5G Security

Alessandro Castelli
ID:147073
E-mail: castelli.alessandro@spes.uniud.it

October 19, 2024

5

Abstract

Negli ultimi decenni, le comunicazioni wireless hanno subito una rapida evoluzione, alimentata dalla crescente domanda degli utenti per connessioni sempre più veloci, affidabili e performanti. Tra le innovazioni tecnologiche più rilevanti, la tecnologia 5G si è affermata come la nuova frontiera delle telecomunicazioni mobili, promettendo una capacità di banda superiore, latenze ridotte e una enorme densità di connessioni per dispositivi intelligenti e IoT. Tuttavia, insieme a queste straordinarie capacità, emergono anche nuove sfide in termini di sicurezza. Il 5G introduce una infrastruttura di rete più complessa e decentralizzata, aumentando il rischio di vulnerabilità e attacchi informatici. Questo articolo esamina i principali aspetti della sicurezza del 5G, evidenziando le vulnerabilità della rete e discutendo le soluzioni tecnologiche avanzate sviluppate per mitigare i rischi.

Contents

1 Introduzione

La storia della comunicazione mobile è un viaggio di innovazione continua. Tutto inizia con il 1G [2], negli anni '70 e '80, quando la trasmissione dei dati era analogica. Era l'inizio, ma con grandi limiti: la qualità era bassa, la sicurezza inesistente e le chiamate potevano essere facilmente intercettate. Tuttavia, consentiva qualcosa di rivoluzionario per l'epoca: la connettività mobile e i primi servizi vocali, anche se in modo rudimentale.

Con l'arrivo del 2G nel 1991, la situazione cambiò drasticamente. La comunicazione diventò digitale, affrontando molti dei problemi del 1G. Ora c'era più sicurezza, efficienza e una maggiore larghezza di banda. Si aprirono così le porte a nuovi servizi come i messaggi di testo (SMS), rendendo la comunicazione mobile più sofisticata.

Successivamente, il 3G introdusse il concetto di banda larga mobile. Non era più solo una questione di chiamate o messaggi, ma anche di videochiamate, navigazione su Internet e una trasmissione dati molto più veloce. Il 3G rappresentava una svolta, anche se soffriva ancora di problemi legati allo spettro e alla latenza, dimostrando che la tecnologia aveva ancora margini di miglioramento.

Quando arrivò il 4G, tra il 2009 e il 2010, il mondo della comunicazione mobile fece un enorme balzo in avanti. Grazie a tecnologie come LTE, la velocità dei dati aumentò significativamente, portando il mobile streaming, i giochi online e i video in alta definizione a portata di mano ovunque. Le velocità di download teoriche potevano raggiungere i 100 Mbps, sebbene nella pratica fossero spesso inferiori.

Infine, con l'avvento del 5G, si entrò in una nuova era. Non si parlava più solo di miglioramenti incrementali, ma di una rivoluzione. Il 5G promette velocità fino a 20 Gbps [3], una latenza ultra bassa e la capacità di connettere miliardi di dispositivi contemporaneamente. È una tecnologia pensata per un mondo interconnesso, dove non ci sono solo smartphone, ma anche automobili, dispositivi IoT, smart cities e sistemi industriali automatizzati. Il 5G è il fondamento di quella che sarà l'Internet of Everything, dove ogni aspetto della vita quotidiana è connesso e integrato in una rete globale.

Il **5G** rappresenta quindi l'ultima evoluzione nella tecnologia di comunicazione mobile, portando miglioramenti significativi come *larghezza di banda elevata* e *latenza estremamente bassa*. Questa tecnologia supporta applicazioni avanzate come la realtà aumentata (AR), la realtà virtuale (VR) e le comunicazioni ultra-affidabili a bassa latenza (URLLC). Nel marzo 2018, il 3GPP ha rilasciato la 15ª release degli standard di comunicazione mobile, stabilendo le basi per il **5G**. La velocità di trasmissione di questa nuova tecnologia consente agli utenti di usufruire di trasferimenti dati notevolmente superiori, in particolare per applicazioni che richiedono un alto throughput, come lo streaming video in alta definizione [3].

La riduzione della latenza è un altro obiettivo chiave, con la previsione di una latenza inferiore a 1 millisecondo, aprendo la strada all'uso in tempo reale di applicazioni critiche come la telemedicina e la guida autonoma. Inoltre, il 5G permette la connessione simultanea di un numero molto maggiore di dispositivi

rispetto alle generazioni precedenti, una caratteristica fondamentale vista la continua crescita del mercato IoT.

Grazie a tutto questo, il 5G diventerà una base per una rete che connette non solo persone, ma anche oggetti, dispositivi e macchine. Si sta parlando, quindi, di un sistema che sta rivoluzionando il modo in cui immaginiamo internet, non più solo come uno scambio di dati tra persone, ma come un'integrazione massiccia tra esseri umani e macchine, e tra macchine stesse.

E qui entrano in gioco i tre scenari fondamentali del 5G: **eMBB, mMTC e uRLLC**. Ognuno di questi rappresenta una sfaccettatura dell'intera visione del 5G [4]: **eMBB** è pensato per una banda larga mobile potenziata, consentendo download rapidissimi e streaming ad altissima qualità; **mMTC** è rivolto alla comunicazione massiva tra macchine, essenziale per supportare l'IoT (Internet of Things); **uRLLC** invece è cruciale per applicazioni che richiedono una latenza minima e un'affidabilità estrema, come la telechirurgia o i veicoli autonomi. Ma quali sono le tecnologie che effettivamente rendono possibile tutto questo?

Il 3GPP ha definito più di 70 tipi di file 5G SA1 necessari a questo scopo, e le tecnologie chiave sviluppate per il 5G includono: **Massive MIMO**, **filter bank based multicarrier (FBMC)**, **Full Duplex**, **Ultra Dense networking (UDN)**, **software-defined networking (SDN)** e **network function virtualization (NFV)** [4].

2 Threat model

In letteratura sono state identificate numerose sfide legate alla sicurezza del 5G. Gli asset principali coinvolti includono i dati sensibili degli utenti, come informazioni personali e dati di navigazione, che transitano attraverso la rete 5G. A questo si aggiungono l'infrastruttura di rete stessa, composta da stazioni base, server e dispositivi di rete, nonché i dispositivi degli utenti finali, tra cui smartphone, tablet e dispositivi IoT, che rappresentano una parte essenziale del sistema. È importante notare che, oltre ai dispositivi finali, i sistemi di controllo della rete, incaricati della gestione del traffico e dell'autenticazione, necessitano di una protezione adeguata per garantire l'integrità e la disponibilità della rete.

Le reti 5G introducono diverse tecnologie innovative, come il *software-defined networking (SDN)* e il *network function virtualization (NFV)*, che offrono vantaggi significativi in termini di flessibilità e scalabilità. Tuttavia, queste tecnologie espongono anche la rete a nuovi rischi di sicurezza, come l'esaurimento delle risorse e vulnerabilità nelle interfacce di programmazione, che possono diventare obiettivi per attacchi mirati. Inoltre, il *Massive Multiple-Input Multiple-Output* (MIMO) e le *comunicazioni a onde millimetriche (mmWave)* aumentano la capacità delle reti, ma devono affrontare problemi di sicurezza legati alla gestione delle risorse e alla segretezza delle informazioni. Anche il *cloud computing* e il *Multi-access Edge Computing* (MEC) possono contribuire a migliorare l'efficienza della rete, ma l'archiviazione e l'elaborazione dei dati nel cloud aumentano il rischio di attacchi ai dati sensibili [1].

I potenziali attaccanti in questo contesto possono variare notevolmente. Da

una parte, ci sono hacker individuali che cercano di intercettare o manipolare i dati per scopi illeciti. Dall'altra, vi sono gruppi di cyber-criminali organizzati, e in alcuni casi anche attori sponsorizzati da stati, il cui obiettivo potrebbe essere ottenere accesso non autorizzato a informazioni sensibili o causare danni alla rete per ragioni economiche o geopolitiche. A rendere più complesso il quadro ci sono anche malintenzionati interni, ovvero personale con accesso legittimo alla rete, che potrebbe abusare delle proprie autorizzazioni. In questo contesto, è cruciale riconoscere che le vulnerabilità non provengono solo dall'esterno, ma anche da configurazioni errate e pratiche di sicurezza inadeguate da parte del personale autorizzato. I vettori di attacco attraverso cui questi attori possono colpire sono molteplici. La sicurezza delle interfacce radio, potrebbe essere compromessa se tali protocolli non vengono implementati correttamente o se si sfruttano vulnerabilità complesse. Questo apre la strada ad attacchi come l'intercettazione delle comunicazioni o i classici man-in-the-middle. Anche l'integrità del piano utente rappresenta un punto critico: nonostante l'introduzione di crittografia avanzata nel 5G, attacchi mirati potrebbero sfruttare eventuali falle nel processo di protezione dei dati, compromettendo così l'integrità dei dati trasmessi senza essere rilevati.

Durante il roaming, un altro momento delicato per la sicurezza, i parametri di protezione degli utenti potrebbero non essere aggiornati correttamente al passaggio tra reti diverse, esponendo gli utenti a potenziali attacchi di intercettazione o manipolazione dei dati. Questa problematica evidenzia la necessità di un'adeguata sincronizzazione e aggiornamento delle misure di sicurezza tra diverse reti, al fine di garantire una protezione continua e coerente.

L'infrastruttura del 5G, inoltre, non è immune da attacchi DoS (Denial of Service). Nonostante i progressi nelle misure di protezione, i sistemi di controllo della rete rimangono visibili e possono essere vulnerabili a interruzioni del servizio, soprattutto se i canali di controllo non sono crittografati adeguatamente. Qui, la gestione delle credenziali e delle configurazioni diventa fondamentale per prevenire accessi non autorizzati.

Infine, un importante vettore di attacco è rappresentato dai dispositivi degli utenti finali. Spesso, questi dispositivi non sono dotati di misure di sicurezza sufficienti a livello di sistema operativo e applicazioni, rendendoli vulnerabili a malware, attacchi DoS o manipolazioni dei dati di configurazione, compromettendo così l'intera rete. Questa vulnerabilità è accentuata dalla crescente diffusione dei dispositivi IoT, che possono presentare vulnerabilità intrinseche dovute a progettazioni inadeguate o a una mancanza di aggiornamenti regolari.

In conclusione, il panorama delle minacce nella rete 5G è complesso e variegato, richiedendo un approccio multifattoriale per la protezione degli asset e la mitigazione dei rischi. Un'attenzione particolare deve essere dedicata non solo alle tecnologie e ai protocolli di sicurezza, ma anche alla formazione continua del personale e alla consapevolezza degli utenti finali riguardo ai rischi e alle migliori pratiche per la sicurezza.

3 Security goals

Describe the security goals that we aim to achieve on the identified assets, according to the CIAAA model.
Ogni sistema di comunicazione affinchè sa considerato sicuro ha bisogno di protocolli e tecnolgie di protezioneche proteggano le risorse usate la comunizazione in modo tale da garantire che i dati rispettino le proprietà di: **Riservatezza**, **Integrità**, **Disponibilità**, **Autenticità, Accountability** [8].
Questi obiettivi sono essenziali per garantire che le reti 5G possano operare in modo sicuro e affidabile, proteggendo i dati e le comunicazioni degli utenti.
Iniziamo con la Riservatezza. Questo obiettivo mira a garantire che solo gli utenti autorizzati possano accedere alle informazioni sensibili. Nelle reti 5G, dove la quantità di dati trasmessi è enorme e include informazioni personali e aziendali, è cruciale implementare misure di crittografia e autenticazione robusta. La riservatezza non è solo una questione di protezione dei dati, ma anche di fiducia degli utenti nel sistema. Se gli utenti percepiscono che i loro dati non sono al sicuro, potrebbero essere riluttanti a utilizzare i servizi offerti.
Passando all'Integrità, questo obiettivo si concentra sulla protezione dei dati da modifiche non autorizzate. In un ambiente 5G, dove i dispositivi IoT e le applicazioni critiche sono sempre più interconnessi, è fondamentale garantire che le informazioni rimangano accurate e non vengano alterate durante la trasmissione.
La Disponibilità è un altro obiettivo chiave. Le reti 5G devono essere sempre disponibili per garantire che gli utenti possano accedere ai servizi in qualsiasi momento. Questo è particolarmente importante per applicazioni critiche come quelle nel settore sanitario o nei trasporti. Per raggiungere questo obiettivo, è necessario implementare soluzioni di ridondanza e resilienza, in modo da mitigare gli effetti di attacchi come i Distributed Denial of Service (DDoS), che possono compromettere la disponibilità dei servizi.
L'Autenticità è fondamentale per garantire che le entità coinvolte nelle comunicazioni siano chi dichiarano di essere. In un contesto 5G, dove le interazioni avvengono tra una varietà di dispositivi e utenti, è essenziale implementare meccanismi di autenticazione robusti. Ciò non solo protegge gli asset da accessi non autorizzati, ma contribuisce anche a costruire un ecosistema di fiducia tra i vari attori coinvolti.
Infine, la Accountability è cruciale per garantire che tutte le azioni e le transazioni all'interno della rete possano essere tracciate e verificate. Questo obiettivo è particolarmente importante per la conformità alle normative e per la gestione delle responsabilità. Implementare sistemi di logging e monitoraggio consente di rilevare attività sospette e di rispondere rapidamente a potenziali incidenti di sicurezza.
In sintesi, il modello CIAAA fornisce un framework completo per affrontare le sfide di sicurezza nelle reti 5G. Ogni obiettivo è interconnesso e contribuisce a creare un ambiente sicuro e affidabile per gli utenti e le applicazioni. La protezione degli asset in un contesto 5G richiede un approccio olistico che integri tecnologie avanzate, politiche di sicurezza rigorose e una continua vigilanza per

affrontare le minacce emergenti.

4 Security service and implementation

Describe the security services to be implemented, and how these are implemented: protocols, algorithms, procedures, etc.

L'architettura del 5G è organizzata attraverso 3 strati: uno strato applicatvo, uno strato di servizio e uno strato di trasporto [5]. Ogni strato è progettato con specifiche funzionalità di sicurezza che, combinate tra loro, creano un sistema sicuro e resistente alle minacce. I principali elementi di sicurezza nel 5G includono:

- **Sicurezza dell'accesso alla rete**: Meccanismi che permettono a un dispositivo utente (UE) di autenticarsi e accedere in modo sicuro ai servizi di rete. L'UE scambia messaggi di protocollo attraverso la rete di accesso con la rete di servizio (SN). Le chiavi crittografiche sono memorizzate nel modulo `USIM` del dispositivo e nell'ambiente dell'operatore. Questo garantisce la sicurezza dei dati e delle comunicazioni, impedendo accessi non autorizzati.

- **Sicurezza del dominio di rete**: Un insieme di caratteristiche che permettono ai nodi della rete di scambiarsi in modo sicuro i dati del piano di controllo e del piano utente all'interno delle reti 3GPP e tra reti diverse. Le tecniche di protezione includono crittografia e integrità per evitare intercettazioni e manomissioni.

- **Sicurezza del dominio utente**: Si concentra sulla protezione del dispositivo dell'utente e dei dati contenuti, impedendo l'accesso non autorizzato al terminale mobile. Sono implementati meccanismi hardware per proteggere il modulo `USIM` e prevenire la manomissione dei terminali, garantendo l'autenticità dell'utente.

- **Sicurezza del dominio dell'architettura basata su servizi**: Protegge la registrazione, la scoperta e l'autorizzazione degli elementi di rete, nonché le interfacce basate su servizi. Consente l'integrazione sicura delle nuove funzioni di rete virtuali del 5G, e supporta il roaming sicuro, coinvolgendo la rete di servizio e la rete domestica.

- **Visibilità e configurabilità della sicurezza**: Consente agli utenti di essere informati sulla presenza di funzioni di sicurezza e offre la possibilità di configurare le caratteristiche di sicurezza in base alle esigenze. Le specifiche di sicurezza del 5G, definite dal 3GPP, stabiliscono funzionalità opzionali, fornendo gradi di libertà per l'implementazione e il funzionamento sicuro della rete.

Le procedure di sicurezza del 5G si basano su un framework a derivazione gerarchica. La chiave a lungo termine `K` è conservata dalla `Authentication`

Credential Repository and Processing Function (ARPF) mentre la USIM conserva la copia corrispondente di tale chiave simmetrica dell'utente [5]. Tutte le altre chiavi sono derivate da essa (per vedere come vengono generate le chiavi guarda 13).

Il 3GPP ha introdotto l'Extensible Authentication Protocol (EAP) per l'Autenticazione e l'Accordo delle Chiavi, definendo l'EAP-AKA e il 5G AKA come metodi obbligatori di autenticazione per i dispositivi (UE) e la rete. Questi protocolli garantiscono un'autenticazione reciproca tra il dispositivo e la rete, oltre a proteggere la sicurezza e la cifratura dei servizi. Durante la registrazione, un dispositivo 5G invia il **SUCI** per avviare il processo di autenticazione basato sul protocollo selezionato.

Le specifiche di sicurezza del 5G definiscono vari contesti di sicurezza per diverse situazioni: per una singola rete di servizio 5G (SN), tra più SN e tra reti 5G e 4G. Quando un dispositivo è connesso a due SN, ciascuna rete deve gestire e utilizzare autonomamente un proprio contesto di sicurezza. Nel caso in cui il dispositivo sia registrato su due SN all'interno della stessa rete pubblica mobile terrestre (PLMN), che siano 3GPP o non-3GPP, il dispositivo stabilisce due connessioni NAS (Non-Access Stratum) separate per ciascuna rete, ma condivide un contesto di sicurezza NAS comune, che include un unico insieme di chiavi e algoritmi di sicurezza.

Le procedure per mantenere o scartare un contesto di sicurezza durante la transizione di stato dicano che la configurazione della tipologia di handover è a discrezione dell'operatore, basandosi sui requisiti di sicurezza individuali. Di conseguenza, la sicurezza durante l'handover diventa una funzione opzionale e non obbligatoria, il che potrebbe portare alcuni operatori a implementare procedure di handover potenzialmente non sicure.

La separazione crittografica e la protezione contro attacchi di replay per due connessioni NAS attive vengono garantite attraverso un contesto di sicurezza NAS condiviso, con parametri distinti per ciascuna connessione. Il NAS impiega algoritmi di cifratura a 128 bit per garantire l'integrità e la riservatezza dei dati. È importante notare, tuttavia, che sono previste anche opzioni di cifratura e protezione dell'integrità nulle. Inoltre, se il dispositivo non dispone di un contesto di sicurezza NAS, il messaggio NAS iniziale viene trasmesso in chiaro, includendo l'identificatore dell'abbonato e le capacità di sicurezza del dispositivo stesso.

Nel controllo delle risorse radio, l'integrità e la riservatezza vengono garantite dal livello PDCP (Packet Data Convergence Protocol) che opera tra il dispositivo e il gNB. È importante notare che nessun livello al di sotto del PDCP è soggetto a protezione dell'integrità. La protezione contro gli attacchi di replay è attivata quando la protezione dell'integrità è in funzione, tranne nel caso in cui sia selezionata la protezione dell'integrità nulla. I controlli di integrità RRC vengono effettuati sia sul dispositivo che sul gNB, e se un controllo di integrità fallisce dopo che la protezione è stata attivata, il messaggio corrispondente viene immediatamente scartato.

Passando al piano utente, la funzione di gestione delle sessioni (SMF) si occupa di fornire la politica di sicurezza per una sessione PDU (Protocol Data

Unit) al gNB durante la fase di stabilimento della sessione. Se la protezione dell'integrità non è attivata per i portatori radio di dati (DRB), né il gNB né il dispositivo saranno in grado di proteggere l'integrità del traffico di tali DRB. Allo stesso modo, se la cifratura del piano utente non è attivata per i DRB, il traffico non verrà cifrato. La SMF locale ha la possibilità di sovrascrivere l'opzione di riservatezza presente nella politica di sicurezza del piano utente ricevuta dalla SMF della rete di origine (HN).

Infine, per quanto riguarda la privacy dello ID di abbonamento, il SUCI rappresenta la versione nascosta dell'identificatore di abbonamento permanente del 5G (SUPI). Questo viene trasmesso via etere per evitare l'esposizione dell'identità dell'utente in chiaro. Il SUCI è generato dal SUPI utilizzando la chiave pubblica dell'operatore e un metodo di crittografia asimmetrica probabilistica, il quale aiuta a prevenire il tracciamento dell'identità. Tuttavia, il sistema di protezione nulla del SUPI è utilizzato durante sessioni d'emergenza non autenticate, se configurato dalla rete di origine (HN), oppure quando la chiave pubblica dell'operatore non è stata fornita. Le specifiche del 5G definiscono anche un identificatore temporaneo, il 5G Globally Unique Temporary Identifier (5G-GUTI), per ridurre l'esposizione del SUPI e del SUCI. Il 5G-GUTI deve essere riassegnato in base ai trigger del dispositivo, ma la frequenza di tale riassegnazione è lasciata alla discrezione dell'implementazione della rete.

5 Attacks and Vulnerabilities

5.1 5G NSA

Il **5G Non-Standalone (NSA)** è un'architettura transitoria che sfrutta la infrastruttura esistente del `4G LTE` per la gestione della segnalazione e del controllo della rete, utilizzando il 5G principalmente per aumentare la capacità e la velocità di trasmissione dei dati. Sebbene questa configurazione acceleri l'adozione del 5G, porta con sé anche una serie di sfide e vulnerabilità di sicurezza. Infatti, le reti NSA dipendono dal core 4G per il controllo, il che significa che molte delle vulnerabilità già presenti nelle reti LTE possono essere trasferite nell'ambito del 5G NSA.
Studiare la sicurezza delle reti 5G NSA diventa quindi cruciale non solo per mitigare le vulnerabilità già presenti, ma anche per prepararsi alla transizione verso il 5G Standalone.
`5G NSA` è un metodo in cui la rete centrale è configurata come un core di pacchetti basata su LTE e vengono utilizzati sia `evolved node B (eNB)` sia `next generation node B (gNB)`. La comunicazione 5G NSA si divide in una componente wireless e una cablata. La parte wireless comprende la rete di accesso radio (RAN), che collega l'apparecchiatura utente (UE) alla stazione base, mentre la parte cablata riguarda la rete centrale (CN), che connette la stazione base alla rete di servizio. In questo contesto, si distinguono due piani: il piano di controllo (CP), responsabile della gestione del traffico di segnalazione tra il terminale e la rete, e il piano utente (UP), incaricato di gestire il traffico dati tra

il terminale e i servizi di rete, come Internet o le chiamate vocali
Il fatto che la configurazione NSA utilizzzi una rete core bassata su EPC (evolved Packet Core) di tipo LTE e il node eNB fa in modo che `5G NSA` erediti le vulnerabilità di sicurezza esistenti in `LTE`.
Le principali minacce alla sicurezza nelle reti `5G NSA` sono quindi [9]:

- Fuga di informazioni
- Attacchi DoS
- Intercettazione
- Uso non autorizzato di dati

5.1.1 Minacce al Radio Access Network

Le minacce alla sicurezza del Radio Access Network (RAN) si concentrano sulle vulnerabilità della parte radio della rete, che include le stazioni base e i dispositivi mobili.

Fuga di informazioni: Le minacce includono lo sniffing del `paging` e la decodifica dell'`IMSI`. Il `paging` è un processo utilizzato per inviare notifiche ai dispositivi mobili riguardo chiamate, messaggi o altre comunicazioni. Le stazioni base trasmettono questi messaggi in broadcast, consentendo ai dispositivi di rispondere e stabilire una connessione. L'`IMSI` è un identificatore unico per un abbonato, fondamentale per l'autenticazione nella rete. Lo sniffing del paging consente a un attaccante di intercettare i messaggi di paging e ottenere l'`IMSI` dell'utente, utilizzando dispositivi come il Software Defined Radio (SDR).

Denial of Service (DoS) per l'utente: Questo tipo di attacco include varie forme, come il DoS alla connessione `RRC` (Radio Resource Control), il DoS di rifiuto `RRC` e il DoS di rilascio `RRC`. Il DoS alla connessione `RRC` è particolarmente grave, poiché sfrutta l'`S-TMSI` (SAE-Temporary Mobile Subscriber Identity) della vittima, precedentemente ottenuto attraverso una fuga di informazioni. Le stazioni base non implementano procedure di autenticazione per i terminali, consentendo agli attaccanti di interferire con l'accesso wireless della vittima. L'attaccante può inviare un messaggio di richiesta di connessione `RRC` utilizzando il valore `S-TMSI` della vittima, portando alla disconnessione della connessione `RRC` della vittima e stabilendo una connessione con l'attaccante, che può poi continuare a inviare richieste per impedire l'accesso legittimo al servizio.

DoS della stazione base: Un attacco DoS può anche mirare a esaurire le risorse della stazione base, rendendo difficile per gli utenti legittimi connettersi. Quando un terminale cerca di stabilire una connessione, utilizza il protocollo RRC, che prevede un processo di accesso casuale. Gli attaccanti possono sfruttare questo processo per inviare richieste non autorizzate, aumentando il numero di connessioni RRC attive e sovraccaricando la stazione base, causando ritardi o interruzioni nei servizi.

Eavesdropping: Sebbene le impostazioni di sicurezza AS dovrebbero prevenire

l'intercettazione, ci sono circostanze in cui ciò può avvenire. Il traffico vocale è gestito tramite il protocollo RTP, e il bearer vocale, a differenza dei bearer dati,è dedicato e garantisce la qualità del servizio. Tuttavia, se un attaccante riesce a registrare la comunicazione vocale cifrata e poi effettua una chiamata utilizzando lo stesso ID del bearer, può estrarre il keystream necessario per decodificare le comunicazioni precedenti.

Utilizzo non autorizzato dei dati: Nelle reti mobili esistono bearer predefiniti e dedicati, progettati per comunicazioni legittime. Un attaccante può sfruttare questi bearer per accedere ai dati in modo non autorizzato, ad esempio stabilendo comunicazioni senza costi. Inoltre, il masquerading del chiamante, noto anche come caller spoofing, è un attacco in cui l'attaccante falsifica l'identità del chiamante, ingannando la vittima.

5.1.2 Core Network Security Threats

Fuga di informazioni: Le reti core 5G NSA possono essere suddivise in dispositivi EPC per l'elaborazione dei dati e dispositivi IMS per i servizi. Gli attaccanti possono colpire il protocollo GTP tra i dispositivi EPC o il protocollo SIP nei dispositivi IMS, in base alle informazioni che desiderano ottenere. Una tecnica comune è l'iniezione di pacchetti GTP-C per estrarre informazioni IP dai dispositivi EPC.
Esaurimento degli indirizzi IP: Utilizzando la tecnica GTP-in-GTP, un attaccante può esaurire il pool di indirizzi IP della rete inviando richieste di sessione con numeri di terminale incrementati, impedendo così ai terminali legittimi di connettersi.
Denial of Service (DoS): Un attacco DoS può essere eseguito inviando ripetutamente messaggi di richiesta di connessione alla rete 5G NSA, sovraccaricando il core di rete e causando l'interruzione del servizio.
Manipolazione del NAS: I messaggi del protocollo NAS, utilizzati per la segnalazione tra terminali e core di rete, non sempre sono protetti da cifratura. Un attaccante può sfruttare questa vulnerabilità installando una stazione base malevola per manipolare i messaggi e alterare i parametri critici per la cifratura e l'integrità dei dati.
Intercettazione: Le comunicazioni vocali nelle reti 5G utilizzano la rete IMS e il protocollo SIP. Se l'attaccante riesce a disabilitare la cifratura IPSec nel terminale della vittima, può intercettare il traffico vocale non criptato attraverso attacchi di tipo man-in-the-middle (MitM).
Spoofing: Lo spoofing di IP è un attacco comune in cui l'attaccante invia pacchetti con indirizzi IP falsificati, causando problemi di fatturazione e potenziali attacchi DoS. Inoltre, lo spoofing del campo `from` nei pacchetti SIP o MMS può essere utilizzato per il voice phishing, presentando numeri falsificati sul terminale ricevente.

5.2 Attacchi alle reti 5G SA

Le minacce alla sicurezza del 5G SA classificate da ENISA sono anche in questo similmente al caso del 5G NSA:

- SPAM
- Spoofing degli identificatori
- Tracciamento della posizione
- DoS
- Frode degli abbonati
- Intercettazione messaggi
- Attacchi al routing delle chiamate
- Attacchi di infiltrazione

Nella Figure 1 mostra la classificazione dei tipi di attacco correlati ai protocolli di rete sulla rete core 5G.

5.3 Attacchi basati sul protocollo

Di seguito sono elencati i principali tipi di attacchi basati su protocolli nelle reti 5G [7].

5.3.1 Attacchi basati sul protocollo RRC

Il protocollo RRC regola l'istituzione, la riconfigurazione e il rilascio delle risorse radio tra l'utente (UE) e la rete di accesso radio. Gli attaccanti possono sfruttare vulnerabilità in questo protocollo per eseguire attacchi come la manomissione dell'ID dell'abbonato, attacchi DoS (Denial of Service) contro le stazioni base e bypass dell'autenticazione dovuti alle debolezze del chipset di base (baseband) dell'UE e dell'attrezzatura della stazione base.

5.3.2 Attacchi basati sul protocollo NAS

Il protocollo NAS, ovvero Non Access Stratum, è composto da messaggi di controllo che gestiscono vari aspetti cruciali nelle reti 5G, come l'autenticazione degli utenti finali, la loro mobilità e la posizione tra il dispositivo utente e l'equipaggiamento della rete core. Questa interazione è fondamentale per garantire che gli utenti siano correttamente autenticati e per gestire il loro spostamento all'interno della rete. Tuttavia, i malintenzionati possono approfittare di questo protocollo per lanciare attacchi DoS (Denial of Service) mirati allo eequipaggiamento MME, il che potrebbe provocare l'interruzione dei servizi per gli utenti. Inoltre, c'è il rischio di perdita di dati sensibili, come le informazioni di identificazione degli abbonati, che potrebbero essere sfruttate in vari modi,

incluso l'attacco man-in-the-middle. Questo accade a causa di vulnerabilità presenti nella specifica del protocollo stesso, così come a causa di bypass delle misure di autenticazione e errori nella gestione dei messaggi, che possono compromettere ulteriormente la sicurezza delle comunicazioni nella rete.

5.3.3 Attacchi basati sul protocollo GTP

Il GTP (GPRS Tunneling Protocol) è un protocollo di controllo che gestisce la creazione e il rilascio dei tunnel all'interno della rete core per la trasmissione di dati IP. Esistono messaggi GTP-C per il controllo delle sessioni di tunneling e messaggi GTP-U per la trasmissione dei dati. A causa della sua progettazione iniziale, il protocollo GTP non ha preso in considerazione la sicurezza, portando a vulnerabilità sfruttabili. Ricerche condotte da Positive Technology, GSMA e KISA hanno evidenziato la possibilità di attacchi man-in-the-middle e DoS tramite la contraffazione dei valori dei campi dei messaggi GTP.

5.3.4 Attacchi basati sul protocollo Diameter

Il protocollo Diameter è utilizzato per l'autenticazione, l'autorizzazione e la contabilizzazione (AAA) ed è fondamentale per il controllo delle politiche di qualità del servizio. Gli attacchi che sfruttano questo protocollo includono il dirottamento delle connessioni e gli attacchi di ripetizione.

5.3.5 Attacchi basati sul protocollo SS7

Il protocollo SS7, sebbene originariamente progettato per 2G e 3G, continua a rappresentare una minaccia a causa del roaming tra paesi collegati a reti legacy. Gli attacchi possibili includono SPAM, spoofing, tracciamento della posizione, frodi, intercettazioni e attacchi DoS. Sebbene l'attenzione si sia concentrata principalmente sugli attacchi di protocollo nel piano di controllo, è previsto che gli attacchi DDoS basati sui messaggi di protocollo nel piano utente diventino un problema significativo.

5.3.6 Attacchi nel piano utente

Nel piano utente, i potenziali attacchi sono classificabili in tre categorie principali:

- **Attacchi basati sul protocollo GTP-U:** Questo protocollo di tunneling opera collegandosi al GTP-C del piano di controllo. Gli attacchi tipici includono DoS che caricano l'equipaggiamento core 5G e possono sfruttare le vulnerabilità del protocollo per ottenere informazioni sulla rete e sugli abbonati.
- **Attacchi basati sul protocollo SIP:** Utilizzato per fornire servizi VoIP su LTE, gli attaccanti possono sfruttare il protocollo SIP per eseguire attacchi DoS e di dirottamento delle chiamate attraverso messaggi come INVITE.

- **Attacchi basati su protocolli IoT:** Con l'aumento del traffico dati generato dai dispositivi IoT, sono previsti vari tipi di attacchi DDoS, mirati all'infrastruttura della rete 5G, ai server di applicazione e ai dispositivi connessi. Gli attacchi possono esaurire le risorse dell'infrastruttura, causando interruzioni su larga scala.

Network Domain 5G NSA Components 5G SA Components			UE Devices	Access Network eNb gNb	 - UPF(MEC)	Core Network SGW AMF	 MME AMF(SMF)	 PCRF PCF	 HSS AUSF	 IMS AF	 PGW UPF	External Network ISP, Roaming Vertical Service
Control Plane	RRC	DoS		O								
		Spoofing	O	O								
		Location Tracking	O	O								
		Routing Attack	O	O								
	NAS	DoS	O	O			O					
		Spoofing	O				O					
		SPAM	O				O					
	GTP-C	DoS				O	O	O			O	
		Fraud				O	O	O			O	
		Routing Attack		ü		O	O	O			O	
	Diameter	DoS						O	O		O	O
		Routing Attack						O	O		O	O
		Information Disclosure						O	O		O	O
		Fraud						O	O		O	O
	SS7	DoS							O		O	O
		Faud							O		O	O
		Location Tracking						O	O		O	O
User Plane	GTP-U	DoS(GTP-in-GTP)				O	O	O	O			
		Fraud				O	O	O	O			
		Sniffing				O	O	O	O			
	Voice over 5G	SIP Signaling DoS	O		O					O		O
		SIP Replay Attack	O		O					O		O
		Location Tracking	O		O					O		O
	IoT over 5G	IoT Aplication DDoS	O	O	O					O		O
		IP based attack	O	O	O					O		O

Figure 1: Classification of 5G Threat based network protocol
Source: 5G core network security issues and attack classification from network protocol perspective, 2020

6 Conclusions

Ecco una versione migliorata del tuo testo:

La tecnologia 5G rappresenta una delle ultime frontiere nel campo delle comunicazioni senza fili. Essa ha il potenziale di rivoluzionare molte attività umane e il nostro modo di concepire le comunicazioni moderne, grazie a elevate velocità di trasmissione, bassa latenza e un alto throughput. Tuttavia, con l'avanzamento della tecnologia mobile, si sviluppano anche nuove minacce che possono compromettere la sicurezza di queste reti.

In questo articolo, vengono analizzate le principali vulnerabilità associate al 5G. Molte di queste vulnerabilità sono ereditate dal 4G, mentre altre sono completamente nuove. La ricerca sulla sicurezza e l'identificazione di soluzioni

innovative rappresentano un compito cruciale per tutti gli attori coinvolti, dai fornitori di servizi di rete a coloro che definiscono i protocolli di comunicazione. Questo diventa particolarmente necessario, considerando che il 5G è sempre più fondamentale per settori della vita quotidiana che possono diventare estremamente delicati se non gestiti correttamente, come la telemedicina e i veicoli a guida autonoma.

A Termini da ricordare

- **Banda Larga Mobile**: La caratteristica principale della banda larga mobile è la possibilità di fornire accesso a Internet in modalità wireless, senza essere limitati a una connessione fissa, come quella via cavo o fibra ottica.

- **Massive MIMO**: I sistemi wireless Multiple Input Multiple Output sfruttano più antenne di trasmissione e ricezione per aumentare la capacità di rete, migliorando il throughput dei dati e servendo un maggior numero di utenti. MIMO suddivide il segnale in sottosegnali a bassa velocità, trasmessi su antenne spazialmente separate sullo stesso canale di frequenza. Grazie alla propagazione su percorsi multipli, il ricevitore separa i segnali in flussi paralleli per recuperare il segnale originale. MIMO aumenta la capacità del canale senza consumare ulteriore larghezza di banda o potenza e la velocità può crescere aggiungendo più antenne. Nel 5G, la tecnologia Massive MIMO va oltre la configurazione 2×2 del 4G, utilizzando numerosi flussi simultanei per aumentare la capacità di rete e l'efficienza spettrale. L'array di antenne più grande permette un'elaborazione coerente del segnale, adattandosi velocemente ai cambiamenti del canale di propagazione [6].

- **mmWave**: Le comunicazioni ad onde millimetriche si rifereiscono all'uso di onde elettromagnetiche molto elevate, tipicamente comprese tra *30 GHz e 300GHz*. Questo onde sono chiamate millimetriche perchè la loro lunghezza d'nda varia tra 1mm e 30mm, che sono molto più corte rispetto alle ond radio tradizionalmente usate. Esse permetono velocità molto elevate e basssa latenza, ma hanno una portata limitata e scarsa capacità di penetrazione, richiedendo infrastrutture dense come small cells e tecnologie avanzate come il beamforming. Utilizzate insieme a frequenze più basse per garantire una copertura completa, le mmWave sono cruciali per migliorare la capacità delle reti in aree ad alta densità di utenti.

- **EAP-AKA**: è un protocollo di autenticazione progettato per consentire l'autenticazione sicura tra un dispositivo mobile e una rete, basato sul concetto di chiavi simmetriche. Quando un dispositivo, desidera connettersi a una rete, invia una richiesta di autenticazione utilizzando un `SUCI`, una versione cifrata del suo identificatore permanente, il `SUPI`, consentendo alla rete di identificare il dispositivo senza rivelare l'identità reale

dell'utente e garantendo la sua privacy. La rete, ricevuta la richiesta, utilizza il SUCI per accedere alle credenziali memorizzate nel database dell'ARPF, dove è custodita la chiave segreta K, condivisa tra il dispositivo e la rete; se viene scelto il protocollo EAP-AKA, la rete avvia il processo di autenticazione generando una sfida per il dispositivo composta da tre elementi: un numero casuale (RAND), un messaggio di autenticazione (AUTN) e la risposta attesa (XRES), che vengono inviati al dispositivo. Questo verifica il valore AUTN utilizzando la chiave K nella sua USIM, e, se l'AUTN è valido, calcola una risposta (RES) basata su RAND e la chiave K, quindi la invia alla rete, che confronta la RES ricevuta con la XRES generata in precedenza; se corrispondono, l'autenticazione ha successo e entrambe le parti hanno verificato l'identità reciproca. Successivamente, si genera la chiave di sessione, derivata dalla chiave K e dai materiali generati nella sfida, con chiavi come CK (per la cifratura dei dati) e IK (per l'integrità dei messaggi), essenziali per proteggere le comunicazioni. Una volta completato il processo di autenticazione e derivate le chiavi di sessione, il dispositivo e la rete possono iniziare a scambiare dati in modo sicuro, sapendo che le comunicazioni sono protette da solide misure di sicurezza.

- **5G AKA**: Il processo 5G AKA inizia con l'invio, da parte del dispositivo, di una richiesta di autenticazione alla rete tramite il SUCI, una versione cifrata del SUPI, che protegge l'identità dell'utente durante la registrazione. La rete riceve questa richiesta e la invia al database delle credenziali, che contiene la chiave segreta K condivisa tra il dispositivo e la rete. Se viene scelto il protocollo 5G AKA, la rete genera una sfida composta da un numero casuale (RAND), un'autenticazione temporanea (AUTN) e una risposta attesa (XRES), che vengono inviati al dispositivo. Il dispositivo, usando la chiave K memorizzata nella USIM, verifica l'AUTN per confermare l'identità della rete; se la verifica è valida, calcola una risposta (RES) basata su RAND e K, che viene poi inviata alla rete. La rete confronta la RES con la XRES generata in precedenza, e se corrispondono, l'autenticazione ha successo. A questo punto, vengono generate le chiavi di sessione per la cifratura e l'integrità delle comunicazioni, garantendo la sicurezza dei dati trasmessi. Una caratteristica importante del 5G AKA è il rafforzamento della privacy dell'utente, grazie alla separazione delle chiavi di cifratura e integrità e a meccanismi più robusti per prevenire attacchi di tracciamento e correlazione delle identità, migliorando significativamente la sicurezza rispetto alle generazioni precedenti.

- **FBMC**: Il Filter Bank Multicarrier (FBMC) è una tecnica di modulazione che divide un segnale in più sottocanali, applicando filtri per ridurre le interferenze tra questi, migliorando così l'efficienza spettrale rispetto all'OFDM.

- **FullDuplex**:Il full duplex è una modalità di comunicazione in cui i dati possono essere trasmessi e ricevuti contemporaneamente tra due dispositivi o punti. In altre parole, entrambe le parti possono inviare e ricevere

informazioni allo stesso tempo, senza dover aspettare che una delle due abbia finito di trasmettere.

- **Ultra Dense Networking**:L'Ultra Dense Networking (UDN) è una architettura di rete progettata per migliorare la capacità e la copertura della rete in ambienti ad alta densità di utenti o dispositivi.DN si basa sull'idea di aumentare il numero di celle o piccole stazioni base (small cells) in un'area geografica, riducendo la distanza tra queste stazioni e i dispositivi connessi. Questo riduce il carico su ogni singola stazione base, migliorando la capacità di banda e la qualità del segnale.

- **Software-Defined Networking**: Software-Defined Networking (SDN) è un approccio alla gestione delle reti che separa il piano di controllo (control plane) dal piano dati (data plane). Tradizionalmente, i router e gli switch svolgono sia il compito di instradare il traffico (piano dati) che di decidere come farlo (piano di controllo). SDN sposta il piano di controllo in un'entità software centrale chiamata `controller`, che ha una visione globale della rete e può programmare dinamicamente come i pacchetti devono essere gestiti dagli switch, semplificando la gestione della rete e migliorandone l'agilità.

- **Network Function Virtualization**: La Network Function Virtualization (NFV) è una tecnologia che virtualizza le funzioni di rete, come firewall, router, load balancer e altri dispositivi di rete, su server standard, eliminando la necessità di hardware specializzato. NFV consente di distribuire e gestire le funzioni di rete come software, migliorando la scalabilità, la velocità di implementazione e riducendo i costi.

- **S-TMSI**: è un identificatore temporaneo utilizzato nelle reti 4G LTE e 5G per rappresentare un abbonato senza rivelarne l'IMSI (International Mobile Subscriber Identity). Esso viene generato dalla rete e cambia periodicamente, riducendo il rischio di tracciamento e attacchi informatici.

- **RRC**: RRC è un protocollo fondamentale nel piano di controllo delle reti mobili ed è responsabile della gesione delle connessioni radio tra l'utente e la rete. Le principali funzioni del protocllo RRC includono: l'instaurazione e il rilascio della connesione radio, la gestione della mobilità, il controllo qalità e la trasmissione di informazioni di confgurazione e segnalazione.

- **eNB**: Rappresenta il nodo di accesso radio delle reti `4G LTE`. eNB è responsabile della trasmissione e ricezione dei segnali radio tra l'utente finale e la rete core `LTE` e ha funzioni di gestione delle risorse radio, codifica e decodifica, controllo di potenza, gestione della mobilità e dellos cheduling dei dati.

- **gNB**: Il next generation Node B è l'elemento della rete di accesso radio nella tecnologia 5G. Oltre a supportare i tradizionali servizi a banda larga,

il gNodeB consente funzionalità avanzatate come le comunicazioni massive per dispositive IoT e La gestione del traffico con qualità del servizio variabile in base alle esigenze dell'applicazione.

- **IMSI**: International Mobile Subscriber Identity è un numero identificativo univoco, composto da 15 cifre associato a ciascun abbonato nella rete mobili. Questo numero è utilizzato per identificare e autenticare un utente all'interno di una rete mobile. `IMSI` è memorizzato nella scheda SIM e include il codice del paese `(MCC)`, il codice dell'operatore `(MNC)` e un numero identificativo dell'abbbonato `(MSIN)`.

- **RTP**: Il Real-time Transport Protocol (RTP) è un protocollo di rete utilizzato per la trasmissione di dati in tempo reale, come voce e video, su reti IP.

- **NAS**: Gestisce la comunicazione tra il dispositivo dell'utente e il core network, occupandosi di autenticazione e registrazione, assicurando che solo i dispositivi autorizzati accedano alla rete. Inoltre, si occupa della mobilità, consentendo agli utenti di passare da una cella all'altra senza interruzioni. Gestisce anche le sessioni di dati, stabilendo e terminando le connessioni e mantenendo la qualità del servizio.

- **MME**: L'Mobility Management Entity (MME) è un componente software nel core network delle reti mobili 4G e 5G, responsabile della gestione della mobilità degli utenti e della segnalazione. Svolge funzioni chiave come l'autenticazione degli utenti, la gestione delle sessioni, il monitoraggio della posizione e l'instradamento delle richieste di servizio verso altre entità di rete. L'MME comunica con dispositivi terminali e altri elementi della rete utilizzando protocolli come NAS (Non Access Stratum) e GTP (GPRS Tunneling Protocol).

References

[1] Ijaz Ahmad et al. "Security for 5G and Beyond". In: *IEEE Communications Surveys & Tutorials* 21 (2019), pp. 3682–3722. DOI: 10.1109/COMST.2019.2916180.

[2] Ramraj Dangi et al. "Study and investigation on 5G technology: A systematic review". In: *Sensors* 22.1 (2021).

[3] Iqra Javid and Sibaram Khara. "5G Network: Architecture, Protocols, Challenges and Opportunities". In: *2022 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*. IEEE. 2022, pp. 1–5.

[4] Xinsheng Ji et al. "Overview of 5G security technology". In: *Science China Information Sciences* 61 (2018). DOI: 10.1007/s11432-017-9426-4.

[5] Roger Piqueras Jover and V. Marojevic. "Security and Protocol Exploit Analysis of the 5G Specifications". In: *IEEE Access* 7 (2018), pp. 24956–24963. DOI: 10.1109/ACCESS.2019.2899254.

[6] Akash R. Kathavate et al. "Critical Aspects of 5G Technology- A Study on the Drivers, Technology Enhancement, Performance, and Spectrum Usage". In: *Asian Journal of Advanced Research and Reports* (2021). DOI: 10.9734/ajarr/2021/v15i530396.

[7] Hwankuk Kim. "5G core network security issues and attack classification from network protocol perspective". In: *J. Internet Serv. Inf. Secur.* 10 (2020), pp. 1–15. DOI: 10.22667/JISIS.2020.05.31.001.

[8] Jaya Preethi Mohan, Niroop Sugunaraj, and Prakash Ranganathan. "Cyber security threats for 5G networks". In: *2022 IEEE international conference on electro information technology (eIT)*. IEEE. 2022, pp. 446–454.

[9] Seongmin Park et al. "5G Security Threat Assessment in Real Networks". In: *Sensors (Basel, Switzerland)* 21 (2021). DOI: 10.3390/s21165524.