DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

Corso di Laurea in
Ingegneria Informatica

Relazione Finale

Evoluzione della sicurezza nelle reti cellulari: analisi delle problematiche e possibili soluzioni

Relatore:
Chiar.mo Prof. Francesco Gringoli

Laureanda:
Elena Filippini
Matricola n. 727828

Anno Accademico 2021/2022

Indice

Capitolo 1

Introduzione

Le reti mobili consentono a un terminale di spostarsi in un territorio esteso collegandosi ai nodi della rete a cui appartiene. I terminali utenti (UE-User Equipment) possono essere di più tipi, ad esempio fisso, portatile (es. antenna cellulare) o mobile (antenna radio su automobile). Nelle reti cellulari i nodi che garantiscono l'accesso alla rete sono le stazioni base. Le stazioni base sono delle antenne che operano su più canali, sia logici che fisici, e possono avere diversi pattern di radiazione in base tipo di copertura specifica. Sono gli eNB o gNB per 4a e 5a generazione. La principale caratteristica delle reti cellulari è la mobilità, che è garantita consentendo a un UE di spostarsi da una BTS a un altra. La zona di copertura viene suddivisa in diverse aree, dette Location Area (LA), ciascuna di esse ha un identificativo univoco (LAI), che viene memorizzato in appositi registri.

La copertura estesa viene garantita all'UE mediante l'utilizzo di Serving Network (SN): un UE può collegarsi alla cella che garantisce la copertura maggiore, anche se si tratta della cella di un altro operatore grazie agli accordi di roaming. Il servizio viene garantito all'UE anche in una zona non coperta dall'operatore di appartenenza ma dalla SN di un altro operatore. Quindi la Serving Network consente di disaccoppiare la funzione di accesso da quella di autenticazione, che deve essere sempre garantita dalla rete dell'operatore di appartenenza, la Home Network (HN), in quanto possiede i parametri utilizzati dal protocollo.

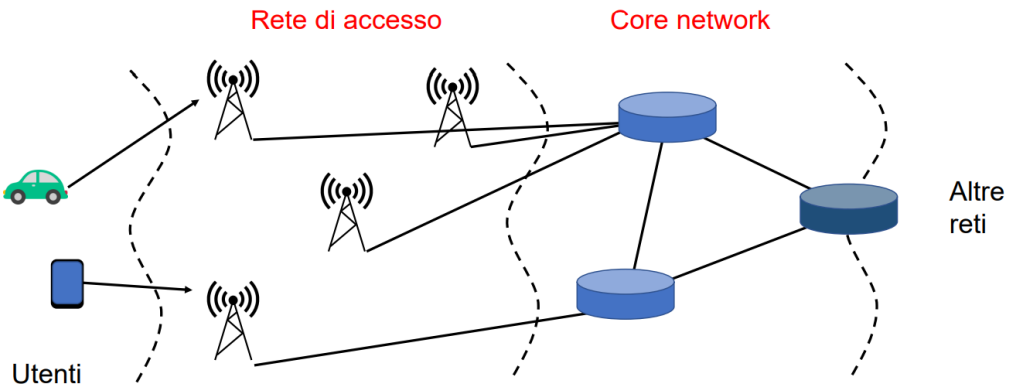


Figura 1.1: L'architettura generica di una rete cellulare [27]

L'utilizzo di protocolli sicuri è fondamentale in un qualunque sistema mobile, per garantire che un attaccante non riesca a generare reti false per compromettere la privacy degli utenti, e viceversa, che non effettui un accesso non legittimo alla rete, dimostrando la conoscenza delle credenziali a lungo termine. Senza che sia garantita mutua autenticazione anche meccanismi aggiuntivi di sicurezza delle comunicazioni successive, come confidenzialità e integrità non sarebbero sufficienti per impedire di intercettare il traffico degli utenti e di impersonarli. Utilizzare protocolli sicuri previene il tracking degli utenti, cioè il risalire al loro identificativo.

La sicurezza nei sistemi mobili è oggetto di studio in quanto tutti i sistemi complessi ingegnerizzati mostrano sempre vulnerabilità dovute a difetti implementativi non prevedibili, ovvero utilizzo di protocolli ill-designed.

Capitolo 2

Protocollo di autenticazione

LTE è una tecnologia interamente a commutazione di pacchetto che riduce la complessità nell'architettura, riducendone anche gli elementi rispetto alle generazioni precedenti. La rete LTE è chiamata Evolved Packet System (EPS), ed è costituita dalla rete di accesso e dalla core network. La rete di accesso è detta Enhanced UTRAN (E-UTRAN). E' una rete "piatta" (non gerarchica) costituita da eNodeB (eNB) [27]. Gli eNodeB concentrano le funzioni dei NodeB della terza generazione (cioè di Base Transceiver Station - BTS) e del RNC, cioè il componente della rete UMTS che è responsabile del controllo dei nodeB ad esso collegati . Per quanto riguarda il livello RNC gli stati possibili di un UE sono ridotti a due: IDLE o CONNECTED, in quanto gli stati delle interfacce sono orientati ad un principio "always on".

La core network in LTE è la Evolved Packet Core (EPC), che è una rete a commutazione di pacchetto. I componenti della EPC sono i seguenti. La Mobility Management Entity (MME) gestisce tutta la segnalazione (stato della mobilità dell'UE,

autenticazione, definizione dei flussi del traffico da eNB a P-GW). Si occupa anche di generare le identità temporanee e assegnarle all'UE. L' Home Subscriber Server (HSS) è il database che viene utilizzato al posto del HLR. Il Serving Gateway (S-GW o SGW) e il Packet Data Network Gateway (PDN-GW o P-GWP) sono dei router. Un SGW è un dispositivo che contribuisce alla gestione del routing dei dati. E' collegato al P-GW, a cui invia i dati provenienti dai terminali che raccoglie dalle stazioni base. Si occupa anche della trasmissione dei dati nella direzione opposta, dal PGW ai terminali. Per cui gestisce il trasporto dei dati IP dall'UE alla core network LTE. Inoltre, fornisce una anchor per l'UE quando si sposta da un eNodeB all'altro.

Il PDN- GW è il gateway verso altre reti (Internet / Intranet), cioè instrada i pacchetti IP da e a altre reti IP. Oltre a ciò, si occupa della assegnazione degli indirizzi IP ai UE e applica diverse politiche relative al traffico IP degli utenti, come il filtraggio dei pacchetti.

Il Policy and Charging Rules Functions (PCRF) è collegato al P-GW in quanto si occupa della tariffazione, in base al consumo dei dati.

Attualmente la maggior parte degli UE accedono ai servizi di rete cellulare (ad esempio Internet, chiamate) utilizzando tecnologie 3G o 4G, utilizzando le schede USIM (Universal Subscriber Identity Module).

Il protocollo Authentication and Key Agreement (AKA) è stato progettato dal gruppo 3rd Generation Partnership Project (3GPP), che è responsabile della standardizzazione delle tecnologie delle reti mobili, con gli obiettivi di garantire autenticazione reciproca tra un dispositivo dotato di scheda USIM e la rete e consentire la derivazione delle chiavi per cifrare la comunicazione successiva.

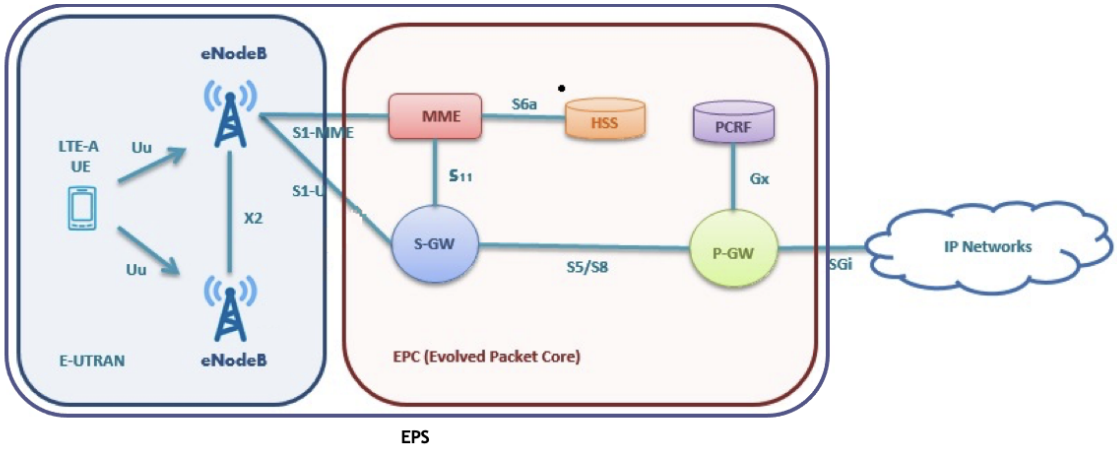


Figura 2.1: In figura i principali componenti di EPS

AKA viene utilizzato anche nei meccanismi basati su EAP (Extensible Authentication Protocol) (ad esempio EAP-AKA). Il protocollo EAP è un framework di autenticazione, per cui deve essere implementato da dei meccanismi specifici, come ad esempio EAP-AKA. Viene utilizzato spesso nelle connessioni PPP, negli access point e nelle architetture di autenticazione generiche, incluse quelle per la protezione dei servizi basati su HTTP.

EAP-AKA è utilizzato nelle reti mobili di 3a generazione, successivamente è stato modificato ed ereditato nelle reti mobili di 4a generazione (Long Term Evolution-LTE) come Evolved Packet System Authentication and Key Agreement (EPS-AKA). Nelle reti LTE, come nelle generazioni precedenti, viene utilizzato GPRS Tunnelling Protocol o GTP, un gruppo di protocolli di comunicazione basati su IP adibiti al trasporto di General Packet Radio Service. Le fonti per questo capitolo sono [21], [9], [19] e [11].

2.1 Protocollo AKA

l protocollo AKA utilizza una chiave K simmetrica precondivisa tra la scheda USIM di un subscriber e l'Authentication Center della corrispondente Home Network (HN).

La chiave K non è leggibile dall'USIM. Il processo di autenticazione effettivo inizia facendo in modo che Home Network produca un vettore di autenticazione AV, a partire da K e un numero di sequenza, e lo trasmetta alla Serving Network (SN).

Il vettore di autenticazione AV destinato alla SN è composto da una serie di challenge di autenticazione. Ciascuna AV_i contiene:

- un valore casuale RAND
- una componente XRES
- una chiave di sessione effimera di 128 bit per garantire l'integrità IK
- una chiave di sessione effimera a 128 bit per la cifratura CK
- una componente AUTN utilizzata dal MS per autenticare la rete
- un numero di sequenza SQN, che rappresenta un nonce implicito, per cui garantisce la protezione da replay attack. Tuttavia, richiede di mantenere la sincronizzazione tra MS e AuC: entrambi devono memorizzare gli ultimi valori utilizzati.
- una componente AK, utilizzata per cifrare il valore SQN

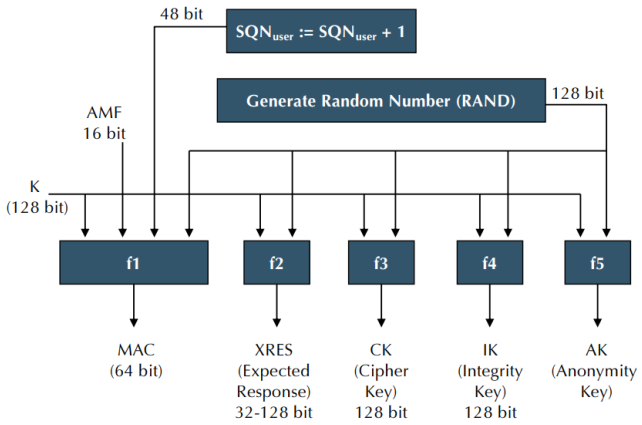


Figura 2.2: In figura le operazioni effettuate dalla HN per ottenere i parametri di autenticazione

I valori di XRES, CK, IK, AK, vengono calcolati rispettivamente con le funzioni f2, f3, f4, f5 con in input la chiave K e RAND. Le funzioni $f1^*$ e $f5^*$ vengono utilizzate nella procedura di riautenticazione al posto di f1 e f5.

Il valore MAC viene calcolato con la funzione f1, con in input K, AMF, SQN_{UE}, RAND.

AMF (Authentication and key Management Field) è un valore costituito da 16 bit, viene utilizzato per la gestione di casi particolari, come ad esempio la selezione di algoritmi diversi da quelli standard.

Le funzioni f1-f5 sono implementate con la funzione hash SHA-1. Come detto sopra, il vettore di autenticazione AV contiene n challenge di autenticazione, in cui:

$AV_i = [RAND|XRES|CK|IK|AUTN]$,

con $AUTN = [AK \oplus SQN|AMF|MAC]$.

Il protocollo AKA può essere suddiviso in tre fasi principali: l'identificazione, la challenge-response e la procedura di risincronizzazione.

2.1.1 Identificazione

Per prima cosa la SN deve identificare l'UE. Se la SN non conosce l'identità corrente dell'UE può richiedere l'IMSI inviando un messaggio di Identity Request. In seguito a ciò, l'UE fornisce l'IMSI in un messaggio di Identity Response. Questa identità consente alla SN di potere richiedere il materiale necessario per le fase successive al HN corretto, in quanto l'IMSI contiene informazioni relative alla nazione e all'operatore. I messaggi scambiati in questa fase vengono trasmessi in chiaro in quanto non sono ancora state derivate le chiavi simmetriche necessarie per la loro cifratura.

2.1.2 Challenge-response

Quando l'HN riceve la richiesta del materiale di autenticazione da un SN contenente l'identità dell'UE, recupera dal suo database la chiave K e il valore SQN, per poi calcolare il vettore di autenticazione. La chiave di cifratura CK e la chiave di integrità IK non vengono inviate dalla SN all'UE. A questo punto viene aggiornato il numero di sequenza con un incremento del contatore. La SN riceve il vettore di autenticazione, e invia una delle challenge di autenticazione all'UE in un messaggio di Authentication Request. L'UE risponde con un messaggio di Authentication Response se l'autenticazione della SN ha esito positivo, altrimenti con un messaggio di errore di autenticazione contenente la causa dell'errore. Per autenticare la rete l'UE estrae

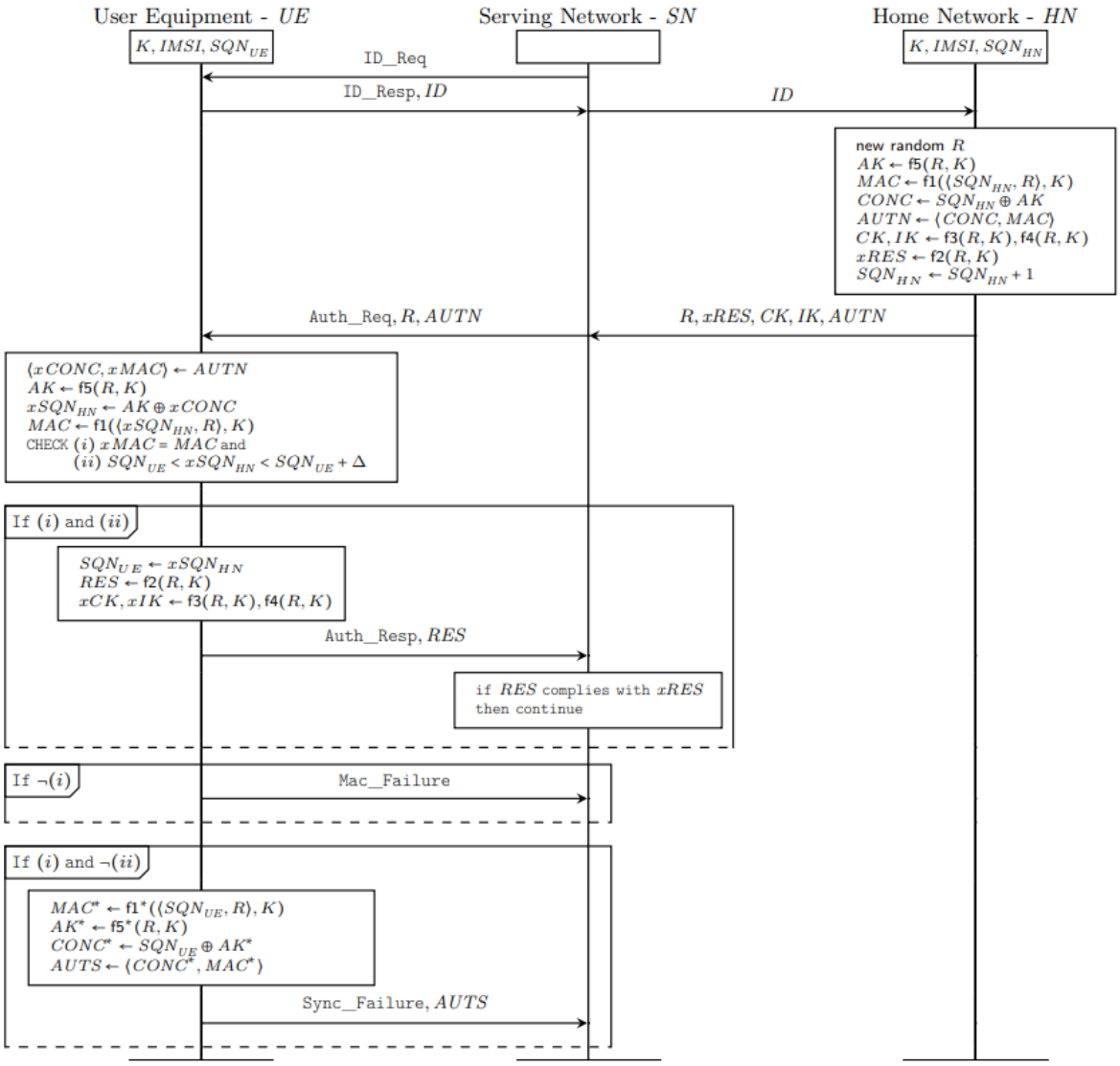


Figura 2.3: In figura le diverse fasi del protocollo AKA

SQN_{HN} da AUTN calcolando AK con RAND (che ha ricevuto) e K. A questo punto verifica che:

1. MAC sia un valore corretto con riferimento a K, altrimenti risponde con Mac_failure;

2. Il messaggio di Authentication Request è nuovo, cioè se $xSQN_{HN} > SQN_{UE}$ e $xSQN_{HN} < SQN_{UE} + \Delta$), altrimenti risponde con (Sync_failure, AUTS). $xSQN_{HN}$ è il valore di SQN che è atteso dall'UE, dato che UE e HN devono mantenerne il valore aggiornato, e che viene ricavato decifrando il messaggio ricevuto. La quantità Δ è una soglia fissata in base a un compromesso tra disponibilità della rete e sicurezza.

Se tutti i controlli vanno a buon fine, l'UE calcola a sua volta la chiave di cifratura CK e la chiave di integrità IK e le memorizza per proteggere i messaggi successivi. Inoltre calcola il valore RES e lo invia al SN includendolo nel messaggio di Authentication Response. Il valore RES non viene calcolato in caso il valore MAC non sia valido. Solo RES è incluso nel messaggio, altri valori calcolati come CK e IK non vengono trasmessi. La SN autentica l'UE verificando se la risposta ricevuta corrisponde a xRES. Il valore xRES (Expected Response) viene ricevuto dalla SN all'interno del vettore di autenticazione, e il suo valore corrisponde al valore RES che un UE legittimo calcola a partire dai parametri ricevuti e con le funzioni crittografiche, come mostrato in figura. In tal caso, il protocollo AKA viene completato correttamente e le comunicazioni successive possono essere protette utilizzando le chiavi segrete IK e CK.

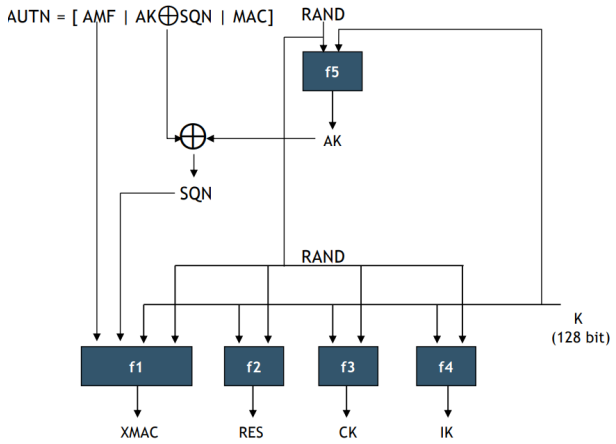


Figura 2.4: In figura le operazioni effettuate lato UE per ricavare i parametri di autenticazione

2.1.3 Procedura di risincronizzazione:

In caso di errore di sincronizzazione, l'UE risponde con (Sync_failure, AUTS).

Il messaggio $AUTS = CONC^*, MAC^*$ consente all'HN di risincronizzarsi con l'UE sostituendo il proprio SQN_{HN} con il numero di sequenza dell'UE: $SQN_{UE} + 1$. Conoscere la variazione del valore SQN nel tempo potenzialmente consente di ottenere informazioni relative alle attività degli utenti o la loro posizione. Per cui viene cifrato:

$CONC^* = SQN_{UE} \oplus AK^*$, con $AK^* = f5^*(RAND, K)$.

Il valore AUTS include anche il valore

$MAC^* = f1^*(K, SQN_{UE}, RAND)$, per consentire alla HN di autenticare questo messaggio come proveniente dall'UE previsto.

2.2 Meccanismo EAP-AKA e EPS-AKA

In seguito viene descritto il protocollo EAP-AKA, in quanto il protocollo EPS-AKA è del tutto analogo. Il meccanismo EAP è un framework di autenticazione che supporta differenti meccanismi di autenticazione e che viene utilizzato soprattutto a livello data-link. Con le reti GSM è stato introdotto il meccanismo EAP-SIM [RFC3748], che è un meccanismo che consente alle reti GSM di effettuare l'autenticazione con le schede SIM. EAP-AKA è stato introdotto in UMTS e consente di utilizzare AKA ad una qualunque tecnologia che supporta un meccanismo EAP.

Per prima cosa il server EAP invia un pacchetto EAP-Request/Identity al UE, il quale risponde con EAP/Response/Identity, che contiene l'identità del UE. Il successivo messaggio EAP-Request/AKA-Challenge può includere un identificativo temporaneo che viene assegnato dalla rete al UE, nel campo AT_ENCR_DATA, che però l'UE non è vincolato ad utilizzare essendo il supporto privacy opzionale. L'UE può decifrare il contenuto del campo e memorizzarlo per le successive autenticazioni. Nel caso in cui l'UE non riceve un identificativo temporaneo può utilizzarne uno ricevuto in precedenza.

La richiesta di identità inviata dal server al peer con EAP-Request/AKA-Identity può includere gli attributi: AT_PERMANENT_ID_REQ, per richiedere l'username permanente, AT_AUTH_ID_REQ, per richiedere un id temporaneo, e AT_ANY_ID_REQ, a cui l'UE può rispondere con l'id temporaneo se ne è in possesso, altrimenti con l'username permanente. L'username permanente è del formato: 0123456789098765@myoperator.com, dove la parte prima @ indica l'identità

permanente dell'utente.

L'identificativo contenente l'IMSI (International Mobile Subscriber Identity) viene trasmesso in chiaro il meno possibile, utilizzando gli identificativi temporanei, TMSI (Temporary Mobile Subscriber Identities), che dovrebbero essere aggiornati di frequente. Dato che questi pseudonimi vengono assegnati dal server al peer nello scambio EAP-AKA, un peer che non ha ancora effettuato scambi (ad esempio perché si registra alla rete per la prima volta) normalmente non ha uno pseudonimo disponibile. Un altro identificativo temporaneo utilizzato in LTE è il Globally Unique Temporary (UE) Identity (GUTI),è assegnato al UE e utilizzato per fare in modo di risalire alla MME di servizio, cioè la MME che conosce la mappatura tra TMSI e IMSI. Il GUTI è costituito da un Mobile Country Code (MCC) e un Mobile Network Code (MNC), che identifica l'operatore, da un MME Group ID per identificare il gruppo MME in cui si trova MME di servizio, da un MME Code per identificare lo specifico MME che ha assegnato il TMSI (MME Group ID e MME Code insieme costituiscono il MMEI) e infine dal TMSI stesso. La scelta di utilizzare TMSI o GUTI dipende dalle esigenze della comunicazione, ad esempio l'UE si sposta ad un altro MME è necessario il GUTI in modo che il nuovo MME possa determinare l'IMSI, mentre in un handover normale il TMSI è sufficiente.

Il server dovrebbe memorizzare lo pseudonimo in una memoria non volatile in modo che possa essere mantenuto tra i riavvii. Un utente malintenzionato che impersona la rete può utilizzare l'attributo AT_PERMANENT_ID_REQ in un messaggio di Authentity Request per richiedere l'IMSI dell'utente. Tuttavia, il terminale può rifiutarsi di inviare l'IMSI in chiaro se ritiene che la rete debba essere in grado di

riconoscere il TMSI. Se il peer e il server non sono in grado di garantire che lo pseudonimo venga mantenuto in modo affidabile, è possibile utilizzare una protezione aggiuntiva con un meccanismo di sicurezza esterno (ad esempio PEAP - Protected Extensible Authentication Protocol).

In seguito alla fase di identificazione inizia la procedura AKA effettiva. Come mostrato nella figura 1.4, il server invia EAP-Request/AKA-Challenge, che include gli attributi AT_RAND, AT_MAC, e opzionalmente AT_IV e AT_ENCR_DATA per garantire la privacy delle comunicazioni successive.

L'attributo AT_ENC_DATA può includere lo pseudonimo dell'utente in AT_-NEXT_PSEUDONYM. Quando riceve questo messaggio, il peer deve elaborare AT_RAND e AT_AUTN prima degli altri attributi. Solo se questi attributi vengono verificati come validi, il peer deriva le chiavi e verifica AT_MAC. Se l'MS ha autenticato con successo il server, invia EAP-Response/AKA-Challenge, altrimenti EAP-Response/AKA-Client-Error. Questo messaggio deve includere gli attributi AT_MAC, AT_RES. In caso la verifica di AUTN non abbia successo, l'UE invia il pacchetto EAP-Response/AKA-Authentication-Reject. Se il numero di sequenza incluso nel campo AUTN non è nel range corretto, il peer invia EAP-Response/AKA-Synchronization-Failure, in cui può includere l'attributo AUTS, il quale può essere utilizzato dal server per risincronizzarsi

L'integrità dei messaggi di AKA-Identity scambiati non è protetta da AT_MAC, dato che non sono ancora stati derivati i componenti necessari per calcolarlo.

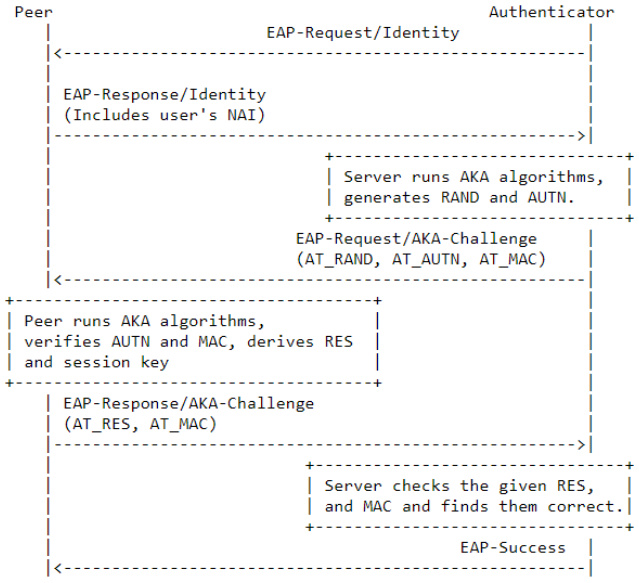


Figura 2.5: In figura la procedura di autenticazione EAP completata con successo

2.3 Scelta di uno schema di cifratura simmetrico

AKA è un tipo di protocollo challenge-response e utilizza un meccanismo di autenticazione basato sulla crittografia simmetrica. Il motivo di questa scelta è legato principalmente a tre trade-off.

Il primo è un trade-off tra sicurezza e costi: l'utilizzo della crittografia asimmetrica richiede di introdurre una Public Key Infrastructure e di utilizzare dei meccanismi di cifratura maggiormente costosi nell'USIM. Per cui la scelta nella progettazione dei sistemi 3G e 4G è stata limitata dai costi elevati. Nel 5G la PKI è stata introdotta, ma solo per proteggere le identità.

Il secondo trade-off è tra sicurezza e disponibilità della rete, cioè l'uso della chiave simmetrica evita il rischio di bloccare gli UE legittimi durante un caso di guasto o

crash della rete. Ad esempio, se il software SN (in particolare MME si arresta in modo anomalo, l'identità temporanea di un UE non può essere riconosciuta. In tal caso, la rete deve richiedere l'identità permanente all'UE.

Il terzo è un trade-off tra privacy ed efficienza della rete: AKA è un protocollo di autenticazione one-round-trip, cioè sono necessari solo due messaggi per stabilire l'autenticazione dopo l'identificazione. Per potere ottenere l'autenticazione reciproca con soli due messaggi è stato scelto il meccanismo basato su SQN. Sarebbe potuto essere scelto un nonce esplicito, cioè un numero casuale, ma ciò richiede delle capacità computazionali superiori rispetto a quelle possedute dai dispositivi mobili negli anni 2000 (quando è stato progettato il 3G AKA). Oltre a questo, uno scambio supplementare di messaggi avrebbe anche un impatto negativo sull'efficienza della rete, in particolare perché richiederebbe uno scambio di messaggi aggiuntivo anche tra HN e SN .

Capitolo 3

Attacchi di identificazione

Questi attacchi sfruttano i messaggi di segnalazione pre-autenticazione non protetti scambiati a livello NAS (Non Access Stratum). Il protocollo NAS viene utilizzato per comunicare tra l'UE e la core network (in particolare MME) ed è il livello più alto del piano di controllo LTE. Il NAS ha due funzioni principali: la gestione della mobilità e la gestione delle sessioni dell'UE. La gestione della mobilità comprende l l'identificazione e l'autenticazione dell'UE attraverso il protocollo AKA. Gli attacchi trattati in questo capitolo sono tratti dalle pubblicazioni [36], [17], [24].

3.1 IMSI Catching

Durante la progettazione del protocollo AKA nel 2000, le stazioni base (BS) false erano considerate costose in termini di costo e capacità dell'attaccante. Tuttavia, oggi possono essere facilmente costruite utilizzando hardware disponibile, come le

Software Define Radio (SDR), e software open source. Gli attacchi di IMSI catching sfruttano la vulnerabilità causata dalla pubblicazione dell'identità dell'utente e hanno lo scopo di raccogliere gli IMSI degli utenti mobili nelle comunicazioni wireless.

Esistono due modi per rilevare l'IMSI di un utente. Il primo modo prevede lo sniffing del messaggio NAS di Attach Request quando l'UE si registra alla core network per la prima volta, in cui include l'IMSI. Lo sniffing dei messaggi utilizza attacchi di intercettazione, che appartengono alla categoria degli attacchi che sfruttano vulnerabilità del livello fisico, e solitamente, come in questo caso, sono un punto di partenza per attacchi con conseguenze più gravi. Gli attacchi di intercettazione prevedono la ricezione dei segnali radio in modo passivo, la loro decodifica e l'estrazione delle informazioni grazie alla conoscenza delle specifiche LTE, che sono pubbliche.

L'altro modo prevede di inviare attivamente il messaggio di Identity Request indicando all'UE di includere il proprio IMSI nel messaggio di risposta . E' stato anche dimostrato che il TMSI utilizzato per l'identificazione dell'utente non garantisce il livello di privacy previsto se il suo aggiornamento non è sufficientemente frequente e casuale.

In entrambi i casi, a partire dai messaggi di segnalazione NAS che vengono trasmessi in chiaro a tutte le stazioni base circostanti è possibile ricavare l'IMSI. I messaggi NAS che vengono scambiati prima di avere stabilito una connessione sicura sono: Identity Request, Authentication Request, Authentication Reject, Attach Reject, Detach Accept, Cell Reselection Tracking Area Update Reject e Service Reject. In questo attacco [24] sono utilizzati i messaggi di Tracking Area Update Reject e Service Reject.

Tracking Area Update Reject

La riselezione cellulare è una procedura che consente all'UE di collegarsi alla cella migliore in termini di condizioni radio. A tal fine, l'UE continua a misurare le qualità del segnale della serving network e delle celle vicine.

Durante la riselezione, l'UE esamina il codice della tracking area (TAC) contenuto in SIB 1. I messaggi di System Information Blocks (SIB) sono dei messaggi che contengono informazioni relative ai parametri della cella e sono suddivisi in gruppi, da SIB 1 a SIB 13. Viene trasmesso anche il MIB (Master Information Block), che contiene informazioni di configurazione per effettuare la ricezione e la decodifica, come la bandwidth della cella. I messaggi SIB e il MIB costituiscono i messaggi di SI (System Information), che sono inviati in chiaro a livello RRC (Radio Resource Control) dalla stazione base.

Una tracking area è costituita da un insieme di eNodeB controllati da uno stesso MME con lo scopo di tenere traccia degli UE che si trovano modalità stanby. Ogni volta che l'UE si sposta in nuova tracking area esegue la procedura di aggiornamento della tracking area (Tracking Area Update-TAU).

Quando l'UE si sposta sotto al MME della nuova tracking area, il nuovo MME utilizza il GUTI dell'UE per identificare l'MME precedente. I due MME condividono l'IMSI dell'UE in modo che non venga divulgato via radio. In casi eccezionali, ad esempio se il precedente MME ha svuotato il database interno, il nuovo MME deve ottenere l'IMSI dall'UE stesso, inviando un messaggio di Identity Request. Dunque in questi casi l'IMSI viene trasmesso in chiaro. Questo fatto può venire sfruttato

da un falso MME, il quale può affermare di non potere ricavare l'IMSI via rete con un messaggio di Tracking Area Update Reject con Causa 9: "UE identity cannot be derived by the network". In seguito a ciò l'UE invia al nuovo MME un messaggio di Attach Request contenente il suo IMSI.

Service Reject

Quando l'UE desidera inviare o ricevere un nuovo traffico dati, invia all'MME un messaggio di Service Request con il TMSI, in modo che gli vengano allocate le risorse di rete e radio necessarie (in uplink o downlink). Le richieste di servizio possono essere attivate da un UE o da una rete.

In ogni caso, quando il falso MME riceve un messaggio di Service Request, risponde con Service Reject con Causa 9: "UE identity cannot be derived by the network". A cui l'UE risponde inviando un messaggio di Attach Request con il suo IMSI.

3.1.1 Implementazione dell'Imsi Catcher

Gli IMSI Catcher sono spesso commercialmente chiamati StingRays, ma, come detto in precedenza, possono essere facilmente implementati anche su SDR a basso costo e utilizzando software open source. Gli IMSI Catcher sono costituiti da due componenti: la falsa rete LTE e il jammer LTE.

Implementazione della falsa rete LTE

Per implementare l'eNodeB dell'attaccante è possibile utilizzare il pacchetto software srsRAN, di cui si utilizza la componente LTE, sviluppato da Software Radio Systems (SRS) [32], o OpenAirInterface sviluppato dalla OpenAirInterface Software Alliance (OSA) [3]. Entrambe le soluzioni includono l'eNodeB, per la gestione dell'interfaccia radio, e l'MME e HSS per la creazione della core network.

Per configurare la falsa rete LTE è necessario impostare gli stessi parametri utilizzati dall'operatore effettivo per la cella, che includono: il Mobile Country Code (MCC), il Mobile Network Code (MNC), il PCI e il TAC. Il PCI (Physical Cell Identifier) indica l'identità della cella a livello fisico, viene utilizzato per identificare le celle durante la procedura di selezione delle celle. Il TAC può essere impostato sia sullo stesso valore utilizzato dall'operatore oppure su un valore differente, nel primo caso comporta un messaggio di Service Request dall'UE, nel secondo un messaggio di Tracking Area Update. MCC e MNC identificano l'operatore, mentre PCI e TAC sono specifici dell'eNodeB.

Un altro insieme di parametri da considerare è l'elenco degli eNodeB alternativi dello stesso operatore nella stessa area, in particolare i loro PCI, TAC e frequenze. E' necessario utilizzare un jammer su tutte queste frequenze, per evitare che l'UE si connetta a uno di questi eNodeB (invece che al falso eNodeB).

Gli attacchi di radio jamming sono degli attacchi a livello fisico che hanno come scopo di interrompere la normale comunicazione tra UE e la stazione base. Sono a loro volta classificabili in barrage jamming e smart jamming. Il Barrage Jamming

trasmette semplicemente segnali di rumore, ad esempio Additive White Gaussian Noise (AWGN), all'intera banda del sistema LTE per degradare il rapporto segnale/rumore (SNR) ricevuto. Una variante è il jamming a banda parziale, che disturba solo una parte della banda operativa del sistema. Per garantire l'efficacia del barrage jamming e del jamming a banda parziale, gli attaccanti tipicamente hanno bisogno di una elevata potenza di trasmissione, rendendo gli attacchi di jamming piuttosto costosi e poco efficienti, oltre che facilmente identificabili. Lo smart jamming consiste in effettuare attacchi di jamming in modo più efficiente, ad esempio, interrompendo il processo di decodifica fisica attraverso jamming protocol-aware, piuttosto che bloccare un'intera banda di frequenza LTE.

Il modo più semplice per recuperare questi parametri sarebbe quello di ottenerli direttamente dall'UE, utilizzando dei tool di monitoraggio della rete, come NetMonster o Netmonitor su Android, mentre su iPhone sono disponibili nel menù Field Test, componendo il numero $'*3001\sharp12345\sharp*'$. Tuttavia, questi metodi richiedono la cooperazione dell'utente vittima, o almeno di un USIM registrato presso lo stesso operatore target.

E' possibile implementare alcuni tool SDR con srsLTE per ottenere i parametri necessari di qualsiasi operatore senza utilizzare senza alcun USIM registrato, monitorando e decodificando le informazioni trasmesse. Questo metodo è composto da tre fasi:

1. Rilevamento automatico della rete:

   Utilizzando il modulo cell_search di srsLTE è possibile conoscere tutte le reti disponibili nell'area target.

2. Recupero delle informazioni di scheduling:

   Il modulo srsLTE cell_measurement consente lo sniffing del segnale trasmesso da ogni operatore, da cui si ottiene il SIB 1 trasmesso in chiaro. La periodicità delle informazioni di sistema (si-Periodicity) è specifica dei gruppi di SIB, mentre la finestra delle informazioni di sistema (si-WindowLenght) è comune a tutti i SIB.

3. Lista di priorità per la riselezione delle celle interfrequenza:

   A partire dai parametri di scheduling contenuti in SIB 1 è possibile ottenere le informazioni di SIB 3 e SIB 5. Infatti SIB1 viene trasmesso con periodicità nota, mentre tutti gli altri SIB vengono trasmessi a cicli specificati dalle informazioni di scheduling in SIB1. Per estrarre le informazioni da SIB 3 e SIB 5, è stato leggermente modificato ed esteso da [24] il modulo cell_measurement srsLTE[1]. SIB 3 contiene parametri per la riselezione cellulare intra-frequenza (basata su ranking delle celle), mentre SIB 5 per la riselezione inter-frequenza, in cui l'UE sfrutta le priorità assolute delle frequenze per accamparsi sulla frequenza con la massima priorità disponibile. Di conseguenza la priorità contenuta in SIB 3 è quella della frequenza della cella da cui è trasmesso, mentre SIB 5 contiene l'elenco delle frequenze e delle relative priorità delle celle vicine utilizzate dall'operatore.

La figura 3.1 mostra parte del contenuto raccolto dall'analisi dei SIB 1, 3 e 5. L'acquisizione è presa da un operatore italiano del mondo reale (rete LTE banda 3 dell'operatore Wind3). Nell'esempio è possibile vedere che la periodicità dell'informazione del sistema è rf 16, cioè sedici radioframe, la finestra delle informazioni di sistema è di 20 ms. L'elenco delle priorità di riselezione delle celle interfrequenza

[1]codice disponibile a: https://github.com/ansresearch

```
<systemInformationBlockType1>
    <mcc>
        <MCC-MNC-Digit>2</MCC-MNC-Digit>
        <MCC-MNC-Digit>2</MCC-MNC-Digit>
        <MCC-MNC-Digit>2</MCC-MNC-Digit>
    </mcc>
    <mnc>
        <MCC-MNC-Digit>8</MCC-MNC-Digit>
        <MCC-MNC-Digit>8</MCC-MNC-Digit>
    </mnc>
    <trackingAreaCode>30520</trackingAreaCode>
    <cellIdentity>80967681</cellIdentity>
    <si-Periodicity>
        <rf16/>
    </si-Periodicity>
    <sib-MappingInfo>
        <sibType3/>
        <sibType5/>
    </sib-MappingInfo>
    <si-WindowLength>
        <ms20/>
    </si-WindowLength>
</systemInformationBlockType1>

<sib3>
    <cellReselectionServingFreqInfo>    \\1350
        <cellReselectionPriority>6</cellReselectionPriority>
    </cellReselectionServingFreqInfo>
</sib3>

<sib5>
    <interFreqCarrierFreqList>
        <dl-CarrierFreq>3350</dl-CarrierFreq>
        <cellReselectionPriority>7</cellReselectionPriority>

        <dl-CarrierFreq>6200</dl-CarrierFreq>
        <cellReselectionPriority>5</cellReselectionPriority>

        <dl-CarrierFreq>150</dl-CarrierFreq>
        <cellReselectionPriority>5</cellReselectionPriority>

        <dl-CarrierFreq>1675</dl-CarrierFreq>
        <cellReselectionPriority>6</cellReselectionPriority>

        <dl-CarrierFreq>1500</dl-CarrierFreq>
        <cellReselectionPriority>1</cellReselectionPriority>

        <dl-CarrierFreq>2900</dl-CarrierFreq>
        <cellReselectionPriority>1</cellReselectionPriority>
    </interFreqCarrierFreqList>
</sib5>
```

Figura 3.1: In figura sono mostrate le informazioni raccolte relative a SIB 1, 3 e 5 [24]

è composto dalla frequenza su cui è trasmesso SIB 3, cioè 1350, e quelli che sono presenti in SIB 5. I risultati sono stati raccolti implementando l'eNodeB con dei computer con Intel Core i7 CPU con clock di 4.5 GHz. Come OS è stato utilizzato Ubuntu 18.04 LTS con kernel con versione 5.3.0-53-lowlatency.

Implementazione del jammer

Nelle aree in cui sono presenti più celle che operano su bande diverse, un utente malintenzionato dovrebbe creare più eNodeB falsi, uno per ogni frequenza cellulare, il che comporterebbe una radio SDR e un laptop dedicati per ogni frequenza. Tuttavia, è possibile sostituire diversi falsi eNodeB con un solo hopping jammer. Spostandosi periodicamente attraverso le frequenze delle altre celle, il jammer disturba la comunicazione tra l'UE e l'eNodeB attualmente connesso, in questo modo l'UE selezionerà ripetutamente un nuovo eNodeB fino a quando non si connette all'IMSI Catcher e rivela il suo IMSI. Per aumentare l'efficienza del disturbo è opportuno utilizzare un jamming con un segnale con una struttura LTE. Il segnale generato non copre l'intero spettro LTE durante un intervallo di salto T_{hop}, ma una piccola finestra di N_{sub} sottoportanti contigue che si sposta rapidamente all'interno del canale LTE nel tempo, con periodo configurabile T_{subhop}. Per creare il segnale di disturbo, il software lavora nel dominio della frequenza e assegna ampiezze e fasi casuali a ciascuna delle portanti che compongono il subframe generato. Successivamente ricrea il segnale nel dominio del tempo applicando l'IDFT disponibile nella libreria FFTW3.

Model	OS	Modem	3GPP Rel./LTE Cat.	OpenAirInterface				srsLTE			
				w/o jammer		w/ jammer		w/o jammer		w/ jammer	
				Service Request	TAU Request	Service Request	TAU Request	Service Request	TAU Request	Service Request	TAU Request
Samsung Galaxy S9	Android 9	Exynos 9810	13 / 18	✓	✓	✓	✓	✓	✓	✓	✓
Samsung Galaxy A7 2018	Android 10	Exynos 7885	11 / 12	✓	✓	✓	✓	✓	✓	✓	✓
Samsung Galaxy Note Pro	Android 5	Snapdragon 800	8 / 4	✓	✓	✓	✓	✓	✓	✓	✓
Nexus 5	Android 6	Snapdragon 800	8 / 4	✓	✓	✓	✓	✓	✓	✓	✓
Realme X2 Pro	Android 10	Snapdragon X24	13 / 20	✓	✓	✓	✓	✓	✓	✓	✓
Realme 6	Android 10	Helio G90T	12 / 13	✓	✓	✓	✓	✓	✓	✓	✓
Xiaomi Redmi Note 7	Android 9	Snapdragon X12	11 / 12	✓	✓	✓	✓	✓	✓	✓	✓
Xiaomi Mi A1	Android 9	Snapdragon X9	10 / 7	✓	✓	✓	✓	✓	✓	✓	✓
Huawei Mate 20 Pro	Android 9	HiSilicon Kirin 980	13 / 21	✓	✓	✓	✓	✓	✓	✓	✓
Huawei P30 Lite	Android 9	HiSilicon Kirin 710	11 / 12	✗	✓	✓	✓	✗	✓	✓	✓
Huawei P8 Lite	Android 7	HiSilicon Kirin 655	10 / 6	✓	✓	✓	✓	✓	✓	✓	✓
Asus Zenfone 2	Android 5	Intel XMM 7260	8 / 4	✓	✓	✓	✓	✓	✓	✓	✓
Vodafone Smart Ultra 6	Android 5	Snapdragon X5	8 / 4	✓	✓	✓	✓	✓	✓	✓	✓
Orange Neva 80	Android 6	Snapdragon X8	10 / 6	✓	✓	✓	✓	✓	✓	✓	✓
ZTE Blade v8 lite	Android 7	MediaTek MT6750	10 / 6	✓	✓	✓	✓	✓	✓	✓	✓
ZTE Blade A910	Android 6	MediaTek MT6735	8 / 4	✓	✓	✓	✓	✓	✓	✓	✓
ZTE Blade A452	Android 5	MediaTek MT6735	8 / 4	✓	✓	✓	✓	✓	✓	✓	✓
iPhone 11	iOS 13/14	Intel XMM 7660	13 / 18	✗	✗	✓	✓	✗	✗	✓	✓
iPhone SE 2020	iOS 14	Intel XMM 7660	13 / 18	✗	✗	✓	✓	✗	✗	✓	✓
iPhone XS	iOS 13	Intel XMM 7560	12 / 16	✗	✗	✓	✓	✗	✗	✓	✓
iPhone 8	iOS 13	Intel XMM 7480	12 / 16	✗	✗	✓	✓	✗	✗	✓	✓
iPhone 7	iOS 13	Intel XMM 7360	11 / 9	✗	✓	✓	✓	✗	✓	✓	✓
iPhone SE	iOS 12/14	Qualcomm MDM9625M	8 / 4	✓	✓	✓	✓	✓	✓	✓	✓
iPhone 5S	iOS 12	Qualcomm MDM9615M	8 / 3	✓	✓	✓	✓	✓	✓	✓	✓
Huawei E3272 USB Stick	-	HiSilicon Balong 710	8 / 4	✓	✓	✓	✓	✓	✓	✓	✓
Huawei E392 USB Stick	-	Qualcomm MDM9200	8 / 3	✓	✓	✓	✓	✓	✓	✓	✓
iPhone 12	iOS 14	Snapdragon X55	15 / 22	✓	✓	✓	✓	✓	✓	✓	✓
Xiaomi Mi 10	Android 10	Snapdragon X55	15 / 22	✓	✓	✓	✓	✓	✓	✓	✓
Oppo Reno	Android 10	Snapdragon X50	N/A	✓	✓	✓	✓	✓	✓	✓	✓
Quectel AG550Q	Android custom	AG215S	N/A	✓	✓	✓	✓	✓	✓	✓	✓

✓ : IMSI captured
✗ : IMSI not captured

Figura 3.2: In figura sono mostrati i risultati relativi alla riuscita dell'Imsi Catching per differenti dispositivi in condizioni differenti

3.1.2 Risultati sperimentali

Risultati con diversi telefoni

Sono stati fatti esperimenti su diverse marche di telefoni cellulari. Infatti, dato che i produttori conoscono le vulnerabilità che rendono possibili questi attacchi potrebbero progettare dispositivi con dei meccanismi che li rendano più difficili da realizzare. I risultati mostrano che i telefoni commerciali non implementano tali meccanismi, infatti quasi tutte le marche di telefoni testate cedono immediatamente anche senza jamming.

Dipendenza dal sistema operativo

Sono stati considerati anche dispositivi con differenti SO, in modo da analizzare come quest'ultimo influenza il comportamento del dispositivo. Sono incluse diverse versioni del sistema operativo sia per Android che per iOS. A prima vista sembrerebbe che il sistema operativo abbia un ruolo rilevante, in quanto i modelli di Iphone da 7 a 11 inclusi mostrano l'IMSI solo dopo jamming esplicito. Tuttavia, dato che il modello 12 (che utilizza lo stesso iOS-14 dell'iPhone 11) mostra un comportamento analogo a quello dei modelli Android si può escludere una dipendenza dal SO.

Dipendenza dal modem

Come mostrato nella tabella, tutti i modem considerati sono vulnerabili a questi attacchi, indipendentemente dalla versione 3GPP che supportano (che va dalla release 8 fino alla release 15). Ciò dimostra che gli operatori non hanno implementato alcuna correzione contro gli attacchi di IMSI Catching, o che comunque i meccanismi introdotti non hanno avuto effetto. Tuttavia, come descritto nel paragrafo precedente, nel caso dell'iPhone dal modello 7 fino al modello 11 incluso è necessario effettuare jamming esplicito per acquisire l'IMSI, il che può richiedere diversi minuti. Ciò non avviene invece con l'iPhone12, che mantiene lo stesso SO, ma utilizza un modem di un marchio differente (da Intel a Qualcomm Snapdragon). Comunque, questo non sembra un comportamento intenzionalmente progettato da Intel per prevenire questi attacchi, ma piuttosto la conseguenza di una diversa gestione di mitigazione delle interferenze.

Dipendenza dall'operatore

Tutte le procedure e i parametri coinvolti negli scenari di IMSI Catching sono gestiti dall'operatore presso cui l'UE è registrato, tuttavia le vulnerabilità che sfruttate da questo attacco sembrano maggiormente legate al modem radio e al firmware del dispositivo. Effettuando degli esperimenti su USIM di tutti e quattro gli operatori italiani (Wind3, Vodafone, TIM, Iliad) con uno dei telefoni Android (Realme X2 Pro di Android 10), non è emersa alcuna correlazione con l'operatore della vittima. Infatti, come mostrato in figura, l'attacco ha avuto successo per tutte le combinazioni dei quattro casi dell'attacco: i quattro operatori, le due tecnologie di rogue BS, le due tecniche di attacco e l'utilizzo o meno del jamming.

Esperimenti con diverse strategie di jamming

Per i seguenti esperimenti sono stati utilizzati i dispositivi: Nexus 5 con Android, iPhone SE, iPhone 11 e iPhone 12. Sono stati utilizzati segnali provenienti da quattro eNodeB reali: due sono celle primarie (con banda 3 e 1) e due sono secondarie (con banda 7 e 20).

In questo esperimento i telefoni sono assegnati alla cella primaria sulla banda 3 o alla secondaria sulla banda 7, in quanto sono le celle con i livelli di segnale più elevati. Sono state utilizzate due strategie di attacco, chiamate attack mode 1 (m1) e attack mode (m2) Attack mode 1 inizia con i tre jammer e l'IMSI Catcher sintonizzati sulla stessa cella primaria, dunque il telefono è costretto a connettersi ad una delle tre celle rimanenti (l'altra primaria e le due secondarie). A questo punto i tre jammer vengono

ri-sintonizzati, ognuno su una cella differente, e si misura l'intervallo di tempo prima che l'IMSI venga trasmesso all'IMSI Catcher. Attack mode 2 inizia con i tre jammer pre-sintonizzati su celle differenti, in modo tale che il telefono sia già collegato alla cella target quando l'IMSI Catcher viene acceso. Anche in questo caso viene misurato il tempo necessario prima che l'attacco abbia successo. In entrambi gli scenari l'IMSI Catcher è configurato per coprire una cella da 6 PRB , l'esperimento viene ripetuto 20 volte, per un tempo di osservazione di 200 s. Il tasso di successo per le due strategie di attacco è identico per iPhone SE e 12, mentre con iPhone 11 e Nexus 5 la modalità m2 fallisce nel 20% dei casi. Questi fallimenti si verificano perché i telefoni eseguono il downgrade a EDGE o 3G e non tornano a LTE entro il tempo di osservazione. Ciò può essere dovuto al fatto che i due telefoni considerano la comparsa improvvisa dell'IMSI Catcher come indicatore di un canale rumoroso e vietano il canale per un tempo maggiore del tempo di osservazione.

Attacco eseguito su più dispositivi nelle vicinanze

In caso di attacco eseguito su più dispositivi, tutti contemporaneamente in prossimità dell'eNodeB falso, attuato con tecnica m1, si ha comunque che il tasso di successo è quasi del 100%. I tempi mediani dell'intervallo di tempo per ottenere l'IMSI non cambiano rispetto alle altre modalità di attacco m1 e m2, ma si osserva una variabilità maggiore per Nexus 5 e iPhone SE, il che dovrebbe essere dovuto alla configurazione dei parametri RACH (Random Access CHannel). Questo esperimento [24] è un indicatore della fattibilità dell'attacco in uno scenario reale, in cui molte persone che utilizzano più dispositivi stanno vicine l'una all'altra.

	con jamming		senza jamming	
	% di successo	T_{max}	% di successo	T_{max}
iPhone SE	70%	32s	100%	138s
iPhone 11	0	-	75%	190s
iPhone 12	25%	23s	100%	74s
Nexus 5	35%	80 s	95%	100s

Tabella 3.1: Percentuali di successo e tempi massimi per questo attacco senza e con hopping jammer

Esperimenti in condizioni di attacco persistente

Finora sono stati considerati attacchi mirati, cioè attacchi che vengono attivati quando viene rilevata la presenza della vittima, ma esistono anche scenari in cui l'attacco è persistentemente attivo e viene utilizzato come strumento di monitoraggio dell'ambiente. Al riguardo sono stati effettuati una serie di esperimenti in cui il rogue eNodeB è costantemente attivo sopra la cella primaria di banda 3. Per ogni telefono è stato misurato il tempo T_{IMSI}, senza controllare la cella a cui si collega inizialmente. Anche in questo caso l'esperimento è stato ripetuto 20 volte, con e senza hopping jammer, e con tempo di osservazione di 200 s. Nella tabella 3.1 sono indicate le percentuali di successo e i tempi massimi osservati T_{IMSI}. Questi risultati confermano i dati riportati in precedenza.

Per quanto riguarda risultati senza hopping jammer si può osservare che le percentuali di successo dell'attacco sono basse, ma anche i tempi massimi di attacco lo sono. Questo si verifica nello scenario in cui i telefoni sono inizialmente connessi a ud una cella con la stessa banda utilizzata dal rogue eNodeB, e, dopo aver rilevato l'eNodeB quando viene acceso, tendono a collegarvisi immediatamente, in quanto ha un livello del segnale più elevato. Per quanto riguarda i risultati con hopping jammer si osserva che il tasso di successo aumenta fino al 100%, ma aumenta anche la durata dei tempi

di attacco massimi. Questi risultati si verificano quando i telefoni sono inizialmente collegati a una cella con frequenza diversa da quella della rogue eNodeB: iniziano a spostarsi dalle frequenze, che vengono consecutivamente occupate dal jammer, fino ad arrivare casualmente alla cella IMSI Catcher. Nel caso di iPhone 11, è stato verificato che con tempi di osservazione più lunghi è possibile ottenere l'IMSI, il che conferma che non viene eseguito alcun algoritmo contro gli attacchi di IMSI Catching.

3.2 Attacchi con overshadowing

L'attacco Signal Overshadowing (SigOver) [18] è un attacco sul livello fisico LTE, e appartiene alla categoria di attacchi di manipolazione di messaggi e segnali, come gli attacchi di spoofing. SigOver è un tipo di attacco di iniezione del segnale in cui l'attaccante trasmette un subframe in una posizione tempo-frequenza del canale broadcast e paging LTE con una potenza maggiore rispetto a quella del segnale legittimo trasmesso dall'eNodeB dell'operatore. L'attacco sfrutta l'effetto di cattura, cioè l'UE quando riceve più segnali sovrapposti contemporaneamente decodifica quello con potenza maggiore. Pertanto, l'attacco SigOver può manipolare i messaggi ricevuti dall'UE sovrascrivendo una parte del segnale legittimo trasmesso dal normale eNodeB, senza interferire con la comunicazione e la sincronizzazione tra eNodeB e UE.

Una causa che determina la fattibilità dell'attacco è che il protocollo LTE a livello fisico non è abbastanza robusto e flessibile per far fronte in modo corretto ed efficace a varie situazioni anomale, ad esempio quando un UE rileva un Primary Synchronization Signal (PSS) valido senza un Secondary Synchronization Signal (SSS) associato. Il PSS e SSS sono canali del livello fisico utilizzati per la sincronizzazione: il PSS contiene

l'identificativo della cella a livello fisico (PCI), mentre il SSS contiene l'identificativo del gruppo di celle a livello fisico e viene utilizzato per la sincronizzazione dei frame. Pertanto, gli attacchi di spoofing PSS possono essere realizzati trasmettendo PSS falsi con potenza maggiore per impedire all'UE di rilevare un PSS legittimo.

Un'altra ragione alla base di questo attacco sono i messaggi broadcast e i messaggi iniziali tra l'UE e la rete, che non utilizzano meccanismi di protezione adeguati, come la protezione d'integrità. Questi attacchi sono più difficili da individuare rispetto ad attacchi basati su false BS, hanno una maggiore efficienza energetica e una maggiore sostenibilità. Possono essere utilizzati per causare violazione della privacy degli utenti e attacchi DoS.

In seguito vedremo alcuni esempi di attacchi basati su questa tecnica.

3.2.1 AdaptOver

AdaptOver è un sistema di attacco MITM (Man-In-The-Middle) progettato per le reti cellulari, in particolare per LTE e 5G-NSA, basato su overshadowing adattativo. Implementa sniffing adattivo del downlink e l'overshadowing adattativo sia sul downlink che sull'uplink (è il primo framework che lo permette), consentendo a un utente malintenzionato di iniettare messaggi a livello NAS. Utilizzando l'overshadowing in uplink, AdaptOver può modificare i messaggi provenienti dall'UE in qualsiasi punto all'interno di una cella, indipendentemente dalla posizione dell'UE o dell'attaccante.

Assunzioni sull'attacco

Per questi attacchi si presume che l'utente malintenzionato non abbia accesso ad alcun materiale crittografico e non sia in grado di compromettere nessuna parte dell'infrastruttura della rete o delle apparecchiature dell'utente. L'utente malintenzionato opera solo sul canale wireless. Inoltre l'attaccante si trova all'interno o in prossimità della cella target, in modo tale che possa decodificare il downlink, oltre che essere in grado di ricevere e decodificare i messaggi trasmessi dall'UE target. Inoltre per effettuare l'overshadowing l'attaccante deve trasmettere con una potenza sufficiente in modo tale che il suo segnale sia 3dB più forte del segnale legittimo al ricevitore della vittima (o della stazione base in caso di overshadowing uplink). Poiché la potenza di trasmissione di un UE è regolata nello standard LTE e dipende dalla distanza dalla stazione base, risulta più facile effettuare overshadowing in uplink, oltre che richiedere meno potenza. Viene utilizzato hardware commerciale off-the-shell (COTS) per decodificare le comunicazioni e inserire messaggi. Un variante di questo attacco prevede che l'attaccante è a conoscenza anche del numero di telefono della vittima.

Raccolta delle informazioni di connessione

Ogni messaggio inviato sul downlink o uplink di una particolare stazione base viene identificato con un identificatore a breve termine RNTI (Radio Network Temporary Identifier). E' un identificatore di livello 2 assegnato a connessioni radio attive all'interno della stessa cella. Un RNTI può essere assegnato a un particolare UE o riservato per uno scopo specifico (ad esempio, configurazione del sistema broadcast, paging o random access).

Una caratteristica distintiva di AdaptOver è il suo adattamento a ciascuna connessione UE; questo obiettivo viene raggiunto ascoltando sul downlink. Come mostrato

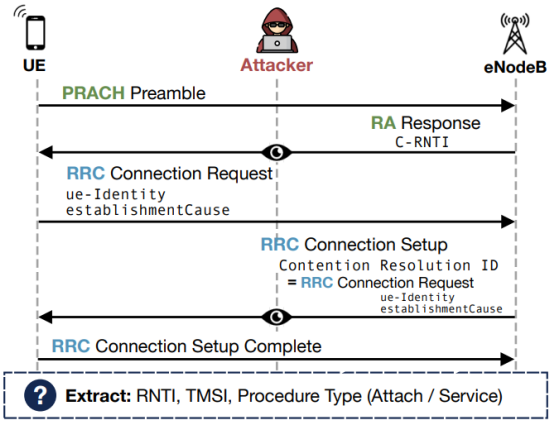


Figura 3.3: Sniffing in downlink di AdaptOver

in figura 3.3, AdaptOver intercetta le risposte RA e quindi conosce il C-RNTI di tutte le connessioni. Successivamente, l'UE invia una richiesta di connessione RRC (RRC Connection Request). A seconda della procedura che sta avvenendo, il campo ue-Identity contiene un numero casuale (Attach Request) o TMSI (Service Request). Il campo establishmentCause indica inoltre il tipo di procedura di connessione successiva. L'eNodeB accetta questa richiesta con una risposta di configurazione della connessione RRC (RRC Connection Setup). A livello MAC questa risposta contiene il campo Contention Resolution ID, che codifica la RRC Connection Request inviata dall'UE.

Inoltre il messaggio RRC Connection Setup contiene informazioni sulla codifica a livello fisico dei successivi messaggi, che AdaptOver deve utilizzare per generare correttamente il segnale di overshadowing.

AdaptOver: Imsi Extractor in uplink

AdaptOver effettua l'overshadowing della Attach/Service Request con una Attach Request contenente un TMSI casuale sconosciuto all'MME. Dato che l'MME non è in grado di associare l'identificativo temporaneo ad una connessione UE precedente, invia un messaggio di Identity Request. Di conseguenza l'UE risponde con il suo IMSI incluso nella Identity Response. L'attaccante è in grado di ricevere l'IMSI inviato dall'UE, per le assunzioni fatte in precedenza.

La procedura continua con la procedura di autenticazione, ma ha esito negativo a causa della modalità di protezione. Questo perché, nel Security Mode Command (comando di modalità protezione), la rete riproduce le funzionalità/risorse UE ricevute nella Attach Request. Poiché AdaptOver ha oscurato quella richiesta di collegamento con funzionalità non corrispondenti a quelle dell'UE (cioè tutte impostate su false), l'UE reagirà con Security Mode Reject e interromperà l'intero tentativo di connessione. Tuttavia, l'UE ritenterà immediatamente la procedura originale di Attach/Service Request, stavolta con il TMSI valido. Questo consente di collegare tra loro mediante intercettazioni passive le connessione precedenti e future contenenti solo il TMSI.

Implementazione

Decodifica della trasmissione downlink

La stazione base pianifica le trasmissioni di tutti gli UE in uplink. Invia allocazioni di risorse di tempo e frequenza agli UE, consentendo a più UE di trasmettere dati contemporaneamente senza interferire. Successivamente la stazione base decodifica

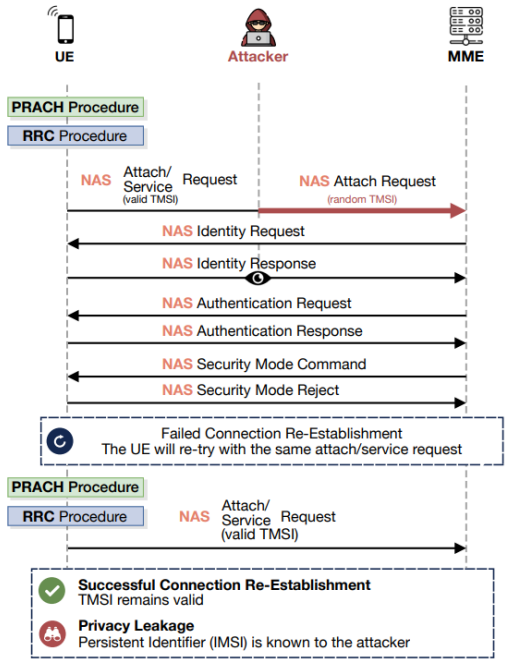


Figura 3.4: In figura AdaptOver in uplink

le risorse precedentemente assegnate all'UE. Di conseguenza, AdaptOver deve decodificare e bufferizzare tutte le allocazioni di risorse uplink destinate alla vittima. Inoltre, per consentire attacchi selettivi alle UE in base al loro TMSI, AdaptOver traccia e decodifica la connessione UE fino a che non riceve un messaggio RRC Setup Connection contenente il campo Contention Resolution a livello MAC, da cui acquisisce il TMSI.

Gestione potenza

L'attaccante e l'UE legittimo trasmettono contemporaneamente sulla stessa frequenza: grazie all'effetto di cattura solo il segnale ricevuto con la potenza più elevata viene decodificato dalla stazione base. La potenza di trasmissione dell'UE legittimo nella procedura PRACH (Physical Random Access Channel) è controllata ad anello

aperto, cioè basata su un modello statico. Successivamente, la stazione base controlla attivamente la potenza di trasmissione dell'UE inviando comandi TPC (Transmit Power Control) a livello MAC. Gli UE più vicini alla stazione base trasmettono con bassa potenza, mentre quelli più lontani con potenza maggiore. Grazie a questo meccanismo di controllo della potenza, AdaptOver può oscurare un UE legittimo ovunque in una cella poiché la potenza richiesta rimane gran parte del tempo costante. Inoltre, dato che la potenza erogata da un SDR è limitata è necessario amplificare il segnale se non è molto vicino alla stazione base. Per determinare la potenza richiesta per una determinata posizione l'attaccante può misurare la potenza ricevuta della stazione base e aggiungere il margine di potenza del path loss stimato oppure può aumentare il guadagno della trasmissione fino a quando l'attacco non funziona in modo affidabile.

Sincronizzazione

Per allineare i tempi di ricezione di più trasmissioni UE la stazione base indica all'UE di inviare i propri dati un certo intervallo di tempo in anticipo o in ritardo, indicato nel comando Timing Advance (TA). AdaptOver è progettato per ignorare tutti i comandi TA e applica uno sfasamento temporale statico. Se la posizione della stazione base è nota, l'attaccante può calcolare questo valore, altrimenti può connettersi alla stazione base con srsUE e leggere il valore TA inviato all'UE.

Setup in laboratorio

Per verificare il comportamento dell'UE è possibile configurare una rete LTE privata utilizzando Amarisoft Callbox [8], una scatola schermata [5], con all'interno l'UE target e un USRP B210 per implementare l'attaccante.

Esperimenti con reti reali

Per implementare l'attaccante è stata utilizzata una software defined radio USRP B210 collegata tramite USB 3.0 a un laptop con una CPU Intel Core i7-11800H. Per amplificare i segnali due schede di valutazione dell'amplificatore Qorvo (TQP9111-PCB2600), collegate ad un alimentatore da 5V. Il filtraggio è stato effettuato utilizzando un duplexer dielettrico per la banda target. Infine, è stata utilizzata l'antenna Mikrotik mAnt LTE 5o 5dBi. Dopo avere collegato ogni telefono alla rete commerciale vengono inviati una serie di SMS silenti (Short Message Type 0), che non provocano notifiche o segnali acustici, all'UE per estrarre il suo TMSI. Successivamente, dopo avere lanciato l'attacco IMSI Extractor è stato verificato di aver ricevuto un messaggio di Identity Request in downlink. I telefono che sono stati considerati in questo esperimento sono: Huawei P20, chePro, Huawei P30, Huawei P30 Lite, Huawei P40, Samsung A8, Samsung S10, Samsung S21, LG Nexus 5X, iPhone 6S, iPhone 7, iPhone 8, iPhone 11 , iPhone X, Xiaomi Mi 9, Xiaomi Mix 3, Pixel 2, Pixel 3a, Pixel 4 , Pixel 5, OnePlus 9 Pro. L'attacco ha avuto esito positivo per tutti i telefoni considerati.

Sono disponibili diverse app che consentono di rilevare la presenza di Imsi Catcher, come ad esempio CellularPrivacy e SnoopSnitch. Queste app non sono progettate per riconoscere attacchi effettuati con AdaptOver, come si può verificare dal loro codice sorgente. Le app di rilevamento di IMSI Catcher si basano sul rilevamento di anomalie da parte dell'UE, ad esempio il numero di celle vicine, per cui anche in questo caso non rilevano l'attacco. I meccanismi di rilevamento attuali contro IMSI Catchers funzionano rilevando false BS. Questi framework funzionano confrontando

le posizioni open source delle stazioni base con i rapporti misurati dagli utenti o da dispositivi speciali o rilevando anomalie nel comportamento delle stazioni base da parte delle UE. Per cui queste tecniche non funzionano poiché un UE si collega a una stazione base reale.

AdaptOver: Imsi Extractor in downlink

Per effettuare questo attacco[17] è necessario utilizzare degli sniffer sia in downlink che in uplink. Come per il caso precedente, l'attacco viene attivato quando l'eNodeB invia un messaggio di RRC Connection Setup, che avviene quando l'UE passa da uno stato idle a connected.

Overshadowing con Identity Request

Dopo che l'UE invia un messaggio di Attach/Service Request, l'eNodeB dell'attaccante effettua l'overshadowing della risposta con un messaggio di Identity Request, come mostrato in figura 3.5.

Anche se la stazione base legittima procede con una procedura di connessione, il messaggio viene oscurato da AdaptOver che invia un messaggio con una potenza superiore. Pertanto, l'UE decodifica solo la richiesta di identità inviata dall'attaccante. La stazione base legittima non riceve l'Identity Response inviato dall'UE perché AdaptOver modifica anche l'allocazione dell'uplink durante l'attacco. Per effettuare questo attacco è richiesta una potenza di trasmissione leggermente superiore rispetto a quella della stazione base. L'utilizzo del messaggio di Identity Request è solo una possibile implementazione concreta di IMSI Extractor. E' possibile utilizzare altri

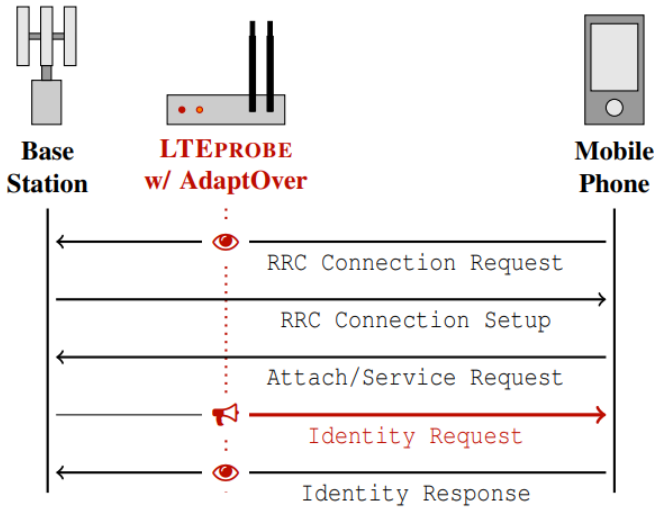


Figura 3.5: In figura AdaptOver in downlink

messaggi che attivano la trasmissione dell'IMSI da parte dell'UE (ad esempio, Service Reject con causa 9, "L'identità UE non può essere derivata dalla rete").

Dal punto di vista dell'eNodeB, la connessione con l'UE si è interrotta (ad esempio, a causa di una cattiva ricezione lato l'UE), quindi non rileva alcuna anomalia. Inoltre, questo attacco risulta conforme alle specifiche del protocollo sia dal punto di vista della stazione base che dell'UE, per questo motivo questo attacco non è rilevabile dai framework esistenti.

Implementazione

IMSI Extractor è stato valutato utilizzando un software di stazione base di Amarisoft sull'hardware AMARI Callbox Mini [4]. L'attacco è stato eseguito contro 17 telefoni sia per i messaggi di Attach Request che di Service Request. Come è mostrato in figura, l'attacco ha avuto successo per tutti i 17 telefoni nel caso di Attach

UE model	Identification Attach Request	Identification Service Request
Samsung Galaxy s10	yes	yes
Samsung Galaxy a8	yes	yes
Huawei P20 Pro	yes	yes
Huawei P30 Lite	yes	yes
Huawei P30	yes	yes
Xiaomi Mi9	yes	yes
Xiaomi MiX 3	yes	yes
Google Nexus 5X	yes	yes
Google Pixel 2	yes	yes
Google Pixel 3a	yes	yes
HTC U12+	yes	yes
OnePlus 7T	yes	yes
iPhone 6s	yes	yes
iPhone 7	yes	no
iPhone 8	yes	yes
iPhone X	yes	yes
iPhone 11	yes	yes
iPhone 11 Pro	yes	yes

Figura 3.6: In figura i risultati ottenuti per i diversi telefoni considerati e le due tipologie di messaggi

Request, mentre nel caso di Service Request è andato a buon fine per tutti i telefoni eccetto iPhone7. Gli UE, dopo aver trasmesso l'Identity Response, si sono connessi correttamente alla rete. L'attacco ha funzionato correttamente anche con la rete di un operatore nazionale. La configurazione consisteva in un vero e proprio Ericsson eNodeB, collegato alla core network dell'operatore. Le antenne dell'operatore e i dispositivi d'attacco sono stati installati all'interno di una gabbia di Faraday di 5×6 m, in modo da potere eseguire i test utilizzando la stessa configurazione della rete esterna senza influenzare gli utenti reali.

Capitolo 4

Vulnerabilità logiche del protocollo AKA

Esistono diversi attacchi esistenti che sfruttano le debolezze di progettazione del protocollo AKA, cioè non legate alla loro implementazione da parte degli operatori di reti mobili.

In questo capitolo andremo ad analizzare in particolare gli attacchi di "AKA linkability" e "SQN disclosure". L'attacco di "SQN exposure" consente a un utente malintenzionato di ricavare la posizione di un UE vittima, mentre "AKA linkability" consente di identificare e confermare la presenza di un UE in una specifica area e di tracciarlo. Il materiale presentato è tratto dalle pubblicazioni [9] e [36].

4.1 AKA linkability

Gli attacchi di linkability AKA [36] sfruttano il fatto che l'UE target e gli altri UE rispondono in modo diverso a un messaggio replicato di Authentication Request o di Security Mode Command. Nel caso di un messaggio di Authentication Request replicato, l'UE target include nella risposta (Authentication Failure message) un errore di sincronizzazione come causa dell'errore, mentre gli altri UE usano "MAC failure" come causa.

4.2 SQN disclosure

Il seguente attacco [9] sfrutta delle vulnerabilità logiche che sono presenti in tutte le versioni del protocollo AKA (comprese le varianti 5G AKA e EAP). Infatti in tutte queste varianti è possibile conoscere parzialmente il valore di SQN con attacchi di replay mirati, a causa dell'utilizzo di Exclusive-OR (XOR) e della mancanza di casualità.

Conoscere anche solo parzialmente il valore di SQN porta ad una nuova tipologia di attacchi alla privacy (ad esempio, attacchi di monitoraggio dell'attività): un attaccante attivo può sfruttare le stazioni base false per apprendere informazioni sul consumo di servizi mobili degli utenti e tracciarli, anche quando si allontanano dall'area di attacco. In effetti, anche quando gli utenti utilizzano servizi mobili al di fuori dell'area di attacco, informazioni relative a questi servizi possono essere comunque apprese da un avversario la volta successiva in cui l'UE entra di nuovo

nell'area di attacco. Questo perché, indipendentemente dalla sua posizione, l'attività dell'UE ha come effetto l'incremento del contatore SQN memorizzato nell'HN.

Come riportato anche nella specifica del protocollo AKA, conoscere il valore di SQN consente di violare la privacy degli utenti. Di conseguenza il protocollo prevede che venga nascosto utilizzando la Anonimity Key AK, trasmettendo il valore in AUTN:

$CONC^* = SQN_{HN} \oplus AK$, che consente all'UE di estrarre SQN_{HN} calcolando AK come riportato sopra.

4.2.1 Acquisizione del SQN

Di seguito viene mostrato come un utente malintenzionato attivo che conosce l'identità di qualsiasi UE (temporanea o permanente) è in grado di appendere gli n bit meno significativi di SQN_{HN}. Le vulnerabilità sfruttate da questo attacco sono la mancanza di casualità e l'uso di XOR in AUTS.

Il numero di sequenza trasmesso in caso di procedura di riautenticazione:

$CONC^* = SQN_{UE} \oplus AK^*$ dove $AK^* = f5^*(RAND, K)$.

Il valore RAND viene inviato all'UE all'interno del messaggio di Authentication Request, insieme ad AUTN. Pertanto, se l'UE riceve due volte una stessa challenge (R, AUTN) che genera due errori di sincronizzazione, vengono trasmessi i valori:

$CONC_1^* = SQN_{UE}^1 \oplus AK_1^*$ e $CONC_2^* = SQN_{UE}^2 \oplus AK_2^*$ tale che $AK_1^* = f5^*(R, K) = AK_2^*$. Pertanto, un attaccante che ha una challenge autentica può trasmetterla in due istanti di tempo differenti t_1 e t_2, e ricavare i valori $CONC_1^*$ e $CONC_2^*$ per calcolare:

$$CONC_1^* \oplus CONC_2^* = (SQN_{UE}^1 \oplus AK_1^*) \oplus (SQN_{UE}^2 \oplus AK_2^*) = SQN_{UE}^1 \oplus SQN_{UE}^2$$

dove SQN_{UE}^i è il valore di SQN_{UE} all'istante t_i.

Scegliendo opportunamente gli istanti di tempo t_i è possibile conoscere il valore di SQN. L'attaccante recupera prima $2^n + 2$ nuove sfide di autenticazione consecutive destinate all'UE di destinazione e ne trasmette 2 (n + 2) all'UE.

In una prima fase (ciclo for i = da 0 a 2^n, in figura 4.1), l'attaccante deve recuperare le challenge consecutive $(R_i, AUTN_i)$ destinate al UE target. Queste challenge vengono ottenute dall'utente prima che sia effettuata l'autenticazione, e dunque sia stabilito un canale sicuro, ma dopo che sia avvenuta l'identificazione. Per cui per ottenere queste challenge l'attaccante deve prima ottenere un'identità valida dell'UE (ad esempio, IMSI o un TMSI/GUTI). Inoltre, dato che SQN_{HN} viene incrementato di 1 dopo il calcolo di ogni challenge viene calcolato in funzione di un valore SQN pari a $SQN_{UE}^0 + i$ (in seguito verrà indicato con $SQN_{HN}(AUTN_i)$).

Subito dopo la prima fase, l'attaccante invia all'UE la prima challenge che ha ottenuto: $(R_0, AUTN_0)$ in un messaggio di Authentication Request, come è visibile in figura 4.1. Per l'UE questa challenge è autentica: sia la verifica con il MAC ha successo, sia quella con $SQN_{HN}(AUTN_i) = SQN_{HN}^0 + i$ (la verifica di freschezza).

A questo punto (prima del secondo ciclo), SQN_{UE} è pari a $SQN_{HN}^0 + 1$. Quindi, l'attaccante invia nuovamente la challenge $R_0, AUTN_0$, stavolta producendo un errore

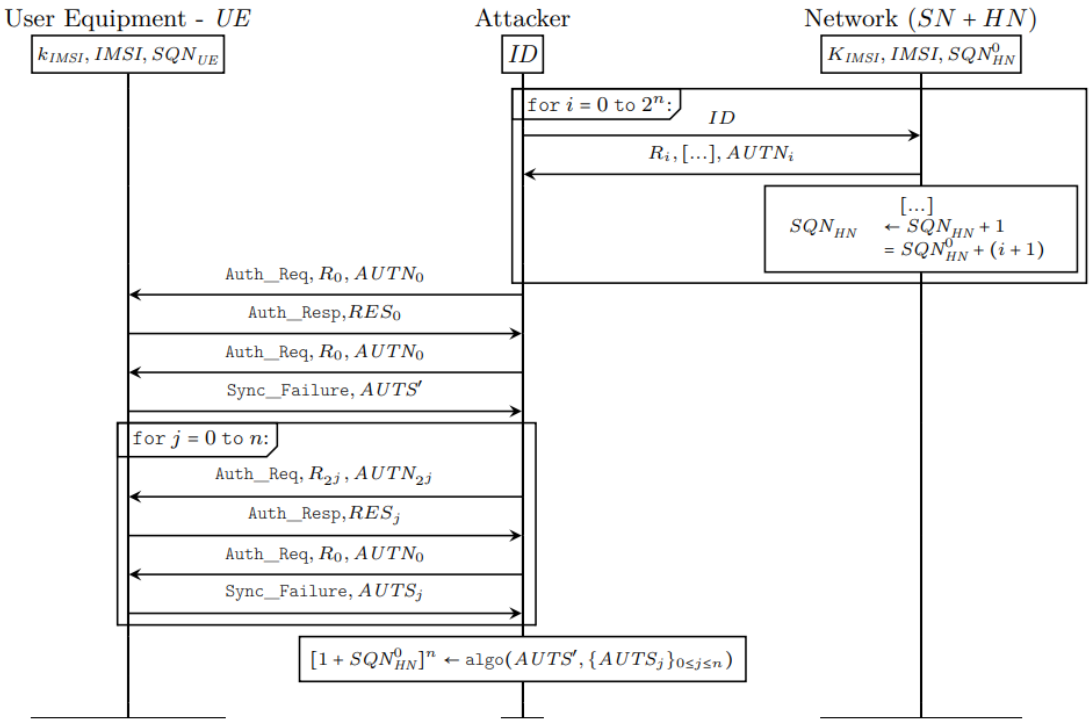


Figura 4.1: I messaggi scambiati durante tutte le fasi di questo attacco.

di sincronizzazione $Synch\_Failure$ contenente:

$AUTS' = <c', MAC^*>$ dove $c' = (SQN0_{HN} + 1) \oplus f5^*(RAND_0, K)$ include SQN nascosto.

Nell'ultima fase (ciclo da j = 0 a n), l'attaccante invia $R_{2^j}, AUTN_{2^j}$ che viene accettato dall'UE, in modo tale che l'UE aggiorni il suo SQN_{UE} a:

$SQN_{UE} = SQN_{HN}(AUTN_{2^j}) + 1 = SQN^0_{HN} + 2^j + 1$.

Dopo ogni iterazione del ciclo, l'attaccante trasmette nuovamente $R_0, AUTN_0$ provocando un errore di sincronizzazione contenente

$AUTS_j = <c^*_j, MAC^*_j>$ con $c_j = (SQN^0_{HN} + 2^j + 1) \oplus f5^*(RAND_0, K)$.

L'algoritmo $algo()$, visibile in 4.2, ha in input gli n + 2 messaggi AUTS e produce in output gli n bit meno significativi di $1 + SQN^0_{HN}$.

Dato che $c' = (SQN^0_{HN} + 1) \oplus f5^*(RAND_0, K)$, per ogni $0 \leq j \leq n$ vale che:

$c' \oplus c_j = (1 + SQN^0_{HN}) \oplus (2^j + 1 + SQN^0_{HN})$.

Indichiamo con δ_i il valore $c' \oplus c_i$ e con $X = 1 + SQN^0_{HN}$, che è la quantità di cui si deducono gli n bit meno significativi.

Si ha che $\delta_i = (2^i + X) \oplus X$ per ogni $0 \leq i \leq n$.

L'algoritmo consiste nell'analizzare come i resti di $(2^i + X)$ si propagano in posizione del bit i e i + 1 (in notazione little-endian) osservando δ_i.

Si noti che questo algoritmo può essere eseguito completamente offline sui dati raccolti.

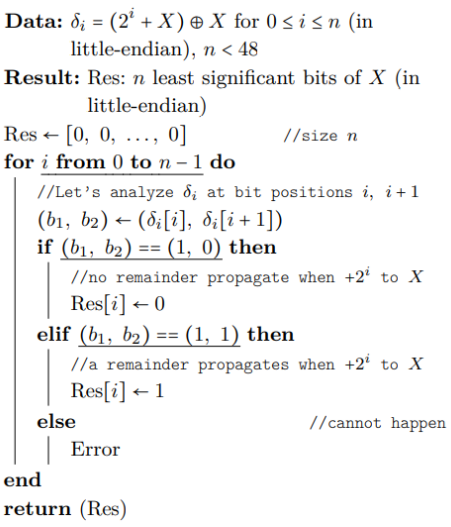


Figura 4.2: L'algoritmo algo utilizzato.

4.2.2 Implementazione dell'attacco

Innanzitutto è necessario utilizzare una piattaforma che raccolga le challenge di autenticazione della vittima.

Inoltre è necessario anche in questo caso utilizzare dei tool software per fare in modo che l'UE della vittima si colleghi a una stazione base falsa 4G in modo da inviare i messaggi di segnalazione.

Ottenere le challenge di autenticazione

E' possibile utilizzare il software srsUE della suite srsLTE configurato con l'IMSI del target con USRP B210, che impersona l'USIM target. Ogni sessione di autenticazione ha esito negativo perché srsUE non conosce la chiave segreta K del reale UE (quindi

non può calcolare il RES) ma, prima del messaggio di errore, viene trasmessa una nuova e autentica challenge.

Recupero dei messaggi AUTS utilizzando una stazione base falsa

E' possibile configurare una rogue BS per imitare un operatore reale, ad esempio con software OpenLTE in esecuzione su un USRP B210. Grazie alla procedura di riselezione cellulare è possibile fare in modo che l'UE vi si connetti. A questo punto è possibile recuperare i messaggi AUTS che un UE invia in seguito a un errore di sincronizzazione.

E' stato osservato che gli operatori non pongono un rate limit per quanto riguarda la richiesta di token di autenticazione, per cui è stato possibile ottenere un rate di 1 challenge per secondo con una singola BS falsa. Più challenge consecutive si ottengono, più bit di SQN_{UE} si possono decifrare.

4.2.3 Fattibilità dell'attacco

Questo attacco sfrutta vulnerabilità presenti nel protocollo AKA, che è implementato nell'USIM, per cui riguarda tutti i dispositivi 3G/4G che utilizzano schede USIM. Dato che il protocollo AKA è eseguito nell'USIM e nel circuito baseband, questo attacco non è individuabile dal SO, con il quale vengono scambiate poche informazioni.

Il protocollo AKA utilizza SQN sia per prevenire attacchi di replay che per garantire la sincronizzazione tra UE e HN.

Per consentire la risincronizzazione viene utilizzato il messaggio AUTS, che contiene $SQN_{UE} \oplus AK^*$, tuttavia questo messaggio manca di casualità, in quanto la chiave AK^* utilizza in input lo stesso valore RAND presente nella challenge. Per cui questo attacco evidenza una mancanza di protezione da replay attacks per l'AUTS.

Uno dei motivi per cui un utente può recuperare le challenge di qualsiasi UE da qualsiasi rete è la mancanza di autenticazione tra SN e HN nelle architetture 3G e 4G.

Una possibile soluzione è limitare la velocità delle richieste di autenticazione per un UE (in base al tempo o al numero), tuttavia un attaccante può venire a conoscenza di questo tipo di limite di velocità semplicemente testando la rete. E'comunque possibile aggirare questi limiti effettuando richieste di autenticazione da più SN.

Capitolo 5

Attacchi nella procedura di paging

Il protocollo di paging nasce con lo scopo di bilanciare tra qualità del servizio e consumo della batteria di un dispositivo. Dato che la ricezione e la trasmissione di pacchetti radio sono tra le funzioni più esigenti in termini di consumo di energia, un dispositivo può passare ad uno stato idle a basso consumo quando la rete rileva un periodo predefinito di inattività (circa 10 s). Tuttavia è fondamentale garantire che in caso sia presente un servizio in attesa (sia in downlink che in uplink), il dispositivo può tornare in uno stato attivo. Per consentire ciò ogni dispositivo si riattiva periodicamente dallo stato idle per individuare eventuali messaggi di paging attivati dalla core network. Questi messaggi di paging sono utilizzati per notificare i servizi in attesa a tutti i dispositivi al'interno di una tracking area. Oltre per le notifiche di servizio, i messaggi di paging vengono utilizzati anche per diffondere messaggi di emergenza, come ad esempio avvisi di terremoti e tsunami, per cui gli attacchi contro questo protocollo possono avere ripercussioni gravi. Gli attacchi

contro il protocollo di paging che andremo a descrivere in questo capitolo sono tratti da [12], [30] e [29].

5.1 Protocollo di paging

Il paging si riferisce al processo che viene utilizzato quando un MME ha bisogno di localizzare un UE in una particolare tracking area e fornire un servizio di rete, come ad esempio una chiamata in arrivo. Poiché l'MME potrebbe non conoscere l'esatto eNodeB a cui è connesso l'UE, genera un messaggio di paging, che inoltra a tutti gli eNodeB in una TA, come mostrato in 5.1. Tutti gli eNodeB nel TA trasmettono un messaggio di paging RRC per individuare l'UE. Contemporaneamente, MME avvia un timer di paging (T3413) e si aspetta una risposta da UE prima della scadenza di questo timer.

I messaggi di paging contengono identità dell'UE, cioè l'IMSI o il S-TMSI, l'identificatore temporaneo (SAETemporary Mobile Subscriber Identity) che compone il GUTI. Per cui nel corso di questo capitolo col termine GUTI ci si riferirà a questo componente. L'UE in stato IDLE decodifica i messaggi di paging RRC. Se rileva il suo IMSI, avvia una nuova procedura di Attach per ricevere un GUTI. Se UE rileva il suo GUTI, effettua la Random Access Procedure per acquisire un canale radio per richiedere una connessione RRC all'eNodeB. La successiva procedura "RRC Connection Setup" ha come fine la configurazione di risorse radio per lo scambio di messaggi di segnalazione, cioè il dispositivo si prepara per il servizio ristabilendo una connessione sicura con la core network. La richiesta e il completamento della connessione RRC viene effettuata con una procedura di handshake RRC a tre vie. A

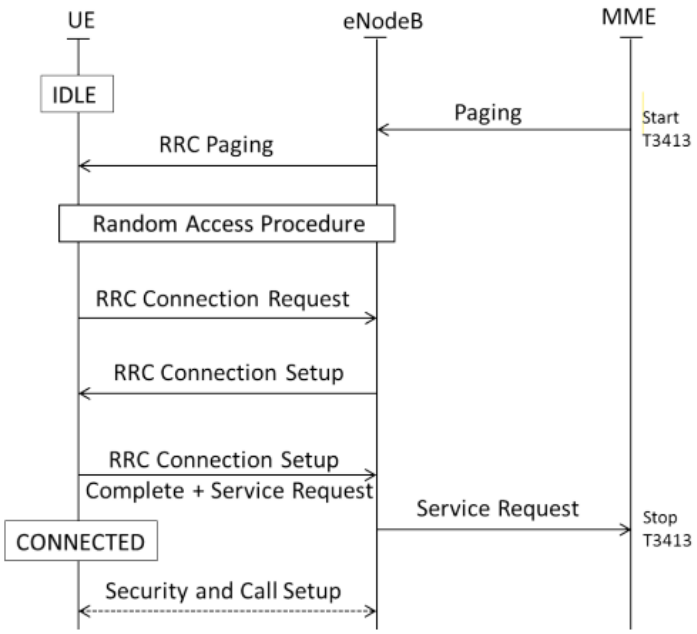


Figura 5.1: La procedura di paging LTE

questo punto l'UE passa dallo stato idle allo stato connected. L'eNodeB inoltra il messaggio di Service Request a MME, che a sua volta arresta il timer di paging.

Ciclo di paging

Quando è in modalità idle, l'UE si riattiva periodicamente (per circa 1 ms) per verificare se c'è una notifica per i servizi in ingresso, in un intervallo di tempo predeterminato all'interno di un ciclo di paging. Un ciclo di paging può avere una durata di tempo compresa tra 320 ms (32 radio frame) e 2,56 secondi (256 radio frame) a seconda dei parametri di rete I periodi di tempo esatti in cui il dispositivo si riattiva sono detti paging occasion, e sono fissati alla progettazione, in funzione dell'IMSI e dei parametri pubblici trasmessi dalla serving network.

Paging occasion

Il frame radio in corrispondenza del quale l'UE si attiva in ogni ciclo di paging per verificare la presenza di un messaggio di paging è detto frame di paging (PF). Viene calcolato utilizzando:

- il valore del ciclo di paging T $\in \{32, 64, 128, 256\}$
- il parametro pubblico: nB $\in \left\{4T, 2T, T, \frac{T}{2}, \frac{T}{4}, \frac{T}{8}, \frac{T}{16}, \frac{T}{32}\right\}$
- l'identificativo dell'UE_ID, con UE_ID = IMSI mod 1024.

con PF= $(\frac{T}{N})$ × (UE_ID mod N), dove N = min (T, nB)

Il valore di PF varia tra 0 e 255 T e nB sono parametri di sistema condivisi nei messaggi SIB system_info_block trasmessi dalla stazione base. Anche il sottoframe del frame di paging viene calcolato utilizzando i parametri sopra menzionati e una tabella di ricerca. Il frame di paging e il subframe costituiscono la paging occasion (PO) per l'UE.

Risposta ad un messaggio di paging

Un singolo messaggio di paging può contenere fino a 16 record di paging indirizzati a diversi UE. Ogni record contiene l'identificativo dell'UE (GUTI/IMSI). Se un'UE nota il proprio identificativo, passa a uno stato attivo e avvia la procedura per stabilire una connessione con la core network.

Smart paging

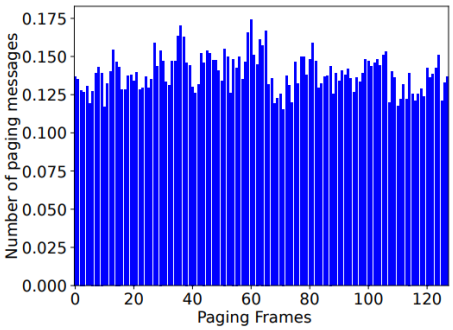
In GSM i messaggi di paging vengono inviati a un'intera tracking area, per cui l'attaccante può localizzare l'UE solo in una area abbastanza vasta. Tuttavia, in LTE è supportato il cosidetto smart paging, che è diretto a una piccola cella anziché a un TA di grandi dimensioni. Tale smart paging consente a un utente malintenzionato di localizzare un utente all'interno di un'area molto più piccola (ad esempio, 2 km^2). Questo perchè lo smart paging consiste nell'inviare i messaggi di paging nell'ultimo eNodeB (cella) in cui l'UE è stato presente. Se non viene ricevuta risposta, il paging viene ripetuto nell'intero TA.

5.2 Vulnerabilità nella progettazione del protocollo

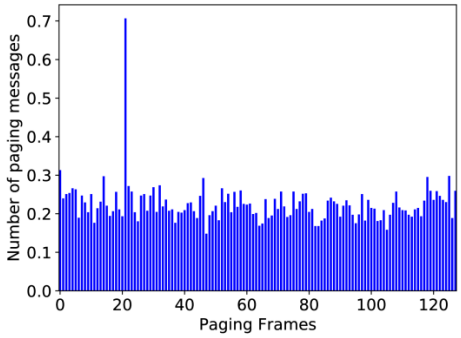
5.2.1 Paging occasion basata sull'IMSI

Per un particolare dispositivo in una cella specifica le paging occasion sono fisse (sono calcolate a partire dall'IMSI e da altri parametri trasmessi dalla stazione radio base).

Questo consente di ottenere informazioni side-channel sfruttabili dall'attacco ToRPEDO (TRacking via Paging mEssage DistributiOn). Per tracciare la posizione della vittima, l'avversario intercetta i messaggi di paging trasmessi da una stazione base nell'area target per apprendere la distribuzione dei messaggi di paging in ogni paging occasion.



(a) Numero medio di messaggi di paging in diverse occasioni di paging con T=nB=128



(b) Numero medio di messaggi di paging in diverse occasioni di paging all'interno di un ciclo di paging con T=nB=128 quando l'avversario effettua diverse telefonate

5.2.2 Mancanza di autenticazione

Il protocollo di paging non fornisce nè autenticazione nè garanzia di integrità dei messaggi. Ciò consente a un avversario di inviare messaggi di paging falsificati in un canale di paging a tutti i dispositivi in un'area target, includendo avvisi di emergenza. Ciò può essere effettuato semplicemente installando una stazione base con un segnale di potenza più elevata di quella vicino all'UE vittima e inviare gli avvisi durante tutti i frame di paging. Questo consente anche di effettuare un attacco DoS trasmettendo messaggi di paging vuoti per impedire agli UE in determinate aree di ricevere notifiche di servizi in arrivo dalla core network.

La mancanza di autenticazione si può attribuire all'obiettivo originale del protocollo di bilanciare tra consumo della batteria del dispositivo e qualità del servizio. Infatti fornire garanzie di riservatezza attraverso l'uso della crittografia richiederebbe al dispositivo di eseguire fino a 16 operazioni di decifratura costose, una per ogni record di paging, per ogni occasione di paging per verificare la presenza di un servizio in

arrivo, e ciò è in contrasto con la caratteristica prevista di conservare la batteria.

Tuttavia il 3GPP stabilisce che dati due record di paging, un utente malintenzionato non dovrebbe essere in grado di determinare se appartengono allo stesso utente. Per cui si dovrebbe utilizzare il GUTI come identificativo del dispositivo nei record di paging invece che l'IMSI.

5.3 Vulnerabilità nell'implementazione del protocollo

5.3.1 Utilizzo dell'IMSI come identificativo del dispositivo

È stato dimostrato che alcuni operatori di rete utilizzano l'IMSI come identificativo del dispositivo nei record di paging anziché il TMSI come indicato dal 3GPP. L'attacco PIERCER (Persistent Information ExposuRe by the CorE netwoRk) [12] sfrutta questa vulnerabilità insieme a quella progettuale legata all'utilizzo di una paging occasion prefissata e alla mancanza di riservatezza per l'IMSI della vittima.

5.3.2 Aggiornamenti poco frequenti di TMSI

Nonostante lo standard 3GPP per le reti 4G suggerisca di cambiare frequentemente il TMSI per prevenire attacchi di mappatura (ad esempio, da numero di telefono a TMSI), non indica dei parametri specifici per la frequenza alla dovrebbe essere aggiornato. Di conseguenza, le implementazioni del protocollo di paging non aggiornano di frequente il TMSI per evitare di dover eseguire operazioni aggiuntive, o comunque scelgono il nuovo TMSI in modo prevedibile. Questi aspetti consentono spesso a un utente

malintenzionato di identificare e tracciare la presenza di un utente in un'area target. Per fare questo l'attaccante ha bisogno di una mappatura da GUTI all'identità della vittima, per ottenerla può effettuare più chiamate telefoniche silenziose al dispositivo della vittima in modo da attivare i messaggi di paging, e con una software defined radio (SDR) può intercettare e decodificare i canali di paging per estrarre il GUTI. Se l'avversario individua uno stesso GUTI nei diversi messaggi di paging, deduce che la vittima è presente nell'area di copertura della stazione base e può quindi tracciare la sua posizione a grandi linee.

5.3.3 Metodi per attivare messaggi di paging

Utilizzo delle chiamate VoLTE:

I tempi di connessione delle chiamate VoLTE sono molto brevi a circa 3 secondi. Pertanto, l'utente malintenzionato deve scegliere la durata della chiamata in modo che sia abbastanza lunga per la trasmissione di una richiesta di paging da parte di eNodeB ma sufficientemente breve da non attivare alcuna notifica sull'interfaccia utente dell'applicazione dell'UE. VoLTE ha un'alta priorità e quindi le sue richieste di paging vengono trasmesse a tutti gli eNodeB in un TA, quindi è sufficiente monitorare ogni singola cella all'interno della TA.

Utilizzo di social network e applicazioni di messaggistica:

Per attivare lo smart paging per localizzare l'UE in una cella specifica si possono utilizzare i messaggi di Facebook. Infatti i messaggi di persone che non sono nella

lista degli amici vengono indirizzati alla cartella "Altro" e non vengono notificati all'utente, ma attivano un messaggio di paging. L'intercettazione dei messaggi deve essere fatta per ogni singola cella, ma si può anche posizionare sniffer in ogni cella per accelerare la procedura di localizzazione. La presenza dell'UE viene determinata con successo in una cella che è tipicamente di dimensioni 2 km^2 , cioè molto più piccola di una cella GSM.

WhatsApp si può utilizzare in modo simile con la funzione di "notifica di digitazione", che attiva un messaggio di paging. In questo caso, l'attaccante ha bisogno del numero di telefono per identificare l'utente su WhatsApp, inoltre, le impostazioni sulla privacy devono consentirgli di visualizzare il suo profilo. Innanzitutto, l'utente malintenzionato invia un messaggio alla vittima e l'applicazione WhatsApp del destinatario lo elencherà nella posta in arrivo. Successivamente, l'utente malintenzionato apre la sua finestra di chat attiva corrispondente al destinatario e compone un messaggio senza inviarlo.

Capitolo 6

Attacchi DoS

Gli attacchi Denial-of-Service (DoS) sono degli attacchi che hanno l'obiettivo di impedire a un UE di accedere alla rete e attualmente sono tra gli attacchi più diffusi sulle reti wireless.

Uno degli obiettivi della rete EPS era quello di garantire un'elevata disponibilità della rete, tuttavia gli attacchi [35], [34], [29], [36] trattati in questo capitolo mostrano che in LTE è ancora possibile impedire a un terminale di fornire un servizio a causa di difetti legati alle specifiche tecniche. Inoltre verrà analizzato anche l'impatto di questi attacchi su diversi dispositivi. In LTE gli attacchi DoS riguardano diversi livelli: il livello fisico, il livello MAC, e i livelli superiori: RRC, NAS e IP.

6.1 Livello fisico

Oltre che forzare un UE a connettersi a una determinata stazione radio base, gli attacchi di jamming consentono anche di effettuare attacchi DoS, ad esempio trasmettendo dei segnali di rumore sul canale radio.

Ad esempio, uno studio [33] ha dimostrato che è possibile disabilitare una rete telefonica 4G di una città con jamming al centro 6 RB della larghezza di banda downlink LTE per impedire la ricezione dei canali di controllo fisici e dei messaggi broadcast.

Gli attacchi DoS a livello fisico possono anche venire effettuati con overshadowing [18].

6.1.1 DoS con AdaptOver

AdaptOver mediante overshadowing consente di effettuare attacchi DoS, sia in downlink che in uplink.

Attacco DoS in downlink

L'attaccante intercetta ciò che viene trasmesso in downlink durante lo stabilimento della connessione tra l'UE e l'eNodeB per individuare il tipo di procedura di connessione che seguirà.

In caso di Attach Procedure (primo riquadro della figura 6.1), l'utente malintenzionato effettua l'overshadowing della risposta ad una Attach Request inviata dal

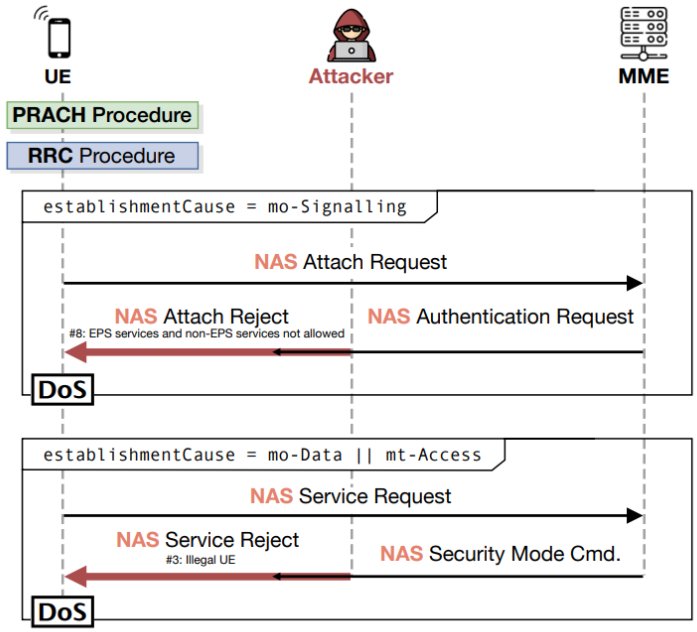


Figura 6.1: In figura l'attacco DoS in downlink.

MME con una Attach Reject. AdaptOver sovrascrive continuamente in downlink con questo messaggio per 250ms, in modo da trasmettere tutti gli acknowledgement necessari e per assicurarsi che la risposta della MME legittima non venga ricevuta. Dopo l'attacco, l'UE non tenterà di riconnettersi a nessun'altra cella dell'operatore nella stessa tracking area per 30-60 minuti o per più di 12 ore, a seconda del modello del telefono.

In caso di procedura di Service Request (secondo riquadro della figura 6.1), l'attaccante sovrascrive il Security Command con un messaggio di Service Reject. In questo caso, AdaptOver deve solo oscurare per 50ms, dato che deve venire trasmesso solo un acknowlegment.

Attacco DoS in uplink

Come nel caso precedente, AdaptOver innanzitutto apprende quale procedura di connessione utilizzerà l'UE.

Nel caso sia una procedura di Service Request (secondo riquadro della figura 6.2), questa richiesta inviata dall'UE verrà oscurata con una analoga ma con un MAC non valido. Secondo la specifica, l'MME deve rispondere con un Service Reject #9, spingendo l'UE ad avviare una Attach Request per riconnettersi immediatamente.

Invece se si tratta di una Attach Request (primo riquadro della figura 6.2), la sovrascrive con un messaggio contenente un IMSI bloccato dalla rete, causando un Attach Reject con causa # 8. Dopo aver ricevuto l'Attach Reject #8, l'UE entrerà in uno stato DoS e non tenterà di riconnettersi per almeno 12 ore. Affinché questo attacco funzioni, l'IMSI utilizzato deve causare un Attach Reject che comporti un DoS persistente, come #8 o #15.

Un IMSI adatto a questo scopo può essere recuperato da una SIM bloccata o non valida e forzando lo spazio IMSI o leggendo l'IMSI di una vecchia SIM scaduta.

L'impatto dei messaggi DoS causati da messaggi di risposta all'UE come Attach/-Service Reject è ben noto, tuttavia questo attacco rimuove la necessità di utilizzare una falsa stazione base per inviare effettivamente il messaggio.

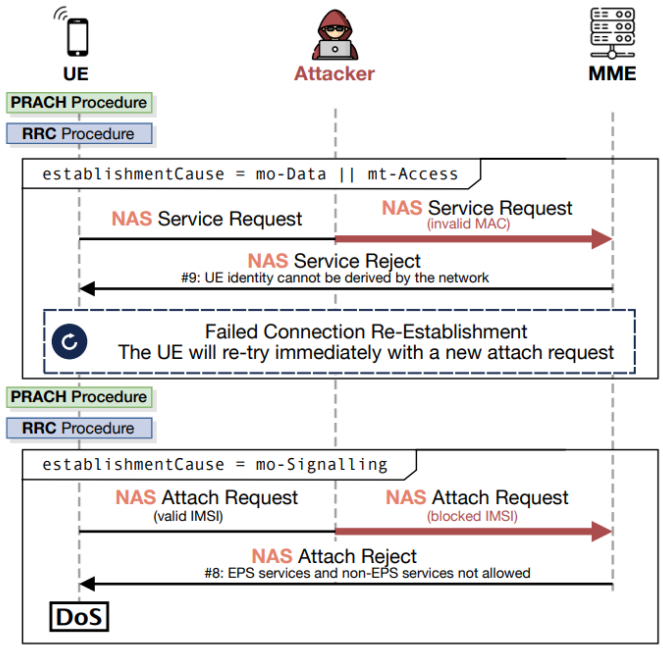


Figura 6.2: In figura l'attacco DoS in uplink.

Risultati sperimentali

Il comportamento degli UE in reazione agli attacchi DoS è specificato in 3GPP TS 24.301, ed è stato verificato in [18] utilizzando l'overshadowing in downlink con stazioni base reali nella gabbia di Faraday degli operatori.

E' stato misurato per quanto tempo ogni telefono non ha cercato di riconnettersi alla rete, in figura 6.3 sono mostrati i risultati del test. Alcuni degli UE più recenti testati hanno implementato il timer T3247, come indicato nella specifica di TS 24.301. Questo timer indica all'UE di non riprovare prima di 30-60 minuti e successivamente di riprovare fino al raggiungimento di un numero massimo di tentativi. Quando questo numero viene raggiunto, tutti gli smartphone testati hanno mostrato un DoS

Phone	DoS Time Attach Reject #8
Huawei P20 Pro	> 12h
Huawei P30	> 12h
Huawei P30 Lite	> 12h
Huawei P40 5G	> 12h
Samsung A8	> 12h
Samsung S10	> 12h
Samsung S21 5G	> 12h
LG Nexus 5X	> 12h
iPhone 6S	> 12h
iPhone 7	> 12h
iPhone 8	> 12h
iPhone 11	> 12h
iPhone X	> 12h
Xiaomi Mi 9	> 12h
Xiaomi Mix 3 5G	> 12h
Pixel 2	> 12h
Pixel 3a	> 12h
Pixel 4	> 12h
Pixel 5 5G	2x 30s, >12h
OnePlus 9 Pro 5G	5x 30-60min, 10x 10s,>12h

Figura 6.3: I risultati per i diversi telefoni testati.

$\geq$ 12h quando sottoposti a un Attach Reject /#8.

L'utente può ripristinare la connessione, ad esempio riavviando il telefono o reinserendo la scheda SIM. In assenza di queste azioni, il telefono non cerca di utilizzare nessun'altra cella dello stesso operatore.

Quando la rete riceve una Service Request con MAC non valido con un Service Reject #9, come previsto . Utilizzando IMSI casuali è possibile trovare una serie di IMSI che sono stati bloccati e che causano un Attach Reject /#8 quando utilizzati. Gli IMSI non validi attivano l'AttachReject /#15, che ha un effetto DoS persistente simile.

6.2 Livello NAS

Gli attacchi DoS a livello NAS riguardano sia il protocollo NAS, il protocollo RRC e IP.

6.2.1 Attacchi DoS che sfruttano i messaggi RRC

Gli attacchi DoS RRC sfruttano i messaggi di segnalazione RRC e si suddividono in due tipologie: il primo tipo ha come target la stazione base, di cui mira a esaurire le risorse limitate o a mandare in crash un software della BS, e quindi impedisce agli utenti di connettersi. Questo tipo di DoS può essere realizzato utilizzando una botnet di dispositivi mobili per creare tempeste di segnalazione RRC [36]. L'altro tipo di DoS nega il servizio ad un utente target stabilendo una connessione radio con l'eNodeB utilizzando S-TMSI dell'UE vittima.

Dal punto di vista delle specifiche, la causa principale di questi attacchi che sfruttano i messaggi broadcast RRC è la mancanza di un meccanismo di protezione (nessuna crittografia né protezione dell'integrità) per i questi messaggi.

6.2.2 Attacchi DoS che sfruttano i messaggi NAS

Analogamente ai messaggi RRC, esistono due tipi di attacchi DoS che sfruttano i messaggi di pre-autenticazione non protetti a livello NAS: DoS originati dalla segnalazione e attacchi DoS mirati ai dispositivi. Il primo tipo riguarda il lato rete e si riferisce agli attacchi DoS che saturano gli eNodeB della core network sfruttando

i messaggi di segnalazione NAS necessari per attivare e disattivare i portanti EPS dedicate. Di conseguenza gli UE non possono più collegarvisi.

Gli attacchi DoS mirati al dispositivo sfruttano i messaggi di segnalazione NAS di tipo Reject message (ad esempio, Attach Reject, TAU Reject e Authentication Reject) e Detach Request che costringono i dispositivi vittima a disconnettersi dalla rete. Rientrano in questa categoria anche gli attacchi effettuati con AdaptOver. Questi attacchi possono impedire l'accesso alla rete a uno specifico UE oppure a tutti gli UE all'interno di una cella.

L'attacco DoS originato dalla segnalazione è consentito a causa del fatto che la core network ha risorse limitate e non gestisce correttamente il flooding di segnalazioni. La causa degli attacchi DoS mirati invece è il difetto delle specifiche che autorizzano gli UE a elaborare la segnalazione di rifiuto del NAS prima che venga stabilito il contesto di sicurezza. Nella tabella 6.1 sono indicati i messaggi che l'MME può elaborare prima di avere stabilito una connessione sicura.

Messaggi EMM	Note
IDENTITY REQUEST	se il parametro di identificazione richiesto è l'IMSI
AUTHENTICATION REQUEST	-
AUTHENTICATION REJECT	se la causa EMM non è #25
ATTACH REJECT	-
DETACH ACCEPT	-
TRACKING AREA UPDATE REJECT	se la causa EMM non è #25
SERVICE REJECT	se la causa EMM non è #25

Tabella 6.1: I messaggi che possono essere sfruttati in questo attacco prima dell'autenticazione reciproca

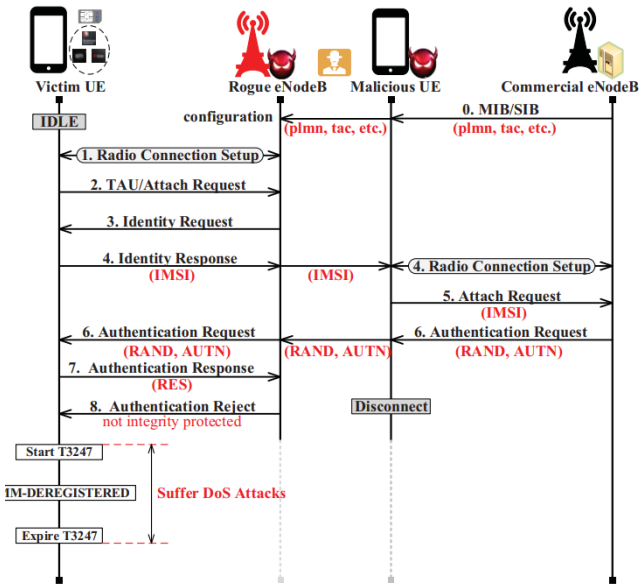


Figura 6.4: Le divese fasi dell' attacco DoS.

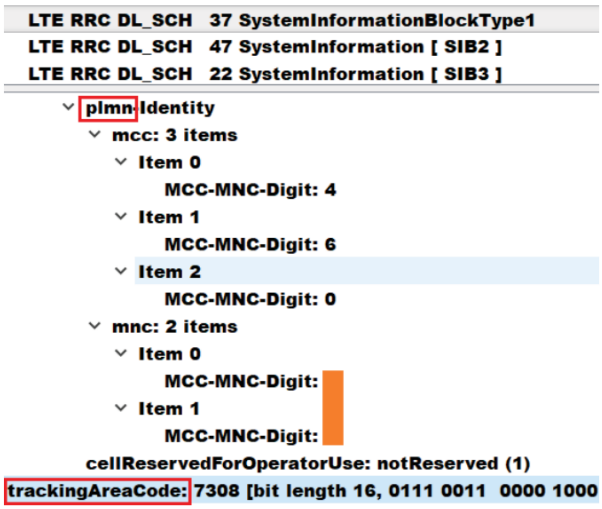
Attacco DoS che sfrutta i messaggi di autenticazione

E' stato osservato che gli attacchi DoS realizzati con messaggi di Authentication Request/Authentication Reject hanno conseguenze più gravi rispetto agli altri messaggi di rifiuto dei servizi.

In figura 6.4 la descrizione dell'attacco. La verifica di questo attacco è realizzata con un MITM.

Prima di tutto, l'UE illecito, implementato con srsUE, sniffa dalla rete LTE le informazioni necessarie, come EARFCN (E-UTRA Absolute Radio Frequency Channel Number), PLMN (Public Land Mobile Network) e TAC, contenute nei messaggi MasterInformationBlock (MIB) e SystemInformationBlock (SIB) trasmessi

Figura 6.5: Alcune informazioni ottenuto con sniffing della rete.



dall'eNodeB, che vengono normalmente utilizzati per stabilire una connessione RRC con l'UE.

In figura 6.5 sniffing delle informazioni della rete LTE. Queste informazioni sono utilizzate per configurare correttamente e avviare l'eNodeB dell'attaccante. L'UE vittima si connette all'eNodeB attraverso la procedura di riselezione cellulare o con una procedura di Attach, come è visibile in figura. Al ricevimento del messaggio di richiesta NAS (di Attach o TAU) da parte dell'UE,l'eNodeB effettua una procedura di identificazione per acquisire l'IMSI dell'UE target. A questo punto l'avversario può inviare un Attach Request alla rete commerciale utilizzando l'IMSI dell'UE vittima. L'avversario dovrebbe ricevere un vettore di autenticazione dalle rete dell'operatore, inclusi AUTN e RAND. In seguito a ciò, spegne l'srsUE per disconnettersi dalla rete. L'eNodeB illegittimo trasmette i parametri di autenticazione, che erano destinati all'UE falso, all'UE target e supererà con successo la verifica dell'UE. Infine,

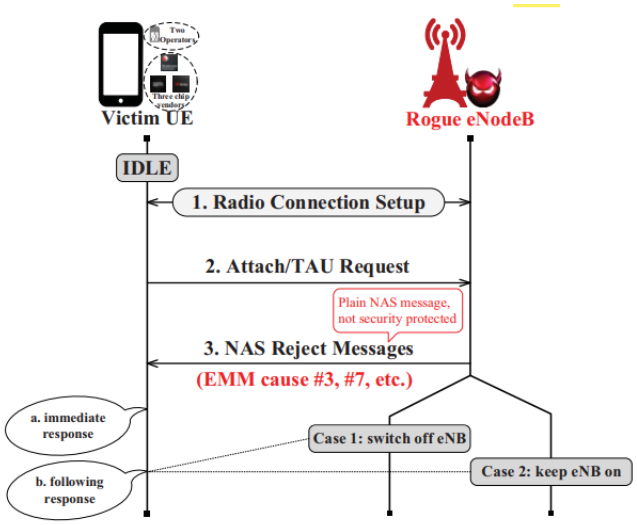


Figura 6.6: Attacco DoS sulla procedura di autenticazione

l'avversario invia un messaggio Authentication Reject non protetto alla vittima UE.

Risultati sperimentali Le variabili nel test sono:

a) Operatori: le carte USIM sono di due diversi operatori, indicati con Operatore1 e Operatore2.

b) Cellulari: sono considerati telefoni cellulari con diversi baseband chip (Qualcomm, Hisilicon, Media Tek ecc.).

c) Messaggi di rifiuto: vengono testati diversi messaggi di rifiuto NAS (Attach / TAU / Authentication Reject).

d) Cause EMM: vengono testate varie cause contenute nella segnalazione di rifiuto.

Le procedure possono essere riassunte in figura 6.6.

Impact Levels (identifier icon)	*Case 1 (shut off eNodeB)*		*Case 2 (keep eNodeB on)*	
	Device's Reaction	**Conditions for Returning to Normal**	**Device's Reaction**	**After airplane mode, USIM reinsertion or device reboot**
Level 1 (⬟)	ECO, NS[a]	a. reinsertion of USIM card b. device reboot c. expiration of the relevant timer	ECO, NS	remained in the previous states or re-attached to the rogue eNodeB
Level 2 (⬟)	ECO, NS	a. switch back from airplane mode b. conditions in *Level 1*	DG to 2G/3G	remained in the previous states or re-attached to the rogue eNodeB
Level 3 (⬟)	DG[b] to 2G/3G	a. reinsertion of USIM card b. device reboot c. expiration of the relevant timer	ECO, NS	back to normal states
Level 4 (⬟)	DG to 2G/3G	a. switch back from airplane mode b. conditions in *Level 3*	DG to 2G/3G	back to normal states
Level 5 (⬟)	ECO, NS, DG to 2G/3G	a. after a short period of time (less than 3 minutes)	ECO, NS, DG to 2G/3G	returned to normal states spontaneously
Level 6 (⬠)	normal state	none	Normal state	no need

Figura 6.7: I diversi livelli di impatto in cui sono stati classificati i risultati dei test

Una volta che il telefono si connette all'eNodeB falso, verrà inviata una segnalazione di rifiuto NAS. In seguito ci sono 2 diverse situazioni possibili:

Caso 2: prevede di mantenere l'eNodeB falso ancora attivo per un certo tempo

Caso 1: prevede di spegnere il sistema subito dopo

In entrambi i casi viene registrata la successiva risposta dell' UE.

In figura 6.8 le reazioni al test dei cellulari con baseband chip Qualcomm e Media Tek dei due operatori. L'attacco ha causato ai dispositivi dell'operatore 1 l'assenza di reti mobili disponibili mentre i dispositivi di test nell'operatore 2 hanno effettuato downgrade a 2G / 3G senza notifiche. In entrambi i casi i telefoni sono rimasti in questo stato fino al riavvio o al reinserimento dell'USIM.

Per valutare meglio gli effetti sugli utenti, i risultati dei test [35] sono stati classificati in 6 diversi livelli di impatto. La gravità dell'impatto degli attacchi DoS

Figura 6.8: La reazione dell'UE di due diversi operatori a un Authentication Reject.

diminuisce gradualmente dal livello 1 al livello 6, con il livello 1 che indica gli effetti più gravi mentre il livello 6 indica che non vi è alcun impatto.

Livello 1:

- Caso 1: il dispositivo di test è rimasto nello stato "Nessun servizio (NS)" o "Solo chiamate di emergenza (ECO)" fino al reinserimento di USIM o il riavvio dei dispositivi o la scadenza del timer corrispondente.

- Caso 2: i dispositivi erano inizialmente in stato NS o ECO, dopo essere tornati dalla modalità aereo o aver ricollegato USIM o riavviato i dispositivi, i dispositivi sono rimasti negli stati precedenti o ricollegati all'eNodeB canaglia .

Livello 2:

-Caso 1: il dispositivo di test è rimasto negli stati NS o ECO fino al ritorno dalla modalità aereo.

-Caso 2: downgrade alle reti 2G / 3G , e dopo il passaggio dalla modalità aereo o la riconnessione di USIM o il riavvio dei dispositivi, i dispositivi sono rimasti negli stati precedenti o ricollegati all'eNodeB canaglia.

Livello 3:

-Caso 1: downgrade alle reti 2G/3G fino al reinserimento di USIM o al riavvio del dispositivo o alla scadenza del timer corrispondente.

-Caso 2: i dispositivi erano inizialmente negli stati NS o ECO e, dopo il passaggio dalla modalità aereo o il ricollegamento di USIM o il riavvio dei dispositivi, sono tornati agli stati normali

Livello 4:

-Caso 1: il dispositivo ha effettuato il downgrade alle reti 2G/3G fino al ritorno dalla modalità aereo.

-Caso 2: i dispositivi effettuano il downgrade alle reti 2G / 3G e, dopo il ritorno dalla modalità aereo o la riconnessione dell'USIM o il riavvio, i dispositivi sono tornati agli stati normali.

Livello 5:

Il dispositivo di test inizialmente ha effettuato il downgrade alle reti 2G / 3G o è rimasto in stato NS / ECO, ma è tornato alla normalità dopo un breve periodo (sia nel caso 1 che nel caso 2).

Livello 6:

L'attacco DoS non ha alcun effetto sul dispositivo (sia il caso 1 che il caso 2).

Analisi dei risultati

I risultati sperimentali sono riportati nella tabella 6.9. Dai risultati, si può dire che l'intero insieme delle variabili considerate (operatori, cause EMM ecc.) contribuiscono al livello di impatto di questo attacco. Il livello di impatto massimo su diversi telefoni di test sotto un particolare operatore è lo stesso. Ad esempio, il grado di impatto massimo degli attacchi all'operatore 1 è il livello 1 (i dispositivi rimangono costantemente negli stati NS/ECO) mentre l'operatore 2 è il livello 2 (i dispositivi subiscono continuamente attacchi DoS di downgrade). Gli impatti nel caso 1 sono generalmente più gravi rispetto al caso 2 a parità di condizioni. Come anticipato, gli attacchi DoS che utilizzano i messaggi di Authentication Reject di solito causano l'impatto più grave sugli utenti.

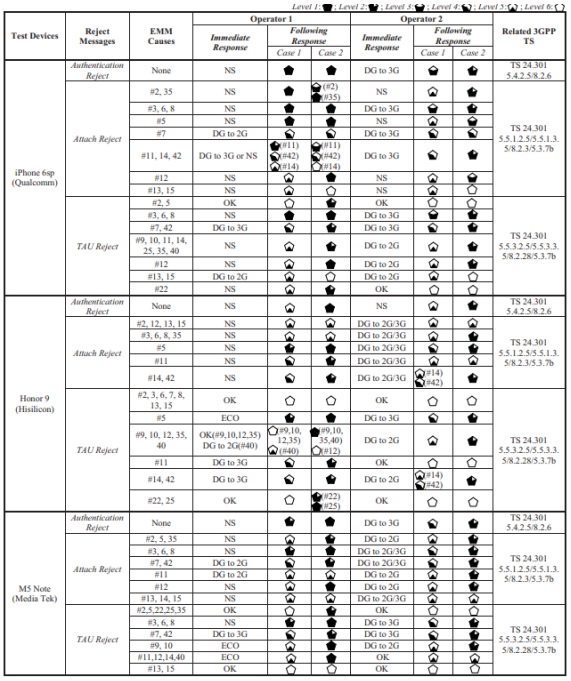
Attacco DoS che sfrutta i messaggi di TAU

Come mostrato in figura 6.10, questo attacco è suddiviso nelle seguenti fasi:

• Connessione normale tra la stazione base legittima e l'UE vittima:

quando l'UE vittima è acceso, stabilisce una connessione con la stazione base legittima dopo aver ricevuto le informazioni di trasmissione. Mentre l'UE è collegato alla stazione base legittima misura periodicamente la potenza del segnale di riferimento ricevuto (RSRP) e la qualità del segnale di riferimento ricevuto (RSRQ) di quella stazione base e calcola Srxlev (la potenza del segnale) e Squal (la qualità del segnale):

$$Srxlev = Q_{rxlevmeas} - (Q_{rxlevmin} + Q_{rxlevminoffset}) - P_{compensation} \tag{6.1}$$



Test Devices	Reject Messages	EMM Causes	Operator 1			Operator 2			Related 3GPP TS
			Immediate Response	Following Response		Immediate Response	Following Response		
				Case 1	Case 2		Case 1	Case 2	
iPhone 6sp (Qualcomm)	Authentication Reject	None	NS			DG to 3G			TS 24.301 5.4.2.5/8.2.6
	Attach Reject	#2, 35	NS		(#2) (#35)	NS			TS 24.301 5.5.1.2.5/5.5.1.3. 5/8.2.3/5.3.7b
		#3, 6, 8	NS			DG to 3G			
		#5	NS			NS			
		#7	DG to 2G			DG to 3G			
		#11, 14, 42	DG to 3G or NS	(#11) (#42) (#14)	(#11) (#42) (#14)	DG to 3G			
		#12	NS			NS			
		#13, 15	NS			NS			
	TAU Reject	#2, 5	OK			OK			TS 24.301 5.5.3.2.5/5.5.3.3. 5/8.2.28/5.3.7b
		#3, 6, 8	NS			DG to 3G			
		#7, 42	DG to 3G			DG to 3G			
		#9, 10, 11, 14, 25, 35, 40	NS			DG to 2G			
		#12	NS			DG to 2G			
		#13, 15	DG to 2G			DG to 2G			
		#22	NS			OK			
Honor 9 (Hisilicon)	Authentication Reject	None	NS			NS			TS 24.301 5.4.2.5/8.2.6
	Attach Reject	#2, 12, 13, 15	NS			DG to 2G/3G			TS 24.301 5.5.1.2.5/5.5.1.3. 5/8.2.3/5.3.7b
		#3, 6, 8, 35	NS			DG to 2G/3G			
		#5	NS			DG to 2G/3G			
		#11	NS			DG to 2G/3G			
		#14, 42	NS			DG to 2G/3G	(#14) (#42)		
	TAU Reject	#2, 3, 6, 7, 8, 13, 15	OK			OK			TS 24.301 5.5.3.2.5/5.5.3.3. 5/8.2.28/5.3.7b
		#5	ECO			DG to 3G			
		#9, 10, 12, 35, 40	OK(#9,10,12,35) DG to 2G(#40)	(#9,10, 12,35) (#40)	(#9,10, 35,40) (#12)	DG to 2G			
		#11	DG to 3G			OK			
		#14, 42	DG to 3G			DG to 2G	(#14) (#42)		
		#22, 25	OK		(#22) (#25)	OK			
M5 Note (Media Tek)	Authentication Reject	None	NS			DG to 3G			TS 24.301 5.4.2.5/8.2.6
	Attach Reject	#2, 5, 35	NS			DG to 2G			TS 24.301 5.5.1.2.5/5.5.1.3. 5/8.2.3/5.3.7b
		#3, 6, 8	NS			DG to 2G/3G			
		#7, 42	DG to 2G			DG to 2G/3G			
		#11	DG to 2G			DG to 2G			
		#12	NS			DG to 2G			
		#13, 14, 15	NS			DG to 2G/3G			
	TAU Reject	#2,5,22,25,35	OK			OK			TS 24.301 5.5.3.2.5/5.5.3.3. 5/8.2.28/5.3.7b
		#3, 6, 8	NS			DG to 3G			
		#7, 42	DG to 3G			DG to 3G			
		#9, 10	ECO			DG to 2G			
		#11,12,14,40	ECO			OK			
		#13, 15	OK			OK			

Figura 6.9: I risultati dei test effettuati sotto ogni condizione

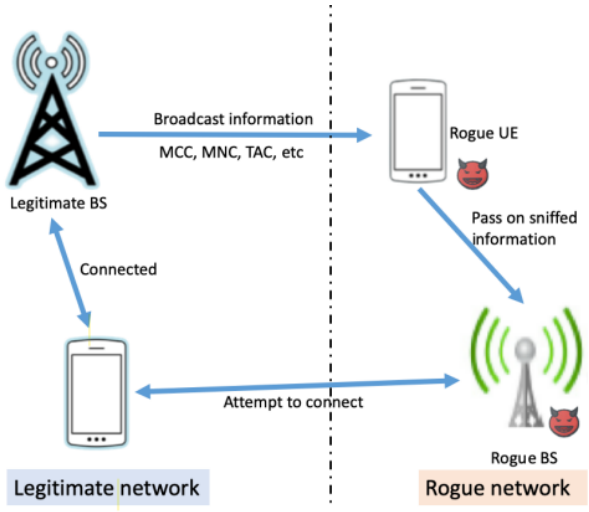


Figura 6.10: Attacco DoS che utilizza i messaggi di TAU

$$Squal = Q_{qualmeas} - (Q_{qualmin} + Q_{qualminoffset}) \tag{6.2}$$

dove $Q_{rxlevmeas}$ è l'RSRP misurato, e $P_{compensation}$ è la potenza di compensazione [34].

• Sniffing di informazioni e configurazione di una stazione base falsa:

L'UE falso effettua lo sniffing delle informazioni nel MIB e SIB, che vengono trasmessi in chiaro. Questi parametri vengono utilizzati per configurare la falsa BS, in particolare sono necessari MIB, PLMN, MCC, MNC, TAC dal SIB 1, la frequenza della portante downlink , la Cell Reselection Priority delle celle vicine in SIB 5.

• Misurazione delle cellule eseguita dalla vittima UE:

l'UE confronta Srxlev e Squal della cella di servizio con le soglie prestabilite $S_{nonintraSearchP}$ e $S_{nonintraSearchQ}$, rispettivamente. Quando Srxlev è inferiore a $S_{nonintraSearchP}$ oppure Squal è inferiore a $S_{nonintraSearchQ}$, UE inizia a eseguire la misurazione delle celle sulle stazioni base circostanti. L'UE valuta i valori di Squal' e Srxlev' dalle celle non di servizio. Per essere una stazione base candidata idonea, Squal' e Srxlev' devono essere superiori alle soglie fornite dalla cella di servizio, ovvero ThreshX, HighQ e ThreshX, HighP.

• Riselezione cellulare:

una volta che l'UE ha identificato una nuova stazione base idonea, inizia a eseguire la riselezione delle cellule verso quella stazione base. In accordo alla specifica l'UE effettua la valutazione per la riselezione cellulare solo per le frequenze a cui è associata una priorità. Per fare in modo che l'UE target si connetta alla BS dell'attaccante è

opportuno impostare la sua priorità assoluta con il valore più elevato possibile. Dato che LTE non supporta soft handover, l'UE deve prima disconnettersi dalla stazione base legittima.

- Rivelazione di IMSI e DoS:

dopo che l'UE invia un messaggio di Attach Request alla stazione base illecita, riceve un messaggio di Identity Request, in cui viene richiesto l' IMSI. In seguito questa stazione base non invia ulteriori messaggi all'UE, risultando in un DoS.

Implementazione dell'attacco

Step 1: Ricezione e decodifica dei messaggi broadcast

Per configurare l'eNodeB è necessario ottenere alcune informazioni contenute nei messaggi trasmessi, cioè MIB, SIB 1, SIB 3 e SIB 5. In srsLTE, queste informazioni possono essere ottenute utilizzando la funzione pdsch ue.c

Step 2: Impersonare la stazione base legittima.

Per rendere più affidabile la stazione base dell'attaccante è opportuno scegliere di impersonare una stazione base a cui l'UE vittima si è precedentemente connesso. In questo esperimento è stata scelta la cella Amarisoft. Per fare ciò i campi Mobile Country Code (MCC), Mobile Network Code (MNC), Tracking Area Code (TAC) e downlink bandwidth (DL BW) ottenuti da MIB e SIB sono stati impostati con gli stessi valori nei file di configurazione.

Step 3: Assegnare la priorità alla stazione base non autorizzata.

La priorità della cella nella riselezione cellulare è specificata in SIB 5, quindi l'UE conosce le priorità delle celle circostanti. Nello specifico, nel campo "interFreqCarrierFreqList" di SIB 5 è presente l'elenco delle celle vicine e alcuni loro parametri. Per la BS dell'attaccante è stata scelta quella con la priorità più elevata.

Step 4: Forzare l'UE ad eseguire la riselezione cellulare.

Secondo le equazioni 6.1 e 6.2, è necessario ridurre la potenza del segnale di riferimento ricevuto (RSRP) o la qualità del segnale di riferimento ricevuto (RSRQ) per diminuire Srxlev o Squal della cella di servizio. In uno scenario di attacco reale, ciò potrebbe essere ottenuto riducendo la potenza del segnale ricevuto o aumentando la potenza del rumore nell'UE. In questo esperimento, è stato utilizzato un attenuatore radio per ridurre la potenza del segnale della stazione base legittima installando l'attenuatore sull'USRP collegato alla cella Amarisoft. Aumentando gradualmente l'attenuazione, è stato osservato che l'UE inizia a eseguire misurazioni sulle celle circostanti quando Srxlev diventa inferiore alla soglia di misurazione cellulare.

Risultati sperimentali

Dalle informazioni acquisite dalla stazione base legittima nel passo1: $Q_{rxlevmin} = 100$ dBm, $Q_{rxlevminoffset} = 0$ dBm e $P_{compensation} = 0$ dBm. Sulla base dell'equazione, lo Srxlev è stato valutato come

$Srxlev = RSRP - (-100 + 0) - 0 = RSRP + 100 < ThreshX, high$, dove ThreshX,high = 4 dBm. Pertanto, il criterio UE per eseguire la misurazione delle cellule era RSRP < -96 dBm, ottenibile con l'attenuatore radio utilizzato. Con la

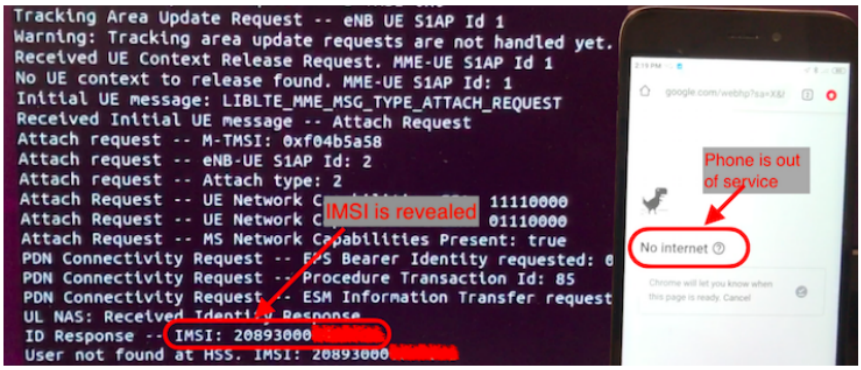


Figura 6.11: Ciò che viene mostrato sul terminale di srsLTE e dal telefono in seguito all'attacco

configurazione corretta presso la stazione base non autorizzata, effettuata la procedura DoS come previsto, ovvero la vittima UE si disconnette dalla stazione base legittima e tenta di collegarsi alla stazione base non autorizzata. E' stato osservato che l'UE va fuori servizio quasi immediatamente dopo l'accensione della stazione base non autorizzata e la potenza del segnale della stazione base legittima viene gradualmente ridotta.

Ciò è stato verificato controllando i pacchetti catturati dall'analizzatore di protocollo di rete Wireshark, e anche eseguendo un test ping sul telefono per verificare che fosse disconnesso, figura 6.11.

Come mostrato in figura 6.11, viene anche rivelato l'IMSI della vittima UE nella ID Response e stampato nel terminale del programma srsLTE.

Lo stesso esperimento [34] è stato condotto anche su un dispositivo Mbed a basso costo per le comunicazioni IoT, come mostrato in 6.12. Il dispositivo IoT inizialmente comunicava con il server IoT attraverso la rete legittima e, dopo aver attivato la stazione base non autorizzata, la connessione non è riuscita e non è stato possibile

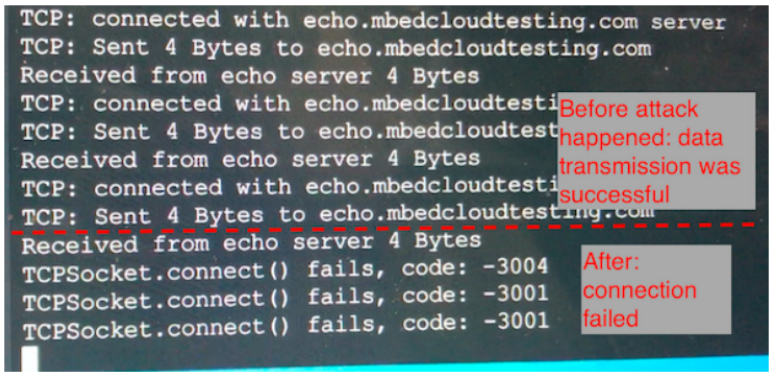


Figura 6.12: Risultati sperimentali di un device Mbed IoT

trasmettere altri dati, per cui l'attacco funziona sia su telefoni LTE commerciali che su dispositivi IoT.

Dopo aver inviato la Attach Request e ricevuto la Identity Request gli UE hanno risposto con il proprio IMSI in Identity Response senza cifratura. Inoltre, quando all'UE è stato negato il servizio è rimasto fuori servizio per molto tempo e non ha tentato di trovare un'altra cella fino a quando non è stato eseguito un riavvio manuale.

Capitolo 7

Modello di sicurezza delle reti 5G

In questo capitolo verrà trattata l' architettura delle reti 5G alla luce dei requisiti delle specifiche 3GPP [6] e delle nuove tecnologie introdotte. La descrizione della nuova rete 5G è tratta dalle pubblicazioni [16], [7], [15], [25], [20], [28], [2], [6] e [13].

7.1 Architettura 5G

Le reti 5G utilizzeranno nuovi concetti tecnologici per soddisfare i requisiti di accesso a banda larga ovunque, elevata mobilità di utenti e dispositivi e connettività di un numero elevatissimo di dispositivi (tra cui Internet of Things) in modo ultra-affidabile.

Gli organismi di standardizzazione delle telecomunicazioni stanno lavorando all'integrazione di questi nuovi concetti di rete come Software Defined Networking (SDN), Network Function Virtualization (NFV), cloud computing, Multi-access Edge

Computing (MEC), Network Slicing (NS) nelle reti 5G, con l'obiettivo di progettare una nuova rete mobile softwarizzata [7].

Il concetto SDN propone di disaccoppiare il piano di controllo e il piano dati dei dispositivi di rete e consente la programmazione di entrambi. Il controllo e la gestione della rete sono collocati in un controller logicamente centralizzato, che corrisponde al piano controllo. Inoltre, può offrire una astrazione dell'infrastruttura di rete sottostante per le funzioni di controllo e il livello dell'applicazione. Il piano dati invece è gestito con dispositivi programmabili sempre più standard, che consentono di modificare le funzioni senza cambiare dispositivo. Viene distribuito il ruolo di P-GW, e potrebbe eliminarsi la distinzione tra S-GW / P-GW. Introduce protocolli per qualsiasi funzione, inclusa la gestione (in cui attualmente non sono utilizzati, ma sono utilizzati algoritmi locali o globali coordinati). Quindi SDN porta innovazione nel networking per mezzo di astrazione e programmabilità da un lato e dall'altro semplifica la gestione della rete attraverso il controllo logicamente centralizzato, come mostrato in figura 7.1.

NFV propone un nuovo approccio per creare, implementare e gestire i servizi di rete. Questo approccio ha l'obiettivo di disaccoppiare le funzioni di rete dall'hardware proprietario, per eseguirle come istanze software. Inoltre offre maggiore scalabilità consentendo l'acquisto di potenza di calcolo mediante cloud e Mobile Edge Computing (MEC) [1] piuttosto che nuovo hardware. SDN e NFV abilitano la realizzazione di network slicing.

Il concetto di network slicing è può essere visto come la realizzazione del paradigma Network as a Service, cioè viene realizzata una rete logica end-to-end che sfrutta un

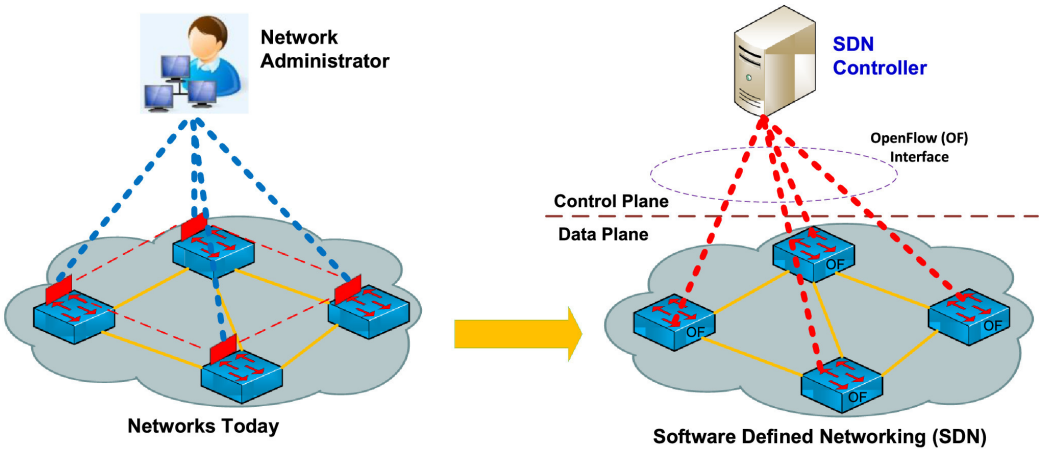


Figura 7.1: L'evoluzione nel newtorking introdotto da SDN.

insieme di risorse comuni sottostanti e che può essere gestita direttamente dal service provider. In questo modo è possibile offrire reti che soddisfano requisiti differenti a seconda del caso d'uso (vehicular, di emergenza, telefonia, videoconferenza, ecc) senza dovere realizzare fisicamente una rete diversa per ciascun servizio. Questo nuovo paradigma di progettazione dei servizi di rete è detto "verticals".

In figura 7.2 è mostrata l'architettura ad alto livello delle reti 5G.

Il 5G supporterà diverse RAT (Radio Access Technologies) per collegare diverse tipologie di dispositivi. Inoltre, il 5G prevede di introdurre una serie di nuove tecnologie radio come NOMA (Non-Orthogonal Multiple Access), massive MIMO, già utilizzata in LTE ma in modo più limitato, mmWave (millimeter Wave) e diverse altre tecnologie di comunicazione IoT.

Come evidenziato nella figura 7.2 il backhaul della rete 5G può essere suddiviso in tre diversi livelli: il livello infrastruttura, livello di controllo e livello di applicazione business. Il livello dell'infrastruttura contiene i dispositivi di connettività di base

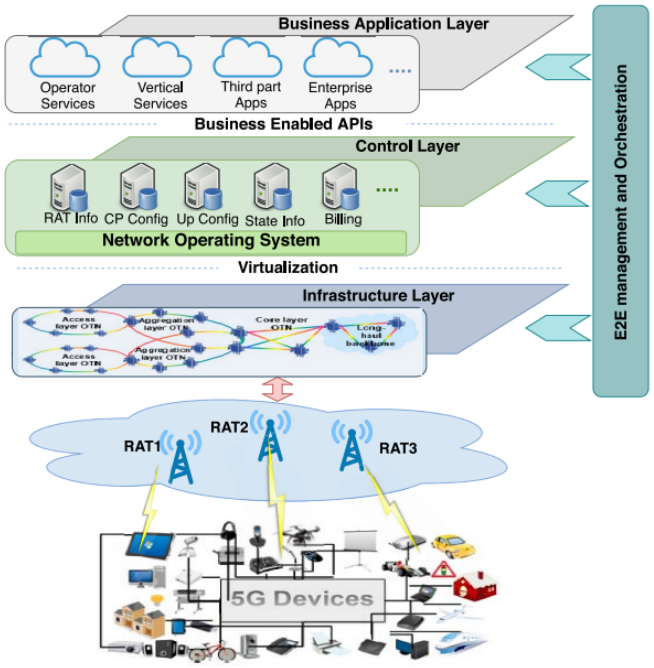


Figura 7.2: Descrizione ad alto livello dell'architettura delle reti 5G

come BS, router e switch. A differenza della rete pre-5G, i dispositivi a livello di infrastruttura non sono abilitati con una "intelligenza". Come affermato sopra, tutte le funzionalità di controllo della rete e le entità decisionali sono collocate nel livello di controllo, che interagisce con il livello di business delle applicazioni situato al di sopra. Inoltre, può tradurre le richieste di servizio di rete provenienti dal livello business in comandi di controllo e trasmetterli ai dispositivi del livello di infrastruttura. Pertanto, tutti i servizi di rete e le applicazioni di business sono implementati nel livello business. Inoltre, il livello di "gestione E2E (End to End) e di Orchestrazione" viene utilizzato in parallelo per sincronizzare il funzionamento di tutti e tre i livelli.

La sicurezza associata alle tecnologie 5G è stata considerata come uno dei requisiti chiave relativi sia ai sistemi 5G che oltre. Inoltre, la maggior parte dei modelli di

sicurezza nelle reti pre-5G (cioè 2G, 3G e 4G) non può essere applicata direttamente al 5G a causa della nuova architettura e dei nuovi servizi. Comunque, alcuni di questi meccanismi possono essere utilizzati con alcune modifiche.

Componenti dell'architettura 5G

In seguito verranno descritti i componenti architetturali della rete 5G con riferimento alla Service-Based Architecure, che è il framework di progettazione dell'architettura raccomandato in quanto è maggiormente adatto all'utilizzo delle nuove tecnologie di NFV, Cloud, ecc. In SBA i componenti dell'architettura sono indicati come "Network Function" piuttosto che entità di rete ("Network Entities"). Attraverso le interfacce di un framework comune, ogni dato NF offre i suoi servizi a tutti gli altri NF autorizzati, e in generale a qualsiasi "consumatore" che è autorizzato a fare uso di questi servizi.

Per quanto riguarda gli UE, sono composti da MS e schede USIM come per le generazioni precedenti. La rete di accesso è detta NG-RAN ed è composta principalmente da next-generation node-B (gNodeB/gNB, 'g' indica il 5G). I gNodeB sono a loro volta suddivisi in un gNB-Central Unit (gNB-CU) e due o più gNB- Distributed Unit (gNB-DU), connessi mediante una interfaccia, la F1, come mostrato in figura 7.3.

La rete di accesso (R)AN è connessa alla rete centrale mediante diverse interfacce, principalmente N2 e N3, come mostrato in figura 7.4 Il punto d'accesso è costituito dalle Network Function AMF e UPF (funzioni della core network, mostrata in figura 7.4): la User Plane Function (UPF) gestisce i dati dell'utente e e il piano di segnalazione (ha una funzione simile a PGW User Plane e SGW User Plane), la Access and Mobility management Function (AMF) effettua l'accesso tra UE e RAN. La AMF

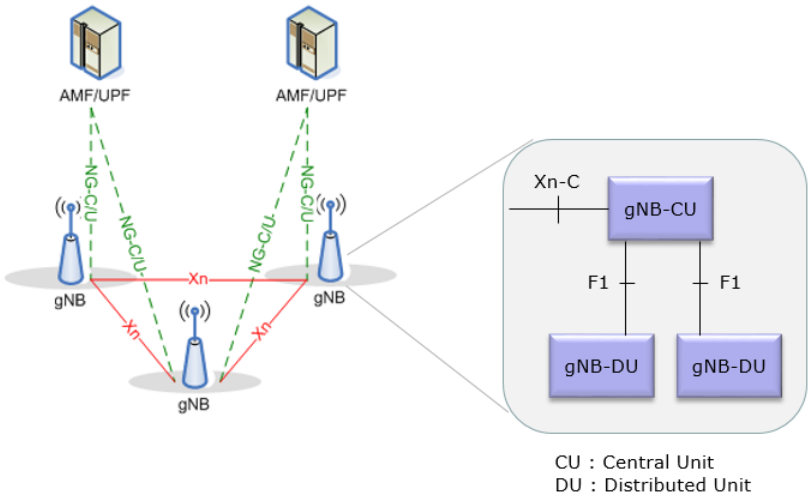


Figura 7.3: In figura l'accesso alla rete 5G

è l'unico punto di accesso per l'UE e si occupa di gestione della mobilità, gestione della connessione e della registrazione (ha delle funzioni simili a MME di LTE). Sulla base del servizio richiesto seleziona il corrispondente SMF (Session Management Function) per la gestione della sessione con l'utente, tra cui l'allocazione degli indirizzi IP, e contatta la UPF di conseguenza. La Authentication Server Function (AUSF) consente all'AMF di autenticare l'UE. Altre funzioni rilevanti sono la rete dati (DN) (esterna), per lo più nel piano utente e l'Application Function (AF), che controlla le applicazioni.

La UDM (Unified Data Management) e l'ARPF (Authentication Credential Repository and Processing Function) sono responsabili delle funzioni relative alla gestione dei dati e alla selezione dei metodi di autenticazione che utilizza AUSF. La funzione SIDF (Subscriber Identifier De-concealing Function) viene utilizzata per estrarre il SUPI dal SUCI (questo argomento verrà trattato nel capitolo successivo). Un'altra

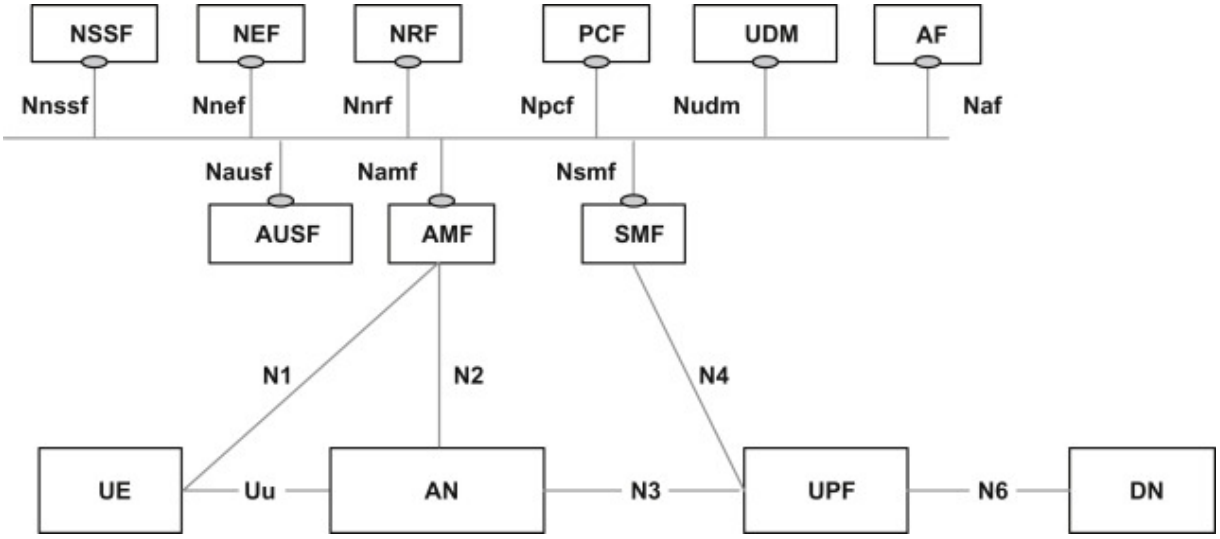


Figura 7.4: In figura la core network della rete 5G

funzione rilevante per quanto riguarda la sicurezza è la SEAF (Security Anchor Function), si trova nella serving network e può essere vista come una sorta di proxy durante il processo di autenticazione, in quanto si basa sulle informazioni ricevute dal AUSF della home network. Può rifiutare un'autenticazione dell'UE, ma può accettarne una solo se indicato dalla HN.

Modalità SA e NSA

3GPP [20] ha identificato cinque opzioni di architettura di rete SA e NSA, dato che l'opzione NSA 3 e SA 2 sono quelle maggiormente implementate normalmente ci si riferisce a queste.

La compatibilità della NG-RAN 5G con la RAN della rete LTE dovrebbe essere garantita per prevenire la possibile perdita di servizio: grazie alla softwarizzazione della rete 5G è possibile utilizzare la core network 4G con una NG-RAN. In generale, l'architettura SA NR si riferisce a un sistema 5G costituito da NR e 5GC in cui NR è

l'anchor del Control Plane, mentre l'architettura NR NSA si riferisce a un sistema che utilizza LTE come anchor del Control Plane per NR. Nell'architettura SA quando un dispositivo 5G è all'interno della copertura di NR, si "ancora" alla 5GC e la sua mobilità è gestita dal 5GC. Quando si sposta fuori dalla copertura NR, l'UE si collega a una rete EPC, come un dispositivo LTE. Quindi un UE che utilizza 5G SA funziona solo in modalità 5G o 4G. L'implementazione di SA NR consente le funzionalità della rete E2E, ad esempio, accesso iniziale rapido, slicing di rete e MEC.

Nell'architettura NSA il dispositivo è ancorato al sistema LTE / EPC e la NR viene utilizzata come pipe dati aggiuntivo quando è disponibile la copertura NR, cioè il nodo LTE è il Master mentre il nodo 5G è secondario (solo user-plane). La gestione della mobilità di NR con NSA è completamente controllata dal sistema LTE. Un UE che utilizza NSA funziona come un UE con LTE quando si sposta al di fuori della copertura NR . NSA NR richiede che il dispositivo supporti la "dual connectivity", il che significa che il dispositivo deve mantenere contemporaneamente i collegamenti di trasmissione radio LTE e NR.

7.2 Modello di sicurezza del 5G

Attualmente, il 5G è stato per lo più implementato nella modalità Non-Standalone (NSA), per sfruttare il 4G esistente e altre reti legacy. Inoltre, alcuni protocolli 4G come GTP sono utilizzati anche nelle reti 5G. Per queste ragioni, è possibile che le vulnerabilità nelle reti e nei protocolli legacy rappresentino delle minacce anche alla rete 5G Core.

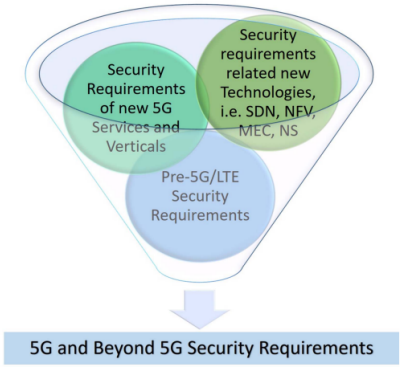


Figura 7.5: Requisiti delle reti 5G

La sicurezza delle reti 5G ha tre aspetti da tenere in considerazione, sottolineati in figura 7.5. In primo luogo, quasi tutte le minacce alla sicurezza e i requisiti di sicurezza relativi alle generazioni precedenti sono ancora applicabili, perlomeno per la modalità NSA. In secondo luogo, il 5G avrà una nuova serie di problematiche di sicurezza legate all'aumento del numero di utenti, all'eterogeneità dei dispositivi connessi, ai nuovi servizi di rete, ai nuovi requisiti, anche relativi alla privacy, per supportare l'IoT e le applicazioni mission-critical. In terzo luogo, la softwarizzazione della rete e l'utilizzo di nuove tecnologie come SDN, NFV, MEC e NS introdurranno una nuova serie di sfide per la sicurezza e la privacy.

I parametri principali che costituiscono il modello di sicurezza 5G sono: confidenzialità, integrità, policy centralizzata, visibilità e disponibilità. Il significato, nel contesto del 5G, è il seguente:

1) Riservatezza: La proprietà di riservatezza ha lo scopo di proteggere i dati trasmessi dalla loro divulgazione a entità non autorizzate e da attacchi passivi (ad esempio, intercettazioni). Come nelle generazioni precedenti, può essere utilizzato

un algoritmo di crittografia a chiave simmetrica per cifrare e decifrare i dati con una chiave privata precondivisa.

2) Integrità: E' necessaria per prevenire la perdita di informazioni. L'integrità del traffico 5G New Radio (NR) è protetta in modo simile a al 4G. In 5G NR, l'integrità del traffico dati wireless è garantita a livello di Packet Data Convergence Protocol (PDCP). Tuttavia, uno dei principali progressi nella protezione dell'integrità prevede che 5G NR offra anche la protezione di integrità del piano utente, a differenza del 4G. Inoltre, anche il meccanismo di autenticazione 5G-AKA utilizza segnali protetti da integrità.

3) Disponibilità: La disponibilità delle reti nel contesto del 5G significa la garanzia che le risorse di rete risultino accessibili ogni volta che sono necessarie agli utenti legittimi. E' un aspetto rilevante poiché influisce anche sulla reputazione del fornitore di servizi. La disponibilità misura anche la sostenibilità della rete contro gli attacchi attivi, ad esempio gli attacchi DoS.

4) Politica di sicurezza centralizzata: nella rete 5G, le attuali architetture di sicurezza 3GPP 4G non possono essere applicate direttamente ai nuovi casi d'uso 5G in quanto sono dedicate al tradizionale modello di fiducia operatore-UE. Pertanto, per supportare le innovazioni introdotte (come NFV e SDN), è necessario un sistema centralizzato di gestione delle policy di sicurezza. Gli operatori possono fornire Security-as-a-Service (SaaS) come potenziale soluzione per diversi clienti, come i fornitori di IoT, che offra agli utenti la comodità di accedere alle applicazioni e alle risorse.

5) Visibilità: la visibilità consente la gestione E2E del piano di controllo delle reti

mobili, che consente di affrontare in modo efficiente i problemi base della rete. Le reti 5G devono utilizzare strategie di sicurezza end-to-end, che dovrebbero coprire tutti i livelli della rete, compresi i piani di applicazione, segnalazione e dati. Per implementare questo meccanismo di sicurezza, è fondamentale che gli operatori 5G monitorino e mantengano la visibilità nelle reti per rilevare e mitigare gli attacchi.

7.3 Aree chiave nella sicurezza del 5G

I problemi di sicurezza sono relativi alle aree chiave nel 5G, ovvero controllo degli accessi, autenticazione, comunicazione e crittografia.

Autenticazione

L'autenticazione costituisce un ruolo significativo per quanto riguarda la sicurezza in un qualsiasi sistema di comunicazione. I meccanismi di autenticazione e di accordo delle chiavi (AKA) sono utilizzati anche nel 5G per stabilire la fiducia tra l'UE e la serving network.

Ne 5G l'autenticazione è suddivisa in autenticazione primaria e secondaria. L'autenticazione primaria consente l'autenticazione reciproca tra dispositivo e rete sia in 4G che in 5G. Questi meccanismi sono obbligatori per un UE per accedere a qualsiasi rete mobile e sono indicati come AKA primari nelle specifiche 5G. Le reti 5G devono obbligatoriamente supportare il protocollo di autenticazione 5G-AKA oppure EAP-AKA. I meccanismi di autenticazione secondari possono essere necessari quando un UE tenta di accedere a una rete di dati esterna (DN).

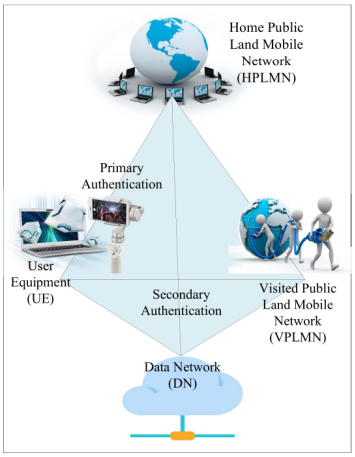


Figura 7.6: I due diversi tipi di autenticazione

Grazie alla funzione SEAF descritta in precedenza, è la home network ad essere responsabile dell'autenticazione primaria anziché la serving network. Questa è una differenza rispetto alle reti 4G, in cui, nonostante la home network venga consultata durante il processo di autenticazione per generare i vettori di autenticazione, non determina gli esiti dell'autenticazione. In questo modo si riduce il rischio di connessione a serving network che sono rogue BS. La figura 7.6 riassume le diverse tipologie di connessione.

Controllo degli accessi

Lo scopo principale del controllo degli accessi è la restrizione selettiva dell'accesso alla rete. Le reti di controllo degli accessi sono controllate dai provider di rete. Vengono confermati solo gli accessi degli utenti autenticati al sistema.

Inoltre, gli eventi di roaming possono verificarsi molto frequentemente nella rete 5G, principalmente a causa dell'utilizzo di reti 5G locali o di microoperatori 5G. La

maggior parte di questi operatori 5G locali non ha un livello di sicurezza elevato come i principali MNO (Main Network Operators). Pertanto, è piuttosto probabile di incontrare una rete 5G locale illegittima come serving network . Di conseguenza, l'autenticazione 5G svolge un ruolo fondamentale nel garantire che non vengano instaurate connessioni con tali reti.

Cifratura

La crittografia è particolarmente importante per garantire la riservatezza dei dati. Dato l'elevato numero di nuovi servizi di rete, la crittografia E2E è significativa nel 5G. Il traffico trasmesso via etere è criptato a livello PDCP (Packet Data Convergence Protocol). In modo analogo alla rete 4G LTE, vengono utilizzate tre diverse chiavi di crittografia a 128 bit per: il piano utente, Non-Access Stratum (NAS) e Access Stratum (AS).

Inoltre, alcuni degli algoritmi di crittografia 4G verranno utilizzati nel 5G New Radio. Secondo gli standard 3GPP, continueranno a essere utilizzati gli algoritmi: null, SNOW3G e Advanced Encryption Standard (AES) basati su EPS Encryption Algorithms (EEA).

La RAN 5G NR raggiunge un'elevata resilienza contro gli attacchi grazie al fatto che una singola BS è implementata con due unità, l'unità centrale e l'unità distribuita, come visto in precedenza. Questa suddivisione consente un' implementazione personalizzata delle funzioni d'accesso alla 5G NR sulla base della sensibilità alla sicurezza. Ad esempio, la crittografia del piano utente viene implementata in una posizione

centrale sicura e le funzioni non sensibili alla sicurezza vengono implementate in posizioni distribuite meno sicure.

Inoltre, la crittografia svolge un ruolo fondamentale nella protezione della privacy nel 5G. Per conformarsi alle recenti direttive sulla privacy, come il regolamento generale sulla protezione dei dati (GDPR) in Europa, è necessario considerare la protezione della privacy un requisito con priorità elevata. Di conseguenza la protezione della privacy dei subscriber è considerata fin dalla progettazione dei sistemi 5G (privacy by design). Nel 5G, gli identificativi dei subscriber, sia a lungo termine che temporanei, sono protetti utilizzando un meccanismo basato sullo schema di crittografia a curva ellittica (ECIES) e che utilizza la chiave pubblica dell'operatore.

Sicurezza della comunicazione

Le comunicazioni 5G hanno l'obiettivo di fornire elevata larghezza di banda dei dati, bassa latenza delle comunicazioni e una copertura estesa del segnale per supportare un'ampia gamma di verticals. Pertanto, come l'architettura, anche la comunicazione 5G deve essere aggiornata, anche in seguito all'integrazione delle nuove tecnologie. Tuttavia, questi cambiamenti possono comportare rischi elevati per la sicurezza nelle future reti mobili 5G.

Gli attacchi alla comunicazione 5G possono essere indirizzati a diversi segmenti della comunicazione 5G: l'UE, le reti di accesso e la core network degli operatori. È necessario considerare anche gli attacchi a cui sono soggetti i sistemi mobili legacy (ad esempio, 2G / 3G / 4G), in quanto alcuni di questi sono tuttora applicabili alle reti 5G.

Il traffico di core network 5G può essere classificato in due tipi: traffico di controllo e traffico dati utente. Entrambi sono vulnerabili, ma sono soggetti a diverse minacce alla sicurezza. Il problema chiave relativo al traffico di controllo è la mancanza di sicurezza a livello IP. Nella core network 5G basata su SDN attualmente esistente, vengono utilizzati i protocolli di sicurezza dei livelli superiori (livello applicazione) come le sessioni TLS (Transport Layer Security) / Secure Sockets Layer (SSL) per proteggere la comunicazione del canale di controllo. Questi protocolli hanno vulnerabilità note a livello IP, come lo spoofing IP, gli attacchi di modifica dei messaggi, gli attacchi di intercettazione, TCP SYN DoS, e gli attacchi di reset TCP. Pertanto, è necessario utilizzare anche meccanismi di sicurezza a livello IP.

Nelle reti SDN su larga scala, come le reti mobili, vengono utilizzati più controller SDN per controllare i diversi segmenti di rete. L'interfaccia SDN est/ovest viene utilizzata per stabilire la Inter-Controller Communication (ICC), cioè la comunicazione tra questi controller SDN. Questo consente la condivisione di informazioni per il controllo delle policy di sicurezza, gestione della mobilità, gestione del traffico e monitoraggio della rete. Pertanto, la sicurezza di questi canali ICC è indispensabile per garantire il corretto funzionamento delle funzioni elencate. I canali ICC degli attuali sistemi SDN sono vulnerabili a una vasta gamma di attacchi IP e Web-based come DDoS, attacchi di replay, IP port scanning e dirottamento del DNS. Inoltre, i canali ICC 5G sono anche vulnerabili a minacce fisiche come guasti tecnici, errori umani e guasti legati a catastrofi. Per cui l'ICC 5G sarà inevitabilmente vulnerabile ad un numero elevato di minacce sia informatiche che fisiche.

Capitolo 8

Protocolli di autenticazione 5G

La sicurezza delle comunicazioni tra i subscriber mobili e i loro fornitori di servizi richiede l'autenticazione reciproca e l'accordo delle chiavi. Lo standard 3GPP per la sicurezza 5G prevede due protocolli Authenticated Key Agreement (AKA): Extensible Authentication Protocol AKA' (EAP-AKA') e 5G-AKA. EAP-AKA' è basato sul meccanismo EAP ed è specificato in RFC 5448 mentre 5G-AKA è dettagliato in TS 33.501. I due protocolli sono per lo più identici, quindi in seguito viene descritto solo il protocollo 5G-AKA. Il protocollo è descritto con riferimento a [10], [19] e [14].

8.1 5G-AKA

5G-AKA è istanziato con un insieme di sette algoritmi a chiave simmetrica non correlati, indicati come $f1, ..., f5, f1^*$ e $f5^*$. Gli algoritmi $f1, f2$ e $f1^*$ sono utilizzati

come funzioni di autenticazione dei messaggi, mentre i $f3, f4, f5$ e $f5^*$ sono utilizzati per implementare le funzioni di derivazione delle chiavi.

La chiave segreta a lungo termine precondivisa K, il numero di sequenza SQN e l'identità a lungo termine SUPI sono memorizzati sia nell'UE che nell'HN durante la registrazione dell'USIM. I numeri di sequenza sono utilizzati per garantire la freschezza nel 5G-AKA. Tutte le chiavi derivate per 5G-AKA sono ottenute utilizzando la funzione di derivazione chiave (KDF) specificata in 3GPP TS 33.220. Il 5G-GUTI è costituito da MCC, MNC, dal AMF Identifier dal Globally Unique AMF Identifier (GUAMI) e 5G-TMSI Il GUAMI è composto da AMF Region ID, che indica la "regione" del AMF, AMF Set ID, che indica il gruppo di AMF nella regione e AMF Pointer che specifica un singolo AMF. Tutti i parametri utilizzati dal protocollo sono mostrati in figura 8.2. Il protocollo 5G-AKA [14] funziona come mostrato in figura 8.1:

1. Per avviare l'autenticazione, l'UE invia il 5G-GUTI al SN in un messaggio di "Registration Request" o il SUCI in un messaggio di "Identifier Response", in risposta a un messaggio di richiesta di identitità.

2. In caso fosse stato richiesto un 5G-GUTI, la SN estrae il SUPI corrispondente dal suo database e lo trasmette insieme al nome della serving network stessa (name SN) al HN in un messaggio di "Authenticate Request". In caso di richiesta del SUCI invece, il SUPI viene sostituito con il SUCI nel messaggio alla HN.

3. Se la HN riceve il SUCI nel messaggio di "Authenticate Request" estrae il SUPI. Deriva inoltre la risposta prevista $XRES^*$ e genera il vettore di autenticazione AV. L'AV è composto da: una challenge casuale RAND, un token di autenticazione

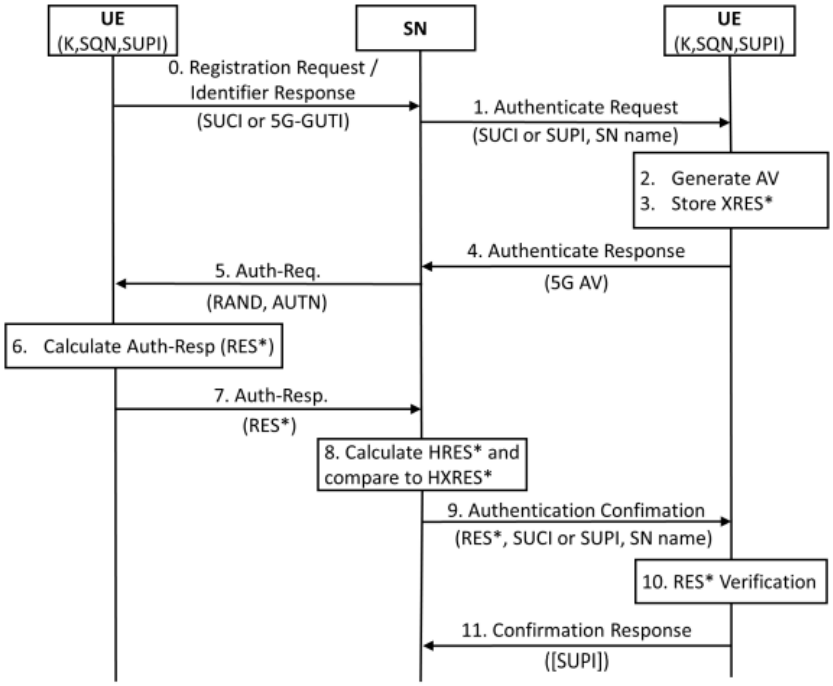


Figura 8.1: Lo scambio di messaggi di 5G-AKA

AUTN, un hash della risposta attesa $HXRES^*$ e una chiave anchor KSEAF, che è crittograficamente legata al SN richiedente.

4. L'HN memorizza $XRES^*$.

5. L'HN inoltra il 5G AV (RAND, AUTN, HXRES*, KSEAF) in un messaggio di Authenticate Response al SN.

6. Il SN inoltra (RAND, AUTN) all'UE in un messaggio Auth-Req.

7. Dopo aver ricevuto (RAND,l'AUTN), l'UE verifica la freschezza e l'autenticità. In seguito calcola la risposta RES^* e ricava la chiave di ancoraggio KSEAF da utilizzare per stabilire il canale sicuro con la SN.

8. L'UE restituisce RES^* in un messaggio Auth-Resp al SN.

9. Il SN calcola l'hash della risposta $HRES^*$ dal RES ricevuto e confronta $HRES^*$ con $XHRES^*$. Se sono uguali, la SN considera l'autenticazione riuscita.

10. La SN invia quindi RES^*, come ricevuto dall'UE, all'HN in un messaggio di "Authentication Confirmation" (contenente il SUPI o il SUCI e il name SN).

11. Quando l'HN riceve un messaggio di conferma, confronta RES* con il XRES* memorizzato. Se sono uguali, l'HN considera il messaggio di conferma come verificato correttamente.

12. Infine, la HN indica alla SN in un messaggio di "Confirmation Response" se la conferma è andata a buon fine o meno. Se la HN ha ricevuto un SUCI dal SN quando è stata avviata l'autenticazione e se la conferma ha esito positivo, allora la HN include anche il SUPI in questo messaggio.

Parameter	Content/Description
$RAND$	128 bit Random Challenge
SQN	48 bit Sequence Number
AMF	16 bit Authentication Management Field
$SNname$	Serving Network Name
AK	$f_5(K, RAND)$
CK	$f_3(K, RAND)$
IK	$f_4(K, RAND)$
RES	$f_2(K, RAND)$
MAC	$f_1(K, SQN \| RAND \| AMF)$
$AUTN$	$(SQN \oplus AK \| AMF \| MAC)$
$RES^*/XRES^*$	$KDF(CK \| IK, SNname \| RAND \| RES/XRES)$
$HXRES^*/HRES^*$	$SHA256(RAND \| XRES^*/RES^*)$
K_{AUSF}	$KDF(CK \| IK, SNname \| SQN \oplus AK)$
K_{SEAF}	$KDF(K_{AUSF}, SNname)$
AV	$(RAND \| AUTN \| HXRES^* \| K_{SEAF})$

Figura 8.2: I parametri utilizzati in 5G-AKA

Si può notare che nella fase 11 del 5G-AKA 8.1, la HN fornisce il SUPI dell'UE al SN dopo che l'autenticazione è riuscita, il che non è necessario ai fini dell'autenticazione.

Ciò è invece necessario per soddisfare i requisiti di intercettazione legale (LI): le forze dell'ordine di quasi tutti i paesi richiedono che i fornitori di servizi locali abbiano la capacità di localizzare e tracciare un qualsiasi utente mobile all'interno del paese.

Il SUPI viene successivamente utilizzato come input per la funzione di derivazione della chiave di sessione tra UE e SN. Questo garantisce che il SUPI fornito dalla HN sia quello dichiarato dall'UE, altrimenti la comunicazione viene interrotta.

8.1.1 Riservatezza dell'identità nel 5G

Nel sistema 5G, il Subscription Hidden Identier (SUCI) è un identificativo che preserva la privacy, in quanto contiene il SUPI. L'UE genera un SUCI utilizzando uno schema di protezione con la chiave pubblica dell'HN, che è stata fornita in modo sicuro all'USIM durante la registrazione dell'USIM.

Per supportare la protezione dell'identità del subscriber, la chiave pubblica e l'identificativo del meccanismo di protezione devono essere memorizzati nell'USIM. Se ciò non avviene, il ME (Mobile Equipment dell'UE) selezionerà il meccanismo "null-scheme", a quel punto il SUPI non sarà protetto. Secondo le specifiche l'UE genera un SUCI utilizzando il "null-scheme" solo nei seguenti tre casi:

- se l'UE sta effettuando una sessione di emergenza non autenticata e non dispone di un 5G-GUTI nella rete selezionata.
- se la home network ha configurato come schema da utilizzare "null-scheme".
- se la home network non ha fornito la chiave pubblica necessaria per generare un SUCI (come detto sopra)

Un SUPI è definito nella specifica 3GPP TS 23.501 come una stringa di 15 cifre decimali. Le prime tre cifre rappresentano il Mobile Country Code (MCC) mentre le successive due o tre formano il Mobile Network Code (MNC) che identifica l'operatore di rete. Le restanti cifre (nove o dieci) sono note come MSIN (Mobile Subscriber Identication Number) e identificano il singolo utente di quel particolare operatore.

Lo schema di protezione nasconde solo la parte MSIN del SUPI, mentre l'identificatore dell'operatore (MCC/MNC) viene trasmesso in chiaro.

Il SUCI è composto dai seguenti campi:

- Protection Scheme Identier: Questo campo contiene lo schema di protezione utilizzato, eventualmente indica lo schema "null".

- Home Network Public Key Identier: Contiene la chiave pubblica fornita dalla HN. In caso di schema "null", questo campo è anch'esso impostato con "null".
- Home Network Identier: Questo campo contiene le componenti MCC e MNC del SUPI.
- Protection Scheme Output: Questo campo rappresenta l'output dello schema di protezione basato su chiave pubblica (applicato al MSIN come descritto sopra).

Il meccanismo di identificazione del subscriber ne consente l'identificazione via radio tramite il SUCI. Questo meccanismo viene solitamente invocato dal SN con una richiesta di identità all'UE, quando questo non è identificabile mediante un'identità temporanea. L'UE risponde con un messaggio di Identier Response, contenente il SUCI. Inoltre, se l'UE invia un messaggio di Registration Request di tipo "Initial Registration" a una rete mobile per la quale non dispone già di un 5G-GUTI, al suo posto deve includere un SUCI nella Registration Request.

8.1.2 Schema di protezione basato su ECIES

Per calcolare un nuovo SUCI, l'UE genera una nuova coppia di chiavi pubbliche-private effimere ECC (Elliptic Curve Cryptography) utilizzando come parametro la chiave pubblica HN.

L'output finale di questo schema di protezione, mostrato in figura 8.3 è la concatenazione tra: la chiave pubblica appartenente alla coppia (pubblica, privata) di chiavi effimere ECC, il testo cifrato (il SUCI), MAC ed eventuali altri parametri aggiuntivi. La HN utilizza la chiave pubblica effimera ECC ricevuta e la propria chiave privata K

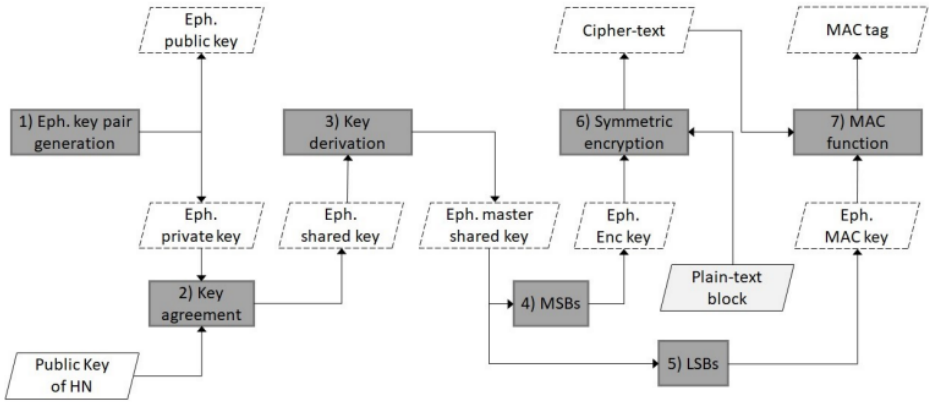


Figura 8.3: In figura la cifratura lato UE

come parametri input alla KDF per ottenere la chiave per decifrare il SUCI ricevuto, come mostrato in figura 8.4.

8.1.3 Limiti dello schema di protezione 5G

Sebbene lo schema basato su ECIES sia indipendente dalla sincronizzazione tra l'UE e HN e utilizzi chiavi effimere vi sono ancora aspetti che richiedono ulteriori miglioramenti.

Poiché lo schema basato su ECIES utilizza ECC per fornire la riservatezza dell'identità, il suo livello di sicurezza è legato al fatto che il problema del logaritmo discreto è difficile nel campo delle curve ellittiche (ECDLP). Per cui questo schema può essere facilmente decifrato inviando query a un computer quantistico mediante l'algoritmo quantistico di Shor.

Qualsiasi terza parte arbitraria può sempre selezionare un SUPI noto e inviare il corrispondente SUCI alla corrispondente HN. Successivamente l'avversario può

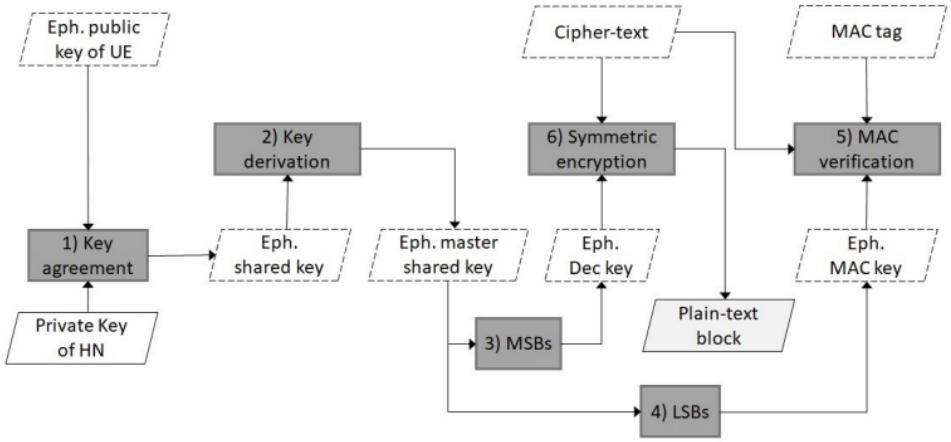


Figura 8.4: In figura la decifratura lato HN

distinguere tra le diverse risposte dall'HN, a seconda che l'utente target sia presente in quella cella o meno. Sulla base delle variazioni nelle risposte ricevute sarebbe possibile confermare o negare la presenza del target in quella particolare cella. In questo schema non esiste alcun meccanismo per prevenire questo tipo di attacchi.

Inoltre, lo schema ECIES non ha alcun meccanismo intrinseco per fornire garanzie di freschezza all'HN ed è quindi soggeto ad attacchi di replay. Un avversario può inviare nuovamente un SUPI cifrato in precedenza (un SUCI precedente) all'HN e ottenere diversi tipi di risposte (una sfida di autenticazione o un messaggio di errore). Sulla base della risposta ricevuta è possibile tracciare un dispositivo di cui non si conosce il SUPI.

Un avversario attivo che simula una falsa BS può forzare l'UE a utilizzare una della generazioni precedenti (3G/4G) e quindi può entrare in possesso dell'IMSI utilizzando un messaggio di Identity Request. Questi attacchi non possono essere del tutto contrastati fino a quando non sarà avvenuta la transizione completa al 5G.

Nelle attuali specifiche di sicurezza 5G, il SUPI viene derivato direttamente dall'IMSI, per cui gli attacchi di bidding down compromettono anche il SUPI.

Potrebbero anche verificarsi situazioni che richiedono che l'HN disponga di un modo sicuro per aggiornare rapidamente la propria chiave pubblica per gli utenti UE. Uno di questi scenari potrebbe essere un attacco malware che tenta di recuperare la chiave privata della home network.

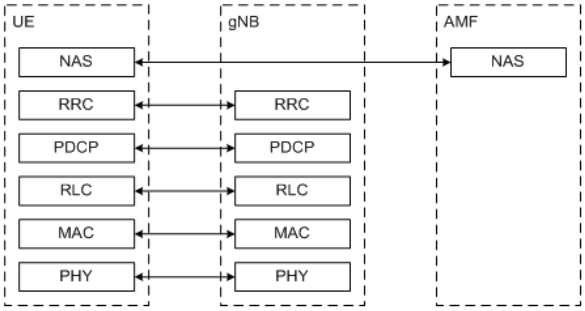
Capitolo 9

Situazione corrente: soluzioni e problematiche rimanenti

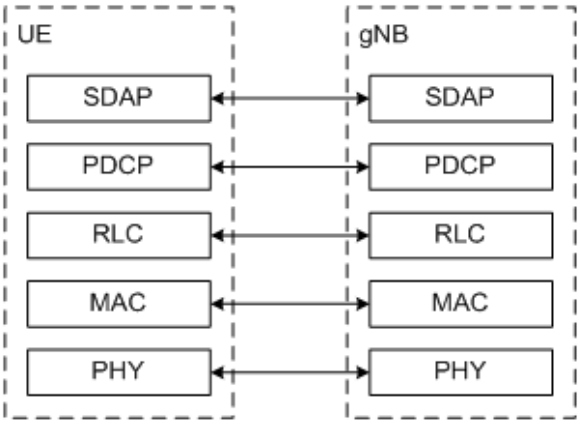
Lo stack protocollare delle reti 5G è rimasto molto simile a quello di LTE, come è mostrato in 9.1a e 9.1b. Per cui in seguito viene fatta un'analisi per livelli dell'applicabilità delle vulnerabilità note di LTE alle reti 5G, verificando i rimedi che sono stati apportati. Le fonti per questo capitolo sono [36], [25], [10] e [23].

9.1 Livello fisico

Il Physical Layer Security (PLS) può essere considerato il framework chiave per la sicurezza 5G, in quanto contribuisce alla protezione di ogni livello. Tuttavia, attualmente non vi sono indicazioni su quali standard relativi alle nuove soluzioni per la sicurezza saranno eventualmente implementati.



(a) Control plane della rete 5G



(b) User plane della rete 5G

Le principali innovazioni tecnologiche 5G sono: reti eterogenee (HetNet), massive MIMO e mmWave. HetNet si riferisce ad una rete in cui coesistono diversi tipi di celle (macro, micro, pico e femto) e tecnologie di accesso, e ha un ruolo fondamentale nell'espansione della rete 5G, in quanto consente di realizzare la densificazione della rete, utilizzando celle di dimensione minore. Massive MIMO (massive multiple-input multiple-output) prevede l'implementazione di stazioni base con un numero di antenne più elevato rispetto alla precedente tecnologia per aumentare l'efficienza energetica e spettrale, in genere centinaia di antenne in un unico array di antenne. mmWave (onde millimetriche) prevede di utilizzare frequenze di trasmissione più elevate.

Poiché i segnali sono wireless è possibile intercettarli e interferirvi, per cui anche nel 5G sono possibili attacchi di intecettazione, radio jamming e manipolazione del messaggio.

Dato che 5G NR introduce la tecnologia beamforming per inviare e ricevere segnali in modo direzionale (utilizzata in Massive MIMO), riduce la portata a dell'area fisica di intercettazione da parte degli attaccanti passivi. Tuttavia, l'interfaccia radio 5G è ancora soggetta a minacce di intercettazione perché non esiste ancora una protezione per le informazioni broadcast e altri messaggi di pre-autenticazione. Sia gli UE che la stazione base si fidano di questi messaggi di pre-autenticazione prima che sia definito il contesto di sicurezza, tuttavia, come affermato in precedenza, l'identità permanente dell'utente è cifrata con la chiave pubblica dell'operatore.

Gli attacchi di jamming nelle reti 5G sono ancora possibili, anche se sono stati resi molto più difficili da implementare, in quanto non sono state apportate delle soluzioni che rimuovono le cause che li consentono. Infatti, rispetto a LTE, l'interfaccia radio 5G

aggiunge più funzionalità dinamiche nella progettazione del protocollo. Ad esempio, per determinare le posizioni delle risorse tempo-frequenza del Physical Uplink Control Channel PUCCH nella NR, l'UE deve conoscere vari parametri forniti dal livello superiore e il PUCCH ha anche un meccanismo di hopping intra-slot, che rende il jamming del PUCCH complicato e costoso. La specifica rimuove anche alcuni aspetti vulnerabili del protocollo come il Physical Control Format Indicator Channel (PCFICH). In LTE il canale di controllo fisico Physical Control Format Indicator Channel (PCFICH) trasporta in downlink un Control Format Indicator (CFI) a 2 bit, che indica il numero di simboli della codifica in un subframe dedicati al canale di controllo.

NR trasmette i PSS, SSS e PBCH in un Synchronization Signal Block (SSB) situato in un determinato raster di sincronizzazione anziché al centro della larghezza di banda di 6 PRB.

Inoltre, la frequenza elevata utilizzata e la larghezza di banda comportano requisiti più stringenti per il supporto hardware, il che rende oggettivamente più difficile realizzare gli attacchi di jamming. Ad esempio, il SSB contenente PBCH occupa 240 sottoportanti nel dominio della frequenza (cioè 20 RB), molte di più che in LTE.

Tuttavia, una volta che i dispositivi hardware che supportano la 5G NR sono disponibili, anche se con difficoltà leggermente superiore rispetto LTE, è comunque possibile effettuare attacchi di smart jamming contro lo strato fisico NR.

Gli attacchi di spoofing sono ancora possibili, in particolare lo spoofing del PSS è una minaccia che non può essere ignorata nel 5G perché le specifiche ancora non forniscono indicazioni precise riguardo a come comportarsi quando l'UE rileva un

PSS senza un SSS associato. Inoltre, dato che le specifiche 5G NR non aggiungono alcun meccanismo di protezione ai messaggi non protetti, sono ancora possibili anche gli altri tipi di attacchi di spoofing e attacchi di overshadowing.

9.2 Livello 2

Come visto in LTE, gli attacchi di identificazione e tracciamento sono favoriti dal fatto che il TMSI rimane statico per un lungo periodo di tempo e/o che lo schema di riallocazione manca di casualità. Per questo motivo, la specifica 5G adotta un meccanismo più rigoroso per l'aggiornamento degli identificativi temporanei, incluso il 5G-TMSI.

Per cui la specifica 5G fornisce delle indicazioni più specifiche relative ai tempi per riallocare 5G-GUTI in modo casuale:

• Dopo aver ricevuto un messaggio di richiesta di registrazione da un'UE, che può essere di "registrazione iniziale", "aggiornamento della registrazione della mobilità" oppure "aggiornamento periodico della registrazione".

• Dopo aver ricevuto un messaggio di Service Request dall'UE in risposta a un messaggio di Paging.

In LTE ci sono due vulnerabilità note del protocollo che consentono di effettuare attacchi di manipolazione dati utente a livello 2: vale a dire la divulgazione di informazioni in chiaro sotto il sottolivello PDCP e la mancanza di protezione dell'integrità per i dati degli utenti.

Per fare fronte a questi attacchi, la specifica del 5G prevede che sia l'UE che nella stazione base devono obbligatoriamente supportare la protezione dell'integrità per i dati degli utenti, a qualsiasi velocità di dati supportata. Tuttavia, la specifica indica anche che "La protezione dell'integrità dei dati dell'utente tra l'UE e il gNB è facoltativa da utilizzare.": anche se la funzione di protezione dell'integrità è supportata, gli operatori possono scegliere di non implementarla nella pratica.

Inoltre, i livelli inferiori al PDCP non hanno dei meccanismi di protezione e la cifratura nasconde il contenuto dei dati, ma non modifica la lunghezza dei pacchetti trasmessi. Di conseguenza rimangono possibili attacchi che sfruttano i metadati che vengono rivelati, che costituiscono informazioni side-channel (attacchi fingerprinting).

9.3 Livello RRC

Gli attacchi contro il livello RRC in LTE possono essere classificati in tre tipi: Paging, broadcast di informazioni di sistema e messaggi di segnalazione RRC.

9.3.1 Attacchi paging e Sys info block

Secondo le specifiche, il 5G/NR utilizza ancora il protocollo di paging per notificare agli UE i servizi in sospeso nella rete e trasmette messaggi MIB/SIB contenenti le informazioni di sistema necessarie per assistere gli UE 5G nella procedura di accesso iniziale. Nonostante le funzionalità e le strutture complessive di questi due tipi di messaggi di trasmissione in 5G siano quasi le stesse di LTE, ci sono diversi miglioramenti.

In primo luogo, per evitare la collegabilità tra l'identificatore permanente dell'utente e la PO, la nuova specifica adotta il calcolo della PO dell'utente dal 5G-STMSI anziché IMSI.

In secondo luogo, come descritto sopra, lo standard 5G sottolinea che la rete deve riassegnare un nuovo identificatore temporaneo all'UE in modo imprevedibile in seguito ad un messaggio di Service Request dell'UE in risposta a un messaggio di paging.

In terzo luogo, il paging basato sull'identificatore permanente (il SUPI in 5G) non è più supportato nel sistema 5G. Questi miglioramenti rendono più molto più difficile tracciare gli utenti 5G mediante messaggi di paging.

Per quanto riguarda il broadcast di informazioni di sistema, una differenza significativa è che ci sono due diversi tipi di SIB nella 5G / NR. Il primo tipo è detto periodic SIB: si tratta di SIB che vengono trasmessi periodicamente attraverso il canale aperto indipendentemente dal fatto che l'UE ne abbia bisogno o meno, come in LTE. L'altro tipo, detto on-demand SIB, viene trasmesso solo quando viene effettivamente richiesto dal UE. Pertanto, nel 5G, gli attaccanti passivi possono intercettare solo il primo tipo di SIB. Tuttavia, non esiste ancora una protezione dell'integrità per i messaggi di broadcast, per cui gli attacchi che utilizzano i messaggi di spoofing ancora fattibili.

9.3.2 Messaggi RRC

Come visto in LTE, sfruttando i messaggi RRC è possibile implementare diverse tipologie di attacchi DoS. I messaggi non protetti di pre-autenticazione esistono ancora

in 5G/NR, compresi i messaggi RRC sfruttati dagli attacchi. Pertanto, un utente malintenzionato può comunque esaurire una stazione base 5G stabilendo connessioni radio eccessive. Fortunatamente, le specifiche 5G indicano che l'UE invia i rapporti di misurazione solo dopo l'attivazione della sicurezza AS.

Inoltre, le reti possono conoscere la capacità dell'UE solo dopo l'istituzione della sicurezza RRC, come specificato in TS 38.331.

I protocolli 5G RRC indicano inoltre che se la sicurezza AS non è attivata, l'UE ignora qualsiasi campo incluso nel messaggio di rilascio RRC, incluso redirected-CarrierInfo. Di conseguenza, gli attacchi che sfruttano questi messaggi RRC per reindirizzare l'UE a reti non sicure come GSM non dovrebbero essere fattibili. Inoltre, dato che l'UE non è ancora dotato di un meccanismo di verifica dell'autenticità della stazione base, risulta ancora possibile l'attacco di iniezione di rapporti di misurazione falsi.

9.4 Attacchi contro il livello NAS

Gli attacchi relativi al livello NAS principali sono attacchi di identificazione, attacchi che sfruttano vulnerabilità del protocollo AKA e attacchi che sfruttano i messaggi NAS pre-autenticazione.

La rete mobile 5G adotta ancora uno schema di crittografia a chiave simmetrica, che si basa fortemente sulla fiducia implicita nei messaggi di pre-autenticazione. La legittimità di questi messaggi, e di altre segnalazioni sfruttate, non può essere

verificata. Quindi, gli attacchi DoS e downgrade sono ancora possibili nel contesto del 5G.

Rispetto a LTE, tuttavia, la specifica 5G fornisce un meccanismo di protezione aggiuntivo per i messaggi NAS iniziali. L'UE duplica i messaggi iniziali corrispondenti nel messaggio NAS Security Mode Complete (Modalità di sicurezza NAS completata). In questo caso, solo un set limitato di IE (chiamati IE in chiaro) come gli identificatori di sottoscrizione e le funzionalità di sicurezza UE vengono divulgati nei messaggi NAS iniziali. La capacità di rete UE IE non è uno degli IE in chiaro.

Nei sistemi 4G, tutti i messaggi NAS iniziali non sono cifrati, poiché i messaggi NAS iniziali crittografati non possono essere decrittografati dalla Mobility Management Entity (MME). I sistemi 5G crittografano il messaggio NAS iniziale completo nel contenitore NAS. Sebbene i messaggi cifrati non possono essere decifrati dall'AMF, l'AMF può richiedere all'UE di inviare nuovamente il messaggio NAS iniziale dopo l'autenticazione.

È qui che risiede la sicurezza: il messaggio NAS iniziale completo viene inviato all'AMF solo dopo aver stabilito il contesto di sicurezza, impedendo così alle reti false di dirottare i messaggi NAS iniziali in chiaro e inviare falsi messaggi NAS Reject all'UE, che come visto in precedenza sono sfruttati da molti attacchi DoS. Se l'UE non dispone di un contesto di sicurezza NAS, il messaggio NAS iniziale contiene solo l'IE. Se l'UE ha stabilito un contesto di sicurezza, deve essere incluso nel contenitore dei messaggi NAS anche il messaggio cifrato NAS iniziale completo. Se l'AMF non dispone dello stesso contesto di sicurezza dell'AMF locale o dell'ultimo a cui l'UE ha acceduto, cioè quelli con cui l'UE ha stabilito il contesto di sicurezza

in precedenza, non è in grado di decifrare il container del messaggio NAS. Quindi l'AMF deve autenticarsi con l'UE e inviare l'identificativo contenuto nel messaggio NAS di richiesta iniziale. L'UE dovrebbe quindi rispondere con un messaggio NAS Security Mode Complete contenente l'intero il messaggio NAS iniziale cifrato. Solo a questo punto l'AMF risponde al messaggio NAS iniziale.

Nella specifica viene indicato che la protezione dell'integrità per il piano di controllo è obbligatoria per essere supportata (dai dispositivi) e utilizzata (dagli operatori), inclusi i segnali RRC e NAS. La riservatezza è obbligatoria per essere supportata (dai dispositivi) ma l'implementazione è facoltativa per gli operatori.

Nei sistemi 5G, il piano utente e il piano di controllo sono separati, il che consente un miglioramento indipendente della funzionalità di ciascun piano.

Sebbene il 4G supporti la riservatezza e la protezione dell'integrità dei messaggi RRC e NAS, manca la protezione dell'integrità del UP, a causa dell'overhead nelle prestazioni percepito dai dispositivi. Il 5G invece impone il supporto sia della riservatezza che della protezione dell'integrità per UP da parte di UE e gNB. Tuttavia, entrambe queste funzionalità sono facoltative da implementare per l'operatore di rete. La protezione del piano utente in 5G viene segnalata dal SMF (una componente della CN) a gNB e poi da gNB a UE. In particolare, da SMF a gNB: viene fornita la policy di sicurezza del UP al gNB per indicare se la riservatezza del UP e/o la protezione dell'integrità di UP devono essere attivate.

Da gNB a UE: gNB invia un messaggio di riconfigurazione della connessione RRC all'UE per attivare la sicurezza UP, in base alla policy di sicurezza ricevuta.

9.4.1 Suci-catchers attack

Come in LTE, la stazione radio base può sempre richiedere l'identificativo permanente in seguito a un messaggio di richiesta di registrazione, però, come già visto, viene inviato questo identificativo cifrato con la chiave pubblica dell'operatore (SUCI). Dopo questa fase di identificazione viene eseguito il protocollo AKA, i cui messaggi sono trasmessi in chiaro, in quanto sono messaggi pre-autenticazione. Attualmente la specifica definisce due schemi di cifratura, entrambi basati su curve ellittiche: EC25519 e secp256r1. Comunque, la cifratura del SUPI è opzionale, in caso l'operatore decide di non abilitarla viene selezionato lo schema "null", come descritto in precedenza.

Questo attacco è basato sulla linkability del protocollo AKA: il messaggio iniziale di Registration Request dell'UE alla rete è sempre associato alla sua identità. In seguito, la rete invia una Authentication Request all'UE, il quale può accettare o rifiutare tale richiesta.

L'attacco SUCI-Catcher [10] sfrutta questo: recupera una sfida di autenticazione associata all'identità del subscriber cercato e invia la corrispondente Authentication Request a tutti gli UE che gli si connettono. Solo l'UE che accetta la richiesta è il subscriber cercato. L'attacco è diviso in due fasi: Discovery Phase, in cui vengono raccolti i SUCI dei subscriber di interesse, e la Attack Phase, in cui una volta che un certo UE si è connesso viene stabilito se si tratta del subscriber cercato oppure no, , come mostrato in figura 9.1.

Per raccogliere i SUCI dei UE target sono possibili due metodi a seconda se l'IMSI è noto oppure no. Nel primo caso è possibile recuperarlo con sniffing del traffico della

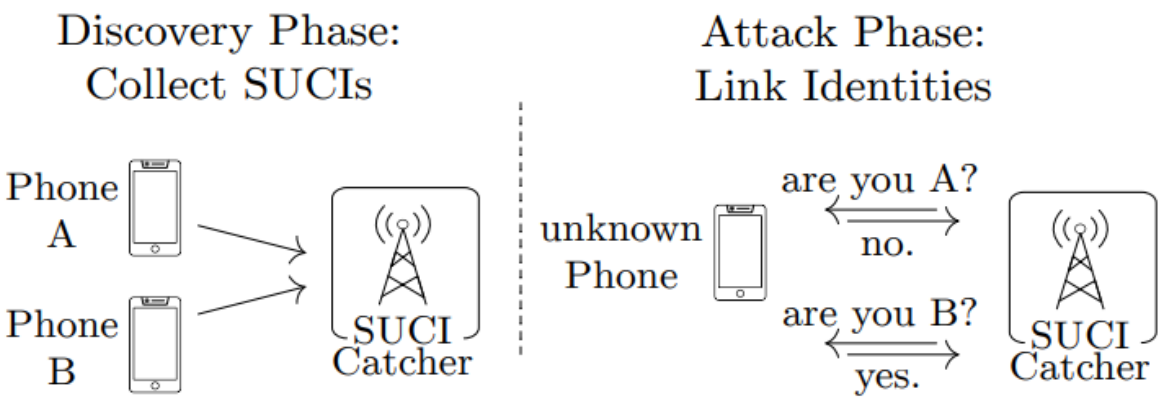


Figura 9.1: In figura le due diverse fasi di questo attacco.

sua rete o inviando direttamente una Identity Request se è connesso a una fake BS. Nel secondo caso, è possibile ottenere il SUCI cifrando l'IMSI con la chiave pubblica dell'operatore, che è nota.

Nella successiva fase dell'attacco (Attack Phase), è necessario verificare se $UE_{sconosciuto}$ connesso al SUCI-Catcher corrisponde al UE target.

Questa fase è a sua volta suddivisa in due fasi: SUCI-Probe e Reset&Synch.

SUCI-Probe:

- Richiesta dei vettori di autenticazione: la richiesta di registrazione stessa non è autenticata e l'utente malintenzionato può inserire nel campo dell'identità il SUCI raccolto nella fase precedente. La rete cerca l'identità e invia la corrispondente Authentication Request a cui solo l'utente associato a $SUCI_{cercato}$ può rispondere.
- UE conferma la sua identità: quando l'UE riceve la Authentication Request, può verificarsi uno dei due casi seguenti:

1. l'$UE_{sconosciuto}$ è effettivamente $UE_{cercato}$: l'autenticazione della rete va a buon fine e l'UE risponde con Authentication Response oppure con Authentication Failure con causa indicata Synch Failure

2. l'$UE_{sconosciuto}$ non è $UE_{cercato}$: l'UE invia un Authentication Failure con causa MAC Failure al SUCI-Catcher.

Reset&Synch:

Dopo due Authentication Failure consecutivi l'UE annulla il tentativo di registrazione, per cui, con questa limitazione risulterebbe possibile ricercare a massimo due persone. Tuttavia, è possibile risolvere questo problema eseguendo una fase di reset, in cui UE e la rete si autenticano con successo prima della fase SUCI-Probe, per evitare che l'errore di autenticazione legato alla fase precedente impedisca la richiesta di registrazione. E' necessario gestire anche gli eventuali errori di Synch Failure per evitare che si verifichi più di un errore consecutivo durante SUCI-Probe, e quindi di non potere più inviare richieste di identificazione.

Pertanto, grazie a questa fase l'attacco è scalabile anche in caso di UE cercati multipli, in quanto consente di eseguire più procedure di autenticazione consecutive senza forzare l'UE a riconnettersi a livello radio. In caso di N persone di interesse l'attaccante deve inviare 2N Authentication Request (in quanto una per la fase Probe e una per quella di reset), per cui deve richiedere 2N vettori di autenticazione alla home network reale.

Le due diverse fasi di SUCI-Probe sono visibili in figura 9.2

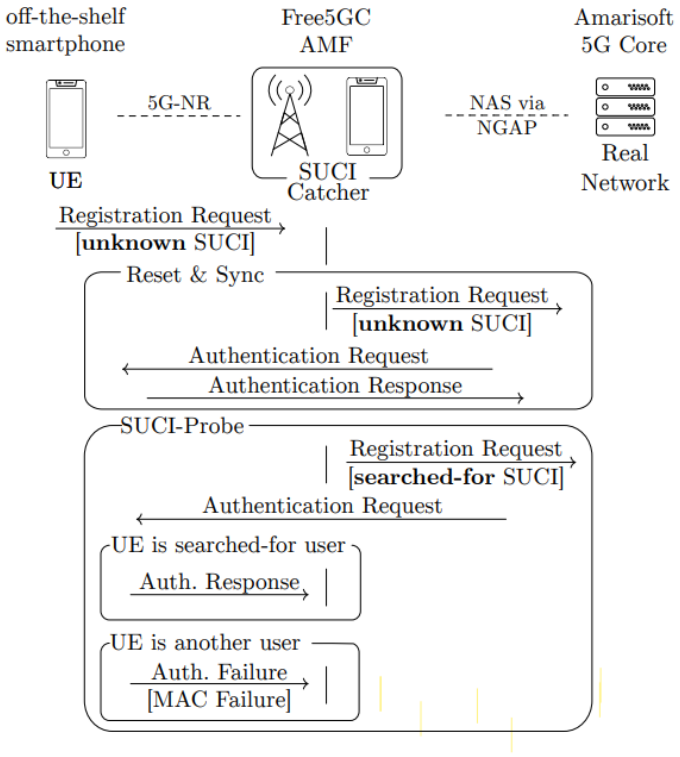


Figura 9.2: Le due diverse fasi della Attack Phase.

Valutazione dell'attacco

La procedura presuppone che i) la rete reale fornisca nuove challenge di autenticazione senza alcun limite ii) l'UE vi risponda Per cui sono stati eseguiti degli esperimenti dedicati per individuare dei limiti pratici a questo attacco.

Questo attacco è stato valutato in una rete di laboratorio 5G-Standalone (SA) con uno smartphone off-the-shell. Tutti i test sono stati eseguiti con una scheda Quectel RM500Q e un OnePlus 8 off-the-shell contenente il chipset Qualcomm X55 5G. L'implementazione dell'attaccante MITM si basa sulla core network opensource Free5GC e su Amarisoft gNodeB. L'UE della vittima e il gNodeB dell'attaccante utilizzano un collegamento radio 5G NR in modalità standalone. La rete legittima è la core network Amarisoft.

Fattibilità dell'attacco

Sono state utilizzate le schede USIM sysmocom che includono la chiave pubblica della rete e abilitano la cifratura dell'identificatore permanente. La modalità "null scheme" è esplicitamente disabilitata per garantire che il SUPI venga sempre cifrato.

Nel set-up di laboratorio è stato possibile testare fino a 500 SUCI al secondo e mantenere un UE connesso a una cella per due ore consecutive inviando periodicamente dei messaggi di autenticazione. Anche se la configurazione di laboratorio riflette una configurazione 5G standalone realistica, sono state utilizzate schede SIM da laboratorio potenti e una core network senza molto carico e che non effettua throttling. Pertanto, sono state valutate ulteriormente le prestazioni di autenticazione di reti commerciali

e schede USIM. Dato che al momento di questo esperimento [10] le reti 5G SA e la protezione con SUCI non sono ancora state implementate (28 giugno – 2 luglio 2021), i test sono stati effettuati sul 4G, ma il risultato è lo stesso che ci si aspetta per il 5G dato che dipende dalla politica dell'operatore piuttosto che dalla tecnologia.

Il test per più UE richiede: 1) che l'UE non annulli la procedura di registrazione 2) la rete reale deve fornire continuamente nuove Authentication Request 3) l'USIM deve rispondere. Tutti i componenti devono rispondere il più rapidamente possibile per ridurre al minimo il tempo di esecuzione dell'attacco per consentirne l'applicazione in scenari pratici. In realtà, gli USIM sono ottimizzati per il basso costo piuttosto che per la velocità, inoltre le reti possono applicare throttling alla messaggistica.

Secondo le specifiche, il ritardo tra un messaggio e il successivo non deve superare il timer NAS dell'UE T3516 di 30 secondi che interrompe le procedure di autenticazione non riuscite. Inoltre, il gNodeB dell'attaccante deve configurare il timer di inattività RRC ad un valore molto elevato. Nella pratica, è stato riscontrato che l'UE annulla la connessione se non viene ricevuto alcun messaggio entro 15 secondi o dopo due tentativi di autenticazione falliti, come detto in precedenza. Per questo viene utilizzata la fase di reset & sync.

Per le schede SIM, è stato verificato con che velocità rispondono a richieste di autenticazione valide e non valide. Le schede SIM testate sono di tre operatori commerciali e una di sysmocom. I risultati sono mostrati in figura 9.3.

L'attacco è limitato a 0,5 test di identità al secondo per la scheda SIM più lenta e 12 test al secondo per quella più veloce.

		Lab	Commercial Network A	B	C
USIM Auth. Responses	Valid	12.5/s	0.9/s	4.8/s	18.1/s
	Invalid	16.6/s	1.1/s	6.3/s	35.1/s
Network Auth. Requests	First 5s	282/s	2.0/s	1.4/s	2.0/s
	… 30s	282/s	0.8/s	0.8/s	0.9/s
	… 60s	282/s	0.6/s	0.7/s	0.8/s
	… 240s	282/s	0.5/s	0.5/s	1.1/s
UE	RM500Q	8.3/s	-	-	-
	OnePlus 8	8.3/s	-	-	-
10 PoIs	[worst case]	1.2 s	20 s	20 s	9,1 s
500 PoIs	[worst case]	60 s	16 min	16 min	7.5 min

Figura 9.3: I risultati per gli esperimenti effettuati.

Per quanto riguarda il throttling della rete, è stato riscontrato che tutte e tre le reti limitano la velocità di invio dei vettori di autenticazione dopo le prime richieste. Il throttling è applicato alle richieste di autenticazione nella fase di sync&reset, e non a quella SUCI-Probe, dato che in quest'ultima viene richiesta l'autenticazione per una identità alternativa ogni volta.

E' possibile parallelizzare le fasi dell'attacco: il recupero del token di autenticazione per la fase di Reset&Sync può essere eseguito in attesa della risposta alla Authentication Request della fase SUCI-Probe.

Nell'esperimento di laboratorio, in cui non è presente throttling, è stato possibile testare 500 identità entro 60 secondi. In questo caso il numero di identità è limitato unicamente dal numero di tentativi dell'UE prima che blocchi il procedimento. In tutti gli esperimenti effettuti su reti commerciali, indipendentemente dall'operatore, il throttling della rete è il fattore più limitante (0,5/s, 0,5/s, 1,1/s). Supponiamo che

l'attaccante cerchi 10 o 500 persone di interesse (PoI). Considerando solo lo scenario peggiore, si deduce che l'attacco si adatta bene a gruppi di dimensione ridotta. Nelle reti A e B, sarebbero necessari 20 secondi per verificare se la persona sconosciuta è o meno tra i 10 PoI. Nel caso di 500 PoI, il tempo necessario aumenta già a 16 minuti (reti A, B) o 7,5 minuti (C).

Per cui l'attacco di IMSI-Catcher rimane fattibile finché sia la linkabilità che la generazione di nuovi vettori di autenticazione rimangono fattibili.

9.4.2 Implementazione della specifica 5G

Come visto, la specifica 5G ha tra gli obiettivi principali l'aumento del livello di sicurezza, per cui sono stati introdotti dei meccanismi per risolvere alcune vulnerabilità note presenti in LTE. Questi meccanismi prevedono la cifratura dell'identificativo permanente, la protezione dei messaggi NAS, come descritto sopra, la protezione di confidenzialità Control Plane e Data Plane.

Uno studio [23] ha verificato la conformità delle reti commerciali 5G alle specifiche di sicurezza.

I risultati di questo studio mostrano che esiste una discrepanza significativa tra gli standard di sicurezza 5G e la loro implementazione nel mondo reale, specialmente per quanto riguarda la protezione user plane (UP) e la protezione degli identificativi. Pertanto, i rischi per la sicurezza noti, come la violazione della privacy degli utenti e gli attacchi Denial-of-Service (DoS), sono ancora applicabili alle reti commerciali 5G

Meccanismo per effettuare le misurazioni

Lo studio è stato condotto a Maggio 2022 a Pechino, una delle prime città a utilizzare reti 5G. Sono state considerate due diverse aree: in una è utilizzata sempre la modalità NR, mentre nell'altra è utilizzata solo per la fase di registrazione, per poi passare a ENDC. Sono state testate le reti 5G commerciali di tre operatori mobili, indicati come operatori A, B e C. L'esperimento è stato condotto con Pilot Pioneer [26], un software commerciale di test per la 5G NR. Questo software è in grado di monitorare e decodificare i segnali del livello di controllo lato UE in tempo reale. I log dei dati possono essere acquisiti e archiviati per poi essere analizzati offline.

Per quanto riguarda l'UE utilizzato è stato scelto uno smartphone 5G commerciale, Samsung S20, con schede SIM 5G commerciali degli operatori A, B e C.

Sono stati analizzati i messaggi critici di segnalazione tra telefoni e reti, tra cui: messaggio Security Mode Command per la selezione degli algoritmi di sicurezza, messaggio di riconfigurazione della connessione RRC per l'attivazione dello stato di sicurezza UP, Identity Response per nascondere SUPI, accettazione della registrazione per la riallocazione 5G-GUTI e richiesta di registrazione per la protezione dei messaggi NAS iniziali.

Inoltre, è stata condotta un'analisi statistica dei valori 5G-GUTI in diversi scenari per verificare se la riallocazione di 5G-GUTI viene attivata nelle condizioni indicate nelle specifiche. Secondo le specifiche, 5G-GUTI deve essere aggiornato dopo:

1.la registrazione dell'UE alla rete 2. che l'UE invia un messaggio di richiesta di servizio in seguito a un messaggio di paging.

Per verificare se il 5G-GUTI viene aggiornato in al caso 1, è stato configurato l'UE in modo tale che si registra e annulla automaticamente la registrazione alla rete con una frequenza media di 30 volte all'ora con Pilot Pioneer.

Per verificare che l'aggiornamento dopo che l'UE invia un messaggio di richiesta di servizio in risposta a un messaggio di paging (caso 2), sono stati inviati continuamente messaggi di Short Messaging Service (SMS) (circa 20 volte in 1 ora) all'UE testato, per attivare un messaggio di paging per quell'utente.

Analisi dei risultati

Il supporto degli algoritmi crittografici in tutte e tre le reti 5G è fondamentalmente conforme alle specifiche 3GPP, sia per RRC che per NAS. Infatti tutti e tre gli operatori supportano la protezione dell'integrità dei dati di segnalazione. Tuttavia, gli operatori A e B non supportano la protezione alla riservatezza per NAS, che è specificata come opzionale.

Protezione UP

Dato che, secondo la specifica, l'attivazione della protezione UP viene eseguita dal gNB inviando messaggi di riconfigurazione della connessione RRC all'UE, sono stati analizzati i campi presenti nei messaggi di RRC per verificare se questi messaggi vengono effettivamente utilizzati per attivare la sicurezza UP.

Sono stati individuati due campi chiave utilizzati per indicare la cifratura aggiuntiva e la protezione dell'integrità, che sono:

- cipheringDisabled, indica se la cifratura è disabilitata per questa portante radio Data Radio Bearer (DRB).
- integrityProtection, indica se la protezione dell'integrità è configurata per questa portante radio.

I risultati dell'analisi mostrano che gli operatori B e C non hanno attivato la cifratura, cioè la protezione della riservatezza UP e tutti e tre gli operatori non supportano la protezione dell'integrità.

Cifratura del SUCI

Dallo studio emerge che tutti e tre gli operatori utilizzano il SUCI con "null scheme" nelle risposte di identità, ovvero l'identificativo permanente del subscriber viene trasmesso in chiaro. Pertanto, nelle reti commerciali 5G testate, un utente malintenzionato potrebbe ancora utilizzare una falsa stazione base e inviare richieste di identità all'UE target per acquisire informazioni sulla sua identità e per effettuare ulteriori attacchi, come il tracciamento della sua posizione.

Per cui, i risultati dei test indicano che tutti e tre gli operatori non configurano le loro schede USIM con la cifratura del SUPI o che le loro reti non sono configurate per supportare uno schema di crittografia diverso da "null-scheme".

Riallocazione del 5G-GUTI

Come descritto in precedenza, gli standard 5G stabiliscono dei requisiti espliciti sui tempi della riassegnazione dell'identificativo temporaneo dell'UE. Tuttavia, i risultati dei test mostrano che le reti commerciali 5G non aderiscono agli standard, in quanto

aggiornano l'identità temporanea solo dopo le registrazioni e non dopo l'invio di richieste di servizio. Come visto nel capitolo precedente, il 5G-GUTI è costituito da GUAMI e 5G-TMSI, poichè MCC e MNC sono fissi e l'AMF Identifier può essere considerato costante, il lavoro si concentra solo sul valore del 5G-TMSI (32-bit).

Dai messaggi di segnalazione raccolti, è emerso che ogni volta che l'UE invia una richiesta di registrazione e attiva la sicurezza NAS tramite la procedura Security Mode Command, viene assegnato un nuovo 5G-GUTI tramite il messaggio di trasferimento DLinformation o il messaggio Registration accept. Dai test della procedura di registrazione si deduce che tutti e tre gli operatori hanno randomizzato sufficientemente i GUTI riallocati, senza utilizzare degli schemi evidenti o dei valori fissi.

Secondo la specifica di sicurezza 5G, 5G-GUTI dovrebbe anche essere riallocato dopo che la core network riceve un Service Request dalll'UE in risposta ai messaggi di paging. Tuttavia, i risultati mostrano che tutte e tre le reti testate non aggiornano il valore 5G-TMSI. Quindi, è stato osservato per quanto tempo il valore di 5G-GUTI viene mantenuto. E' emerso che, dopo che un UE si registra alla rete, il GUTI non viene aggiornato finché l'UE non effettua una chiamata o si registra presso una nuova rete.

Come visto per LTE, se l'identificativo temporaneo rimane invariato, conoscendo il numero di telefono dell'UE è possibile ottenere una mappatura esatta tra l'identificativo temporaneo e il numero di telefono, e quindi tracciare la posizione della vittima.

Protezione dei messaggi NAS iniziali

Operators:		A	B	C
Security Algorithm Selection	NAS Confidentiality Protection	-	-	✓
	NAS Integrity Protection	✓	✓	✓
	AS Confidentiality Protection	✓	✓	✓
	AS Integrity Protection	✓	✓	✓
UP Security Activation	Ciphering Protection	✓	-	-
	Integrity Protection	-	-	-
SUPI Concealing		-	-	-
5G-GUTI Reallocation	After Registration	✓	✓	✓
	After Service Request	-	-	-
Initial NAS Message Protection		-	-	✓

- : vulnerable configuration

Figura 9.4: I risultati ottenuti in questo studio.

Tutti e tre gli operatori hanno implementato il meccanismo di ritrasmissione del messaggio NAS iniziale dopo l'autenticazione, che è compatibile con lo standard di sicurezza.

Inoltre, è stata analizzata la cifratura dei messaggi NAS iniziali. Normalmente il messaggio NAS iniziale è un messaggio di richiesta di registrazione o una richiesta di servizio. Quando un telefono con un contesto di sicurezza invia una richiesta di registrazione alla rete, il messaggio NAS contiene, non solo IE in chiaro (cioè l'identificativo dell'UE), ma anche il container dei messaggi NAS. Come visto in precedenza, il 5G richiede che il container NAS sia crittografato. Tuttavia, i risultati dei test hanno mostrato che gli operatori A e B trasmettono semplicemente il container NAS in chiaro. Solo l'operatore C ha crittografato il container dei messaggi NAS.

In figura 9.4 sono riassunti i risultati ottenuti in questo studio.

Capitolo 10

Conclusioni e sviluppi futuri

Nel corso di questo elaborato sono stati visti gli aspetti più critici legati alla sicurezza delle reti mobili, in particolare della rete LTE, e come queste problematiche note sono state affrontate nel 5G. Si è descritto il protocollo di autenticazione e le caratteristiche dello schema di cifratura scelto nelle reti LTE. In seguito sono state descritte quattro diverse tipologie di attacchi, analizzando le vulnerabilità che li consentono, sia del protocollo che legate all'implementazione da parte degli operatori, soffermandosi anche sui diversi livelli del protocollo che sono coinvolti e ai dettagli implementativi degli attacchi. Le tipologie di attacchi che sono state analizzate sono: attacchi di identificazione, attacchi legati a vulnerabilità logiche del protocollo, attacchi di paging e attacchi DoS.

Nella seconda parte dell'elaborato si è proceduto a fare una panoramica sull'architettura 5G dal punto di vista della sicurezza, sia in riferimento agli attacchi descritti, che alle nuove tecnologie utilizzate.In seguito, è stata descritta l'evoluzione del pro-

tocollo AKA nel 5G. E' stata analizzata nello specifico la realizzazione in 5G di un attacco presentato in precedenza. Infine si è visto uno scenario reale di instaurazione di rete 5G per verificare l'attuazione delle contromisure indicate dalle specifiche e la loro efficacia. Questo ha mostrato una discrepanza per quanto riguarda le indicazioni presenti nelle specifiche e quanto implementato dagli operatori

Sulla base dell'evoluzione delle reti cellulari nelle generazioni precedenti è possibile prevedere requisiti e problematiche relative alla sicurezza nel 6G [22]. Nel passaggio da 4G a 5G si è visto che gli operatori preferiscono integrare le nuove tecnologie mantenendo quelle attuali (5G SA e NSA), sia per una questione di capitale, sia per garantire maggiore connettività. Dunque il 6G probabilmente conserverà diverse vulnerabilità attuali delle reti LTE. L'altro aspetto da tenere in considerazione è che le nuove tecnologie, oltre che migliorare le caratteristiche delle reti, introducono anche nuove minacce per la sicurezza.

Una delle tecnologie che si prospettano per il 6G sono gli schemi di crittografia quantum-safe, dato che i quantum computer rappresenteranno una minaccia concreta per il 2030, periodo in cui si prevede l'installazione del 6G. Inoltre, mentre 5G la PKI è utilizzata solo per la cifratura degli IMSI, nel 6G si potrebbe superare l'utilizzo di uno schema di cifratura simmetrico. Dato l'elevato numero di dispositivi e il fatto che la CA (Certificate Authority) di PKI sia un single point of failure, si prospetta l'utilizzo di blockchain e registri distribuiti (Distribuited Ledger Technologies-DLT), che eliminano le problematiche legate ad una autorità centralizzata e garantiscono gli aspetti positivi legati alle reti peer-to-peer verificabile dai nodi stessi, come elevata scalabilità, affidabilità e trasparenza (tutti i record vengono memorizzati con data

e pseudonimo). Rimangono tuttavia problemi legati al consumo elevato di energia e risorse di calcolo. Una novità chiave è l'utilizzo di intelligenza artificiale (AI) con diverse tecniche di machine learning per la difesa contro attacchi. Una delle modalità con la quale lintelligenza artificiale potrà venire utilizzata per la sicurezza delle reti ("security design by AI") è aumentando la potenza dei sistemi di rilevamento delle intrusioni, consentendogli di apprendere dall'ambiente e prendere decisioni autonome riguardo input nuovi. Nonostante i benefici dell'utilizzo di AI, essa stessa può diventare un target degli attacchi: AI è particolarmente vulnerabile agli attacchi avversari. Tra i possibili attacchi, quello di "data poisoning" rappresenta la casistica principale, dato che la maggioranza degli input è accessibile. Inoltre AI può essere utilizzata per realizzare attacchi in modo efficiente, analizando la rete e individuando le vulnerabilità che possono venire sfruttate. Nonostante gli attacchi basati su AI siano stati ampiamente studiati nella letteratura, l'analisi della loro applicabilità al 6G è ancora allo stadio iniziale, e dunque richiede maggiore approfondimento, dato il ruolo centrale che svolgerà nel 6G.

Ringraziamenti

A conclusione di questo elaborato, desidero menzionare tutte le persone che hanno permesso il raggiungimento di questo obiettivo. Ringrazio il mio relatore, Prof. Gringoli, che mi ha guidata nelle ricerche e nella stesura dell'elaborato. Ringrazio di cuore la mia famiglia per avermi sempre sostenuta durante questi anni. Infine desidero ringraziare Dario per avermi supportata moralmente anche nei momenti più difficili.

Bibliografia

[1] URL: https://en.wikipedia.org/wiki/Multi-access_edge_computing.

[2] URL: https://www.rajarshipathak.com/2020/01/beginners-guide-for-5g-core-network-architecture.html.

[3] OpenAirInterface Softare Alliance (OSA). *Openairinterface, 5g software alliance for democratising wireless innovation.* URL: n.%20https://www.openairinterface.org/.

[4] Amarisoft. 2022. *AMARI Callbox Series.* URL: https://www.amarisoft.com/products/test-measurements/amari-lte-callbox/.

[5] MOS Equipment. 2022. *Mission Darkness™ BlockBox Lab XL.* URL: https://mosequipment.com/products/mission-darkness-blockbox-lab-xl.

[6] 3GPP. URL: https://www.3gpp.org/technologies/5g-system-overview.

[7] Ijaz Ahmad et al. *Overview of 5G Security Challenges and Solutions.*

[8] *Amarisoft. 2022. AMARI Callbox Series.* URL: https://www.amarisoft.com/products/test-measurements/amari-lte-callbox/.

[9] Ravishankar Borgaonkar et al. *New Privacy Threat on 3G, 4G, and Upcoming 5G AKA Protocols.* 2019.

[10] Merlin Chlosta et al. *"5G SUCI-Catchers: Still catching them all?"* 2022.

[11] Università degli studi di Brescia Francesco Gringoli slide del corso di "Network Security".

[12] Syed Rafiul Hussain et al. *Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information*. 2019.

[13] Roger Piqueras Jover. *The current state of affairs in 5G security and the main remaining security challenges*.

[14] Haibat Khan, Benjamin Dowling e Keith M. Martin. *Identity Confidentiality in 5G Mobile Telephony Systems*.

[15] John A. Khan e MD Minhaz Chowdhury. *Security Analysis of 5G Network*. 2021.

[16] Rabia Khan et al. *A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions*, 2020.

[17] Martin Kotuliak et al. *LTRACK: Stealthy Tracking of Mobile Phones in LTE*.

[18] Simon Erni Martin Kotuliak et al. *AdaptOver: Adaptive Overshadowing Attacks in Cellular Networks*. 7 settembre 2022.

[19] Adrien Koutsos. *The 5G-AKA Authentication Protocol Privacy*.

[20] Guangyi Liu et al. *5G Deployment: Standalone vs. Non Standalone from the Operator Perspective*.

[21] J. Arkko Network Working Group e Ericsson. *rfc4187*. 2006. URL: `https://www.rfc-editor.org/rfc/rfc4187.txt`.

[22] Van-Linh Nguyen et al. *Security and privacy for 6G: A survey on prospective technologies and challenges*.

[23] Shiyue Nie et al. *Measuring the Deployment of 5G Security Enhancement*. 2022.

[24] Ivan Palamà et al. *IMSI Catchers in the wild: a real world 4G/5G assessment*. 2021.

[25] Jin Ho Park et al. *A Comprehensive Survey on Core Technologies and Services for 5G Security: Taxonomies, Issues, and Solutions*. 2019.

[26] Ltd. DingLi Corp. [n.d.]. Pilot Pioneer. *The specialized field test solution for directed radio access network troubleshooting and optimization.* URL: `https://www.dingli.com/PilotPioneer.php`.

[27] Università degli studi di Brescia Renato Lo Cigno e Luca Carlett slide del corso di "Reti Cellulari e 5G".

[28] Mamoon M. Saeed et al. *A comprehensive review on the users' identity privacy for 5G networks.*

[29] Altaf Shaik et al. *Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems.* 2016.

[30] Ankush Singla et al. *Protecting the 4G and 5G Cellular Protocols against Security and Privacy Attacks.* 2020.

[31] Prajwol Kumar Nakarmi Srinath Potnuru. *BERSERKER: ASN.1-BASED FUZZING OF RADIO RESOURCE CONTROL PROTOCOL FOR 4G AND 5G.* 2021.

[32] Software Radio Systems. *srslte, your own mobile network.* URL: `https://www.srslte.com, %20Last%20accessed%20on%202020-11-23.`.

[33] D. Talbot. *One simple trick could disable a city 4G phone network, mit technology review.* 2012. URL: `https://www.technologyreview.com/2012/11/%2014/84825/one-simple-trick-could-disable-a-citys-4g-phone-network/`.

[34] Sili Wu et al. *Identifying Security and Privacy Vulnerabilities in 4G LTE and IoT Communications Networks.* 2021.

[35] Chuan Yu e Shuhui Chen. *On Effects of Mobility Management Signalling Based DoS Attacks Against LTE Terminals.* 2021.

[36] Chuan Yu et al. *"Improving 4G/5G air interface security: A survey of existing attacks on different LTE layers.* 2021.