UNIVERSITÀ
DEGLI STUDI
DI PADOVA

DIPARTIMENTO
DI INGEGNERIA
DELL'INFORMAZIONE

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:

Indice

Elenco delle figure

Elenco delle abbreviazioni

MS Mobile system. 8

MSC Mobile switching center. 6

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 abituati. In questa tesi si tratterà della loro struttura e funzionamento, analizzando le diverse tecnologie cellulari che con il tempo si sono susseguite. Dopodichè si procederà ad analizzare nel dettaglio i meccanismi di autenticazione dei dispositivi, mettendo in luce le rispettive vulnerabilità per le diverse tecnologie cellulari. Sfruttando delle vulnerabilità nel sistema di autenticazione si dimostrerà come un attacco di tipo Denial of Service sia possibile, spiegando le possibili disastrose conseguenze che potrebbe comportare.

2 La rete cellulare

2.1 Definizione

La rete cellulare è la struttura *hardware* e *software* che consente il corretto funzionamento delle comunicazioni cellulari. Grazie alla loro capillarità, i vari gestori telefonici riescono a garantire il servizio per la gran parte del territorio mondiale.

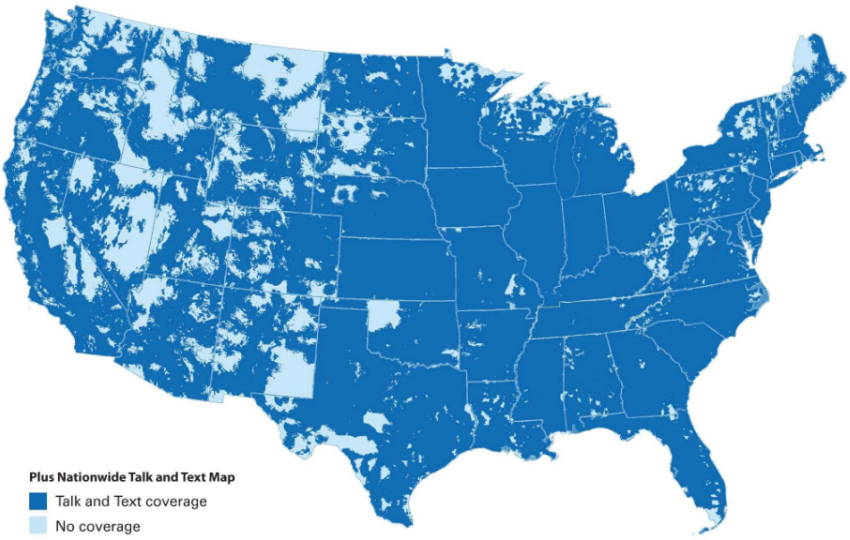

Figura 1: Mappa compertura AT&T negli USA

La loro struttura e architettura ha subito notevoli cambiamenti nel corso degli anni, nelle prossime sezioni si analizzeranno gli elementi fondamentali di una rete cellulare che qualsiasi generazione possiede.

2.2 Infrastruttura

Per rendere possibile il collegamento di dispositivi in zone molto vaste vengono usati i ripetitori di segnale chiamati *base station*. 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, che chiameremo *mobile station*, 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: Base station

Ogni cella ha un determinato raggio di azione determinato 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.

2.3 Architettura

L'architettura di una rete cellulare può essere risassunta con alcuni fondamentali componenti. La *mobile sation* si connette all'antenna della zona di competenza ossia la *base transceiver station*, quest'ultima quando riceve l'informazione la inoltra alla rispettiva *base station controller*, ossia un componente che si occupa di raggruppare diverse *base station*. Diversi *BSC* sono raggruppati nel *mobile switching centre* Mobile switching center (MSC)

3 Generazioni cellulari

Nel corso degli anni, si sono susseguite diverse generazioni di tecnologie cellulari, che hanno apportato notevoli cambiamenti alla loro architettura. Di seguito verranno presentati le principali caratteristiche delle più notevoli generazioni cellulari, in modo tale da rendere di facile comprensione l'analisi dei meccanismi di autenticazione che verranno approfonditi nella prossima sezione.

3.1 0G/1G

3.2 2G

3.2.1 GSM

3.2.2 GPRS

3.2.3 EDGE

3.3 3G

3.3.1 UMTS

3.3.2 HSPA/HSPA+

3.4 4G

3.5 5G

4 Attacco Denial of Service al sistema di identificazione

4.1 Denial of Service

L'attacco di tipo *Denial of Service* (DOS) consiste nel rendere non disponibili servizi offerti da computer o altri dispositivi [1]. Questo avviene esasperando di richieste la macchina o infrastruttura che viene scelta come vittima. La risorse della vittima verranno quindi interrogate in modo massivo fino al punto di indurre il sistema al collasso.
Una variante dell'attacco DOS è il *Distributed Denial of Service* (DDOS), in cui l'attaccante non è composto solamente da una sola macchina, ma bensì da una rete intera chiamata *botnet*. Questa seconda versione è più difficile da realizzare ma al tempo stesso molto più efficacie. Solitamente, la *botnet* è composta dagli *zombies*, ovvero dispositivi di utenti normali ignari del fatto di essere stati infettati da un *malware* che consente all'attaccante di averne il controllo.
Le reti cellulari non sono esenti da questo tipo di attacchi, anzi, sono una delle tipologie più frequenti e sopratutto difficile da risolvere poichè le vulnerabilità che sfruttano sono organiche nell'architettura della rete.

4.2 Identificazione

Il meccanismo di identificazione è la procedura per verificare che un determinato dispositivo è abilitato a connettersi alla rete. Il 5G apporta una modifica organica del suo funzionamento, per questo si è deciso di analizzare nelle successive sezioni solamente i meccanismi di autenticazione della rete UMTS e 5G.
L'identificazione rappresenta un meccanismo molto vulnerabile ad attacchi di tipo *Denial of Service* poichè, in alcuni casi, si riesce a consumare delle onerose operazioni computazionali anche con dispositivi che non sono abilitati, quindi senza SIM.

4.2.1 UMTS

Il meccanismo presente nella rete UMTS è lo stesso usato nelle generazioni cellulari GSM, GPRS e EDGE. Inoltre, il suo funzionamento è molto simile a quello delle reti LTE (4G), pertanto si è deciso di presentarlo solamente una volta.
Un MS che si vuole collegare alla rete deve procedere con la fase di autenticazione o identificazione anche detta *Authentication and key agreement* (AKA). In questa fase, viene interrogata la rispettiva HLR/AuC dove l'IMSI del dispositivo viene validato, se tutto procede correttamente viene notificato il SGSN che inoltra al MS l'avviso di autenticazione completata.

4.2.2 5G

4.3 Risultati

5 Conclusioni

Riferimenti bibliografici

[1] Kevin Hattingh et al. ≪DoS! Denial of Service≫. In: ().