ovvero l'infrastruttura fisica di antenne per la ricezione e trasmissione di informazioni per il dispositivo
- *Core Network* ovvero i componenti della sua architettura

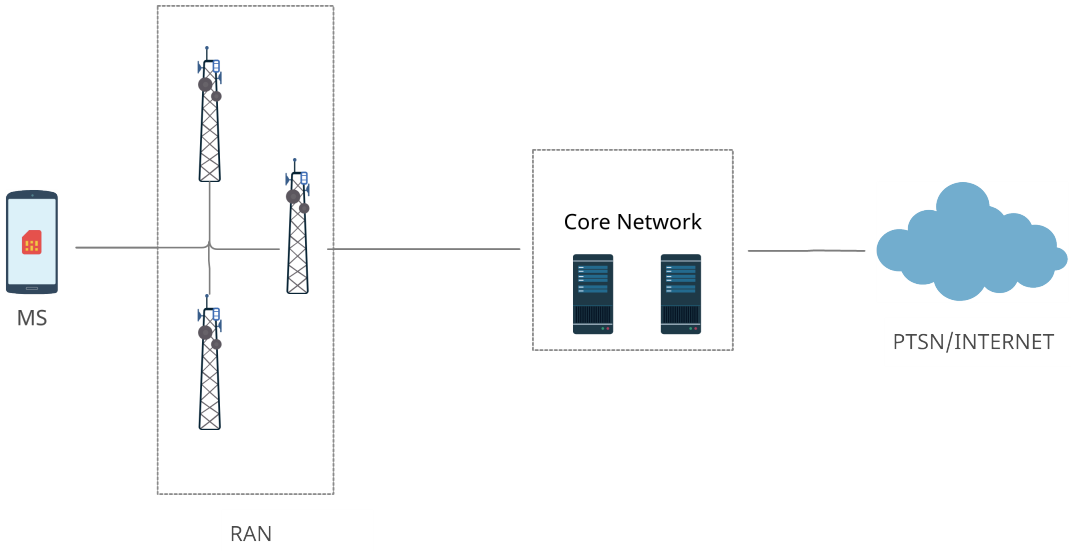

Figura 2.2: Schema di una rete cellulare

La RAN è composta ripetitori di segnale chiamati *Base Station* (BS). Questi vengono disposti in modo capillare sul territorio, suddividendolo in diverse aree di competenza chiamate celle. Ognuna di queste può gestire un numero limitato di dispositivi in contemporanea, per questo, in caso di aree densamente popolate vengono ridotte le aree di competenza di ciascuna antenna. Le celle quindi, possono avere una dimensione variabile che dipende dal contesto in cui devono essere inserite.

Figura 2.3: *Base Station*

Ogni cella ha un determinato raggio di azione che dipende dalle caratteristiche fisiche dell'antenna stessa. Inoltre, ha a disposizione un determinato range di frequenze su cui instaurare la comunicazione con i vari dispositivi, che solitamente sono differenti rispetto a quelle usate dalle celle vicine per evitare interferenze. Celle sufficientemente distanti possono utilizzare le stesse frequenze poiché non corrono il rischio di interferenza, questo rappresenta un grande vantaggio per questa tecnologia.

Per identificare e autenticare ogni MS nella rete è necessario che sia fornito del *Subscriber Identity Module* (SIM), ossia una scheda fisica che contiene le chiavi per autenticarsi alla rete.

Figura 2.4: *Subscriber Identity Module*

2.2 Architettura

L'architettura di una rete cellulare è l'insieme dei componenti che permettono il suo corretto funzionamento come l'autenticazione e lo smistamento delle informazioni.
Nella sezione seguente verranno trattate nel dettaglio tutte le architetture: dal 1G al 5G, elencando i loro componenti principali. Si può comunque stilare una lista di elementi che devono essere in una architettura cellulare:

- Archivio delle chiavi di autenticazione dei *subscribers*.
- Archivio della posizione dei *subscribers*, per permettere il raggiungimento del MS.
- Un *controller* centrale che si occupa di interpellare gli archivi e smistare le informazioni.
- Componente per la commutazione a pacchetto, in caso la rete si interfacci a *internet*.

Capitolo 3

Generazioni cellulari

Nel corso degli anni, si sono susseguite diverse generazioni di tecnologie cellulari, che hanno apportato notevoli cambiamenti alla loro architettura e infrastruttura per consentire il raggiungimento di prestazioni migliori[1].
Di seguito verranno presentati le principali caratteristiche delle diverse generazioni cellulari, in modo tale da rendere di facile comprensione l'analisi dei meccanismi di autenticazione che verranno approfonditi nelle prossime sezioni.
Oltre ad elencare le principali caratteristiche di ogni generazione verranno analizzate nel dettaglio le specifiche dell'architettura di rete.

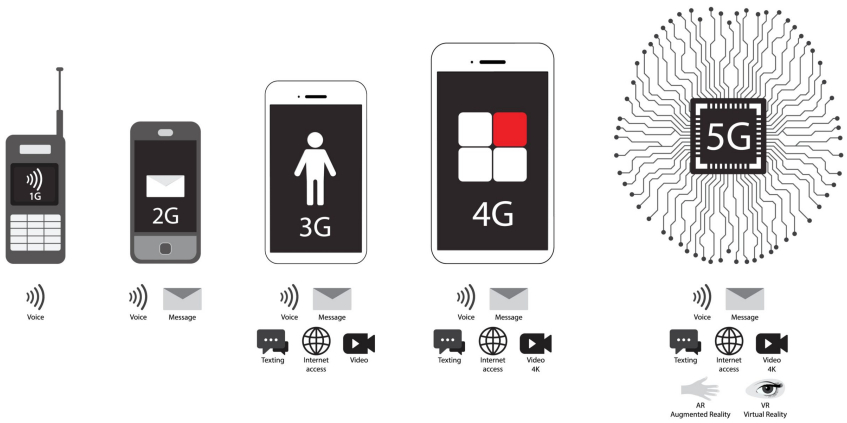

Figura 3.1: Schema delle generazioni cellulari

3.1 1G

La generazione 1G è uno dei primi standard di comunicazione cellulare. Il suo funzionamento era completamente analogico e ormai è stata rimpiazzata totalmente dalle generazioni digitali successive.
L'architettura di questa generazione è molto semplice, è composta da tre componenti principali:

- Antenne per la trasmissione
- *Mobile Telephone Switching Office* (MTSO)
- Unità mobile (cellulare)

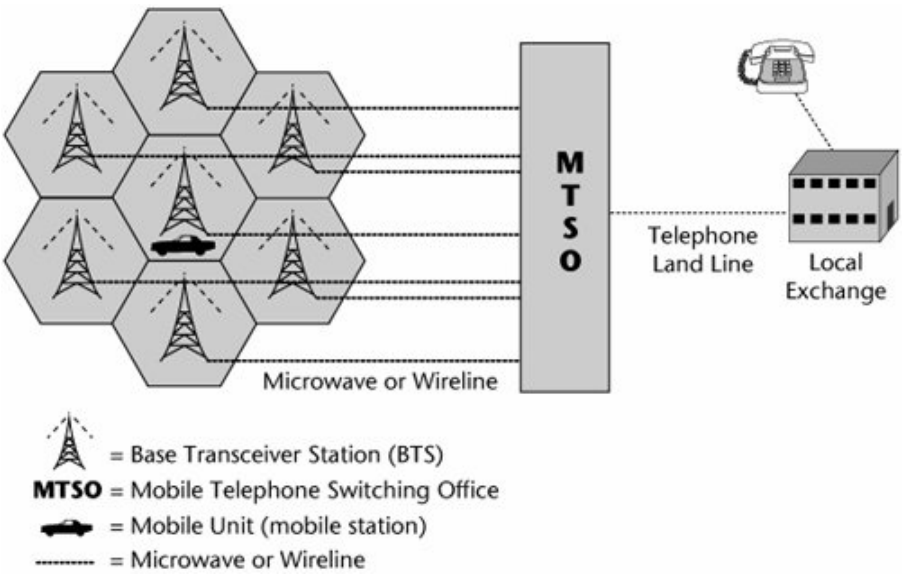

Figura 3.2: Architettura 1G

Si basava sulla *frequency-division multiple access* (FDMA) in cui ogni dispositivo che si connetteva alla stazione radio aveva assegnata una specifica sotto banda[2].

3.2 2G

A differenza della prima generazione, la seconda introuduce per la prima volta una rete completamente digitale. Questa tecnologia cellulare è composta da diverse versioni che si sono susseguite nel corso degli anni aggiungendo nuove funzionalità. Anche la sua architettura subisce delle modifiche, per questo verranno trattate separatamente in seguito.

GSM

Il GSM, ovvero *Global System for Mobile Communications*[3] è uno standard di seconda generazione che introduce importanti novità.
Le principali caratteristiche introdotte sono:

- Maggiori velocità di trasmissione
- Cifratura della comunicazione
- Introduzione di nuovi servizi come gli SMS

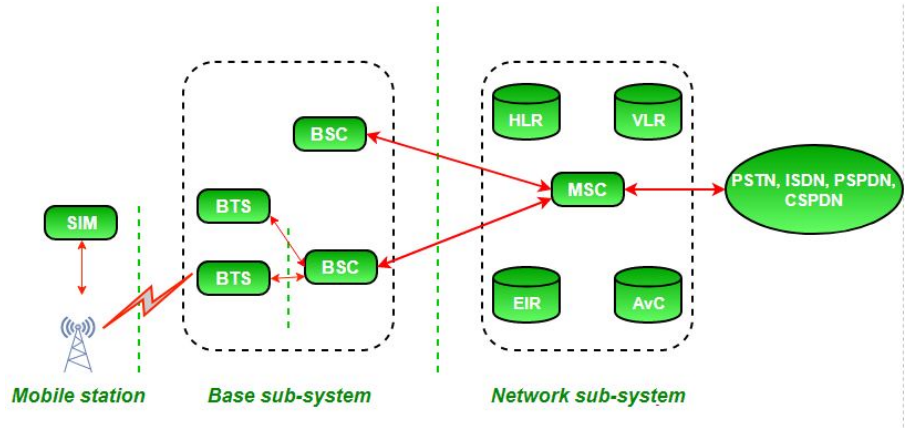

Figura 3.3: Architettura GSM

La sua architettura è composta da due macro aree: La BSS *Base Station SubSystem* e la NSS *Network SubSystem*. Il BSS è l'insieme delle antenne ricevitori che rappresentano il primo collegamento con il MS, mentre il NSS rappresenta il *core network* del GSM.
Il NSS è formato dai seguenti componenti:

- *Mobile Switching Centre* (MSC) è l'elemento centrale dell'atchitettura GSM, si occupa di interfacciare i BTS con la rete telefonica PTSN.
- *Home Location Register* (HLR) *database* centrale che contiene informazioni inerenti a tutti i *subscribers*, molte delle informazioni che contiene sono dei puntatori agli archivi seguenti.
- *Visitor Location Register* (VLR) *database* che memorizza la posizione degli utenti.
- *Equipment Identity Register* (EIR) *database* di identificazione degli IMEI dei dispositivi. Grazie a questo archivio è possibile creare delle *blacklist* per evitare l'accesso a determinati dispositivi. con l'autenticazione.
- *Authenticaton Center* (AuC) *database* di informazioni di sicurezza associate agli utenti registrati.

3.2.1 GPRS

La rete *General Packet Radio Service* (GPRS)[4] introduce per la prima volta un trasferimento dati a commutazione di pacchetto per rendere possibile l'utilizzo dei servizi *internet* con il proprio dispositivo cellulare[5]. La sua architettura è la stessa di quella del GSM ma con dei componenti aggiuntivi che consentono la trasmissione dei pacchetti. Per esempio, il *Serving GPRS Support Node* (SGSN) è un componente per la gestione dei dispositivi connessi alla rete.

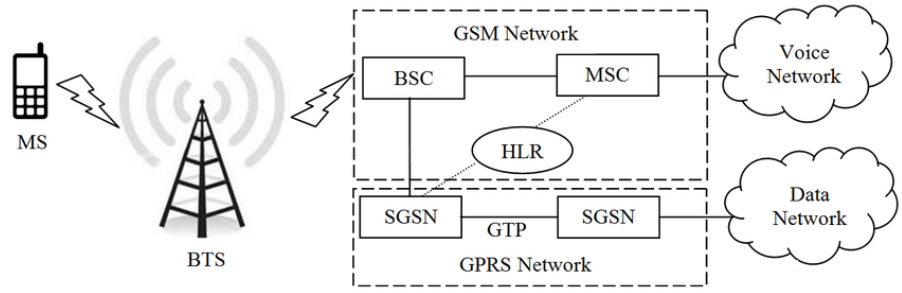

Figura 3.4: Architettura GPRS

3.2.2 EDGE

Evoluzione del GPRS che consente maggiori velocità, l'architettura resta invariata[4].

3.3 3G

L'architettura della terza generazione riprende quella già vista nella seconda. Infatti, questa generazione ha avuto come principale obbiettivo quello di consolidare l'integrazione della rete internet nei sistemi cellulari ed aumentare la velocità di trasmissione per consentire l'utilizzo di nuovi servizi.
L'accesso al canale radio avviene con la tecnologia *Wideband Code Division Multiple Access* (W-DCMA) con canale di banda 5 MHz.

3.3.1 UMTS

L'UMTS ovvero *Universal Mobile Telecommunications System*[6] è il primo standard di terza generazione. La sua architettura è composta dai seguenti elementi principali:

- *Mobile Switching Centre*, componente che ha la stessa funzione di quello in 2G, questa volta il VLR è integrato al suo interno.
- HLR/AuC e EIR
- SGSN e GGSN componenti ripresi dalla rete GPRS per la commutazione a pacchetto.

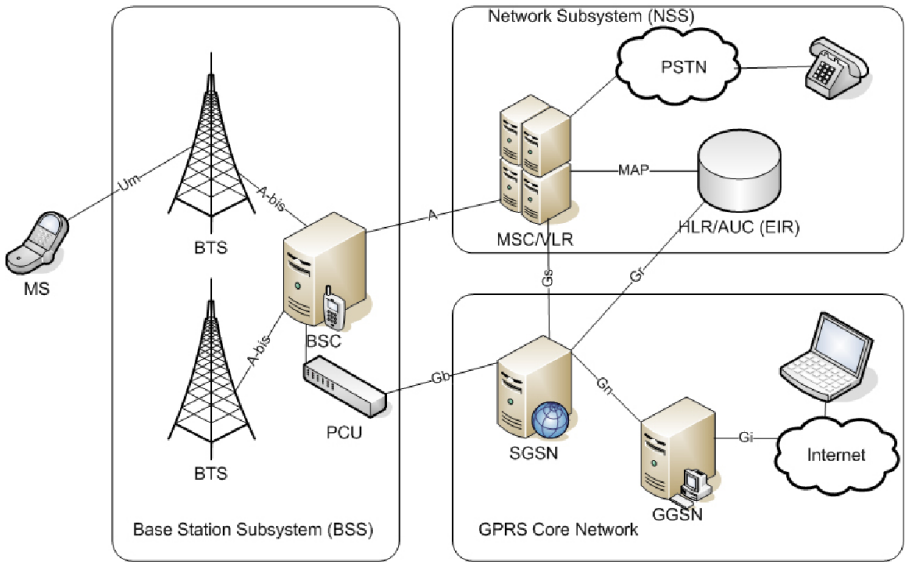

Figura 3.5: Architettura UMTS

3.3.2 HSPA/HSPA+

Evoluzione del UMTS per consentire velocità maggiori apportando modifiche nella trasmissione del segnale. Con questo nuovo standard si riescono a raggiungere velocità di 42 Mb/s[7].

3.4 4G

La quarta generazione è al momento quella più utilizzata, permette di avere dei servizi basati su velocità molto alte. A differenza delle precedenti generazioni che dovevano gestire due *core network*: uno per la rete telefonica e un altro per *internet*, per la prima volta il 4G introduce un unico *core network* basato su *Internet Protocol* (IP).
Per consentire un aumento consistente della velocità le maggiori modifiche di questa generazione sono state apportate nella *radio interface*, mentre l'architettura rimane con una struttura simile a quella precedente.

3.4.1 LTE

Il *Long Term Evolution* è uno standard di quarta generazione che ha i seguenti componenti architetturali[8]:

- *Home Subscriber Server* (HSS) è il *database* centrale dei *subscriber* come l'HLR del GSM/UMTS.
- *Mobility Management Entity* (MME) il corrispettivo del VLR in GSM/UMTS.
- *Serving - Gateway* (S-GW) è un componente che svolge il ruolo di *router* indirizzando i dati dalla *base station* al P-GW.
- *Packet data network - Gateway* (P-GW) è il componente per interfacciare il *core network* con *internet*.
- *Policy Control and Charging Rules Function* (PCRF) è un componente responsabile delle regole di gestione per il flusso di informazioni.

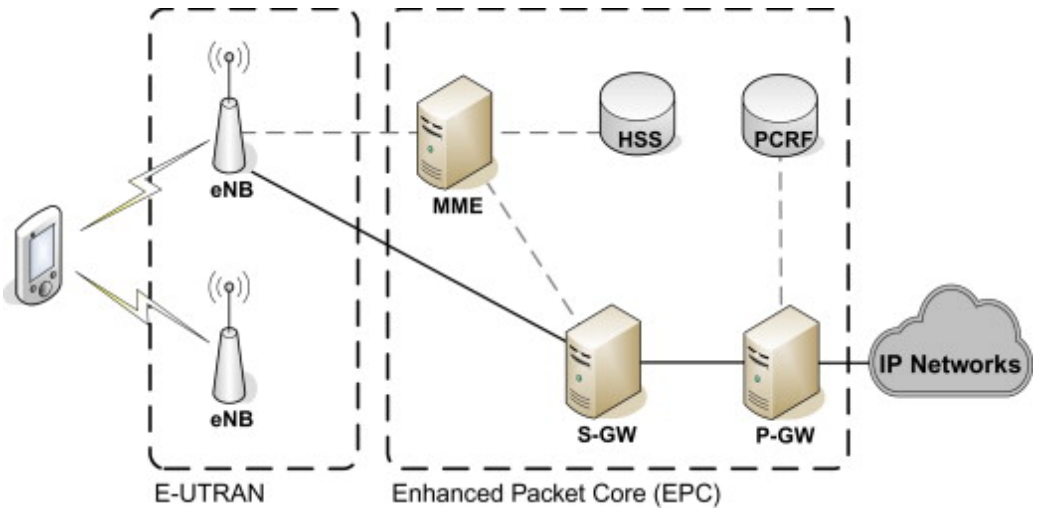

Figura 3.6: Architettura LTE

3.5 5G

Il 5G, ovvero lo standard di quinta generazione rappresenta l'ultima frontiera della tecnologia cellulare. Il suo principale scopo è consentire l'*Internet of Things* massivo, ossia un *network* che sia in grado di gestire la connessione di molti dispositivi con latenze molto piccole. Per consentire velocità fino a 10 Gb/s si sono dovute apportare importanti modifiche strutturali che rendono la sua architettura molto diversa da quelle viste fin'ora. L'architettura implementata prende il nome di *Service-Base Architecture* (BSA). La BSA consiste nel dividere tutte le funzioni in una serie di *microservices*[9]. Questa nuova struttura è stata introdotta per garantire la scalabilità del sistema, migliorare le prestazioni (velocità) e per permettere di realizzare il *massive IOT*, che richiede la gestione simultanea di molti dispositivi.
I principali blocchi che la compongono sono:

- AMF *Core Access and Mobility Management Function* responsabile dell'autenticazione e localizzazione del dispositivo.
- SMF *Sesson Management Function* per la gestione della sessione di ogni UE.
- PCF*Policy Control Function* per la gestione delle *policy*.
- UDM *Unified Data Management* per la gestione dell'identità dell'utente, questo compito era precedentemente svolto da HSS o HLR.
- AUSF *Authentication Server Function* per effettuare l'autenticazione dell'utente.
- SDSF *Structured Data Storage Network Function* è un helper per la memorizzazione di dati strutturati.
- UDSF *Unstructured Data Storage Network Function* è un helper per la memorizzazione di dati non strutturati.
- NEF *Network Exposure Function* per esporre determinate funzionalità a servizi di terze parti.
- NRF *NF Repository Function* per scoprire tutti i servizi disponibili.
- NSSF *Network Slicing Selector Function* per selezionare una determinata partizione di *network*.
- UPF *User Plane Function* trasporta il traffico dal RAN all'internet.

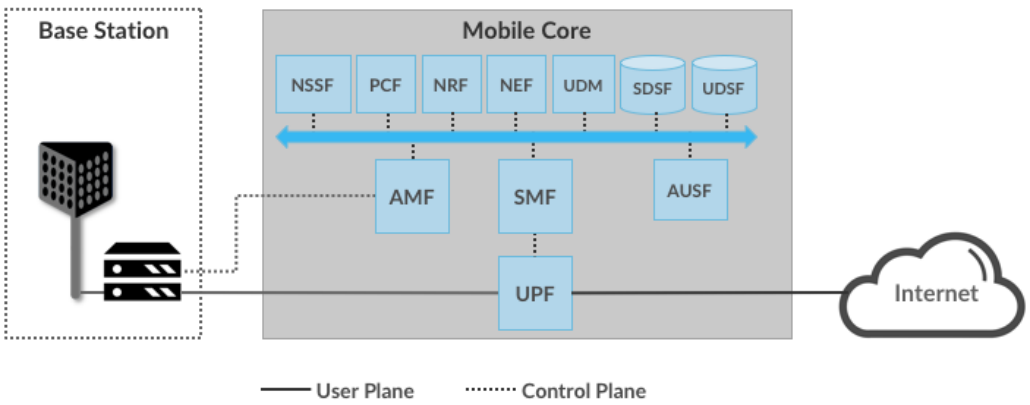

Figura 3.7: Architettura 5G[9]

3.5.1 Network Slicing

Il *Network Slicing* rappresenta una delle caratteristiche più importanti del 5G. Con questo termine si intende il partizionamento della rete in diversi "piani" ciascuno con caratteristiche e requisiti particolari, indipendente e autonomo. Questo risulta fondamentale nella realizzazione dell' IOT massivo, infatti in questo modo la gestione del traffico terrà conto dell'applicazione che viene utilizzata nel dispositivo per decidere quali prestazioni sono richieste da quel dispositivo.

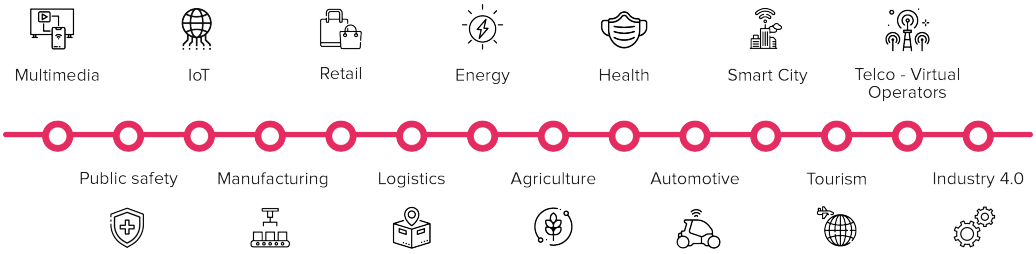

Figura 3.8: Esempi di applicazioni per il 5G

Ogni segmento virtuale del network ha uno specifico identiicativo che deve essere indicato nella fase di autenticazione come verrà illustrato nella sezione 5.3. Per ogni *slice* sono richieste delle prestazioni differenti, per esempio il settore delle *critical communication* deve avere delle latenze molto basse.

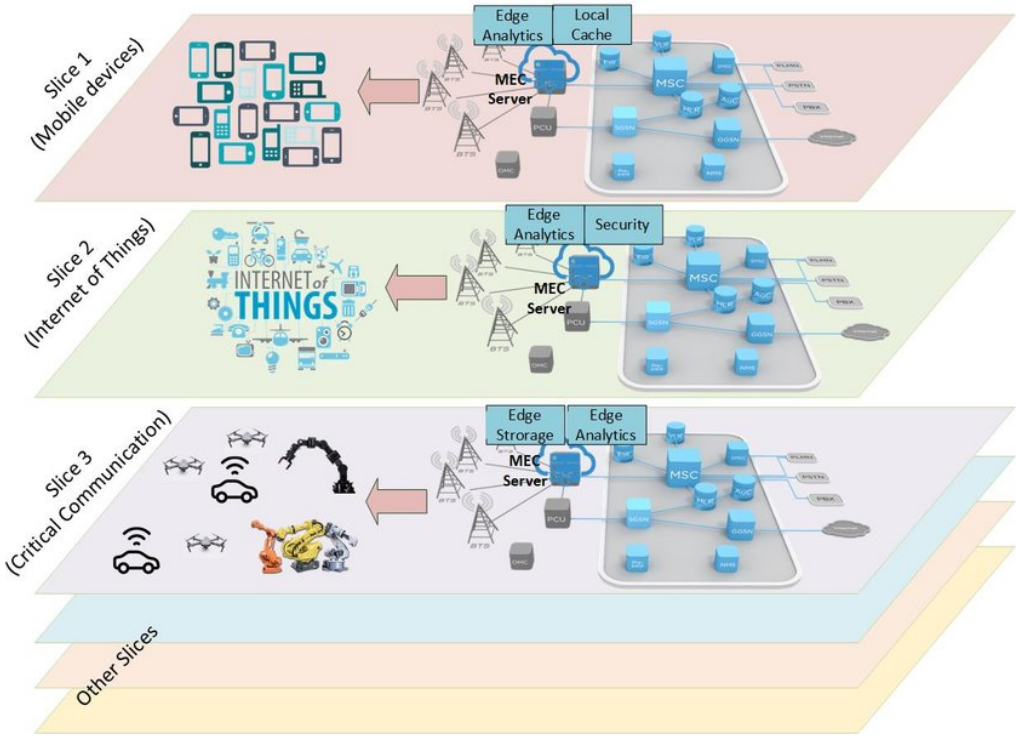

Figura 3.9: *Network slicing* nel 5G

La realizzazione del *Network Slicing* avviene tramite i *Software Degined Network* che nella prossima sezione verranno approfonditi.

3.5.2 *Software Defined Network* e *Network Function Virtualization*

I *Software Defined Network* (SDN) sono dei programmi per la virtualizzazione della rete. Sono necessari per interfacciarsi a livello applicativo con i dispositivi cellulari in modo da gestire il traffico della rete in modo efficace[10].

Capitolo 4

Attacco Denial of Service

L'attacco di tipo *Denial of Service* (DOS) consiste nel rendere non disponibili servizi offerti da computer o altri dispositivi [11]. Questo avviene esasperando di richieste la macchina o infrastruttura che viene scelta come vittima.

4.1 Vulnerabilità nelle reti cellulari

Le reti cellulari non sono esenti da questo tipo di attacchi, anzi, sono uno degli obiettivi più ambiti e sopratutto difficile da risolvere poichè le vulnerabilità che sfruttano sono spesso organiche nell'architettura della rete. Sono diversi i componenti che possono essere vulnerabili a un attacco DOS in una rete cellulare, gli obiettivi identificati come ottimi sono quelli che comportano un maggior utilizzo delle risorse della rete.
Nelle prossime sezioni verranno illustrate le principali metodologie per fare un attacco di tipo *Denial of Service* alle reti cellulari[12].

4.1.1 Radio Jamming

Il *Radio Jamming* è una tipologia di attacco *Denial of Service* che consiste nel disturbare il segnale cellulare emettendo delle onde radio. La realizzazione di questo tipo di attacco è molto semplice, basta procurarsi un trasmettitore che invia segnali ad alta energia nella banda cellulare di riferimento.
Un miglioramento del classico *radio jamming* è lo *smart jamming* che consiste nel saturare uno o più canali di comunicazione della rete. Questo fa sembrare il *network* non disponibile a tutti gli utenti collegati a quella determinata cella.

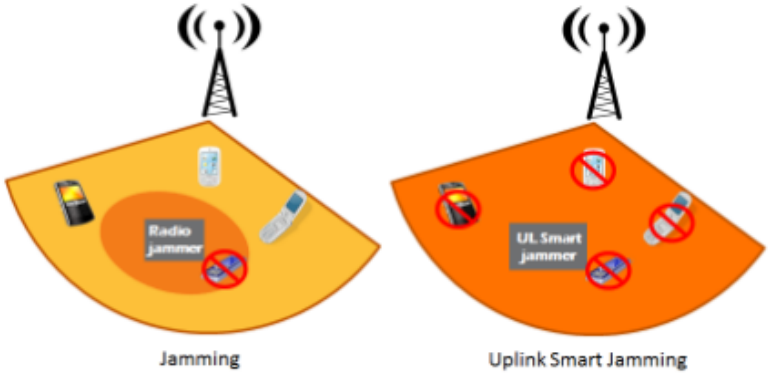

Figura 4.1: *radio* e *smart jamming*[12]

4.1.2 Vulnerabilità di sistema

Un altro classico modo per creare un interruzione di sistema in una rete cellulare è sfruttando le classiche vulnerabilità che si presentano spesso in qualsiasi tipo di computer. Questo ovviamente perchè tutta l'architettura di una rete cellulare non è altro che *server* con specifiche particolari.

4.1.3 Botnet

Questa è sicuramente una delle tipologie più diffuse, ed è modo con cui si realizzano i *Distributed Denial Of Service*. L'attaccante, in questo caso, dispone del controllo di un grande numero di dispositivi infettati da *malware* che possono essere attivati da lui per esasperare di richieste un determinato servizio.

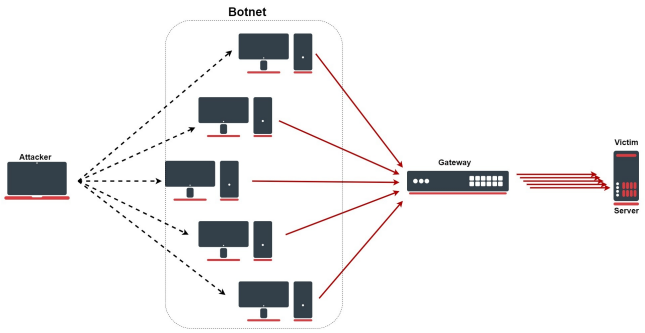

Figura 4.2: *Distributed Denial of Service*

4.1.4 Autenticazione

Questo è uno degli attacchi più pericolosi poichè le vulnerabilità che sfrutta sono molto difficile da risolvere dato che sono intrinseche nell'architettura del sistema. È la tipologia di vulnerabilità che è stata scelta per confrontare la sicurezza dell'architettura 5G con quelle precedenti. Il suo funzionamento si basa sull'esasperare di richieste di autenticazione i sistemi identificativi delle reti cellulari, che solitamente sono i componenti con più traffico della rete come la HLR nelle reti 2G/3G.
Questa vulnerabilità si trova nel meccanismo di autenticazione dei dispositivi denominato *Authentication and Key Agreement* (AKA) dove un dispositivo non autenticato forza delle computazioni all'interno del *Core Network* che consumano più risorse della richiesta stessa[13]. Ad aumentare la pericolosità di questa vulnerabilità è la possibilità di creare computazioni nel *Core Network* senza essere effettivamente autenticati, e quindi senza disporre di una SIM valida. Questa tipologia di attacchi, definiti come SIM-less, verranno presi come riferimento per sfruttare questa vulnerabilità come illustrato per le reti GSM[14] e UMTS[13].

4.2 Misurazione

Per capire quale componente della rete sia il più vulnerabile a un attacco DOS si devono fare delle misurazioni sui vari componenti del *network*. In questo modo è possibile capire in quale punto si possono creare dei rallentamenti o *bottleneck* dovuti a un sovraffollamento di richieste.
In [15] vi è una dettagliata spiegazione di come procedere con queste misurazioni e sopratutto come quantificare il numero di dispositivi che servono all'attaccante per completare l'attacco con successo.
Solitamente le statistiche riguardo alle prestazioni dei componenti del *network* non sono direttamente fornite dagli operatori telefonici quindi bisogna basarsi sui tempi di risposta. Per esempio, l'immagine seguente mostra i tempi di risposta della HLR in una rete UMTS al comando *location updates*.

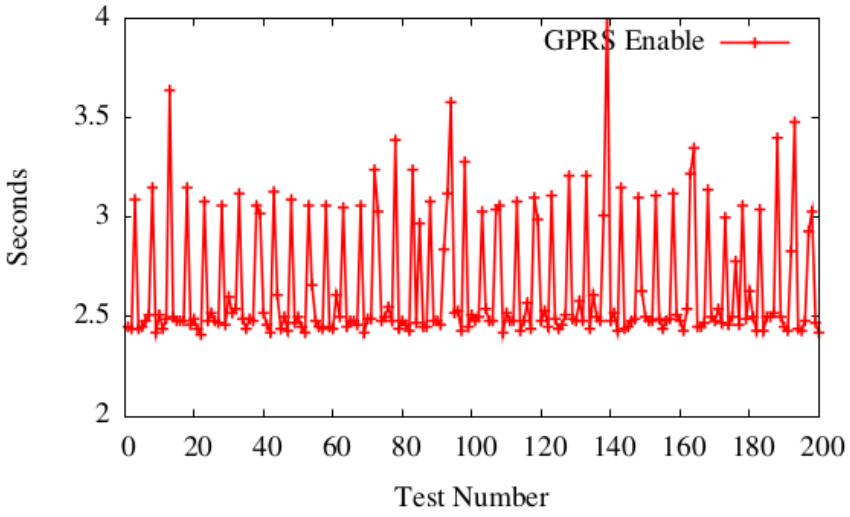

Figura 4.3: Misurazione tempi di risposta HLR con *location updates*[15]

Capitolo 5

Sistema di autenticazione

Il meccanismo di autenticazione è la procedura per verificare che un determinato dispositivo sia abilitato a connettersi alla rete. Questo procedimento avviene tramite l'*Authentication and key agreement* (AKA), procedimento in cui il *core network* abilita un dispositivo a connettersi, e come vedremo, dal 3G anche viceversa (autenticazione mutua).
In questo capitolo verranno trattati le procedure di autenticazione[16] per le generazioni dal 2G al 5G, il 1G è stato escluso poiché ha un funzionamento completamente analogico.

5.1 2G

Il sistema di autenticazione di seconda generazione utilizza principalmente due codici univoci della SIM e del MS:

- *International Mobile Subscriber Identity* (IMSI) ovvero un codice identificatvo della SIM
- *International Mobile Equipment Identity* (IMEI) ovvero un codice identificativo del MS

Questi due codici saranno necessari anche per le prossime generazioni fino al 4G.
La procedura di autenticazione di un MS segue questi passaggi:

1. Il MS invia l'IMSI alla BTS di riferimento che lo inoltra al *core network*, questo avviene ogni volta che il MS vuole connettersi al *network* e non risulta già registrato presso la rete di riferimento. In caso lo fosse, verrà utilizzato il TMSI *Temporary MobileSubscriber Identity* per preservare il suo anonimato.
2. L'AuC cerca la chiave Ki associata all'IMSI e insieme a un numero casuale RAND genera un codice SRES che verrà salvato nel VLR.
3. Viene inviato al MS il RAND generato.
4. La stessa procedura viene fatta dal MS, che genera quindi il suo SRES e lo invia al VLR.
5. Il VLR confronta se l'SRES ricevuto corrisponde a quello generato dall'AuC, se corrispondono l'autenticazione risulta effettuata con successo.

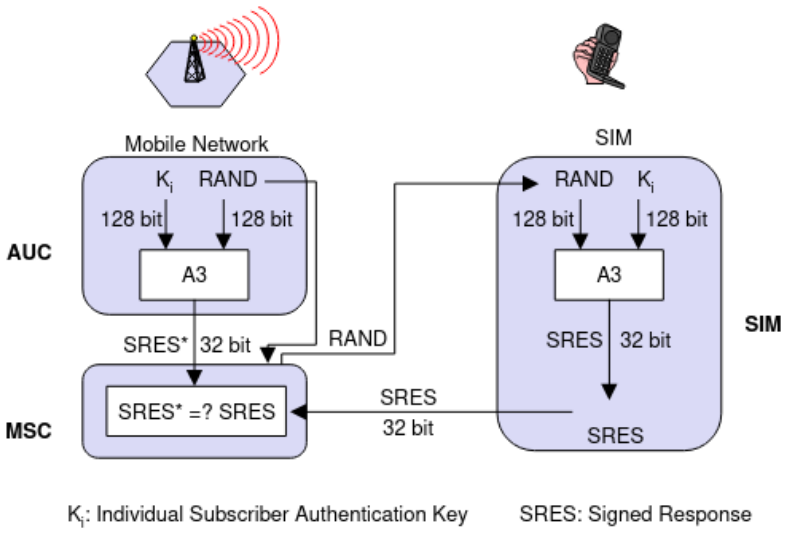

Figura 5.1: Autenticazione nelle reti 2G

5.2 3G-4G

Dato che l'autenticazione nelle reti 3G e 4G è molto simile, verranno trattate insieme in questa sezione. L'autenticazione nell'architettura di terza e quarta generazione è molto simile a quella della seconda salvo i seguenti miglioramenti:

- Viene introdotta l'autenticazione mutua per prevenire l'autenticazione a false *base stations*.
- La lunghezza della chiave Ki viene incrementata da 64 a 128 bit.
- Viene implementato un flag per verificare se le comunicazioni vengono compromesse durante la trasmissione chiamato *Integrity Key* (IK).

Il procedimento di autenticazione è il seguente[17]:

1. Il MS invia l'IMSI alla BTS di riferimento che lo inoltra al *core network*.
2. L'AuC cerca la chiave Ki associata all'IMSI e insieme a un numero casuale RAND genera un codice SRES che verrà salvato nel VLR.
3. Viene trovata la chiave Ki corrispondente all'IMSI dall'AuC, dopodichè viene generato un codice SRES con l'utilizzo di un numero randomico RAND. Inoltre, viene generato un codice AUTN per permettere al MS di autenticare il *network*.
4. Viene inviato al MS il RAND e AUTN.
5. Il MS autentica il *network* confrontando il valore di AUTN ricevuto. Se il *network* è valido, prosegue con la generazione del SRES.
6. Il VLR confronta se il SRES ricevuto corrisponde a quello generato dall'AuC, se corrispondono l'autenticazione risulta effettuata con successo e viene generato,salvato e inviato il TMSI.

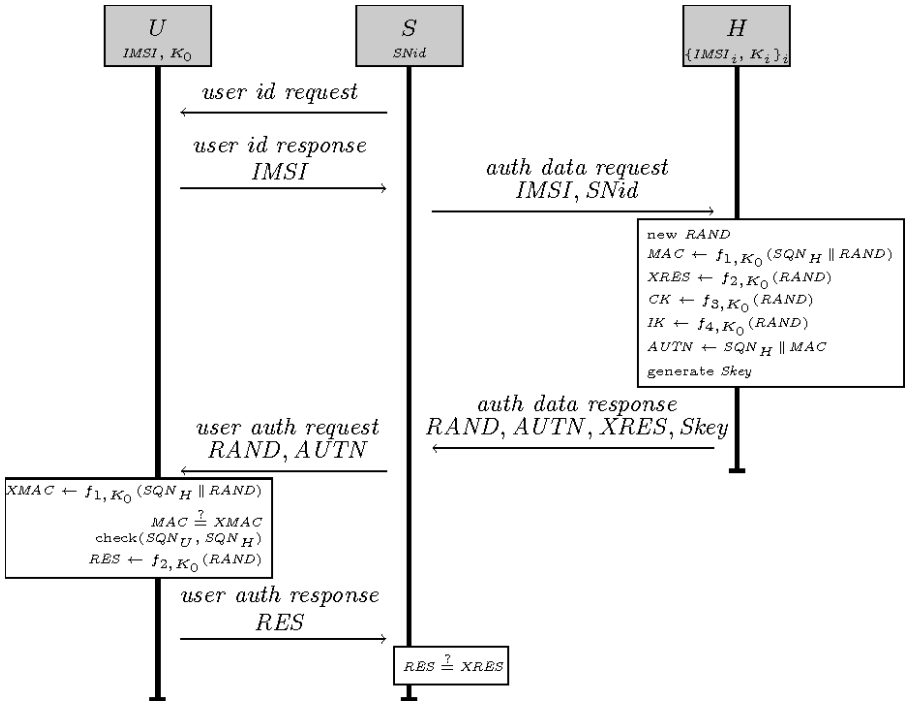

Figura 5.2: Autenticazione nelle reti 3G-4G

5.3 5G

L'autenticazione della generazione 5G è molto diversa dalle precedenti poichè, come illustrato nella sezione 3.5, l'architettura è completamente rivista diventando una ramificazione di microservizi. Sono definiti tre protocolli di autenticazione:

- 5G-AKA: 5G-Authentication and Key Management
- EAP-AKA: Extensible Authentication Protocol – Authentication and Key Management
- EAP-TLS: Extensible Authentication Protocol – Transport Layer Security

Rispetto alle generazioni precedenti ci sono stati i seguenti miglioramenti di sicurezza[18]:

- L'IMSI non viene mai comunicato in chiaro ma sempre criptato
- I componenti del *network* coinvolti sono dei servizi

L'autenticazione è fondamentalmente diviso in due parti: La prima è l'inizializzazione dell'autenticazione e la scelta del metodo di autenticazione. La seconda è invece l'autenticazione mutua come avviene nelle generazioni precedenti. Lo schema di autenticazione è il seguente[19]:

1. Il MS invia il SUCI o 5G-GUTI alla BTS di riferimento che lo inoltra al AMF/SEAF, il GUTI è un identificativo temporaneo simile al TMSI delle generazioni precedenti, invece il SUCI è un identificatore criptato permanente.
2. il SEAF manda l'identificatore del dispositivo (SUCI o 5G-GUTI) e il *Serving Network Name* (SNN) all'AUSF. Il SNN è una concatenazione di codici identificativi di servizi e il codice identificativo del *Serving Network*. Serve per capire a quale *slice* vuole connettersi il dispositivo.
3. L'AUSF controlla che la richiesta dal SEAF sia autorizzata a utilizzare il SNN, in caso non lo fosse risponde con un apposito messaggio di errore.
4. L'AUSF reperisce la chiave associata all'identificativo nell'archivio UDM e genera il rispettivo SRES con un numero randomico RAND.
5. Viene inviato all'MS il RAND e AUTN (per l'autenticazione mutua).
6. Il MS procede con la creazione del SRES e lo invia al SEAF.
7. Il SEAF inoltra il SERS all'AUSF che si occupa di controllare se corrispondono e in caso confermare l'autenticazione.

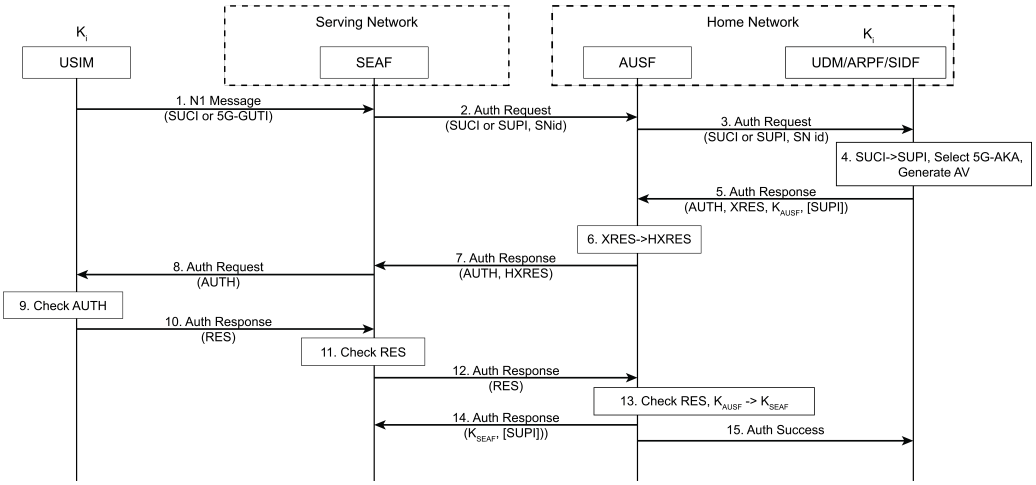

Figura 5.3: Autenticazione nelle reti 5G

Capitolo 6

Attacco all'autenticazione delle reti 2G-4G

Le reti cellulari dal 2G al 4G condividono lo stesso schema architetturale, per questo gran parte delle vulnerabilità che vengono utilizzate negli attacchi di tipo *denial of service* sono comuni. Ci sono numerosi modi per effettuare un attacco DOS all'autenticazione già accennati nella sezione 4.1.4, in questo capitolo verranno messe in pratica nelle reti 2G fino al 4G.
Fondamentalmente, in modo da creare un *denial of service* nel *core network* di una rete cellulare tramite una richiesta di autenticazione bisogna forzare la computazione dei vettori di autenticazione in modo tale da fare spendere risorse computazionali all'infrastruttura cellulare. Nel momento che un dispositivo si collega alla rete cellulare si possono verificare le seguenti casistiche:

- Se il dispositivo ha una SIM valida inizio la procedura di autenticazione.
- Se il dispositivo non ha una SIM valida inizio la procedura di autenticazione ma senza consumare abbastanza risorse nel *network*.
- Se il dispositivo non ha una SIM la procedura di autenticazione non viene iniziata.

Quindi, è chiaro che per effettuare un DOS al sistema di autenticazione degli utenti è necessario disporre o simulare dei dispositivi con delle SIM valide. La validità della SIM è in primo luogo controllata dalla presenza di un IMSI valido come spiegato nella sezione precedente. Di seguito verranno trattate le principali metodologie per effettuare un DOS al sistema di autenticazione.

6.1 Botnet

Il metodo più conosciuto per creare un *denial of service* a una rete cellulare è tramite una *botnet*. In questo modo, l'attaccante ha a disposizione un elevato numero di dispositivi con SIM valida che hanno la possibilità di effettuare massivamente una procedura di autenticazione causando delle dispendiose computazioni all'interno del *network*.
In [15] è descritto come effettuare un DDOS a una rete cellulare di tipo 2G/3G in modo da esasperare di richieste il suo componente più critico: l'HLR. Con 11750 dispositivi infettati è possibile degradare le performance della HLR del 93%[15], garantendo quindi un quasi totale malfunzionamento dell'infrastruttura.
Questa tipologia di attacco è molto pericolosa, e spesso anche la più comune, non è pero esente da diverse problematiche: prima di tutto risulta facilmente rilevabile da un sistema di monitoraggio della rete. Inolte, è richiesto un numero molto elevato di dispositivi, sopratutto se si tiene presente che questi devono appartenere alla stessa zona di competenza della HLR.

6.2 IMSI *catching*

Un metodo alternativo all'utilizzo di una *botnet* è avere a disposizione un *database* di IMSI rubati per effettuare un *flooding* di richieste di autenticazione.
Dato che nelle reti 2G-4G l'IMSI viene trasmesso in chiaro al momento dell'autenticazione riuscire a ottenerli è abbastanza semplice. In [20] vengono citati i modi più comuni per appropriarsene per poi utilizzarli in un attacco.

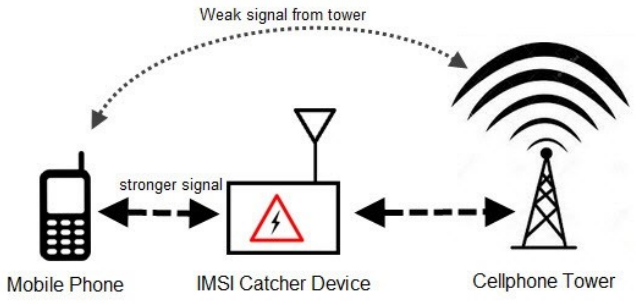

Figura 6.1: Strumento per rubare IMSI

Questi dispositivi sono ormai semplici da reperire *online* a un prezzo abbordabile per chiunque. Per rubare l'IMSI si mette in pratica un attacco di tipo *Man In The Middle* (MITM), spesso utilizzato anche per le intercettazioni da enti governativi.
Nelle reti di seconda generazione questo risulta molto semplice poichè come spiegato nella sezione 5.1, l'IMSI viene trasmesso in chiaro se il MS è la prima volta che si connette al registro di quella specifica zona. Inoltre, dato che nel GSM l'autenticazione non è mutua è possibile creare una *fake basestation* e collezzionare tutti gli IMSI dei dispositivi che si connettono. Sono stati introdotti diversi identificativi temporanei come il TMSI per fare in modo che l'IMSI non debba essere inviato in ogni procedura di autenticazione, ma sono tutti facilmente raggirabili poichè cambiano con una frequenza troppo bassa.
In [21] viene illustrato un metodo per ottenere gli IMSI di qualsiasi dispositivo nello standard UMTS nonostante

l'autenticazione mutua. Infatti viene spiegato come basti mandare al MS una *user identity request* impersonandosi la VLR e il MS risponderà con il proprio IMSI in chiaro.

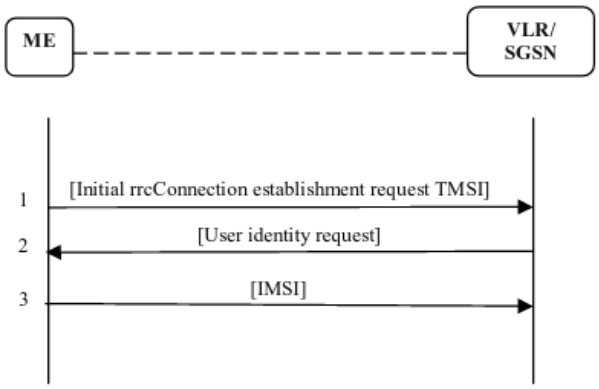

Figura 6.2: IMSI *catching* nelle reti UMTS[21]

6.3 Attacco alle reti con dispositivi SIM-less

In [13] e [14] sono descritti degli attacchi all'autenticazione degli utenti utilizzando dispositivi senza una SIM commerciale, ma bensì delle interfacce di comunicazione programmabili. Questo è stato fatto perchè utilizzare dei MS come dispositivi per effettuare un attacco DOS rappresenta un fattore limitante in termini di prestazioni. Infatti, i sistemi operativi dei MS impongono degli intervalli di tempo fra una richiesta e un'altra.
Entrambi gli attacchi dimostrano che è possibile causare un DOS con un numero di dispositivi senza SIM molto minore rispetto allo stato dell'arte.

6.3.1 GSM

E' stato necessario analizzare la rispettiva *air interface* del GSM per valutare quale è il numero massimo di richieste di autenticazione che possono essere inviate al secondo a una *base station*. Questa misurazione risulta di fondamentale importanza poichè riesce anche a fornire il numero necessario di dispositivi per raggiungere il massimo delle *transation per second* (TPS). Nell'immagine seguente vengono illustrati i messaggi e i canali in cui viaggiano durante l'autenticazione alla rete GSM.

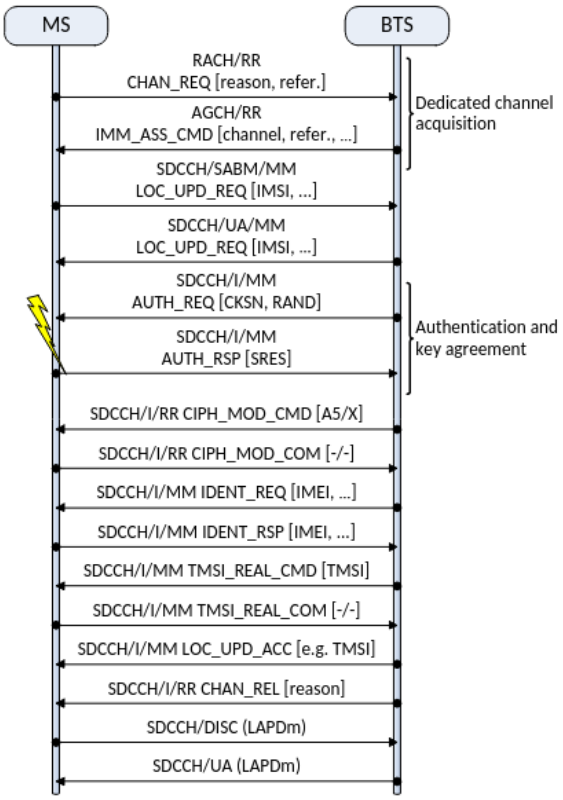

Figura 6.3: Messaggi scambiati durante l'autenticazione in una rete GSM[14]

6.3.2 UMTS

L'immagine seguente rappresenta un semplice schema del dispositivo con SIM programmabile per effettuare DOS a una rete UMTS[13].

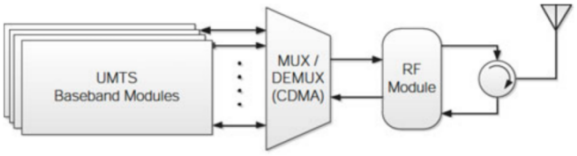

Figura 6.4: Dispositivo per l'attacco DOS alle reti UMTS[13]

Come è stato fatto per la rete GSM, è stato necessario analizzare l'*air interface* dell'UMTS per valutare il numero di TPS. Nell'immagine seguente vengono illustrati i messaggi e i canali in cui viaggiano durante l'autenticazione alla rete UMTS.

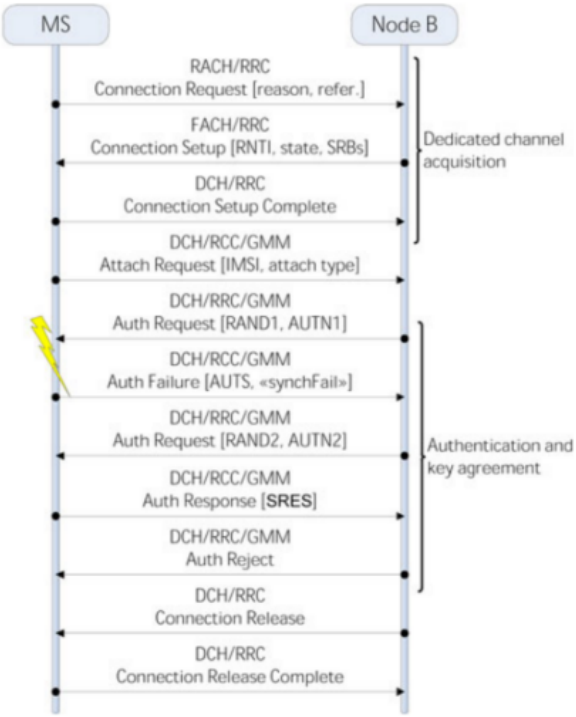

Figura 6.5: Messaggi scambiati durante l'autenticazione in una rete UMTS[13]

Nelle reti UMTS è stato calcolato che il limite più stringente di TPS durante la comunicazione con la *base station* è dato dal canale FACH con 28 TPS. Questo, ha portato a concludere che bastano 446 dispositivi per effettuare una notevole degradazione del sistema, molti di meno rispetto degli 11K necessari per una *botnet*[21]. Nello stesso articolo è spiegato come è possibile duplicare le prestazioni dell'attacco usando delle SIM valide. In questo modo infatti i vettori di autenticazione vengono generati una seconda volta se si segnala al *network* che l'AUTN calcolato non risulta corretto.

Capitolo 7

Attacco all'autenticazione delle reti 5G

In questa sezione verranno trattate le vulnerabilità riguardo un attacco di tipo *Denial of Service* all'autenticazione delle reti 5G. Questa generazione ha risolto alcune delle probematiche legate all'autenticazione, come per esempio a differenza del 4G (LTE) l'identificatore del MS viene criptato con la chiave pubblica prima di essere inviato al *Core network*, evitando così di poter essere intercettato e rubato[18]. Però, con il grande aumento di dispositivi connessi che questa tecnologia vuole incentivare, per esempio nel mondo dell' IOT, gli attacchi DOS saranno senz'altro più semplici da realizzare.
I SDN e NFV, componenti fondamentali per garantire le eccezionali prestazioni del 5G, potrebbero essere un efficace strumento di monitoraggio per identificare possibili attacchi come spiegato in [22].
Allo stesso tempo però, la centralizzazione del controllo del *network* con un SDN e NFV crea le condizioni ottimali per effettuare un attacco DOS con successo[23].
Questa tipologia di attacchi che ha lo scopo di creare una interruzione del servizio hanno una pericolosià maggiore in questa generazione. Infatti, il mondo dell'IOT e le smart cities comprendono dispositivi sensibili come per esempio il mondo della telemedicina.

7.1 IMSI *catching*

Come anticipato, l'avanzamento più importante in termini di sicurezza che questa nuova generazione ha apportato è sicuramente la trasmissione dell'identificativo del MS in forma criptata. Questa innovazione ha reso molto più difficile la pratica dell'IMSI *catching* trattata nella sezione 6.2 fondamentale per effettuare un attacco DOS.

Realisticamente però bisogna sottolineare che questa pratica non risulta completamente debellata. Infatti, tutte le nuove reti 5G, come è stato anche per le generazioni precedenti, devono essere retro compatibili, e quindi per un non determinato lasso di tempo devono essere supportate le procedure degli *standard* precedenti che, come spiegato nel capitolo precedente, soffrono di questa vulnerabilità.

In [24] viene illustrato un metodo per effettuare un attacco MITM nelle reti 5G in modo da ottenere l'IMSI criptato dell'utente: il SUCI. Questo metodo però non sarebbe applicabile per effettuare una raccolta di identificativi per poi effettuare un attacco DOS poichè il SUCI viene rigenerato dopo ogni utilizzo.

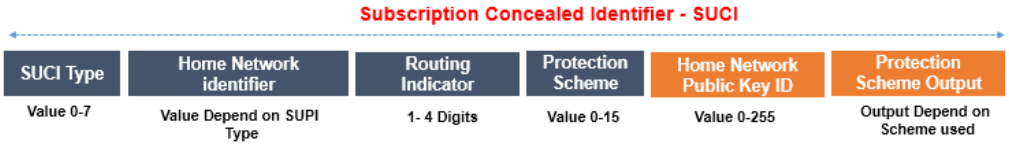

Figura 7.1: Composizione del SUCI nel 5G

7.2 Replicazione dell'attacco SIM-less

Alla base degli attacchi trattati nella sezione 6.3 vi è la costruzione di un *database* di IMSI. Questo *database* può essere agevolmente costruito nelle generazioni precedenti al 5G tramite le tecniche di IMSI *catching* trattate in 6.2. Nel 5G risulta molto più difficile creare un archivio di IMSI poichè questi viaggiano in forma criptata nella rete, ovvero comunicando il SUCI.

Tuttavia, se si riuscisse a ottenere comunque un *database* di IMSI rubati si potrebbe ottenere un attacco dello stesso tipo di [14] e [13] con prestazioni migliori perchè il nuovo protocollo 5G NR[25] per l'*air interface* è stato progettato per supportare il *Massive Machine Type Communications* ovvero l'IOT massivo che richiede latenze molto basse e capacità molto alte. Per questo, sicuramente la capacità dei canali di comunicazione durante la procedura di autenticazione avrebero un valore di TPS molto alto, sufficiente a causare un notevole degradamento delle prestazioni.

7.3 Nuove vulnerabilità

L'implementazione del SUCI e SUPI ha risolto, o quantomeno reso molto più complicata la pratica dell'IMSI *catching*. Allo stesso tempo però ha incrementato il dispendio di risorse durante l'autenticazione di un dispositivo. Come è chiaramente visibile nell'immagine sottostante, prima della generazione dei vettori di autenticazione vengono innestate delle procedure per decriptare il SUCI che avvengono con un algoritmo detto *Elliptic Curve Integrated Encryption Scheme* (ECIES). Questa procedura aumenta inevitabilmente la creazione di possibili DOS all'autentcazione. In [26] è descritto un protocollo che permetterebbe di controllare fin dal primo momento se il MS ha un SUCI valido senza incorrere nella decriptazione.

Capitolo 8

Conclusioni

In questo documento sono state analizzate le più comuni vulnerabilità che consentono di effettuare un attacco di tipo *Denial of Service* alle reti cellulari. In particolare, sono state analizzate le vulnerabilità nelle autenticazioni di tutte le generazioni.
Dopo un attenta analisi dei meccanismi di autenticazione e delle classiche vulnerabilità che vengono usate nelle generazioni 2G-4G, si può finalmente fare un confronto fra la sicurezza dell'ultima generazione 5G e quelle precedenti.
Il 5G ha sicuramente apportato dei consistenti miglioramenti di sicurezza, come ampiamente trattato riguardo la cifratura dell'IMSI.
Nonostante ciò è innegabile che in questa ultima generazione gli attacchi DOS saranno molto più semplici da realizzare, ma sopratutto più pericolosi dati i compiti sensibili che alcuni dispositivi connessi a questa rete dovranno svolgere.

Bibliografia

[1] Massimo Condoluci e Toktam Mahmoodi. «Softwarization and virtualization in 5G mobile networks: Benefits, trends and challenges». In: *Computer Networks* 146 (set. 2018). DOI: 10.1016/j.comnet.2018.09.005.

[2] Fredrick Njoroge e Lincoln Kamau. «A Survey of Cryptographic Methods in Mobile Network Technologies from 1G to 4G». In: (nov. 2018).

[3] 3gpp. *Global System for Mobile Communications*. URL: https://www.3gpp.org/specifications/gsm-history.

[4] 3gpp. *General Packet Radio Service / Enhanced Data rates for Global Evolution*. URL: https://www.3gpp.org/technologies/keywords-acronyms/102-gprs-edge.

[5] M. Rahnema. «Overview of the GSM system and protocol architecture». In: *IEEE Communications Magazine* 31.4 (1993), pp. 92–100. DOI: 10.1109/35.210402.

[6] 3gpp. *Universal Mobile Telecommunications System*. URL: https://www.3gpp.org/technologies/keywords-acronyms/103-umts.

[7] 3gpp. *High Speed Packet data Access*. URL: https://www.3gpp.org/technologies/keywords-acronyms/99-hspa.

[8] 3gpp. *Long Term Evolution*. URL: https://www.3gpp.org/technologies/keywords-acronyms/98-lte.

[9] Larry Peterson e Oguz Sunay. *5G Mobile Networks: A Systems Approach*. URL: https://github.com/SystemsApproach/5G.

[10] Alcardo Alex Barakabitze et al. «5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges». In: *Computer Networks* 167 (2020), p. 106984. ISSN: 1389-1286. DOI: https://doi.org/10.1016/j.comnet.2019.106984. URL: https://www.sciencedirect.com/science/article/pii/S1389128619304773.

[11] Kevin Hattingh et al. «DoS! Denial of Service». In: ().

[12] Roger Piqueras Jover. «Security attacks against the availability of LTE mobility networks: Overview and research directions». In: (gen. 2013), pp. 1–9.

[13] Alessio Merlo et al. «A Denial of Service Attack to UMTS Networks Using SIM-Less Devices». In: *IEEE Transactions on Dependable and Secure Computing* 11.3 (2014), pp. 280–291. DOI: 10.1109/TDSC.2014.2315198.

[14] Nicola Gobbo, Alessio Merlo e Mauro Migliardi. «A Denial of Service Attack to GSM Networks via Attach Procedure». In: (set. 2013). DOI: 10.1007/978-3-642-40588-4_25.

[15] Patrick Traynor. ≪On Cellular Botnets: Measuring the Impact of Malicious Devices on a Cellular Network Core≫. In: (2009).

[16] Prajwol Kumar Nakarmi. ≪Cheatsheets for Authentication and Key Agreements in 2G, 3G, 4G, and 5G≫. In: (2021). arXiv: 2107.07416 [cs.CR].

[17] Cristina-Elena Vintilă, Victor-Valeriu Patriciu e Ion Bica. ≪Security Analysis of LTE Access Network≫. In: gen. 2011.

[18] *A Comparative Introduction to 4G and 5G Authentication*. URL: https://www.cablelabs.com/insights/a-comparative-introduction-to-4g-and-5g-authentication.

[19] David Basin et al. ≪A Formal Analysis of 5G Authentication≫. In: *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security* (gen. 2018). DOI: 10.1145/3243734.3243846. URL: http://dx.doi.org/10.1145/3243734.3243846.

[20] Hamad Alrashede e Riaz Ahmed Shaikh. ≪IMSI Catcher Detection Method for Cellular Networks≫. In: (2019), pp. 1–6. DOI: 10.1109/CAIS.2019.8769507.

[21] Muzammil Khan, Attiq Ahmed e Ahmad Raza Cheema. ≪Vulnerabilities of UMTS Access Domain Security Architecture≫. In: (2008), pp. 350–355. DOI: 10.1109/SNPD.2008.78.

[22] Mathias Kjolleberg Forland et al. ≪Preventing DDoS with SDN in 5G≫. In: (2019), pp. 1–7. DOI: 10.1109/GCWkshps45667.2019.9024497.

[23] M Awais Javed e Sohaib khan Niazi. ≪5G Security Artifacts (DoS / DDoS and Authentication)≫. In: (2019), pp. 127–133. DOI: 10.1109/COMTECH.2019.8737800.

[24] Merlin Chlosta et al. ≪5G SUCI-Catchers: Still Catching Them All?≫ In: WiSec '21 (2021), pp. 359–364. DOI: 10.1145/3448300.3467826. URL: https://doi.org/10.1145/3448300.3467826.

[25] Erik Dahlman e Stefan Parkvall. ≪NR - The New 5G Radio-Access Technology≫. In: (2018), pp. 1–6. DOI: 10.1109/VTCSpring.2018.8417851.

[26] Ikram Gharsallah, Salima Smaoui e Faouzi Zarai. ≪A Secure Efficient and Lightweight authentication protocol for 5G cellular networks: SEL-AKA≫. In: (2019), pp. 1311–1316. DOI: 10.1109/IWCMC.2019.8766448.