Università degli Studi di Padova

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

Università degli Studi di Padova

Dipartimento di Ingegneria dell'Informazione

Corso di Laurea in Ingegneria Informatica

Network Slicing nelle reti 5G: vulnerabilità e soluzioni per la mitigazione

Relatore:
Prof. Mauro Migliardi

Laureando:
Matteo Salvalaio
1216361

Anno Accademico 2021/2022
Data di laurea 21 settembre 2022

Abstract

Con l'avvento della quinta generazione di comunicazione mobile (5G) la necessità di mettere in sicurezza le nuove tecnologie da attacchi informatici, sempre più frequenti, è un requisito di primaria importanza. Una delle nuove tecnologie sviluppate è lo slicing della rete che permette di garantire un supporto a numerosi dispositivi diversificati gestendo reti composte da differenti apparecchiature utente. L'obiettivo di questa tesi è di mettere in luce le criticità sulla sicurezza presenti nella tecnologia del Network Slicing e indagare possibili soluzioni per prevenire il rischio di attacchi esterni. Vengono brevemente descritte le caratteristiche della rete 5G Core ed i suoi obiettivi, le differenze che sono state apportate rispetto alle versioni precedenti, e i benefici che hanno portato allo sviluppo di questa tecnologia. Successivamente sono riepilogate le sfide della sicurezza classificate in base ai dispositivi in cui l'attacco può arrivare durante la vita di una slice. In conclusione sono esposte possibili soluzioni atte a ridurre o eliminare i rischi di attacchi esterni per garantire una maggiore sicurezza dei dati.

Indice

Elenco delle figure

Elenco delle Abbreviazioni

3GPP	3rd Generation Partnership Project
5G AKA	Authentication and Key Agreement of the 4G Evolved Packet System
AF	Application Function
API	Application Programming Interface
BBU	Baseband Unit
C-RAN	Centralized-RAN
CP	Control Plane
D-RAN	Distributed-RAN
DoS	Denial of Service
EPC	Evolved Packet Core, 4G Core
gNB	New Base Radio Station
KDF	Key Derivation Function
MNO	Mobile Network Operators
NF	Funzioni Network
NFV-MANO	Network Functions Virtualization MANagement and Orchestration
NFVI	Network Functions Virtualization Infrastructure
NG-C	Next Generation Core, 5G Core
NR	New Radio
NSI	Network Slice Instance
NSM	Network Slice Manager
QoS	Quality of Service
RAN	Radio Access Network
RRU	Remote Radio Unit
SDN	Software-Defined Networking
UE	User Equipment
UP	User Plane
UPF	User Plane Function

Capitolo 1

Introduzione

La tecnologia 5G rappresenta, attualmente, l'ultima generazione di tecnologie di telefonia mobile e cellulare definita dagli standard del 3GPP. Nel corso dell'ultimo decennio questa nuova tecnologia è stata ideata, sviluppata e migliorata e negli ultimi anni sta iniziando a essere distribuita in tutto il mondo. Progettato per incrementare la velocità, ridurre la latenza e migliorare la flessibilità dei servizi wireless, la tecnologia 5G presenta numerose innovazioni nell'ambito delle comunicazioni e dei servizi di rete. Tuttavia architetture e strutture nuove introducono un aumento delle sfide nell'ambito della sicurezza.

1.1 Obiettivo della tesi

Lo slicing della rete rappresenta una delle novità principali introdotte dalle reti 5G. L'obiettivo di questo documento è presentare ed esaminare i rischi nella tecnologia del Network Slicing ed evidenziare sistemi e meccanismi per mitigare il rischio di attacchi alla sicurezza. Il documento è strutturato in modo da fornire al lettore le competenze necessarie a comprendere la struttura del nuovo sistema di rete mobile descrivendone brevemente l'architettura e gli obiettivi principali. Successivamente sono illustrati i punti di attacco principali che utenti malintenzionati possono sfruttare per violare la sicurezza dei Network Slicing. Infine verranno presentate le soluzioni principali proposte per mitigare tali tipi di attacchi soffermandosi particolarmente sull'isolamento e sul sistema di gestione e coordinazione della sicurezza.

Capitolo 2

Architettura della Rete 5GC

La funzione principale di un Mobile Core è quella di fornire Internet ai dispositivi mobili, garantendone al contempo l'autenticazione. Lo standard 3GPP definisce l'architettura per una rete 5G Core come un insieme di NFs interconnesse, con autorizzazione ad accedere reciprocamente ai propri servizi.
Una caratteristica chiave del Mobile Core è la gestione della mobilità di tutti gli utenti tenendo traccia della loro ultima posizione con la granularità della stazione base di servizio. Il tenere traccia dei singoli utenti nel Mobile Core, cosa non effettuata dall'Internet Core, rende molto complessa la sua architettura.

Sebbene la funzionalità aggregata rimanga sostanzialmente la stessa durante la migrazione dal 4G al 5G, cambia il sistema in cui tale funzionalità viene virtualizzata e presa in considerazione nei singoli componenti. Gli elementi EPC sono stati progettati per essere implementati su nodi fisici virtualizzati, ma non sono stati progettati per essere virtualizzati fin dall'inizio. Il 5G Mobile Core è fortemente influenzato dalla transizione del cloud verso un'architettura cloud native, ovvero basata su microservizi. Si presenta quindi la necessità, per realizzarne appieno il potenziale, di passare a un open software basato su piattaforme cloud. Il core 5G è stato quindi progettato per tre miglioramenti:

- Divisione del piano utente (UP) e del piano di controllo (CP)
- Supporto nativo per Network Slicing per i casi d'uso 5G
- Architettura basata sui servizi forniti come un insieme di NF

2.1 Control and User Plane Separation (CUPS)

La separazione tra il CP e l'UP per l'architettura 4G fu introdotta con la Release 14 del 3GPP nel 2016, la quale ha separato le vie di accesso dei pacchetti consentendo un'implementazione più flessibile e una scalabilità indipendente.

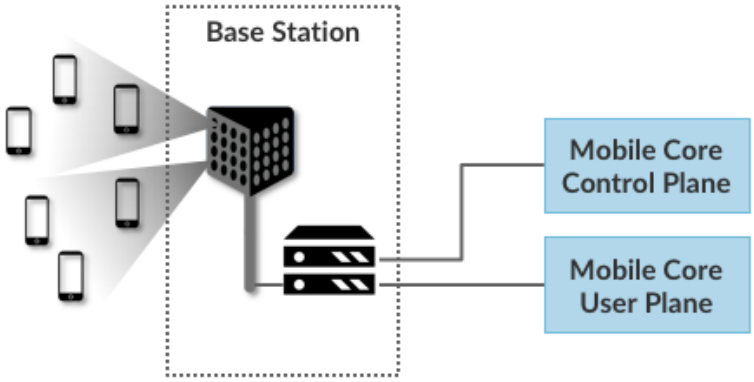

Figura 2.1: Divisione del Mobile Core tra Control Plane e User Plane

Nel passaggio alla rete 5G sono state rinominate, divise o aggregate le entità della rete principale a seconda delle loro funzioni nella nuova architettura. Le tre strutture principali sono la nuova tecnologia di accesso gNB, Il Control Plane e lo User Plane.

2.1.1 Next generation NB (gNB)

La nuova tecnologia di accesso radio è stata nominata New Radio e sostituisce il vecchio LTE, mentre la New Base Radio Station è chiamata NB di nuova generazione. Il gNB gestisce le comunicazioni radio con le apparecchiature utente compatibili con il 5G utilizzando l'interfaccia 5G New Radio.

La stazione base è composta da due parti principali: il Baseband Unit e il Remote Radio Unit. La RRU recupera il segnale e la frequenza radio dall'antenna e trasmette la frequenza radio alla BBU che la elabora digitalmente. La combinazione di entrambe le unità della cella è chiamata architettura Distributed-RAN. La RAN è costituita da un gruppo di stazioni base disposte in modo da formare una rete cellulare. La RAN trasmette il traffico tra i dispositivi e la rete gestendo lo spettro radio, assicurandosi che venga utilizzato in modo efficiente e soddisfi i requisiti di QoS di ogni utente. In un'architettura D-RAN, l'intera stazione base si trova contenuta nella gNB con la RRU e la BBU direttamente collegate tra loro.

La D-RAN presenta diversi problemi di gestione dello spazio e della capacità, entrambi necessari alle stazioni base durante gli orari di picco, siccome le RRU e le BBU non sono state progettate per questo tipo di flessibilità. Nell'architettura Centralized-RAN,

invece, le BBU sono state delocalizzate dalla stazione base con un controllo centralizzato per elaborare i calcoli digitalmente. Aggregando tutte le BBU in un ufficio centrale possono essere organizzate al meglio le risorse tramite l'isolamento logico e la condivisione dinamica delle risorse fisiche.

Figura 2.2: Architettura di un D-RAN e un C-RAN

La centralizzazione delle BBU comporta inoltre una migliore implementazione dei servizi edge e la possibilità di utilizzare tecnologie avanzate che richiedono un'elevata potenza di elaborazione. Per la rete di accesso radio 5G sono previste architetture sia centralizzate (C-RAN) che distribuite (D-RAN).

Si definisce fronthaul il collegamento di rete ottica tra più RRU e BBU, mentre il backhaul è un ponte tra gli elementi RAN e la rete mobile, responsabile della trasmissione dei dati. Nelle reti di comunicazione 5G sono coinvolti diversi parametri, che hanno tutti un impatto sulle prestazioni della rete. La collaborazione tra la RAN e il backhaul apre nuove possibilità per migliorare le prestazioni.

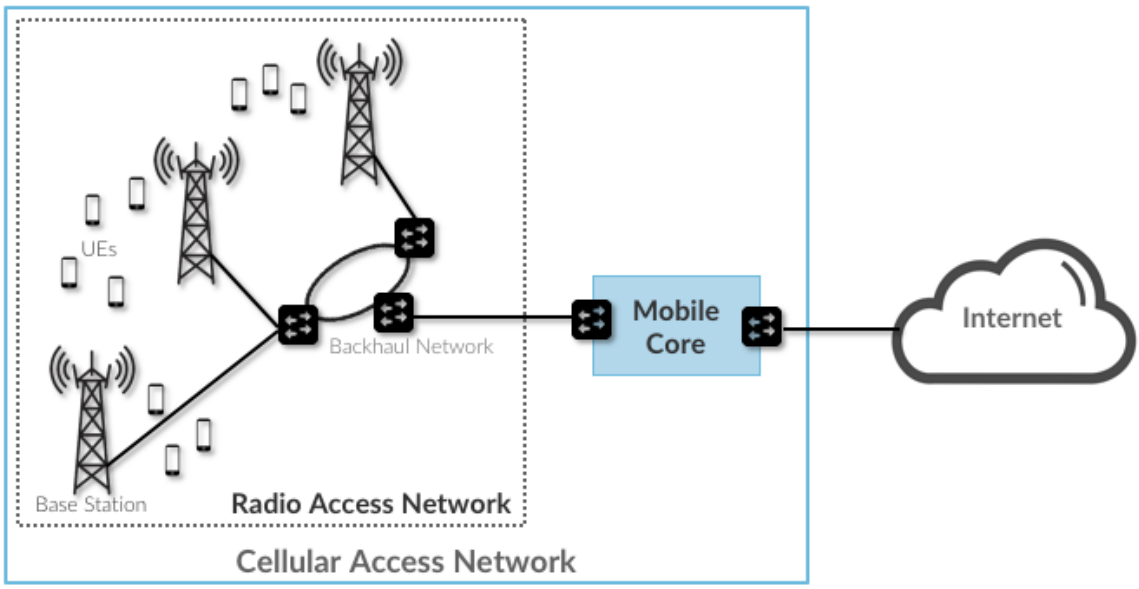

Figura 2.3: Struttura di accesso radio (RAN) e Mobile Core

2.1.2 Control Plane (CP)

Il Control Plane è formato da un insieme di blocchi funzionali. I seguenti blocchi vengono eseguiti nel Control Plane e hanno una controparte nell'EPC.

- AMF (Core Access and Mobility Management Function): responsabile della gestione della connessione e della raggiungibilità, dell'autenticazione e dell'autorizzazione dell'accesso e dei servizi di localizzazione.
- SMF (Session Management Function): gestisce ogni sessione UE, inclusa l'allocazione dell'indirizzo IP, la selezione della funzione UP associata, gli aspetti di controllo della QoS e dell'instradamento UP.
- PCF (Policy Control Function): gestisce le regole dei criteri che altre funzioni del Control Plane applicano.
- UDM (Unified Data Management): gestisce l'identità dell'utente, inclusa la generazione delle credenziali di autenticazione.
- AUSF (Authentication Server Function): corrisponde essenzialmente a un server di autenticazione

I blocchi successivi invece non possiedono una controparte nel EPC.

- SDSF (Structured Data Storage Network Function): un servizio "helper" utilizzato per archiviare dati strutturati. dell'autorizzazione dell'accesso e dei servizi di localizzazione.
- UDSF (Unstructured Data Storage Network Function): un servizio "helper" utilizzato per archiviare dati non strutturati.
- NEF (Network Exposure Function): un mezzo per esporre capacità selezionate a servizi di terze parti, inclusa la traduzione tra rappresentazioni interne ed esterne per i dati.
- NRF (NF Repository Function): un servizio per scoprire i servizi disponibili.
- NSSF (Network Slicing Selector Function): un sistema per selezionare una Network Slice per servire un dato UE.

2.1.3 User Plane (CP)

La funzione del piano utente è costituita da una singola entità UPF che combina le funzionalità dei precedenti gateway di servizio. L'UPF è responsabile dell'instradamento, dell'inoltro dei pacchetti e della QoS.

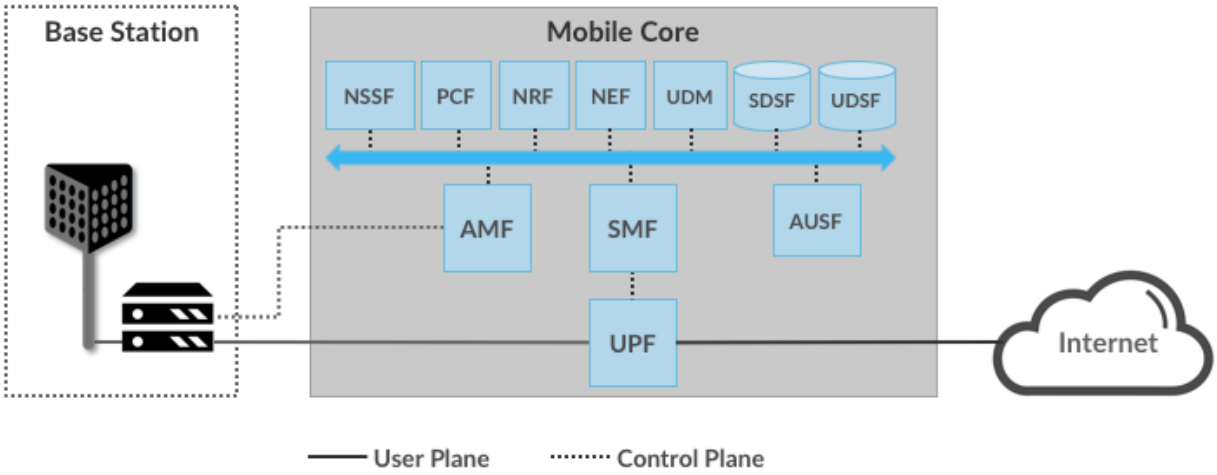

Figura 2.4: 5G Mobile Core (NG-Core)

Applicazioni di terze parti possono essere integrate nel 5G Core tramite l'AF, come l'edge computing e l'IMS Core. Ad oggi, l'IMS Core, necessario per le chiamate vocali e video in tempo reale, è separato dal 5G Core SBA.

Le applicazioni di terze parti integrate nel 5G Core tramite l'AF si basano sulla Network Exposure Function per esporre tutte le altre funzioni di rete, facilitando l'app di terze parti.

2.2 5G Core Service-Based Architecture (SBA)

L'architettura basata sui servizi per le reti 5G principali è definita nella specifica tecnica 3GPP 23.501. Essa utilizza interfacce basate sui servizi tra le funzioni del CP, mentre le funzioni dell'UP si connettono tramite collegamenti point-to-point.

E' un approccio architetturale che consente alle funzionalità di rete 5G di diventare più granulari e disaccoppiate. Ciò consente ai singoli servizi di essere aggiornati in modo indipendente con un impatto minimo su altri servizi

2.3 Network Slicing nelle reti 5G

La rete 5G è orientata al supporto di molteplici modalità d'uso e applicazioni. Per questo i Network Slicing forniscono un modo per partizionare le risorse di rete al fine di differenziare il servizio fornito a utenti diversi.

Il Network Slicing può essere definito come una configurazione di rete che consente di creare più reti virtualizzate e indipendenti su un'infrastruttura fisica comune, e rappresenta una capacità importante per dare efficienza all'utilizzo delle risorse di rete, flessibilità di implementazione e supporto per applicazioni e servizi over the top in rapida crescita. Un Network Slicing funzionante dovrebbe essere in grado di controllare i propri pacchetti dall'inoltro degli UE ai server cloud nella rete centrale senza intaccare le altre slice.

Il 3GPP considera il Network Slicing come una delle caratteristiche chiave del 5G. Un Network Slicing può essere verticale, orizzontale, statico o dinamico. In caso di Network Slicing verticale, una rete viene suddivisa in più slice di rete, ciascuna progettata e ottimizzata per servizi o applicazioni. Lo slicing orizzontale della rete, invece, consente la condivisione delle risorse tra nodi e dispositivi di rete. Entrambi gli approcci possono essere implementati contemporaneamente e possono lavorare insieme. Lo slice verticale si concentra su un mercato di massa, mentre lo slice orizzontale serve per casi di usi specifici. Lo slicing statico può seguire una struttura verticale o orizzontale per servire dispositivi fissi o applicazioni di tipo IoT, mentro lo slice dinamico rimane per la maggior parte l'approccio prominente per le reti di nuova generazione che incoraggia l'emergere delle slice come servizi.

Ogni slice di rete si configura come una rete logica end-to-end isolata ed indipendente. Essa contiene risorse dedicate e condivise, in modo da adattarsi differentemente in base ai requisiti richiesti da una particolare applicazione. Le slice possono estendersi su più parti della rete: sia nella RAN decidendo quali segmenti trasmettere che nel Mobile Core ridimensionando le istanze di microservizi e posizionando tali istanze su server disponibili. Le applicazioni abilitate o potenziate dal 5G necessitano di una maggiore

larghezza di banda, più connessioni e una latenza inferiore rispetto a quanto era possibile con le generazioni precedenti. Ogni modalità d'uso avrà i propri requisiti di prestazioni unici, rendendo obsoleto l'approccio universale alla fornitura del servizio.

Un Core Network Slice è costituito da un gruppo di NFs che sono richieste per i servizi dello slice. Queste NFs possono essere riservate esclusivamente ad una o essere condivise tra più slice e possono essere fisiche o virtualizzate. Un nodo fisico può ospitare più NFs, a seconda della capacità e dei requisiti di sicurezza, e può fornire servizi a più slices. Il 3GPP specifica un insieme standard di sezioni di rete, chiamate valori SST (Standardized Slice Type) che sono così divisi:

Slice/Service type SST value	**SST value**
eMBB (enhanced Mobile Broadband)	1
URLLC (ultra- Reliable Low Latency Communications)	2
MIoT/mMTC (Massive IoT)	3

E' possibile definire una sezione separata per ciascun servizio eMBB, URLLC e mMTC sulla stessa infrastruttura.

- Il Massive Machine Type Communication (mMTC) tratta slices che servono un enorme numero di dispositivi IoT. È tipico che la quantità di dati trasmessi sia bassa o quasi inesistente, pertanto questo tipo di traffico non richiede un'elevata larghezza di banda. Dato il basso traffico un numero enorme di dispositivi possono essere localizzati nella stessa area.
- L'Enhanced Mobile Broadband (eMBB) mira a fornire un trasferimento di dati elevato il più rapidamente possibile. L'eMBB richiede quindi una larghezza di banda maggiore rispetto a URLLC e mMTC e pertanto il network radio ha un ruolo fondamentale. Frequenze di onde millimetriche (mmW) sono necessarie per fornire velocità fino a gigabit/secondo.
- L'Ultra-Reliable Low Latency Communications (URLLC) consente di fornire alta precisione alle applicazioni accompagnata da una bassissima latenza.

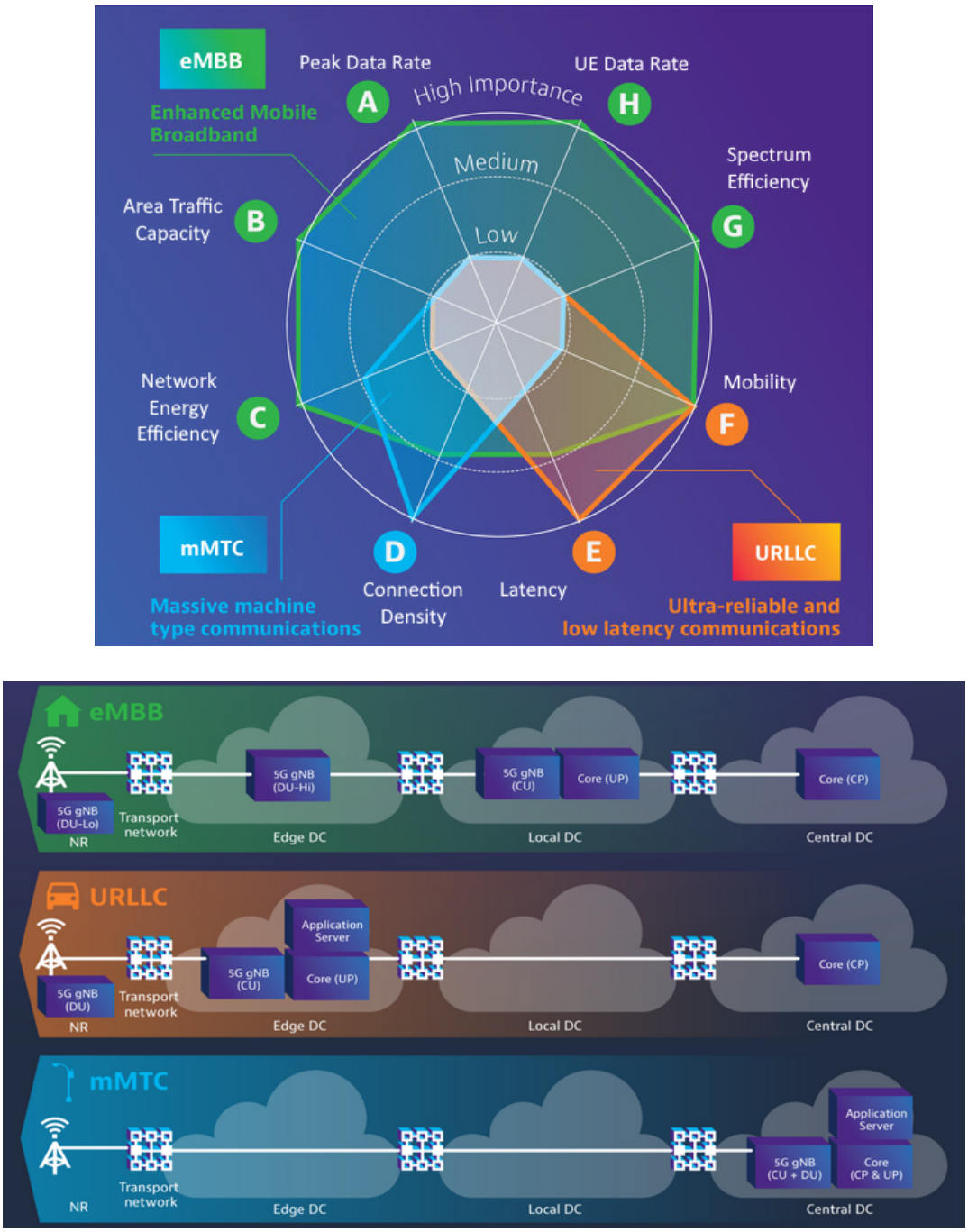

Figura 2.5: Casi d'uso e requisiti del Network Slicing

2.3.1 Architettura dei Network Slice

L'architettura del Network Slicing è composta da tre livelli, ciascuna con le proprie funzioni:

- Resource Layer: è costituito da risorse di rete e NF che servono a fornire servizi a un utente finale in base a una richiesta. Tali risorse e funzioni possono essere fisiche o virtuali.
- Network Slice Instance Layer: è costituito da più sezioni, in cui una delle quali fornisce le capacità di rete richieste dal servizio.

- Service Instance Layer: è costituito da istanze del servizio che consumano le sezioni e vengono offerte ai clienti. Solitamente un servizio può essere fornito da un operatore di rete o da terze parti, quindi l'istanza di servizio può essere costituita sia da servizi dell'operatore che da servizi di terze parti. Una NSI è un insieme di funzioni di rete virtualizzate implementate su risorse che consentono l'esecuzione di queste funzioni di rete. Un'istanza di una slice può essere isolata da un'altra istanza tramite isolamento completo o parziale e isolamento logico o fisico.

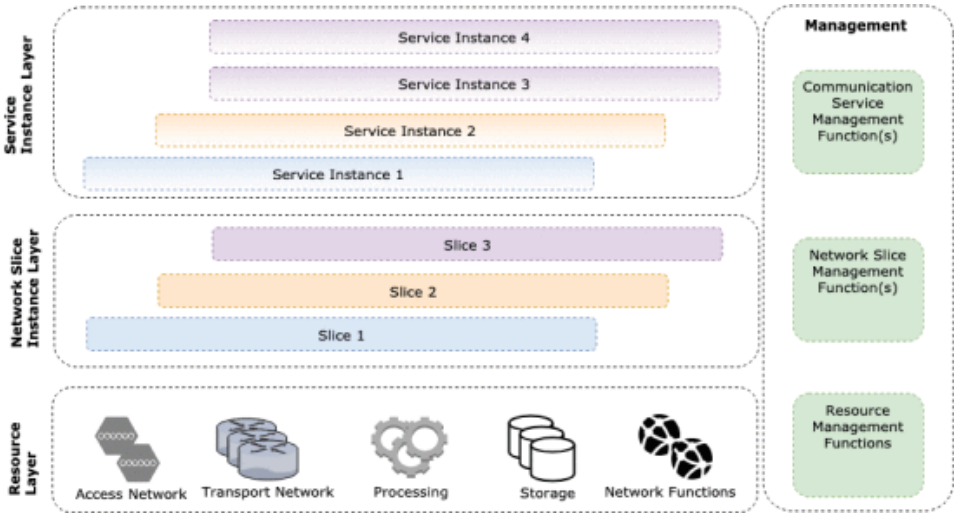

Figura 2.6: Architettura del Network Slicing

2.3.2 Sfide e Vantaggi del Network Slicing

Nonostante gli enormi vantaggi apportati dal Network Slicing restano numerose criticità da valutare e sistemare per operatori e sviluppatori.

Nei Network Slicing gli operatori possono allocare risorse a ciascuna slice, utilizzando la velocità, il throughput e la latenza necessari per coprire l'ampiezza dello slicing di rete in 5G, tuttavia l'aggiunta di più reti sulla stessa infrastruttura fisica può generare ulteriore stress. Tra le sfide più comuni figurano la difficoltà di mantenere la QoS e la garanzia di sicurezza per ogni singola sezione e gestire lo slicing e l'allocazione dello spettro per scenari altamente dinamici.

Pertanto, l'implementazione presenta due sfide chiave: l'isolamento e la gestione delle risorse. Senza un adeguato isolamento le sezioni potrebbero non essere in grado di funzionare adeguatamente, tuttavia se alle sezioni vengono assegnate risorse dedicate potrebbe portare a un approvvigionamento eccessivo di risorse e quindi alla riduzione dei vantaggi comportati dello slicing di rete. I meccanismi di gestione delle risorse sono necessari per trovare un equilibrio per l'implementazione di risorse dedicate e condivise. Inoltre attraverso l'intelligenza artificiale, il Network Slicing fornisce anche un'alternativa sicura ed efficiente per il test e l'implementazione di nuovi servizi. Con la rete divisa, non è

più necessario attuare modifiche che interrompano i servizi esistenti per valutarne di nuovi.

Lo slicing completo della rete end-to-end include l'implementazione nella rete di RAN, ma queste dovranno essere riprogettate per adattarsi allo slicing della rete. Infine sebbene Il Network Slicing sia un componente fondamentale del 5G, non è necessario il contrario. Il Network Slicing può essere comunque implementato su reti 4G / LTE esistenti.

Capitolo 3

Minacce nei Network Slicing

La sicurezza è una criticità fondamentale nelle reti, infatti molti ricercatori stanno lavorando sul miglioramento della sicurezza nella tecnologia 5G. La crescente digitalizzazione richiede infatti che le reti siano più efficienti, resilienti, ad alte prestazioni, sicure e semplici da usare. In termini di sicurezza, le principali minacce che deve affrontare un Network Slice includono principalmente attacchi DoS ed esaurimento delle risorse. Altre possibili minacce possono includere il monitoraggio, il traffic-injection e attacchi di impersonificazione.

I sistemi sottostanti dei network slice non sono sempre omogenei ed è molto probabile che provengano da fornitori diversi, introducendo una forte vulnerabilità dovuta alla mancanza di un livello di sicurezza comune, inoltre ogni slice ha requisiti di sicurezza unici commisurati al caso d'uso che è stata progettata per fornire e richiede l'autenticazione del proprio dispositivo per convalidare gli utenti. Un attacco riuscito da un punto di gestione della rete 5G centrale potrebbe infiltrarsi in molte slice e domini di rete contemporaneamente sfruttando l'anello debole tra le autenticazioni di numerose slice. Per affrontare efficacemente i problemi di sicurezza dello slicing della rete, le responsabilità tra gli operatori e le imprese che utilizzano gli slice dovrebbero essere chiaramente stabilite.

Accessi non autorizzati a un fornitore di servizi di terze parti possono creare vulnerabilità sulla sicurezza a servizi forniti da una Network Slice. Inoltre, gli aggressori possono gestire illegalmente slice o servizi in corso e lanciare attacchi a slice terminandole o compromettendone una funzione di rete critica. Quando parti malintenzionate richiedono continuamente nuove istanze, può verificarsi una congestione nel traffico del gestore creando attacchi DoS e Distributed DoS (DDoS). Gli aspetti chiave della sicurezza dei Network Slice possono essere categorizzati in quattro categorie: protezione, prevenzione, identificazione e gestione. Gli obiettivi della protezione derivano dalle preoccupazioni

Aspect	Subject	Objective
Protection	network infrastructure	network resilience and service availability
Prevention	unauthorized access and inappropriate use	cross-AD resource isolation and robustness to insider threat
Identification	security threats	establishing appropriate security control policies
Management	ADs, virtual environment visibility, subscribers of tenants	increased virtual environment visibility and reduced network risk

Figura 3.1: Categorie chiavi della sicurezza dei Network Slice

sull'infrastruttura di rete per supportare i servizi, dove bisogna verificare la sicurezza delle risorse statiche e dinamiche. Le risorse possono essere create in fase di esecuzione quando l'elasticità della rete è attivata dal traffico e dai servizi di rete e poiché queste risorse di runtime possono sovraccaricare la capacità della slice di rete, influiscono sulla disponibilità dei servizi di rete. Pertanto, bisogna tutelare la disponibilità della rete e l'affidabilità del servizio.

La prevenzione si occupa di tutelare la rete da accessi non autorizzati e l'uso inappropriato delle risorse dell'infrastruttura di rete. L'identificazione delle minacce alla sicurezza è in genere un'attività essenziale per gli MNO prima dell'implementazione della rete. Gli MNO stabiliscono politiche di controllo della sicurezza per la gestione della rete e criteri per la gestione della visibilità dell'ambiente virtuale tramite diverse tecnologie, come la micro segmentazione.

3.1 Rischi durante il ciclo di vita della Slice

Il ciclo di vita di un Network Slice è realizzato con il contributo di molteplici entità logiche e fisiche che possono essere svolte da una o più organizzazioni tra cui, il cliente, fornitori di servizi come il Communication Service Provider (CSP) e il MNO. I meccanismi di tutela della privacy e di protezione dei dati devono essere seguiti dal momento in cui il cliente avvia la richiesta per la creazione di una Network Slice. Durante la vita di una slice, l'interfaccia di interazione utilizzata per la sua gestione deve essere confidenziale e assicurare integrità e la riproduzione protetta dei dati. Ciò deve garantire che solo gli enti autorizzati possano creare, modificare ed eliminare le istanze della slice

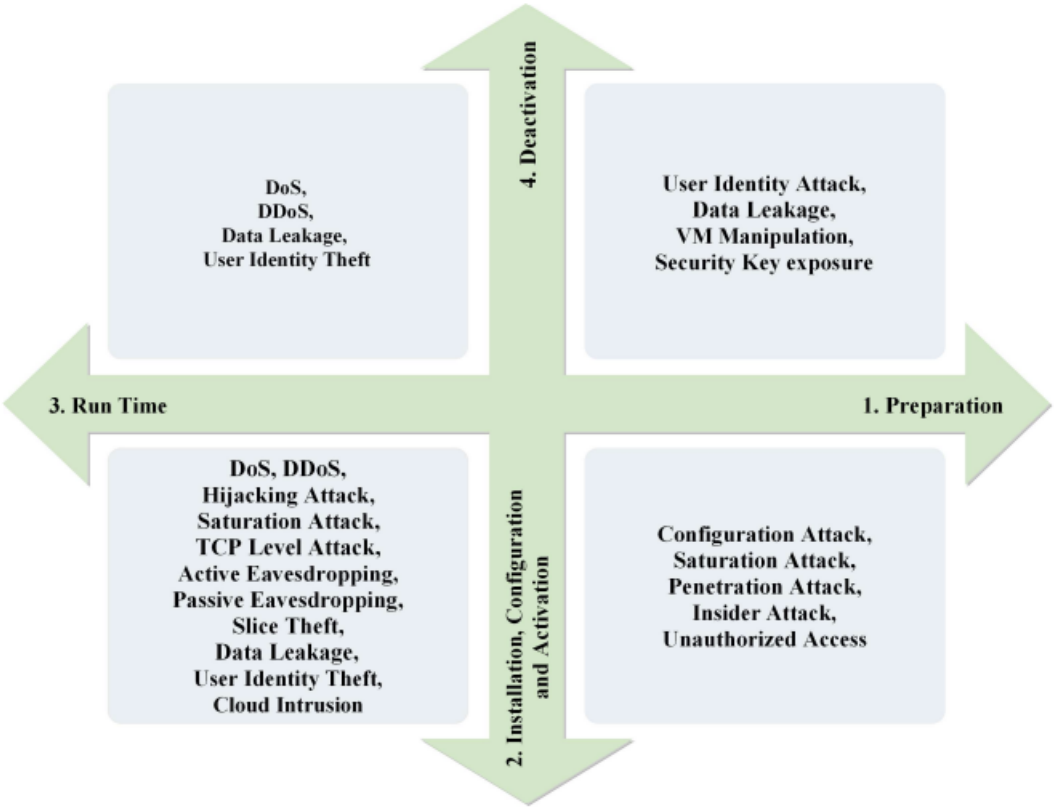

Figura 3.2: Ciclo di vita di una slice e rischi associati

1. **Fase di preparazione**
   La prima fase è dedicata alla preparazione, progettazione, creazione, e modifica della slice. Una slice è composta da un insieme di elementi e dalla loro configurazione. Eventuali errori nel template dello slice, modelli manomessi, mal progettati o implementati in modo errato possono causare attacchi che causano la perdita di dati degli utenti e accessi non autorizzati a canali non crittografati su tutte le sezioni create da esso. Misure come la crittografia e la decrittografia della slice template e l'utilizzo di real-time security possono prevenire tali attacchi. Inoltre la correttezza del slice template deve essere sempre verificata.

2. **Fase di installazione, configurazione e attivazione**
   La seconda fase comprende l'installazione delle slice alla rete, la configurazione dei servizi richiesti e l'attivazione delle slice. La minaccia principale in questa fase è la creazione di fake slices e la riconfigurazione delle slice durante o prima dell'attivazione. I bersagli di questi attacchi sono le API, che possono influenzare l'installazione e la configurazione e fornire errori di attivazione nelle slice. Meccanismi per proteggere le API come l'accesso controllato e la limitazione dei diritti operativi concessi, i quali impediscono ad utenti non autorizzati di accedere e modificare le strutture critiche delle API, e l'utilizzo di Transport Layer Security (TLS) che crittografa i dati o il protocollo di rete O-Auth per l'autenticazione garantiscono maggiore sicurezza nell'accesso. Inoltre, le API dovrebbero consentire l'auditing, il monitoraggio e il reporting in modo sicuro.

3. **Fase di esecuzione**
   Durante questa fase la sezione è in uso e consente gli aggiornamenti riguardanti i requisiti, i cambiamenti di configurazione, l'allocazione, la delocalizzazione delle risorse e funzioni di rete.
   Questa fase è esposta al più ampio numero di attacchi, che includono DoS, attacchi alle prestazioni, furto dei dati e violazioni della privacy. Inoltre, le minacce legate alla gestione, persistono anche in fase di esecuzione. L'API rimane un punto di attacco principale in questa fase, insieme ai servizi che usano la slice. L'autenticazione rimane un punto focale nel prevenire attacchi alla slice e misure come garantire l'integrità delle sezioni di rete per prevenire richieste false, isolamento delle sezioni per prevenire attacchi DDoS e simulazioni dei modelli delle strutture 5G per verificarne le vulnerabilità impediscono accessi non autorizzati e richieste dannose.

4. **Fase di disattivazione**
   In questa fase le risorse e le funzioni di rete vengono alleggerite dato che la slice non è più in uso. La principale minaccia durante e anche dopo la disattivazione delle slice consiste nell'esposizione di dati sensibili che erano stati gestiti in modo improprio durante la disattivazione e l'utilizzo delle risorse liberate in modo improprio per lanciare un attacco DoS. Tecniche di mitigazione includono la distruzione di dati sensibili e la deallocazione di funzioni e risorse di rete in modo che non rimangano occupate.

3.2 Punti di attacco di una Slice

I punti di attacco ad un Network Slice possono essere classificati tra punti che ignorano ogni relazione con altre slice, denominati Intra-Slice e punti che stanno in relazione ad altre slice detti Inter-Slice.

3.2.1 Punti di Attacco Intra-Slice

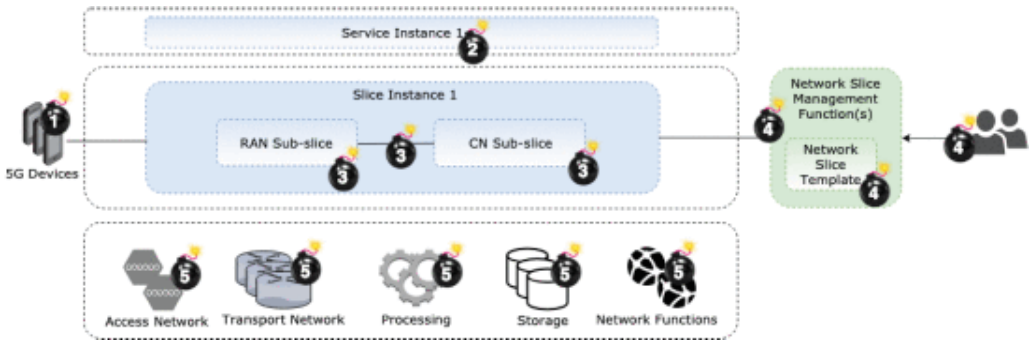

Figura 3.3: Punti di attacco intra-slice

1. **Dispositivi client 5G**
   I dispositivi client sono un punto di attacco per accessi non autorizzati a slice o servizi dando possibilità agli aggressori di consumare risorse e creare attacchi DoS. L'identificazione da parte della slice può diventare una vulnerabilità in correlazione agli identificatori permanenti dei dispositivi client, delimitando gruppi di interessi composti da utenti che utilizzano la stessa slice. Allo stesso modo, devono essere considerati i rischi per la sicurezza che emergono dagli accessi di emergenza i quali si sono rivelati un punto di accesso molto vulnerabile.
   È necessario prestare attenzione quando un dispositivo è associato a più sezioni contemporaneamente o dispositivi associati a sezioni sono in esecuzione su domini diversi. I rischi associati ai dispositivi dei clienti 5G aumentano quando accedono alla porzione di rete tramite reti che non rispettano gli standard 3GPP. Lo studio di un sistema di autenticazione avanzata e il controllo dell'accesso per i dispositivi client 5G, insieme all'isolamento nei dispositivi possono rivelarsi un buon meccanismo di prevenzione da accessi non autorizzati. Inoltre l'utilizzo di un'autenticazione secondaria, specifica per slice, permette una migliore sicurezza. L'autenticazione primaria deve essere standardizzata per consentire il roaming e l'interconnessione di diverse tecnologie e l'autenticazione secondaria dovrebbe essere comunque standardizzata, per ridurre i costi e facilitare l'integrazione. L'autenticazione secondaria deve essere controllata dall'ente che gestisce la slice.
   Infine le limitazioni al numero di dispositivi dei clienti che possono accedere contemporaneamente a una slice di rete, il numero di sessioni attive simultanee e la velocità di trasmissione dati per dispositivo, eseguite a diversi livelli nella rete, possono mitigare i rischi associati ad attacchi DoS.

2. **Interfaccia Servizi Slice**
   Un altro possibile punto di attacco è l'interfaccia tra la slice e i servizi che la usano. Gli aggressori possono quindi danneggiare la slice attaccando direttamente un servizio, causando inoltre ulteriori danni ad altri servizi in esecuzione sulla stessa sezione. Inoltre, nel caso di comunicazione diretta tra i servizi, questo può rivelarsi un ulteriore possibile punto di attacco. L'implementazione di livelli di sicurezza adeguati e configurazioni corrette dei servizi limitando servizi e risorse sono componenti importanti nel garantire la sicurezza. Deve inoltre essere implementato un corretto livello di isolamento tra i servizi e tra la slice dei servizi che consumano.

3. **Sub-Slice**
   Se lo slice è definito come una catena di numerose sub-slice, sia le sub-slice che l'interconnessione tra le sub-slice rappresentano facili punti di attacco. Il livello complessivo di sicurezza in una catena di sottosezioni è sempre dato dalla sottosezione più debole. Tecnologie di mitigazione degli attacchi possono comprendere l'isolamento delle sottosezioni e l'implementazione di meccanismi per ridurre i rischi all'interconnessione, soprattutto se la rete di accesso non segue gli standard 3GPP.

4. **Risorse e Funzioni di Rete**
   Come già discusso precedentemente le risorse e le funzioni di rete possono essere attaccate per danneggiare le slice che utilizzano. Anche in questo fattore l'autenticazione reciproca tra le slice gioca un ruolo fondamentale nel prevenire che un servizio con un sistema di autenticazione più debole finisca col danneggiare gli altri servizi posti sulla stessa slice. Inoltre l'avvio protetto, l'accesso alle credenziali, la sicurezza fisica, la verifica dell'integrità, ed evitare l'utilizzo del co-hosting per diversi livelli di sicurezza o sensibilità, in particolare tra slice che forniscono servizi sensibili e slice che utilizzano codice sperimentale o di test possono mitigare l'effetto o il rischio di attacchi.

3.2.2 Punti di Attacco Inter-Slice

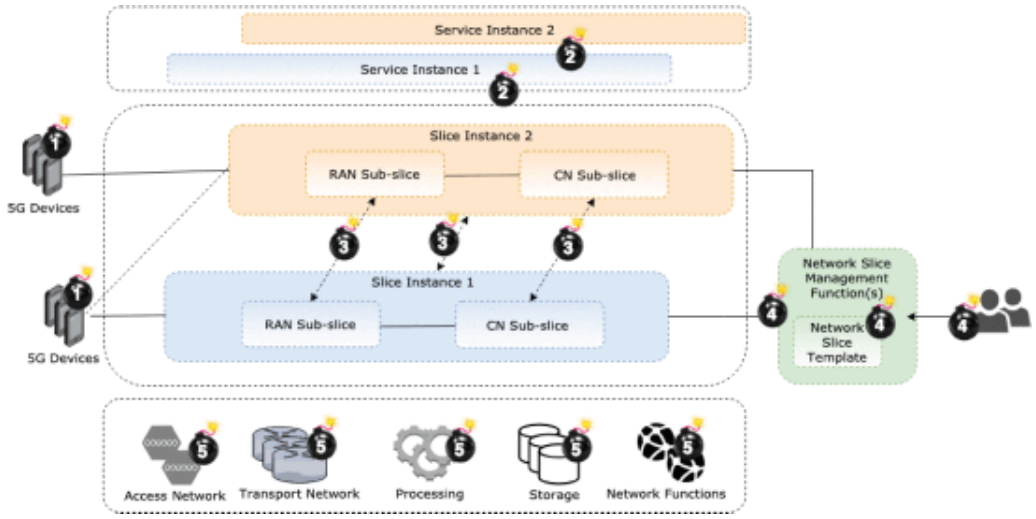

Figura 3.4: Punti di attacco inter-slice

1. **Dispositivi client 5G**
   I dispositivi client 5G che si trovano agli estremi della rete sono uno dei punti di attacco più vulnerabili, la possibilità di accesso a sezioni non autorizzate da parte del dispositivo corrisponde ad una elevata minaccia alla sicurezza. La differenza principale con lo scenario intra-slice è che il dispositivo non viene considerato estraneo e questo potrebbe essere considerato un vantaggio. Analogamente a quanto precedentemente discusso il rischio principale è causato dall'utilizzo di un accesso non autorizzato per danneggiare le prestazioni di una slice o causare un attacco DoS consumando eccessivamente le risorse condivise nella slice a cui è autorizzato ad accedere. Normalmente, un dispositivo dovrebbe essere autorizzato a collegarsi a una singola slice, tuttavia, se il dispositivo necessita di un accesso diversificato ai servizi, gli potrebbe essere consentito collegarsi a più slice contemporaneamente. In tal caso, esiste il rischio che il dispositivo perda dati sensibili dalla sezione più protetta alla sezione meno protetta. Il rischio aumenta sostanzialmente quando le

tecnologie di accesso tra le sezioni sono diverse tra loro. L'isolamento tra le slice rimane una fonte principale di sicurezza insieme al controllo dell'accesso, della riservatezza, dell'integrità, dell'autenticità e del consumo di risorse della slice.

2. **Comunicazione Servizio-Servizio**
   Un possibile punto di attacco è l'interfaccia tra i servizi che utilizzano slice diverse. Attaccando alcuni servizi, un avversario potrebbe riuscire a danneggiarne altri che si trovano su slice diverse. L'analisi del traffico e il rilevamento delle anomalie sono tecniche generali per indagare su comunicazioni non consentite tra i diversi servizi e componenti. Tecniche basate sull'acquisizione del traffico e su meccanismi di difesa che utilizzano l'intelligenza artificiale potrebbero essere utilizzate per proteggere da attacchi avanzati che aggirano i filtri di base.

3. **Comunicazione Intra-Slice e Intra-Sub-Slice**
   Una realtà da considerare è la possibilità di un attacco alla slice meno sicura, ed in particolare alla RAN, per attaccare una slice più sicura. Se la comunicazione tra le slice è consentita, c'è la possibilità che l'attacco riesca ad effettuare un accesso non autorizzato con conseguente perdita di parametri condivisi e dati sensibili trasmessi tra le slice. Se una slice è compromessa, ciò non dovrebbe influire in alcun modo sulle altre slice. La comunicazione tra le slice deve essere controllata e protetta tramite l'isolamento. Per evitare perdite, i parametri crittografici non dovrebbero mai essere condivisi tra le sezioni. Se le chiavi dell'autenticazione primaria vengono utilizzate all'interno delle slice, le chiavi nuove e indipendenti devono essere generate per ogni sezione utilizzando una funzione di derivazione della chiave.

4. **Sistemi di gestione**
   La multi tenancy è un'architettura software in cui una singola istanza software può servire più gruppi di utenti distinti. Un tenant quindi potrebbe tentare di accedere alle sezioni di altri tenant e modificare i parametri condivisi tra le sezioni appartenenti a tenant diversi. Protocolli per mitigare questi attacchi includono restrizioni per eseguire modifiche sui parametri condivisi tra le slice appartenenti a diversi tenant.

5. **Infrastruttura delle risorse**
   Il livello delle risorse è un punto di attacco non solo in termini di consumo esaustivo o DoS, ma anche in altri termini, come gli attacchi software. Tecniche di protezione del codice e isolamento del codice prevengono il rischio di questi attacchi esterni.

Capitolo 4

Soluzioni per la sicurezza dei Network Slicing

Lo slicing della rete fornisce sicurezza alle reti di comunicazione mobile 5G, tuttavia nuove vulnerabilità sono anche insorte, che permettono a persone malintenzionate di sfruttare questa nuova tecnologia per esaurire le risorse in una o più slice e causare il degrado di servizi e risorse comuni tramite attacchi DoS deliberati. Considerando le varie minacce e le sfide discusse, notiamo la necessità di ridurre al minimo queste minacce nello slicing della rete 5G e per questo numerose tecniche e sistemi sono stati implementati per diminuire il rischio di attacchi alla rete.

Un problema da considerare si presenta quando il Network Slicing è implementato su una infrastruttura multidominio in quanto ciò rende i requisiti di sicurezza complessi e richiede eccellenti meccanismi di coordinamento. Oltre all'utilizzo di chiavi di autenticazione, requisito di forte isolamento tra le slice, ci sono molti altri requisiti di sicurezza che possono influenzare la sicurezza e l'affidabilità del Network Slicing, come la comunicazione inter-slice, la privacy e la gestione della fiducia tra le slice. Il Trust model gioca un ruolo importante nella sicurezza del network slicing. Similmente all'architettura generale, la fiducia deve essere considerata a diversi livelli tra gli MNO e i tenants. Le parti devono stabilire un livello di fiducia che si applica nella relazione in uno dei tre livelli architettonici: livelli di risorse, slice e servizi, e tale fiducia deve essere applicata anche a livello tecnico.

Molte delle future applicazioni 5G richiedono un accesso affidabile a varie fonti di informazioni. Le nuove reti di comunicazione mobile sono anche molto spesso integrate con le reti IoT per fornire una vasta gamma di nuovi servizi. Usando lo slicing di rete, i servizi di sicurezza possono essere dinamicamente scalati dentro e fuori secondo il contesto della rete. D'altra parte, il network slicing giocherà un ruolo cruciale per abilitare questi servizi. Nella tabella che segue sono illustrate i possibili tipi di attacchi che possono essere ricevuti da un Network slice e tecniche di difesa che sono state progettate per proteggere la rete.

Table 1: Security threats on the key roles involved in NS life-cycle and potential solutions.

Key role	Description and contribution of NSI life-cycle	Possible security threats	Defense techniques							
			1	2	3	4	5	6	7	8
Communication Service Customer (CSC)	End users who experience the communication services may create requests for Network Slice as a Service (NSaaS).	Impersonate attacks	X							
		Privacy attacks				X				
		Attacks on secrecy		X						
		Fraud attacks	X	X		X				
Communication Service Provider (CSP) and Network Operator (NOP)	NOP offers communication services and responsible for designing, building and providing NSaaS based on customer requirements. This can also be the CSP.	DoS and DDoS attacks	X		X				X	
		Man-in-the-Middle attack	X	X				X		
		Unauthorized access	X							
		Traffic and data modification	X	X						
		Eavesdropping		X				X		
Virualization Infrastructure Service Provider (VISP)	They provide virtualized infrastructure (VI) services based on the NOP's specifications. They are responsible for designing, building, and operating VIs.	Man-in-the-Middle attack	X	X				X		
		Flooding attack					X			
		Unauthorized access	X							
		Data leakages		X						
		Logging and reporting issues			X					
		Hypervisor attacks			X				X	
		DoS attacks on VM	X		X				X	
		VM escape attacks			X				X	
Data Centre Service Provider (DCSP)	Those who provide data centre services based on NOP's requirements to design and operate NSs.	Identity thefts	X	X		X				
		Physical attacks								X
		Unauthorized access	X		X					
		Data leakages, alterations, and thefts		X						
		DoS attacks	X		X				X	

1 - Authentication	2 - Encryption	3 – Access control	4 – Privacy preservation
5 – Attack prevention by puzzle mechanism	6 – Key derivation	7 – Slice isolation	8 – Physical protection

Figura 4.1: Minaccie alla sicurezza di un Network Slice e possibili tecniche di mitigazione

4.1 Gestione e coordinazione della sicurezza

I Network Slice e i loro componenti sono necessari per gestire in sicurezza il segnalamento ed il piano delle comunicazioni. La gestione della sicurezza inizia con l'impostazione delle sezioni e l'avvio della comunicazione nell'ambiente delle sezioni. Successivamente, vengono direzionate le sezioni e controllati la trasmissione dei dati in uno stato di rete stabile. Infine, vengono chiuse le sezioni, eseguite la contabilizzazione della trasmissione e puliti i postumi per prevenire gli attacchi residui. Dato che le istanze delle slice possono essere offerti dinamicamente su richiesta da più operatori di rete, sono necessarie soluzioni di sicurezza multidominio per gestire le politiche di sicurezza. Una possibile soluzione è stata trovata proponendo un'architettura gerarchica sullo standard 3GPP.

Il NSM è responsabile della creazione e della distruzione dinamica delle istanze, della mappatura di una slice di rete e del caricamento negli host fisici disponibili. Una forte autenticazione è richiesta tra l'NSM e le piattaforme host prima di avviare le istanze slice. Se più operatori o host stanno contribuendo per una slice l'NSM deve ottenere l'autenticazione reciproca tra tutti loro prima dell'invio dei dati per evitare attacchi di impersonificazione.

La coordinazione delle slice di rete è direttamente collegata alla coordinazione delle NFV e quindi ne eredita i relativi problemi, inoltre la richiesta di una elevata complessità e flessibilità nelle reti comporta maggiori rischi per la sicurezza. L'integrazione di varie piattaforme e tecnologie è uno dei problemi principali. Un approccio al problema potrebbe essere la standardizzazione delle interfacce di interconnessione, per garantire un livello minimo di sicurezza. Un altro problema di gestione è l'implementazione dei meccanismi di sicurezza corretti per ogni sezione in modo efficiente. In tal caso l'utilizzo di una slice unicamente dedicata alla sicurezza che decide automaticamente le politiche e i meccanismi di sicurezza in base a diversi parametri può rivelarsi una soluzione. Poiché una slice di rete può cambiare dinamicamente nel tempo, la coordinazione, e quindi le politiche di sicurezza della coordinazione, diventano obbligatorie. L'intelligenza artificiale potrebbe quindi aiutare ad automatizzare nel caso di cambiamenti dinamici e frequenti.

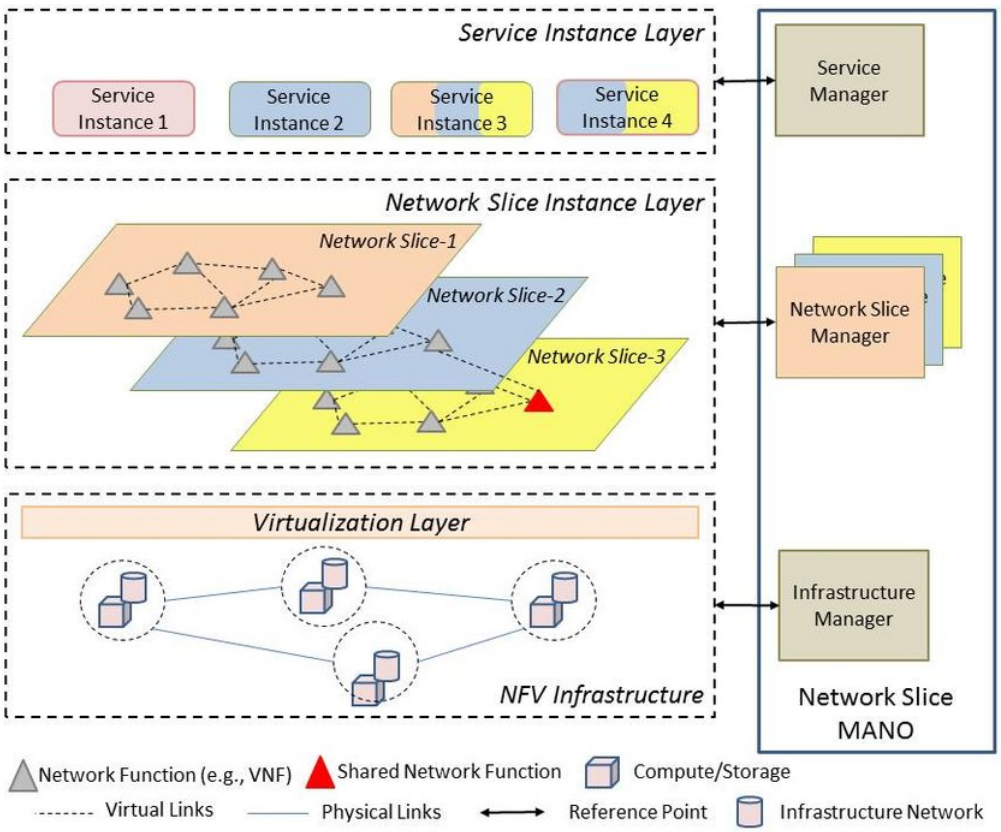

Figura 4.2: Struttura di un NFV e del modello MANO

L'obiettivo principale della coordinazione della sicurezza è rimuovere la necessità di eseguire manualmente controlli con l'interazione umana. La coordinazione della sicurezza sarà responsabile della distribuzione, configurazione, manutenzione, monitoraggio e gestione del ciclo di vita di tutte le funzioni di sicurezza nella rete mobile. Deve essere in grado di garantire la sicurezza end-to-end allineando automaticamente le politiche di sicurezza all'interno dei segmenti di rete sia virtuali che fisici.

4.1.1 Il modello ETSI NFV-MANO

La gestione e la coordinazione del 5G considerano il modello ETSI NFV-MANO (Network Functions Virtualization MANagement and Orchestration). Il quale pretende di soddisfare tutte le aspettative delle reti virtualizzate, compreso il 5G. Lo NFV MANO è un framework sviluppato dall'Industry Specification Group for NFV (ETSI). Il framework viene comunemente considerato solo come gestore e coordinatore degli NFV. L'obiettivo principale del NFV MANO è consentire un'integrazione flessibile. L' ETSI NFV MANO è suddiviso in tre blocchi funzionali:

- **Coordinatore NFV**: responsabile dell'avvio di nuovi servizi di rete e pacchetti di funzioni di rete virtuale e gestione del ciclo di vita dei Network Slice e delle risorse. Convalida e autorizza le richieste di risorse del NFVI.
- **VNF Manager**: supervisiona la gestione del ciclo di vita delle istanze VNF. Coordina e adatta la configurazione e la segnalazione di eventi tra l'infrastruttura NFV e i sistemi di gestione di elementi/rete.
- **Virtualized Infrastructure Manager (VIM)**: controlla e gestisce le risorse di calcolo, storage e rete NFVI.

Poiché il sistema ETSI NFV-MANO è molto generico, non considera esplicitamente problemi di rete reali come l'infrastruttura di rete multi-tenancy e considera lo slicing dell'isolamento solo su un livello base di isolamento delle prestazioni. Uno dei possibili miglioramenti attuabili al modello ETSI NFV-MANO è l'unione con una gestione simile al SDN poiché i sistemi sono compatibili tra loro avendo una struttura basata su piani e strati e l'utilizzo di una gestione centralizzata. Per quanto riguarda la gestione e la

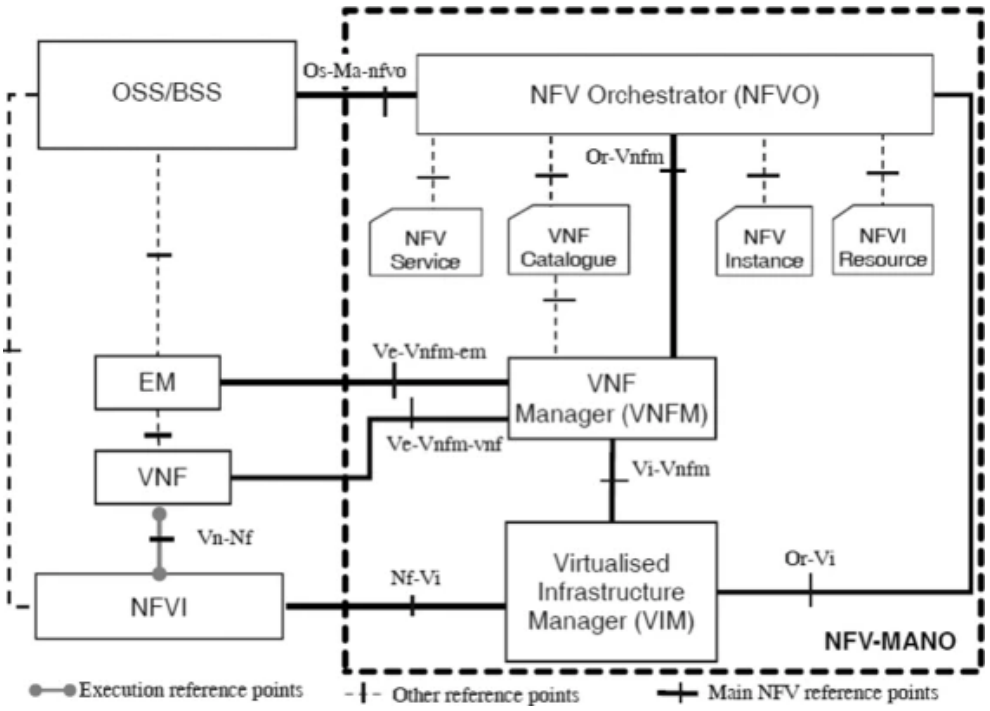

Figura 4.3: Struttura del modello MANO

coordinazione di uno slice isolato multi-dominio e multi-tenant, è stata proposta la suddivisione in diversi sottosistemi MANO interconnessi e gerarchici concentrati su aree e periodi specifici di funzionamento della rete.

- **Network management system**
  - Per l'implementazione di slice isolate
  - Per l'utilizzo di slice isolate
- **Sistema di gestione della sicurezza che include forte isolamento e controlli frequenti**

Il sistema di gestione della rete per la creazione di slice isolate dovrebbe contenere il concatenamento delle slice, oltre a decidere quale servizio virtuale è assegnato esclusivamente a una specifica istanza di slice e quale è condiviso. Deve inoltre occuparsi dell'assegnazione degli utenti a slice specifiche e della condivisione delle competenze tra tutte le parti coinvolte. Il sistema di gestione della sicurezza è fondamentale per un forte isolamento delle sezioni e deve fornire meccanismi per stabilirlo e controllare permanentemente se l'isolamento non è indebolito o perso.

4.1.2 L'Intelligenza artificiale per gestire la sicurezza

Le reti 5G basate sullo slicing della rete dovranno affrontare attacchi più automatizzati e avanzati a causa dell'avanzamento di tecnologie di comunicazione e tecniche di machine learning. L'utilizzo di IA da parte di aggressori per ottenere il controllo delle reti mobili è ormai una realtà. D'altra parte non è possibile continuare ad eseguire meccanismi di sicurezza in modo manuale, quando i servizi di rete e gli utenti stanno aumentando esponenzialmente. Per prevenire attacchi su larga scala, l'utilizzo di intelligenze artificiali sofisticate sono soluzioni necessarie per la sicurezza. L'intelligenza artificiale può essere utilizzata come strumento per progettare soluzioni di sicurezza per lo slicing della rete e algoritmi di deep learning e modelli base possono essere utilizzati per trovare errori di configurazione, vulnerabilità e minacce di sicurezza per ridurre l'intervento umano. Un'architettura standard basata sull'intelligenza artificiale dovrebbe essere strutturata per supportare flessibilità, affidabilità e scalabilità, per garantire una velocità dati più veloce, QoS ed efficienza nella rete.

4.1.3 Slice dedicata per la sicurezza

Diversi meccanismi di sicurezza devono essere implementati per ottenere un sistema di sicurezza sicuro dello slicing della rete. Tuttavia, questi meccanismi devono essere coordinati e comunicare in modo sicuro per garantire la riduzione di un sovraccarico sul meccanismo di sicurezza. Per raggiungere questo obiettivo, l'allocazione di una slice di rete indipendente per la sicurezza è vantaggiosa. Inoltre i sistemi di monitoraggio e gestione degli incidenti di sicurezza possono essere eseguiti in aggiunta in questa slice di sicurezza per garantire il corretto funzionamento della rete. Una sezione di sicurezza dedicata può inoltre garantire la sicurezza end-to-end sulla catena di approvvigionamento dei sistemi. Quando una slice dedicata alla sicurezza è disponibile, le risorse allocate per i servizi di sicurezza possono essere dinamicamente cambiati.

4.1.4 Puzzle Mechanism

In un attacco DoS, un utente malintenzionato tenta di impedire ad utenti legittimi di accedere a informazioni o servizi da un server. Il tipo più comune di attacco DoS si verifica quando un attaccante inonda una rete di pacchetti di informazioni inutili. Queste richieste esauriscono alcune risorse chiave della vittima in modo che le richieste degli utenti legittimi vengano rifiutate.
Un meccanismo di difesa contro il flooding può essere reattivo o preventivo. Un meccanismo reattivo come il pushback, il traceback o il filtraggio tenta di alleviare l'impatto di un attacco sulla vittima rilevando l'attacco e rispondendo ad esso. Un meccanismo preventivo, invece, consente di tollerare l'attacco senza negare il servizio agli utenti legittimi. Questo di solito viene fatto applicando politiche restrittive per il consumo di risorse. Un metodo per limitare il consumo di risorse è l'uso dei puzzle di rete.

I puzzle di rete possono essere utilizzati per prevenire in una certa misura un attacco DoS. In generale, i meccanismi reattivi soffrono di problemi di scalabilità e della difficoltà di identificazione dell'attaccante. Nel caso dell'approccio client-puzzle invece il difensore tratta le richieste in arrivo in modo simile tra loro e non ha bisogno di distinguere tra l'attacco e le richieste legittime.
Questi enigmi fanno sì che il client dell'attaccante impegni le sue risorse per risolvere un enigma prima di ottenere l'accesso ai servizi forniti dal server. Il servizio del server è fornito solo per i clienti che sono in grado di risolvere il puzzle e inviare la soluzione corretta. La funzione principale del server è quella di produrre un puzzle con difficoltà ottimale. Se la difficoltà del puzzle è troppo bassa, l'attaccante sarà in grado di risolverlo e iniziare un attacco intenso. Tuttavia se la difficoltà del puzzle è troppo alta, l'attaccante risponderà inviando risposte casuali e il server dovrà verificare la soluzione dei puzzle provocando l'esaurimento delle risorse del server difensore. Pertanto, il livello di difficoltà dei puzzle dovrebbe essere regolato accuratamente in modo tempestivo per preservare l'efficacia e l'ottimalità del meccanismo.

Il puzzle di rete viene installato sia nel server o nel router di emissione del puzzle che nel proxy intermedio per la risoluzione dei puzzle. Tramite il traceback si può identificare il nodo attaccante dopo che si è verificato un attacco DoS. Combinando sia la tecnica client-puzzle che il traceback, un attacco su un particolare router proxy può essere fermato interrompendo il flusso dei pacchetti al primo router che sta inoltrando i pacchetti. Ciò ridurrà il traffico sul router proxy che sta risolvendo il puzzle per i client. Le copie dei pacchetti utilizzati per l'attacco vengono inviate ad altri router nella rete in modo che se vengono trovati pacchetti simili, i pacchetti possono essere subito eliminati.

4.2 Tecnologie di accesso

Il 5G è stato progettato considerando molteplici meccanismi di sicurezza aventi un controllo sicuro sulla rete per fornire autenticazione reciproca, protezione dell'identità dell'utente, migrazione del servizio e slicing sicuri.
L'utilizzo da parte del 5G di molte tecnologie di accesso contemporaneamente per servizi singoli o multipli di un UE può creare gravi minacce alla sicurezza durante il passaggio tra le tecnologie di accesso infatti tutte le funzioni di rete virtuale disponibili in una istanza di rete devono essere autenticate. I componenti chiave di rete relativi all'architettura di sicurezza delle istanze di rete includono l'autenticazione degli UE, la memorizzazione delle loro credenziali di sicurezza e il mantenimento delle politiche di controllo della sicurezza. Pertanto, un algoritmo crittografico deve essere applicato al canale per proteggere la sessione e le chiavi, con un'analisi della sicurezza in tempo reale per evitare che la rete venga violata.

Quando slice diverse offrono servizi distinti, i loro i vincoli e requisiti di sicurezza varieranno. Servizi con bassa latenza richiederanno tecniche di derivazione delle chiavi molto veloci e meccanismi di gestione delle chiavi a grana fine, mentre per servizi a basso consumo è necessario determinare la frequenza con cui deve essere eseguita la ri-autenticazione. Con l'eterogeneità della fetta, è importante differenziare l'accesso dell'utente finale (UE) a più sezioni in un'istanza con diversi livelli di sicurezza siccome l'UE può essere collegata a diverse slice.

La rete 5G è composta da diversi sottomoduli, ciascuno dei quali ha una funzione essenziale nel garantire la sicurezza della trasmissione dei dati. L'efficienza di una rete sarà danneggiata dall'interferenza del canale e dalla perdita di percorso. In reti eterogenee, la sincronizzazione dell'ora è un problema significativo che influisce sulla coordinazione tra le cellule, che sono direttamente proporzionali tra loro. Di conseguenza, uno slicing di rete efficace aiuta nell'ottimizzazione del traffico di rete, gestione del carico ed efficienza nella gestione del traffico.

4.3 Crittografia e Key Derivation

Le reti 5G spesso forniscono una crittografia del traffico, ad esempio tra l'UE e il eNodeB. Tuttavia non forniscono crittografia intrinseca del traffico dati tra l'utente finale e le applicazioni cloud, basandosi invece su sessioni crittografate over-the-top nel livello dell'applicazione. Questo spesso pone la responsabilità all'utente finale o allo sviluppatore di mantenere la sicurezza nelle applicazioni. La crittografia del traffico a livello di applicazione è un metodo importante per ottenere sicurezza end-to-end, ma le reti 5G richiedono collegamenti critici a più livelli su cui possono fluire grandi concentrazioni di traffico che possono rivelarsi una vulnerabilità.
Un prerequisito fondamentale per una crittografia avanzata è lo scambio sicuro delle chiavi crittografiche. La gestione delle chiavi è una componente cruciale di un sistema di controllo con accesso a un'ampia gamma di risorse. Protegge i dati dagli attacchi e garantisce la conformità alle normative. La gestione delle chiavi si occupa della cifratura delle chiavi: la generazione, la creazione, la protezione, la conservazione e lo scambio.

L'evoluzione di EPS AKA (Authentication and Key Agreement of the 4G Evolved Packet System) dalla rete 4G ha portato allo sviluppo della 5G AKA. Il protocollo 5G AKA fornisce funzionalità di sicurezza come l'autenticazione reciproca, la riservatezza e l'anonimato. Si basa sulla crittografia a chiave pubblica in modo tale che l'UE sia sempre connessa a una rete di servizio autorizzata dalla rete domestica. Tra i meccanismi di funzionamento del protocollo 5G AKA c'è la funzione di key derivation.

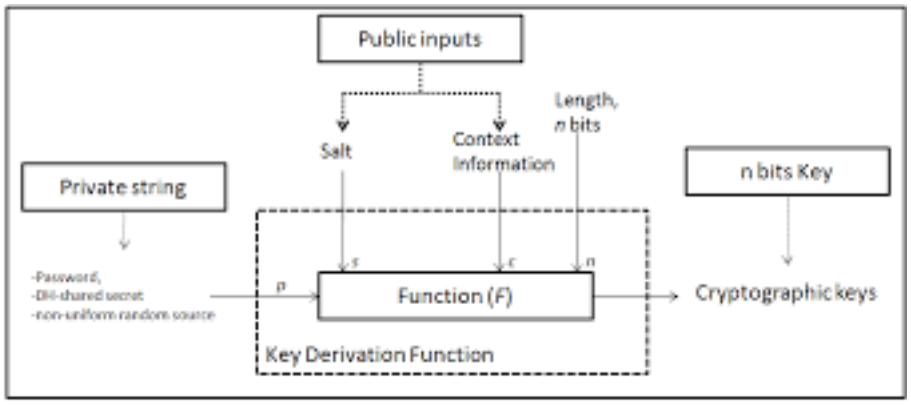

Figura 4.4: Struttura di una KDF

Una funzione di key derivation (KDF) è un componente di base ed essenziale dei sistemi crittografici: il suo obiettivo è prendere una fonte di materiale di codifica iniziale, di solito contenente una buona quantità di casualità, ma non distribuita in modo uniforme o per la quale un utente malintenzionato ha soltanto una conoscenza parziale, e da esso derivare una o più chiavi segrete crittograficamente forti. Una KDF accetta come input quattro argomenti: un valore 'q' campionato da una fonte di chiavi di codifica, un valore di lunghezza 'l' ,un valore di salt 'r' definito su un insieme di possibili valori e una variabile di contesto 'c', il salt e la variabile di contesto sono elementi facoltativi e possono essere impostati su una stringa nulla o su una costante. L'output della funzione di key derivation è una stringa di 'l' bit. La sicurezza e la qualità di un KDF dipendono dalle proprietà delle fonti delle chiavi di codifica da cui viene scelto l'input 'q'.

4.4 L'isolamento

L'isolamento è uno dei requisiti più critici e importanti dei Network Slice. Il 3GPP afferma che "Il sistema 3GPP deve avere la capacità di fornire un livello di isolamento tra le slice di rete che limitano un potenziale attacco informatico a singole slice di rete".
L'isolamento deve essere considerato da diverse prospettive: isolamento tra gli slices di rete, isolamento tra funzioni di rete e isolamento tra utenti. Ciascuno di questi tipi di isolamento ha il proprio ruolo e le possibili falle che comportano rischi per la sicurezza. Il vantaggio primario dell'isolamento è che limita qualsiasi sfida alla sicurezza a una singola fetta piuttosto che all'intera rete, riducendo così la portata degli impatti sulla sicurezza. L'isolamento protegge essenzialmente le risorse e il traffico verso ciascuna porzione della rete da qualsiasi attacco DoS, infatti se si verifica un malfunzionamento o un attacco alla sicurezza su una sezione, esso non influenzerà le altre slice. Dunque, l'aggiunta di più livelli di isolamento proteggerà le slice in caso di intrusi o di aggressori che stanno deliberatamente cercando di attaccare le slice.
L'isolamento può essere ottenuto con diversi mezzi, tra cui:

- Language-based isolation e Sandbox-based isolation: sono adatti per fornire isolamento nel livello dell'istanza del servizio e nel livello dell'istanza della slice di rete.
- Virtual machine (VM) based isolation e Operating system (OS) kernel based isolation: sono applicabili a livello di istanza della slice di rete e a livello di risorsa
- Hardware based isolation e Physical isolation: possono aiutare nella condivisione dell'infrastruttura/infrastruttura virtuale tra le sezioni in particolare sull'interfaccia RAN-CN, che è quella che comporta più difficoltà nell'attuazione dell'isolamento delle slice di rete.

La RAN nel 5G affronta la sfida dell'implementazione fisica con l'uso di Network Slices. Questa usa degli elementi della rete radio per incorporare l'isolamento delle risorse, del traffico e degli utenti. Pertanto, una proposta esistente consiste nell'utilizzare onde millimetriche per coprire piccole celle, le cui ridotte dimensioni fungono da mezzo per isolarle l'un l'altra. Questa proprietà isola naturalmente il traffico tra le diverse celle.
L'utilizzo di due tipi di celle permette un'architettura in cui una parte dei dati è trasmessa da macro-celle (i dati del Control Plane) e il resto è trasmesso da piccole celle (i dati dello User Plane). In termini di slicing, si può guardare a questo come a uno speciale meta-slice, che permette alle apparecchiature dell'utente di comunicare con la RAN.

Tuttavia, le tecnologie esistenti, tra cui la radio cognitiva e l'accesso multiplo non ortogonale, non garantiscono i livelli desiderati di isolamento e di slicing della rete. Pertanto, la selezione e l'adozione di una tecnologia RAN adeguata rimane ancora una sfida per l'isolamento della rete.
Nella rete, i metodi di multiplexing e le tecnologie di accesso sono ampiamente utilizzati, il che divide e condivide le risorse tra i canali. Possiamo quindi suddividere le tipologie di isolamento per questi metodi:

- Isolamento completo, quando ogni canale ha una propria parte di risorse disponibili.
- Isolamento parziale, quando i canali possono condividere parte delle risorse disponibili.
- Zero isolamento, quando tutti i canali utilizzano una parte delle risorse disponibili.

L'isolamento può essere eseguito sia con mezzi fisici che logici. Tuttavia, l'isolamento fisico a volte non è attuabile, quindi devono essere forniti forti meccanismi di isolamento logico. Tecnologie come firewall, gateway e hypervisor possono essere utilizzate per ottenere l'isolamento il quale può, quindi, essere considerato a tutti i livelli a partire da quello fisico. Un ulteriore problema dello slicing della rete è l'instaurazione di una corretta connessione E2E. In una parte fissa della rete, la slice potrebbe essere definita in qualche livello di rete dello stack di protocolli implementato. Un nodo della rete può implementare una o più delle seguenti funzionalità:

- Lo slice switch.
- Lo slice gateway.
- Lo slice multiplexer.
- Lo slice demultiplexer.

Il slice switch e il gateway trasportano i dati da un collegamento di origine a un collegamento di destinazione mentre lo slice multiplexer e il demultiplexer funzionano su più collegamenti laterali. Lo switch può combinare due collegamenti della sezione dallo stesso livello nello stack di protocollo comune. Il gateway è uno switch di slice che può combinare due collegamenti di slice da livelli diversi o stack di protocollo diversi. Il multiplexer può unire più slice in un'unica sezione, che potrebbe essere successivamente suddivisa da un

demultiplexer. Mentre multiplexing e demultiplexing non richiedono un'ispezione approfondita su diversi strati di una slice, siccome i dati di diverse sezioni sono contrassegnati, uno switch e un gateway sono più complicati secondo l'analisi delle sezioni. In alcuni casi, richiederebbero l'accesso ai dati inviati tramite una sezione per trasferirli all'altra sezione. Ciò significa che tali dispositivi richiedono una protezione speciale in base all'accesso ai dati delle sezioni grezze, nonché un'adeguata garanzia per le sezioni di interconnessione, inclusa la prevenzione di interconnessioni errate di sezioni e potenziali perdite di dati.

A causa dell'elevata diversità della rete di ciascun operatore, i meccanismi, le tecnologie o la configurazione utilizzati per l'isolamento delle sezioni saranno diversi in ciascun caso. Per garantire la corretta qualità della progettazione per l'isolamento delle sezioni di rete, dovrebbe esserci un framework sviluppato che copra la raccolta e l'analisi dei requisiti. Tale approccio normalizzato aiuterebbe gli operatori di rete a considerare i problemi di sicurezza più importanti e garantirebbe il raggiungimento degli obiettivi comuni per lo slicing della rete.
Il 5G deve consentire l'interoperabilità continua di diverse tecnologie di rete potenzialmente con diversi livelli di sicurezza senza compromettere il livello di sicurezza di ciascuna slice. Una delle questioni cruciali è la definizione dei parametri di isolamento. L'isolamento delle slice può essere considerato in almeno quattro aree:

- **Isolamento del traffico**: tutte le sezioni utilizzano le stesse risorse di rete, quindi le sezioni di rete dovrebbero garantire che il flusso di dati di una sezione non si sposti a un'altra.
- **Isolamento della larghezza di banda**: tutte le sezioni allocano una parte della larghezza di banda e non devono utilizzare alcuna larghezza di banda assegnata ad altre sezioni. Pertanto, è necessario garantire l'isolamento della larghezza di banda sui collegamenti e sui nodi CPU, storage o capacità di rete.
- **Isolamento dell'elaborazione**: mentre tutte le slice virtuali utilizzano le stesse risorse fisiche, è necessaria un'elaborazione adeguata del pacchetto, che sarà indipendente da tutte le altre slice.
- **Isolamento dell'archiviazione**: i dati relativi a una slice devono essere archiviati separatamente dai dati utilizzati da un'altra slice.

4.4.1 E2E Slice Isolation

La sicurezza end-to-end è strettamente connessa ai concetti di isolamento e coordinazione e può essere vista come un prerequisito. Raggiungere l'isolamento end-to-end non è semplice poiché la creazione delle sotto-sezioni della RAN presenta ancora alcune complessità. Lo slicing RAN è fornito dalla rete 5G, dove operano gli operatori di rete virtuale mobile con i quali condivide la stessa infrastruttura della rete fisica. In base alle esigenze dinamiche degli utenti, viene sostituita l'allocazione delle risorse, passando da risorse statiche a risorse dinamiche. Lo slicing end-to-end è una realtà possibile ma richiede un automatizzato sistema gestionale per la creazione, la cancellazione e l'aggiornamento degli slice in base alle richieste e ai requisiti dell'utente. Il che può essere possibile fornendo una configurazione a livello astratto della rete centrale e di accesso.

Capitolo 5

Conclusioni

In questa tesi sono state presentate le soluzioni proposte per garantire che la tecnologia del Network Slicing possa operare in sicurezza senza creare nuove falle nell'architettura delle reti mobili. L'aumento della complessità delle reti nel corso degli anni per adattarsi ad un ambiente sempre più interconnesso e flessibile aumenterà sicuramente la semplicità e i punti di attacco che utenti malintenzionati possono sfruttare per effettuare attacchi DoS o di impersonificazione, ciononostante il 5G ha introdotto tecnologie e sistemi sostanziali per mitigare quanto possibile il rischio di questi attacchi.

Bibliografia

[1] Tony Saboorian, Amanda Xiang, *Network Slicing and 3GPP Service and Systems Aspects (SA) Standard*, https://sdn.ieee.org/newsletter/december-2017/network-slicing-and-3gpp-service-and-systems-aspects-sa-standard, 2017.

[2] Marin Ivezic, Luka Ivezic, *5G Network Slicing Technology: A Primer*, https://5g.security/5g-security-privacy/5g-network-slicing-primer/ https://www.viavisolutions.com/en-us/5g-network-slicing, 2019.

[3] *5G e Security*, https://www.reply.com/it/Shared%20Documents/5G-security-ITA.pdf.

[4] *5G Network Slicing*, https://www.viavisolutions.com/en-us/5g-network-slicing.

[5] Dave Bolan, *5G Core – Are We Ready?*, https://www.delloro.com/5g-core-are-we-ready/, 2020.

[6] Marin Ivezic, *Introduction to 5G Core Service-Based Architecture (SBA) Components* , https://5g.security/5g-technology/5g-core-sba-components-architecture/, 2020.

[7] Ruxandra F. Olimid, Gianfranco Nencioni, *5G Network Slicing: A Security Overview*, https://ieeexplore.ieee.org/abstract/document/9099823, 2020.

[8] Dimitrios Schinianakis, Ruben Trapero, Diomidis S. Michalopoulos, Beatriz Gallego-Nicasio Crespo, *Security Considerations in 5G Networks: A Slice-Aware Trust Zone Approach*, https://ieeexplore.ieee.org/document/8885658, 2019.

[9] Tomasz Wichary, Jordi Mongay Batalla, Constandinos X. Mavromoustakis, Jerzy Zurek, George Mastorakis, *Network Slicing Security Controls and Assurance for Verticals*, 2022.

[10] Ramraj Dangi, Akshay Jadhav, Gaurav Choudhary, Nicola Dragoni, Manas Kumar Mishra, Praveen Lalwani, *ML-Based 5G Network Slicing Security: A Comprehensive Survey*, 2022.

[11] Yi Shi, Yalin E. Sagduyu, Tugba Erpek, M. Cenk Gursoy, *How to Attack and Defend 5G Radio Access Network Slicing with Reinforcement Learning*, https://www.researchgate.net/publication/348487480_How_to_Attack_and_Defend_5G_Radio_Access_Network_Slicing_with_Reinforcement_Learning, 2021.

[12] Pawani Porambage, Madhusanka Liyanage, *Security in Network Slicing*, https://www.researchgate.net/publication/341435793_Security_in_Network_Slicing, 2020.

[13] Alex Mathew, *Network Slicing in 5G and the Security Concerns*, https://ieeexplore.ieee.org/document/8802852, 2019.

[14] Danish Sattar, Ashraf Matrawy, *Towards Secure Slicing: Using Slice Isolation to Mitigate DDoS Attacks on 5G Core Network Slices*, https://ieeexplore.ieee.org/abstract/document/8802852, 2019.

[15] Sean Hsu, *What is C-RAN? The Evolution From D-RAN to C-RAN*, https://www.ufispace.com/company/blog/what-is-cran-the-evolution-from-dran-to-c 2020.

[16] Volker Jungnickel, Kai Habel, Michael Charles Parker, Stuart D. Walker, *Software-defined open architecture for front- and backhaul in 5G mobile networks*, https://www.researchgate.net/publication/269031371_Software-defined_open_architecture_for_front-_and_backhaul_in_5G_mobile_networks, 2014.

[17] Larry Peterson, Oguz Sunay, *5G Mobile Networks: A Systems Approach*, https://5g.systemsapproach.org/index.html, 2020.

[18] Zbigniew Kotulski, Tomasz Wojciech Nowak, Mariusz Sepczuk, Marcin Tunia, Rafal Artych, Krzysztof Bocianiak, Tomasz Osko, Jean-Philippe Wary, *Towards constructive approach to end-to-end slice isolation in 5G networks*, https://jis-eurasipjournals.springeropen.com/articles/10.1186/s13635-018-0072-0, 2018.

[19] Stan Wong,Bin Han, Hans D. Schotten, *5G Network Slice Isolation*, 2022.

[20] Connor Craven, *What Is NFV MANO?*, https://www.sdxcentral.com/networking/nfv/definitions/whats-network-functions-virtualization-nfv/nfv-elements-overview/nfv-mano/, 2019.

[21] Chandini, NZ. Jhanjhi, Sahil Verma, M. N. Talib, Kavita, Gagandeep Kaur, *A Canvass of 5G Network Slicing: Architecture and Security Concern*, https://iopscience.iop.org/article/10.1088/1757-899X/993/1/012060/pdf, 2020.

[22] Thomas Tovinger, Jean-Michel Cornily, Maryse Gardella, Chen Shan, Chen Ai, Anatoly Andrianov, Joey Chou, Jan Groenendijk, Zhang Kai, Zou Lan, Xiaowen Sun, Weixing Wang, Zhu Weihong, Yizhi Yao, *Management, Orchestration and Charging in the New Era*, https://www.riverpublishers.com/journal/journal_articles/RP_Journal_2245-800X_6110.pdf, 2018.

[23] Paul Wright, Catherine White, Ryan C. Parker, Jean-Sébastien Pegon, Marco Menchetti, Joseph Pearse, Arash Bahrami, Anastasia Moroz, Adrian Wonfor, Richard V. Penty, Timothy P. Spiller, Andrew Lord, *5G network slicing with QKD and quantum-safe security*, https://opg.optica.org/jocn/abstract.cfm?uri=jocn-13-3-33, 2021.

[24] Hugo Krawczyk, *Cryptographic Extraction and Key Derivation: The HKDF Scheme*, https://eprint.iacr.org/2010/264.pdf, 2010.

[25] Rosario Giustolisi, Christian Gehrmann, *Threats to 5G Group-Based Authentication*, https://itu.dk/~rosg/paper/gaka_short.pdf, 2016.

[26] Nicholas A. Fraser, Douglas J. Kelly, Richard A. Raines, Rusty O. Baldwin, Barry E. Mullins, *Using Client Puzzles to Mitigate Distributed Denial of Service Attacks in the Tor Anonymous Routing Environment* , https://apps.dtic.mil/sti/pdfs/ADA497408.pdf, 2007.

[27] Mahran Fallah, *A Puzzle-Based Defense Strategy Against Flooding Attacks Using Game Theory*, https://ieeexplore.ieee.org/abstract/document/4459338, 2010.

[28] Anup Mathew Abraham, Shweta Vincent , *Defending DoS Attacks Using a Puzzle-Based Approach and Reduction in Traceback Time towards the Attacker*, https://link.springer.com/chapter/10.1007/978-3-642-29219-4_49, 2011.

[29] Xiaofeng Wang, M.K. Reiter, *Defending against denial-of-service attacks with puzzle auctions*, https://ieeexplore.ieee.org/document/1199329, 2003.

Ringraziamenti

Un doveroso ringraziamento va a chi mi ha permesso di realizzare questa tesi e in particolare:

- *al mio relatore, il Prof. Migliardi, per la cura e la sua infinita disponibilità con cui mi ha seguito durante la stesura della mia tesi;*
- *un grazie di cuore a mia nonna Lilli per tutte le volte che avevo bisogno di parlare e lei è stata ad ascoltarmi e che ha sempre creduto nelle mie capacità;*
- *ed infine un ringraziamento ai miei genitori, Barbara e Franco, per i sacrifici fatti e per non avermi fatto mai mancare il loro affetto.*