5G CYBERSECURITY: *lacune, valutazione dei rischi, soluzioni,*

Autore: Aldo Pedico – Cybersecurity & Privacy Consultant
Contatto: pedicoaldo@gmail.com

Redatto il 26 aprile 2022 – aggiornato il 16 maggio 2022

PREMESSA

Ho voluto condividere con tutti gli interessati questo argomento attuale che richiede attenzione, approfittando sia della prima bozza del documento pubblicato da NIST, SP 1800-33, che mi permette di sintetizzare gli aspetti salienti della Cybersecurity nella tecnologia di telefonia mobile definita 5G, sia di altro materiale pervenutomi, ad esempio il "GSMA Securing 5G Era".

*Questa versione non contiene ancora tutti i dettagli tecnici necessari a classificare i rischi informatici (oggetto delle prossime versioni) ma fornisce sicuramente una breve descrizione generale dei contesti impattati da questa tecnologia, descritti nel capitolo "*SCENARI DI DIMOSTRAZIONE FUNZIONALE*".*

I capitoli che saranno oggetto di ulteriore implementazione nelle versioni successive sono:

- *DIMOSTRAZIONE DELLE CARATTERISTICHE DI SICUREZZA;*
- *PRESUPPOSTI E LIMITAZIONI;*
- *SCENARI DI DIMOSTRAZIONE FUNZIONALE;*
- *APPENDICE A – SECURITY CONTROL MAP.*

All'interno dei suddetti capitoli ho evidenziato in rosso l'attuale incompletezza.

Questa seconda versione rispetto alla precedente contiene la sensibile modifica del capitolo INTRODUZIONE e i seguenti nuovi capitoli:

- *SCOPO DEL 5G;*
- *MODELLI DI IMPIEGO 5G;*
- *PROTEZIONE DELL'ABBONATO E DEL SERVIZIO;*
- *PROTEZIONE DELLA RETE;*
- *NUOVO STACK DI PROTOCOLLO IT;*
- *TECNOLOGIE VANTAGGIATE DAL 5G.*

INDICE DEGLI ARGOMENTI

Titolo _____ Pag.

1. SCOPO DEL 5G

[Fonte: GSMA – Securing the 5G Era]

Lo scopo del 5G è quello di aprire la rete a un insieme più ampio di servizi e consentire agli operatori mobili di sostenere questi servizi.

È un'opportunità per proteggere i servizi e i consumatori da molte delle minacce odierne.

Il 5G viene fornito con molti controlli di sicurezza integrati in base alla progettazione, sviluppati per migliorare la protezione sia dei singoli consumatori sia delle reti mobili.

Il progresso della tecnologia e l'uso di nuove architetture e funzionalità come lo slicing della rete, la virtualizzazione e il cloud introdurranno nuove minacce che richiedono l'implementazione di nuovi tipi di controlli.

Questa generazione di sistema di telecomunicazioni mira a fornire:

1) *Banda larga mobile potenziata,*
2) *Massive comunicazioni di tipo macchina,*
3) *Comunicazioni ultra affidabili e a bassa latenza.*

L'obiettivo è:

- ✓ *essere più veloci;*
- ✓ *essere più affidabili;*
- ✓ *gestire la scala dei dispositivi prevista per l'Internet delle cose Mobile (MIoT);*
- ✓ *consentire la trasformazione digitale della nostra società, dei processi aziendali e della produzione.*

Per consentire ciò, il 5G fornirà:

1) *slicing (porzioni o parti) multi-rete,*
2) *multi-livello di servizi e*
3) *capacità di rete multi-connettività.*

Per consentire la flessibilità, l'agilità e le economie di scala richieste, queste tecnologie saranno fornite tramite ambienti virtuali e containerizzati. ***Questo è un modo rivoluzionario di lavorare per l'industria.***

Il 5G ha progettato controlli di sicurezza per sostenere molte delle minacce affrontate nelle odierne reti 4G/3G/2G.

Questi controlli includono nuove funzionalità di autenticazione reciproca, protezione avanzata dell'identità dell'abbonato e meccanismi di sicurezza aggiuntivi.

Il 5G offre al settore mobile un'opportunità senza precedenti per elevare i livelli di sicurezza della rete e del servizio.

Il 5G fornisce misure preventive per limitare l'impatto sulle minacce note, ma l'adozione di nuove tecnologie di rete introduce potenziali nuove minacce da gestire per il settore.

Questo articolo discute diversi controlli di sicurezza dell'era 5G, comprese le loro limitazioni, per questo motivo è richiesto un certo livello di conoscenza tecnica.

2. INTRODUZIONE

Alcuni aspetti della protezione dei componenti 5G e dell'utilizzo mancano di standard e linee guida, rendendo più difficile per gli operatori e gli utenti della rete 5G sapere cosa deve essere fatto e come può essere realizzato.

Questo documento, sulla sicurezza informatica, descrive come una combinazione di funzionalità di sicurezza 5G e di controlli di sicurezza di terze parti possa essere utilizzata per implementare le capacità di sicurezza di cui le organizzazioni hanno bisogno per salvaguardare l'utilizzo della rete 5G.

Inoltre, cercherà anche di identificare le lacune negli standard di sicurezza informatica 5G che dovrebbero essere affrontate.

Questa bozza preliminare spiega perché stiamo costruendo la soluzione di esempio per affrontare le sfide della sicurezza informatica 5G, inclusa l'analisi del rischio da eseguire e le capacità di sicurezza che la soluzione di esempio consentirà e dimostrerà.

L'attuale sviluppo degli standard di sicurezza informatica 5G si concentra principalmente sulla sicurezza delle interfacce interoperabili basate su standard tra i componenti 5G.

Gli standard 5G non specificano le protezioni di sicurezza informatica da implementare sui componenti informatici (IT) sottostanti che supportano e gestiscono il sistema 5G.

Questa mancanza di informazioni aumenta la complessità per le organizzazioni che intendono sfruttare il 5G.

Con l'architettura 5G basata sulla tecnologia cloud, i sistemi 5G potrebbero potenzialmente sfruttare le solide funzionalità di sicurezza disponibili nelle architetture di cloud computing per proteggere i dati e le comunicazioni 5G.

*Secondo GSMA, per assicurare la progettazione dovrebbero essere sviluppati degli standard che adottino i principi "**SECURE BY DESIGN**", che portano a:*

- *Uso dell'autenticazione reciproca*

Confermando che mittente e destinatario abbiano una fiducia reciproca stabilita e la relazione end-to-end sia protetta.

- *Una presunta rete "aperta".*

Rimozione di qualsiasi presupposto di sicurezza da prodotti o processi sovrapposti.

- *Un riconoscimento che tutti i collegamenti potrebbero essere sfruttati.*

Imporre la crittografia del traffico inter/intra-rete, assicurando che le informazioni crittografate siano inutili quando vengono intercettate.

Sebbene questa sia una pratica comune nelle soluzioni per altri servizi, come l'on-line banking, si tratta di un importante cambiamento di paradigma rispetto alle pratiche di telecomunicazioni mobili esistenti. Di conseguenza, le reti 5G dovrebbero offrire al consumatore una protezione maggiore rispetto alle reti 4G/3G/2G esistenti.

3. INTERESSATI

Questo volume è destinato ai gestori di tecnologia, sicurezza e privacy che si occupano di come identificare, comprendere, valutare e mitigare i rischi per le reti 5G.

Le informazioni si rivolgono a tre tipi di organizzazioni.

1) *OPERATORI DI RETE MOBILE COMMERCIALE*

   La trattazione fornirà loro una migliore comprensione delle funzionalità di sicurezza cloud che sono già disponibili nei sistemi forniti dai fornitori.

   Queste funzionalità di sicurezza abilitate all'hardware vanno oltre ciò che gli standard 5G attualmente specificano e possono fornire una protezione complementare in questo momento.

   Questo è sempre più importante man mano che le operazioni si spostano su piattaforme e software di base e poiché la tecnologia di rete mobile si fonde con l'IT.

2) *POTENZIALI OPERATORI DI RETE 5G PRIVATI*

   Le reti private 5G dovrebbero diventare una realtà, come nelle università e nelle grandi aziende.

   Qualsiasi organizzazione che consideri l'implementazione e la gestione della propria rete 5G dovrà gestire la propria sicurezza utilizzando un approccio basato sul rischio.

   Il volume spiegherà una gamma di funzionalità di sicurezza e i rischi che ciascuna funzionalità aiuta a mitigare, fornendo informazioni preziose ai fini della gestione dei rischi delle organizzazioni.

3) *ORGANIZZAZIONI CHE UTILIZZANO E GESTISCONO LA TECNOLOGIA ABILITATA AL 5G*

   Prima che le organizzazioni adottino tecnologie abilitate al 5G, dovrebbero prendere decisioni sulla gestione dei rischi per la sicurezza informatica in merito al loro utilizzo, gestione e manutenzione.

   Le informazioni contenute nel volume dovrebbero aiutare a informare tali decisioni.

   Questo volume può essere utile per i partecipanti agli sforzi relativi agli standard relativi al 5G (ad esempio, da organizzazioni che sviluppano standard) che desiderano identificare le lacune negli standard per informare il loro lavoro futuro.

   Anche i ricercatori sulla sicurezza informatica che vogliono costruire banchi di prova per la ricerca sulla sicurezza informatica 5G potrebbero trovare utile questo volume come riferimento.

4. MODELLI DI IMPIEGO 5G

[Fonte: GSMA – Securing the 5G Era]

Gli standard 5G descrivono una serie di modelli di implementazione.

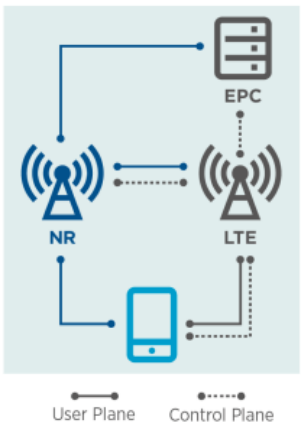
Sebbene ci siano piani per implementare almeno 5 opzioni aggiuntive in futuro, l'unica opzione attualmente implementata è la cosiddetta modalità non standalone (non-standalone (NSA) mode), più precisamente denominata EN-DC.

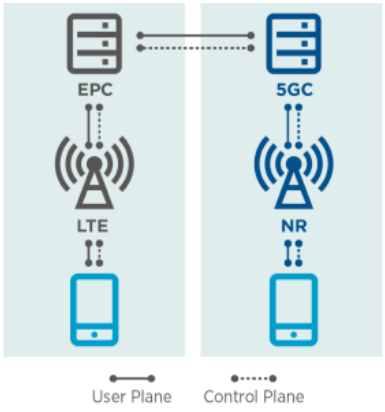
È qui che le stazioni base 5G sono integrate con una rete 4G esistente che lavora in tandem con stazioni base LTE e collegate al core LTE, basandosi sulle misure e sulle protezioni fornite dal core LTE.

La prossima fase dell'implementazione del 5G sarà probabilmente la modalità Stand Alone (Stand Alone [SA] mode), più precisamente SA NR, costituita da una nuova rete radio 5G (NR) connessa a una rete principale 5G (5GC).

Il passaggio a un Core 5G consentirà di realizzare tutte le funzionalità di sicurezza delle specifiche 5G.

Sebbene sia riconosciuto che i nuovi paradigmi (architettura nativa del cloud, basata sui servizi) introdurranno nuove sfide per la sicurezza.





NON-STANDALONE (NSA) DEPLOYMENT STANDALONE (SA) DEPLOYMENT

**77% degli operatori intervistati prevede di implementare SA 5G entro i prossimi tre anni (Fonte: GSMAi, 2019)*

5. PROTEZIONE DELL'ABBONATO E DEL SERVIZIO

[Fonte: GSMA – Securing the 5G Era]

Il 5G migliora la riservatezza e l'integrità dei dati di utenti e dispositivi.

A differenza delle precedenti generazioni di sistemi mobili 5G:

- *Protegge la riservatezza dei messaggi NAS (NON ACCESS STRATUM) tra il dispositivo e la rete. Di conseguenza, non è più possibile tracciare le apparecchiature utente (USER EQUIPMENT [UE]) utilizzando le attuali metodologie di attacco sull'interfaccia radio; protezione contro gli attacchi di MAN IN THE MIDDLE (MITM) e false stazioni base (STINGRAY/IMSI CATCHER).*
- *Introduce un meccanismo di protezione chiamato **HOME CONTROL**. Ciò significa che l'autenticazione finale del dispositivo su una rete visitata viene completata dopo che la rete domestica ha verificato lo stato di autenticazione del dispositivo nella rete visitata. Questo miglioramento preverrà vari tipi di frode in roaming che hanno ostacolato storicamente gli operatori e supporterà il requisito dell'operatore di autenticare correttamente i dispositivi ai servizi.*
- *Supporta l'autenticazione unificata su altri tipi di rete di accesso, ad es. WLAN, che consente alle reti 5G di gestire connessioni precedentemente non gestite e non protette. Ciò include la*

possibilità di eseguire una riautenticazione dell'UE quando si sposta tra diverse reti di accesso o di servizio.

- *Introduce il controllo dell'integrità del piano utente, assicurando che il traffico utente non sia modificato durante il transito.*
- *Migliora la protezione della privacy con l'uso di coppie di chiavi pubbliche/private (chiavi di ancoraggio) per nascondere l'identità dell'abbonato e derivare le chiavi utilizzate nell'architettura del servizio.*

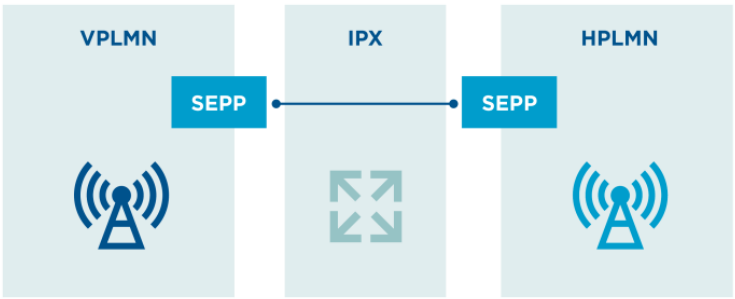
6. PROTEZIONE DELLA RETE

[Fonte: GSMA – Securing the 5G Era]

INTEGRITÀ DEI DATI DI SEGNALAZIONE

Il 5G introduce un nuovo elemento dell'architettura di rete: il SECURITY EDGE PROTECTION 0PROXY (SEPP).

Il SEPP protegge il perimetro della rete domestica, fungendo da gateway di sicurezza sulle interconnessioni tra la rete domestica e le reti visitate.



Il SEPP è progettato per:

1. *fornire sicurezza a livello di applicazione e protezione da intercettazioni e attacchi di riproduzione;*
2. *fornire autenticazione end-to-end, integrità e protezione della riservatezza tramite firme e crittografia di tutti i messaggi in roaming HTTP/2;*
3. *offrire meccanismi di gestione delle chiavi per impostare le chiavi crittografiche richieste ed eseguire le procedure di negoziazione delle capacità di sicurezza;*
4. *eseguire il filtraggio e il controllo dei messaggi, l'occultamento della topologia e la convalida degli oggetti JSON; compreso il controllo delle informazioni su più livelli con le informazioni sull'indirizzo sul livello IP.*

Inoltre, è stata introdotta una maggiore sicurezza dei servizi di roaming internazionale per superare i rischi per la sicurezza esistenti legati all'utilizzo di SS7 e Diameter.

7. NUOVO STACK DI PROTOCOLLO IT

[Fonte: GSMA – Securing the 5G Era]

Storicamente le reti degli operatori hanno utilizzato principalmente protocolli proprietari per la gestione della rete.

5GC passa a uno stack di protocollo basato su IP, consentendo l'interoperabilità con un numero più ampio di servizi e tecnologie in futuro.

I seguenti protocolli, schemi e processi saranno adottati in 5GC:

- *HTTP/2 su N32, sostituendo Diameter dal punto di riferimento S6a;*
- *TLS come ulteriore livello di protezione che fornisce comunicazioni crittografate tra tutte le funzioni di rete (NF) all'interno di una rete mobile pubblica terrestre (PUBLIC LAND MOBILE NETWORK [PLMN]);*
- *TCP come protocollo del livello di trasporto in sostituzione del SCTP.*
- *Framework RESTful con OpenAPI 3.0.0 come Interface Definition Language (IDL)*

Poiché questi protocolli sono utilizzati nel più ampio settore IT, è probabile che il loro utilizzo:

- *porti a una breve vulnerabilità alla sequenza temporale di sfruttamento e a un maggiore impatto delle vulnerabilità che si trovano all'interno di questi protocolli;*
- *ampli il potenziale pool di attaccanti; le reti core 4G e in particolare 3G traggono vantaggio dal fatto che gli aggressori abbiano poca esperienza con gli standard di proprietà utilizzati al loro interno.*

Gli schemi di segnalazione delle vulnerabilità, come il programma GSMA Coordinated Vulnerability Disclosure (CVD) programme, dovranno gestire l'ampliamento della portata di questi protocolli.

Una volta individuato, il tempo necessario per correggere le vulnerabilità rilevanti dovrebbe essere breve.

8. TECNOLOGIE VANTAGGIATE DAL 5G

[Fonte: GSMA – Securing the 5G Era]

VIRTUALIZZAZIONE

L'architettura di rete 5GC sarà basata sui servizi, il che significa che le operazioni della rete centrale possono essere eseguite tramite funzioni esterne alla rete dell'operatore, ad es. la nuvola (Cloud).

Questo è un importante cambiamento rispetto ai controlli di sicurezza della rete di base consolidati, tuttavia offre all'operatore l'opportunità di sfruttare le tecnologie di virtualizzazione.

Con questa opportunità arrivano nuovi vettori di minaccia con cui confrontarsi.

Dovrebbero essere presi in considerazione i tradizionali controlli della virtualizzazione, compreso l'isolamento del tenant e delle risorse.

Controlli di isolamento adeguati riducono il rischio di fuga di dati e l'impatto delle epidemie di malware consapevoli della virtualizzazione.

Vulnerabilità a livello di microprocessore hanno evidenziato che l'isolamento della locazione all'interno di un ambiente virtuale non è garantito, poiché tali inquilini dovrebbero essere alloggiati insieme in base ai requisiti di sicurezza, ad es. non ospitare inquilini di sicurezza di livello inferiore con quelli di sicurezza di alto livello.

La containerizzazione è una tecnologia di virtualizzazione a livello di sistema operativo che sta prendendo piede.

Il sistema operativo host limita l'accesso del container alle risorse fisiche, come CPU, storage e memoria, in modo che un singolo container non possa consumare tutte le risorse fisiche di un host. Riducendo così l'impatto degli attacchi alla disponibilità contro la piattaforma.

Tutte le tecnologie di virtualizzazione consentono la segmentazione della rete e l'isolamento delle risorse, garantendo la sicurezza e riducendo l'impatto di attacchi riusciti.

SERVIZI CLOUD

Basandosi su servizi virtualizzati, il cloud è un abilitatore chiave del 5G; l'architettura 5G è stata progettata per essere nativa del cloud in quanto offre elasticità e scalabilità.

L'uso della tecnologia cloud può complicare la catena di approvvigionamento e la catena di responsabilità.

È necessario seguire pratiche di codifica sicura per garantire che i dati non vengano trapelati e che il codice non possa essere utilizzato per sfruttare il provider di servizi cloud o la rete dell'operatore.

SEZIONAMENTO DELLA RETE

Lo slicing della rete consente all'operatore di personalizzarne il suo comportamento, adattando (slicing) la rete per servire casi d'uso specifici utilizzando lo stesso hardware.

È possibile prevedere diversi livelli di isolamento che vanno da un singolo nodo della rete centrale all'accesso radio completamente dedicato.

Ciascun tipo di isolamento deve essere integrato in fase di progettazione. Ad esempio, una fetta di rete per la chirurgia remota deve considerare la costante identificazione e autorizzazione reciproca per bloccare le minacce MITM (MAN IN THE MIDDLE), ma una fetta per la gestione dei contenuti AR/VR non richiederà lo stesso livello di sicurezza.

MOBILE IOT

Sebbene l'IoT sia già prevalente nelle reti 2G/3G/4G, il numero di connessioni IoT aumenterà esponenzialmente nel 5G.

Più grande non significa che i controlli di sicurezza debbano cambiare in modo significativo, tuttavia devono essere ridimensionati.

L'IoT deve essere codificato, distribuito e gestito in modo sicuro durante tutto il suo ciclo di vita.

La maggior parte dei servizi IoT condivide un'architettura comune e, in quanto tale, gli attacchi a cui sarà sottoposto ciascun servizio probabilmente rientreranno in tre scenari di attacco comuni:

1. *attacchi ai dispositivi (endpoint) tramite le applicazioni in esecuzione sul dispositivo, attacchi remoti da Internet e tramite attacco fisico;*
2. *attacchi alle piattaforme di servizio (es. cloud);*
3. *attacchi ai collegamenti di comunicazione (es. Cellular, WLAN, BLE air interface ecc.).*

ARTIFICIAL INTELLIGENCE (AI)

L'IA dovrebbe essere ampiamente utilizzata nelle reti 5G e dovrebbe favorire la sicurezza.

Gli operatori dovrebbero sfruttare MACHINE LEARNING (ML) e DEEP LEARNING (DL) per automatizzare il rilevamento di minacce e frodi.

L'uso dell'IA è particolarmente rilevante se si considerano i volumi di dati che le reti 5G genereranno.

L'IA potrebbe essere un modo più fattibile per mitigare i precedenti attacchi sconosciuti in tempo reale e può anche essere utilizzata per alimentare reti di autoriparazione in cui il sistema è in grado di identificare i problemi e intraprendere azioni automatizzate per fornire la soluzione.

Tuttavia, questa tecnologia è disponibile anche per l'attaccante e sono previsti attacchi basati sull'IA.

9. DESCRIZIONE/COMPONENTI DELL'ARCHITETTURA DEL SISTEMA DI RIFERIMENTO

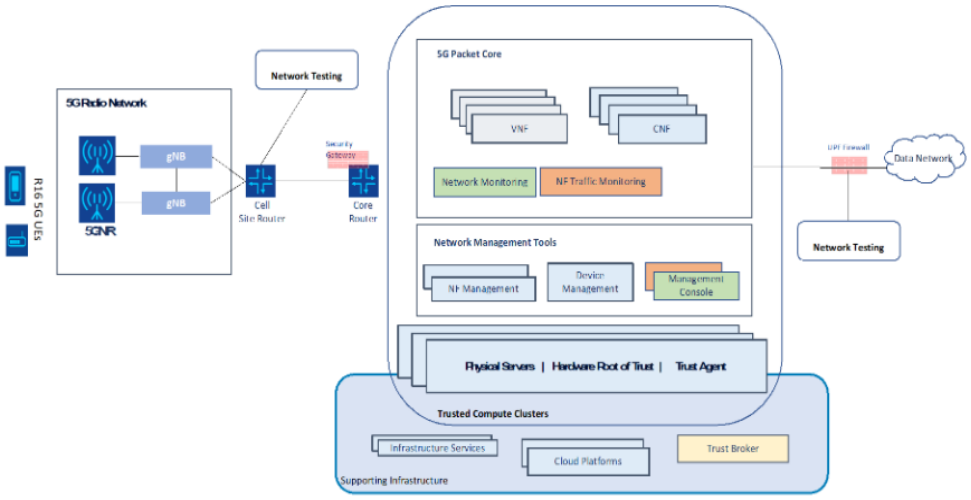
Questa sezione:

- *presenta i diagrammi preliminari dell'architettura per la progettazione del sistema, inclusi i diagrammi logici e fisici;*
- *spiega i componenti principali dell'architettura e riassume lo scopo delle interazioni dei componenti;*
- *inizia con l'architettura di implementazione 5G di alto livello e approfondisce le architetture della soluzione di sicurezza proposta.*
- *spiega le idee di base dell'architettura e non fornisce dettagli esaurienti di ogni componente dell'architettura e delle sue implicazioni sulla sicurezza ma saranno descritte nelle sezioni successive di questo volume e ne discutono le capacità di sicurezza dei componenti in modo più dettagliato.*

HIGH LEVEL ARCHITECTURE

La Figura 3-1 illustra l'architettura di alto livello dell'implementazione NCCoE 5G.

Figure 3-1 High-Level Architecture



Sul lato sinistro del diagramma c'è la rete d'accesso radio 5G.

*È costituito da apparecchiature utente (ovvero dispositivi mobili che utilizzano la rete 5G); radio e antenne; unità in banda base (*BASEBAND UNITS [BBU]*) note come* GNODEB (GNB)*, che generano segnali RF.*

A destra della rete di accesso radio, il diagramma mostra la rete di BACK HAUL*, la connessione tra la rete di accesso radio (cells site) e la rete centrale (data center).*

Il router del sito cellulare e il router principale denotano le due estremità della rete di Back Haul nella nostra implementazione di riferimento.

La terminazione della rete di Back Haul è un gateway di sicurezza opzionale, rappresentato come un firewall. Questo firewall fornisce un tunnel IPsec per proteggere la segnalazione e le comunicazioni del piano utente tra la rete di accesso radio e il core del pacchetto 5G.

Il data center, rappresentato al centro, ospita vari componenti che controllano e gestiscono la rete.

Il core del pacchetto 5G è costituito da numerose funzioni di rete 5G con varie responsabilità (ad es. autenticazione, mobilità, ricarica).

I protocolli e le funzioni del pacchetto core sono specificati negli standard 3GPP*.*

Il data center fornisce anche i servizi di base necessari per la configurazione, la gestione e la manutenzione di tutti i componenti di rete. Ciò include sia i servizi di infrastruttura (ad es. NETWORK FILE SYSTEM *[NFS],* FILE TRANSFER PROTOCOL *[FTP],* NETWORK TIME PROTOCOL *[NTP],* DOMAIN NAME SYSTEM *[DNS]) sia gli strumenti di gestione.*

Infine, il lato destro del diagramma mostra un firewall che collega il data center alla rete dati. Questo firewall protegge le funzioni di rete all'interno della rete centrale nel centro dati dagli attacchi basati su IP (Internet Protocol) provenienti da Internet. Inoltre, il firewall fornisce la topologia nascosta per gli indirizzi IP, quindi non sono direttamente accessibili da Internet.

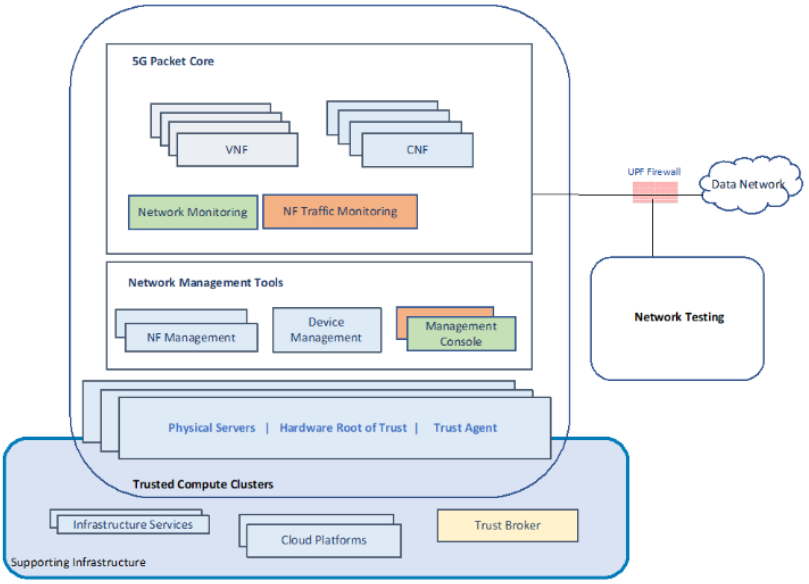
I nodi di test di rete mostrati nella Figura 3-1 consentono la convalida end-to-end dell'infrastruttura, dei servizi e della sicurezza convergenti wireless e cablata. Ad esempio, l'infrastruttura può essere sollecitata utilizzando connessioni simultanee di dati, video o voce osservando la velocità di connessione e il throughput degli utenti simulati.

Un nodo di test può fornire diversi tipi di traffico: legittimo, DDOS (DISTRIBUTED DENIAL OF SERVICE*) e malware. Può simulare protocolli applicativi del mondo reale e consente la personalizzazione e la manipolazione dei dati grezzi.*

DATA CENTER ARCHITECTURE

La Figura 3-2 fornisce una vista più dettagliata dell'architettura del data center specifica per l'implementazione 5G.

FIGURE 3-2 DATA CENTER ARCHITECTURE



Altre reti 5G potrebbero abilitare le stesse funzionalità descritte di seguito in un'architettura diversa o con tecnologie diverse.

Nella nostra soluzione proposta, il data center distribuisce tutte le funzioni di rete core a pacchetto 5G (NETWORK FUNCTION [NF]) come NF basate su macchine virtuali (VIRTUAL MACHINE BASED [VNF]) o NF basate su container (CONTAINER BASED [CNF]) utilizzando tecnologie di cloud computing.

Le piattaforme di calcolo che ospitano queste NF sono cluster di server con processori dei prodotti.

Il data center supporta e fornisce anche la connettività per gli strumenti e i prodotti utilizzati per fornire visibilità e controllo della sicurezza nel traffico di rete.

Questo è importante per il monitoraggio e l'applicazione sia dell'infrastruttura IT di supporto che dell'applicazione e del traffico di segnalazione che attraversa il sistema 5G.

Il data center utilizza più set di strumenti, servizi e piattaforme di cloud computing per abilitare la funzionalità dei carichi di lavoro di cui è responsabile per l'hosting.

Questa infrastruttura IT di supporto è mostrata nell'area "Supporting Infrastructure & Services" nella parte inferiore del diagramma.

Questi tipi di componenti sono spesso ignorati quando si parla di sistemi 5G, ma sono fondamentali per la sicurezza e le operazioni.

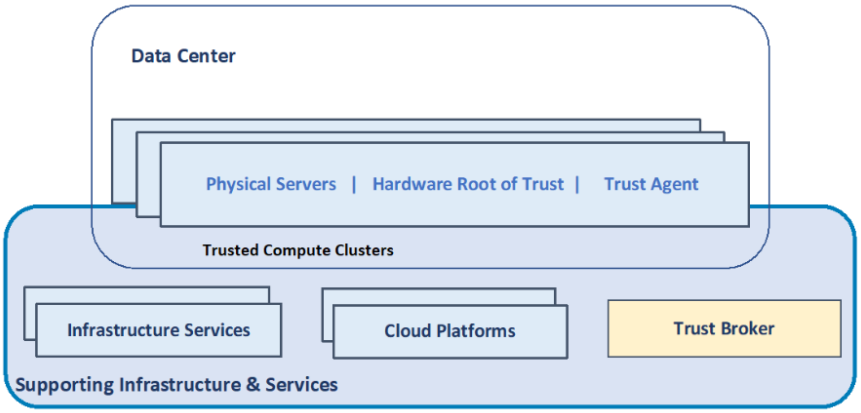
Questa infrastruttura IT è simile a quella utilizzata per le implementazioni di cloud computing e contiene le funzionalità di sicurezza descritte in questo documento.

Tutte le funzioni IT di supporto necessarie (servizi di directory, autorità di certificazione, file server, workstation di manutenzione, time server, servizi di backup e ripristino, ecc.) sono incluse nella "Service Box" di infrastruttura.

TRUSTED COMPUTE CLUSTER ARCHITECTURE

La Figura 3-3 illustra il sottoinsieme dell'ambiente di elaborazione fisico all'interno dell'architettura del data center 5G chiamato Trusted Compute Clusters. Questo nome indica che i server dispongono di funzionalità di root di attendibilità hardware abilitate.

FIGURE 3-3 TRUSTED COMPUTE CLUSTER ARCHITECTURE



Un server con HARDWARE ROOT OF TRUST (HROT) accoppiato con un hypervisor abilitato o un sistema operativo e un container runtime costituiscono la base per una piattaforma di elaborazione più sicura.

Questa piattaforma sicura:

1. *misura l'integrità del firmware, del sistema operativo (OS) e del gestore della macchina virtuale (Virtual Machine Manager [VMM]) all'avvio;*
2. *previene i rootkit o altri attacchi di basso livello,*
3. *stabilisce l'affidabilità del software del server e delle piattaforme host.*

Uno o più Trusted Compute Cluster possono essere utilizzati come base di elaborazione che ospiterà i carichi di lavoro delle funzioni di rete 5G come VNF o CNF.

Gli HRoT abilitano capacità di sicurezza aggiuntive per l'infrastruttura che supporta il 5G oltre a quanto definito nelle specifiche 3GPP.

Queste funzionalità includono controlli basati su hardware per:

1. *misurare l'integrità della piattaforma per ciascun server nell'infrastruttura;*
2. *assegnare etichette specifiche per ciascun server nell'infrastruttura per imporre l'isolamento dei carichi di lavoro critici;*
3. *attestare la misurazione e l'etichetta di ciascun server rispetto alle politiche, inserendo i risultati in un agente di orchestrazione delle politiche per segnalare, avvisare o applicare regole in base agli eventi.*

Queste funzionalità sono abilitate da più componenti nel diagramma, tra cui:

1. *meccanismi hardware per misurare crittograficamente i moduli hardware e firmware che compongono ciascun server;*
2. *un modulo di sicurezza hardware per memorizzare le misure crittografiche su ciascun server;*

3. *un meccanismo su ciascun server in grado di comunicare con il modulo di sicurezza hardware integrato e di riportare le misurazioni a un Trust Broker, abilitato dal sistema operativo o da software di terze parti;*
4. *un server di attestazione remoto, o Trust Broker, che raccoglie le misurazioni dei server nei Trusted Compute Clusters, assegna etichette a ciascun server e si integra con gli scheduler del carico di lavoro dei Trusted Compute Clusters.*

Questi componenti sono integrati insieme in modo che i carichi di lavoro 5G siano distribuiti su hardware affidabile designato per funzionalità specifiche.

Le tecnologie HRoT per gli scheduler del carico di lavoro utilizzano le misurazioni e le etichette della piattaforma come fattore di posizionamento del carico di lavoro.

Le funzionalità descritte in questa sezione si basano sulle tecniche descritte in NIST IR 8320, Hardware Enabled Security: Abilitazione di un approccio a più livelli alla sicurezza della piattaforma per casi d'uso di cloud ed edge computing.

Implementazioni di prototipi specifici per l'attestazione remota e la pianificazione e il posizionamento del carico di lavoro sono disponibili in NIST IR 8320A e NIST IR 8320B.

10. RISK ASSESSMENT

Questa sezione è preliminare e ancora in fase di sviluppo e cataloga le capacità di sicurezza tecnica incluse in questo progetto.

Successivamente, sono discusse le minacce e le vulnerabilità che ciascuna delle funzionalità di sicurezza tecnica intende affrontare.

Una volta completata, questa sezione fornirà un'analisi del rischio per l'architettura di riferimento e le sue funzioni e capacità di supporto.

Queste informazioni potrebbero essere utilizzate da un'organizzazione per informare la propria analisi del rischio e il processo decisionale in merito a come rispondere a ciascun rischio (ad esempio mitigare, accettare, trasferire, evitare).

SECURITY CATEGORY

Le categorie di sicurezza, descritte nella tabella 3-1, sono descrizioni di alto livello utilizzate per catalogare le capacità di sicurezza tecnica presa in considerazione da questa implementazione.

Queste categorie sono importanti e rilevanti per le reti 5G sia commerciali che private e includono sia le funzionalità di sicurezza definite dagli standard 3GPP, sia le capacità di sicurezza disponibili nell'infrastruttura cloud di supporto della rete.

TABLE 3-1 SECURITY CATEGORIES

Security Category	Reference
Infrastructure Security Category (ISC)	
Hardware Roots of Trust Packet Core	ISC-1
Hardware Roots of Trust Virtualized RAN	ISC-2
Infrastructure Recommended Practice	ISC-3
5G Standalone Security Category (5GSC)	
Subscriber Privacy	5GSC-1
Radio Network Security	5GSC-2
Authentication Enhancements	5GSC-3
Interworking & Roaming Security	5GSC-4
API Security	5GSC-5
Network Slicing Security	5GSC-6
Application Security	5GSC-7
Internet Security Protocol Recommended Practice	5GSC-8

SECURITY CAPABILITIES

Il termine capacità di sicurezza è utilizzato per descrivere una caratteristica di sicurezza tecnica importante e rilevante per le reti 5G commerciali o private.

Le funzionalità di sicurezza, descritte nella Tabella 3-2, nel contesto di questo documento includono sia le funzionalità di sicurezza definite dagli standard 3GPP sia le funzionalità di sicurezza disponibili nell'infrastruttura cloud di supporto della rete.

Per ciascuna capacità, la Tabella 3-2 elenca il suo identificatore di sottoriferimento univoco e fornisce una breve descrizione, che spiega anche la capacità.

TABLE 3-2 SECURITY CAPABILITIES

Security Capability	Subreference	Description
Infrastructure Security Categories		
Hardware Roots of Trust Packet Core, ISC-1		
Hardware-Based Platform Measurement	ISC-1.1	Measure platform integrity for each server in the infrastructure using hardware-based controls.
Hardware-Based Labeling	ISC-1.2	Assign specific labels for each server in the infrastructure using hardware-based controls.
Remote Platform Attestation	ISC-1.3	Attest each server's trust measurements and asset tags against policies, and allow services like workload orchestrators access to these findings so the results can be used as factors in workload placement/migration.
Network Function Orchestration Enforcement	ISC-1.4	Deploy and migrate NFs to servers that match platform measurements and labels.
Network Function Image Encryption	ISC-1.5	Encrypt each NF's image, and release the decryption keys only to servers that meet trust policies.
Infrastructure Recommended Practice, ISC-3		
Infrastructure Security Monitoring	ISC-3.1	Provide the visibility across the infrastructure needed to continuously monitor communications patterns, see threats within the extended network, and detect and respond to threats using methods such as behavioral modeling and supervised and unsupervised machine learning.
Network Segmentation	ISC-3.2	Ensure that the infrastructure design and implementation support keeping the different types of network traffic separate from each other.

5G Standalone Security Categories		
Subscriber Privacy, 5GSC-1		
Subscription Permanent Identifier (SUPI) Protection	5GSC-1.1	Encrypt the 5G SUPI with the public key of the home operator to create the Subscription Concealed Identifier (SUCI).
Reallocation of Temporary IDs	5GSC-1.2	Refresh a user device's temporary ID after initial registration, on every mobility registration update, and after use in paging.
Initial NAS Message Security	5GSC-1.3	After the initial service request message, security sensitive messages are re-sent encrypted in a Non-Access Stratum (NAS) Container so sensitive UE-specific information is not sent in the clear.
No SUPI-Based Paging	5GSC-1.4	Use a temporary identifier (5G-S-TMSI) as the basis of paging timing, not a permanent identifier (SUPI).
Respond to Identity Request with SUCI	5GSC-1.5	The network can request SUPI, but the UE only responds with SUCI and never sends SUPI.
Radio Network Security, 5GSC-2		
User Plane Integrity Protection	5GSC-2.1	Apply integrity protection to user plane traffic over the air at the full data rate using 5G's new capabilities.
Cryptographic Algorithms Recommended Practice	5GSC-2.3	Use strong algorithms for the air interface based on US operator-recommended practices.
Authentication Enhancements, 5GSC-3		
Native Extensible Authentication Protocol (EAP) Support	5GSC-3.1	Use access-agnostic authentication via EAP Method for 3rd Generation Authentication (EAP-AKA') to enable mutual authentication between the UE and the network, and to provide keying material that can be used between the UE and the serving network and between the UE and the home network in subsequent security procedures. While EAP support is new in 5G, the evolution of LTE's authentication, referred to as 5G AKA, will also be evaluated. Special EAP configurations like EAP-Transport Layer Security (EAP-TLS) are of interest for future project phases.
Non-3GPP Access	5GSC-3.2	Maintain one security context in the 5G core network for access from both 3GPP networks and non-3GPP networks, e.g., wireless local area networks (WLANs).
Hardware-Based Credential Storage	5GSC-3.3	Store pre-shared keys and credentials in the USIM software container running on tamper-resistant hardware in UEs in either embedded or physical Universal Integrated Circuit Cards (UICCs), commonly referred to as Subscriber Identity Module (SIM) cards.
Security Anchor Function (SEAF)	5GSC-3.4	The Security Anchor Function (SEAF) is collocated with the Access and Mobility Management Function (AMF) to provide primary authentication. The SEAF plays an important role in authentication while roaming and for non-3GPP access.
API Security, 5GSC-5		
API Security for Network Exposure Function (NEF)	5GSC-5.1	Securely expose network services such as voice, data connectivity, charging, and subscriber information to trusted (internal) and untrusted (third-party) applications over application programming interfaces (APIs), with standards defined and recommended practices for API security applied according to security profiles for Transport Layer Security (TLS) implementation and usage following the provisions given in clause 6.2 of 3GPP Technical Specification (TS) 33.210 [1].
Application Security, 5GSC-7		
Subscriber Traffic Security Monitoring	5GSC-7.1	Have complete visibility across the control and user planes. Correlate between UE traffic and permanent equipment identifiers (PEIs) and SUPIs.
User-Plane Security Enforcement	5GSC-7.2	Enforce authorized access for 5G implementing segmentation policies based on SUPI/PEI, Network Slice, Applications, and data. Provide inline network security protections for UE.
Internet Security Protocol Recommended Practice, 5GSC-8		
IPsec/NDS IP	5GSC-8.2	Protect communication between network entities/elements at the network layer via authentication and cryptographic secured Internet Protocol Security (IPsec) tunnels (e.g., communication within RAN, between RAN and core – backhaul, mid-haul and fronthaul and access from untrusted non-3GPP network to 5G core network).

MITIGATED THREATS AND VULNERABILITIES

Ciascuna funzionalità di sicurezza nella Tabella 3-2 ha lo scopo di aiutare a mitigare determinati tipi di minacce e vulnerabilità in modo da ridurre il rischio complessivo a un livello accettabile.

Questa sezione esplora le funzionalità di sicurezza in ordine e per ognuna, riassume le vulnerabilità e le minacce corrispondenti che aiuta ad affrontare e spiega brevemente come mitiga le minacce e le vulnerabilità.

INFRASTRUCTURE SECURITY

HARDWARE ROOTS OF TRUST PACKET CORE, ISC-1		
	Minaccia/Vulnerabilità	**Mitigazione**
ISC-1.1, misurazione della piattaforma basata su hardware	*Il BIOS (Basic Input/Output System) o il codice del firmware potrebbero essere alterati o sostituiti con codice dannoso dando a un utente malintenzionato il pieno controllo del sistema (ad esempio, un rootkit). Ulteriori componenti hardware possono essere aggiunti al sistema per consentire a utenti non autorizzati di accedere al sistema o ai suoi dati all'insaputa del proprietario del sistema.*	*Le misurazioni crittografiche basate su hardware forniscono un meccanismo per verificare l'integrità della composizione del sistema. È possibile misurare il BIOS, il firmware e i componenti hardware collegati in modo che sia noto lo stato di avvio noto e qualsiasi cambiamento o modifica possa essere facilmente rilevato.*
ISC-1.2, Etichettatura basata su hardware	*Senza alcun tipo di etichettatura dei sistemi che comprendono un pool di risorse di calcolo, i carichi di lavoro NF virtuali o containerizzati possono essere istanziati su qualsiasi host all'interno del pool di risorse. Le etichette software vengono spesso applicate a sistemi o insiemi di sistemi per designarli per carichi di lavoro specifici; tuttavia, le etichette vengono spesso applicate a livello di sistema operativo, che può essere aggirato su un sistema compromesso.*	*L'etichettatura dei sistemi basata su hardware fornisce etichette univoche definite dall'utente applicate ai sistemi. Queste etichette possono aiutare a identificare un sistema in base a qualsiasi insieme di attributi, ad esempio informazioni sulla posizione e identificatori univoci per carichi di lavoro specifici. Inoltre, queste etichette, dette anche asset tag, sono firmate crittograficamente e archiviate in hardware a prova di manomissione, che può essere utilizzato per dimostrare l'integrità e la proprietà di queste etichette.*
ISC-1.3, Attestazione piattaforma remota	*I data center sono generalmente costituiti da migliaia di server e tenerne traccia e il rispettivo firmware è un compito arduo per un operatore. Senza la gestione centralizzata delle piattaforme server, potrebbero essere apportate modifiche non approvate al loro firmware e non essere rilevate dall'operatore del data center.*	*L'attestazione della piattaforma remota fornisce l'imposizione di quali componenti possono essere eseguiti su piattaforme server su tutti i sistemi hardware in un data center. Sebbene ISC-1.1 e ISC-1.2 forniscano meccanismi di integrità, non affrontano il monitoraggio centralizzato di tutti i sistemi. La possibilità di verificare rispetto a un elenco di autorizzazioni collettivo di piattaforme server e dei componenti firmware associati, rispetto a un sistema locale che applica una politica della catena di approvvigionamento, offre agli operatori maggiore flessibilità e controllo in modo crittograficamente protetto. Questi meccanismi di applicazione possono incorporare le misurazioni e*

		l'etichettatura della piattaforma basata su hardware in queste politiche di sicurezza. Inoltre, il server di attestazione remoto può anche essere considerato un Trust Broker poiché altri servizi possono interrogarlo per ottenere lo stato di attendibilità dei server nel data center.
ISC-1.4, Applicazione dell'orchestrazione delle funzioni di rete	*I carichi di lavoro NF potrebbero potenzialmente essere istanziati o migrati su server di elaborazione con vulnerabilità o versioni firmware non consentite o al di fuori di un confine logico.*	*I pianificatori dell'orchestrazione del carico di lavoro integrati con un broker fiduciario utilizzano le misurazioni dell'attendibilità e i tag delle risorse come fattori di posizionamento del carico di lavoro. Questo aiuta a garantire che i carichi di lavoro NF vengano istanziati o migrati solo su server di calcolo con misurazioni di affidabilità conformi e tag asset che hanno la loro fiducia radicata nell'hardware.*
ISC-1.5, Crittografia dell'immagine della funzione di rete	*Le immagini del carico di lavoro sono spesso archiviate in una posizione di archiviazione condivisa e possono contenere informazioni riservate o proprietarie. Una violazione dei dati potrebbe verificarsi se le immagini vengono consultate o copiate su un altro sito da un utente non autorizzato.*	*Le immagini del carico di lavoro NF vengono crittografate nella posizione di archiviazione condivisa e solo i server di elaborazione che soddisfano i criteri di sicurezza predefiniti hanno accesso alle chiavi di decrittografia quando ospitano il carico di lavoro NF. Ciò garantisce che solo la piattaforma di hosting possa decrittografare un'immagine del carico di lavoro e accedere alle sue informazioni. Inoltre, la politica di sicurezza per l'accesso alle chiavi di decrittografia include fattori come lo stato di attendibilità e il tag asset e si integra con Trust Broker per ottenere queste informazioni prima di rilasciare una chiave di decrittografia.*
INFRASTRUCTURE RECOMMENDED PRACTICE, ISC-3		
	Minaccia/Vulnerabilità	**Mitigazione**
SC-3.1, Monitoraggio della sicurezza delle infrastrutture	*Le minacce all'infrastruttura potrebbero includere un malintenzionato o un insider che tenta di ottenere o ottenere un accesso non autorizzato senza essere rilevato. Esempi di attacchi potrebbero includere DDoS, man in the middle, escalation dei privilegi, ransomware, rilevamento di anomalie comportamentali, malware e minacce interne. Senza capacità di monitoraggio o rilevamento per trovarli, questi attacchi potrebbero continuare a persistere o peggiorare.*	*Utilizza gli strumenti di monitoraggio della sicurezza dell'infrastruttura che consentono visibilità e informazioni dettagliate sull'infrastruttura e aiutano a identificare le attività sospette. Gli strumenti possono fornire un modo efficiente per rilevare e tenere traccia dei rischi per la sicurezza in modo che l'organizzazione possa intraprendere azioni preventive.*
ISC-3.2, Segmentazione della rete	*Diversi tipi di traffico attraversano la rete 5G, come operazioni infrastrutturali, gestione NF e dati utente. Senza la segmentazione della rete, un normale utente 5G potrebbe potenzialmente interagire con i componenti gestionali e operativi della rete 5G.*	*La segmentazione della rete applica i controlli di accesso a diverse porzioni della rete 5G. Questa tecnica crea segmenti di rete isolati per ogni tipo di traffico all'interno della rete 5G per impedire l'accesso non autorizzato ad altri tipi di traffico.*

5G STANDALONE SECURITY

SUBSCRIBER PRIVACY, 5GSC-1		
	Minaccia/Vulnerabilità	**Mitigazione**
GSC-1.1, Protezione dell'identificatore permanente dell'abbonamento (SUPI).	*Un catcher International Mobile Subscriber Identity (IMSI) è un tipo di stazione base falsa utilizzata per intercettare le informazioni di identificazione dell'abbonato di telefoni cellulari. Essenzialmente una torre mobile "falsa" che impersona il fornitore di servizi, inganna un telefono facendogli inviare la sua identità di abbonato permanente LTE chiamata IMSI. Il falso operatore della stazione base può utilizzare queste informazioni per tracciare la posizione degli abbonati mobili.*	*Se utilizzata senza lo schema di cifratura nullo, questa funzione 5G crittografa l'identificatore permanente dell'abbonamento 5G (Subscription Permanent Identifier [SUPI]) con la chiave pubblica dell'operatore di casa per creare l'identificatore nascosto dell'abbonamento (Subscription Concealed Identifier [SUCI]). Ciò impedisce che l'identificatore permanente (Permanent Identifier [SUPI]) sia inviato in chiaro e rende le informazioni inutilizzabili per il tracciamento degli abbonati.*
5GSC-1.2, Riallocazione di ID temporanei	*Negli attacchi informatici passivi degli abbonati, gli attori malintenzionati raccolgono più identificatori temporanei univoci globali (Global Unique Temporary Identifiers [GUTI]) che possono essere utilizzati per scopi diversi. Un esempio è verificare la presenza di un abbonato in una determinata area e un altro è rivelare i suoi movimenti passati in quell'area e consentire il tracciamento dei movimenti futuri. Quando gli ID temporanei come GUTI non sono aggiornati abbastanza frequentemente, diventano ID quasi permanenti.*	*Questa funzione 5G fornisce un aggiornamento coerente dell'identificatore temporaneo di un dispositivo utente nelle seguenti condizioni: procedure di paging, registrazione iniziale e aggiornamento della registrazione della mobilità. La rete può essere configurata per allocare anche una nuova GUTI dopo ogni richiesta di servizio dell'UE (**User Equipment**). La disposizione più sicura è quando una UE ottiene una nuova GUTI ogni volta che ha utilizzato la sua GUTI in chiaro sull'interfaccia radio. Ciò garantisce che gli ID temporanei non possano essere utilizzati per il monitoraggio degli abbonati.*
5GSC-1.3, Sicurezza messaggio NAS iniziale	*Gli strati inferiori specifici della tecnologia radio (ad esempio, comunicazione tra UE e gNB) del protocollo di comunicazione sono chiamati strato di accesso (Access Stratum [AS]), mentre gli strati superiori radio-agnostici (ad esempio, comunicazione tra UE e Core) sono chiamati strato di non accesso (Non-Access Stratum [NAS]). Il messaggio NAS iniziale è il primo messaggio NAS inviato dopo che l'UE è passata dallo stato inattivo. La richiesta di servizio è un tipo di messaggio NAS iniziale. Se tutte le parti di un messaggio NAS iniziale vengono inviate in chiaro, alcune informazioni specifiche dell'UE potrebbero essere sfruttate.*	*Gli standard 5G impongono che quando l'UE non ha un contesto di sicurezza NAS (cioè, non ha chiavi di crittografia o integrità valide), invii un insieme limitato di elementi di informazione (chiamati IE di testo in chiaro), compresi quelli necessari per stabilire la sicurezza nel messaggio iniziale. D'altra parte, quando l'UE ha già un contesto di sicurezza (cioè, ha chiavi di crittografia o integrità valide), l'UE deve inviare un messaggio che ha il messaggio NAS iniziale completo cifrato in un contenitore NAS insieme agli IE in chiaro, con l'integrità dell'intero messaggio è protetta.*
5GSC-1.4, nessun cercapersone basato su SUPI	*La rete avvisa un cellulare per chiamate o messaggi in arrivo utilizzando un messaggio cercapersone. Nelle precedenti generazioni di reti mobili, questo messaggio di paging poteva contenere l'identificatore permanente dell'abbonato. Gli attacchi al protocollo di paging possono avere gravi ripercussioni. Ad esempio, potrebbe consentire a un aggressore*	*Prima del 5G, i tempi di paging erano in genere determinati sulla base di un identificatore a lungo termine (permanente) (IMSI). Il 5G determina sempre i tempi di paging in base a un identificatore temporaneo (chiamato 5G-S-TMSI). In altre parole, il 5G non ha il paging basato su SUPI.*

	di dedurre la posizione di una vittima in base all'identificatore permanente della vittima o iniettare avvisi di emergenza fabbricati.	
5GSC-1.5, Rispondere alla richiesta di identificazione con SUCI	*In LTE, la rete può richiedere l'identità di una UE durante determinate procedure e impostare specificamente il tipo di ID mobile richiesto come identificatore permanente (IMSI). L'UE è quindi tenuta a rispondere con un messaggio di risposta di identità contenente l'IMSI richiesto nel testo in chiaro. Ciò potrebbe consentire a una stazione base falsa di recuperare l'identità permanente dell'UE.*	*In 5G, la rete non può impostare il tipo di ID mobile richiesto come identificatore permanente in chiaro (SUPI). Tuttavia, può impostare il tipo di ID mobile richiesto come identificatore permanente nascosto (SUCI). Ciò significa che nel messaggio di risposta, l'UE sarà in grado di nascondere il suo identificatore permanente se l'operatore ha abilitato questa caratteristica di sicurezza configurando uno schema SUCI appropriato.*
RADIO NETWORK SECURITY, 5GSC-2		
	Minaccia/Vulnerabilità	**Mitigazione**
5GSC-2.1, Protezione dell'integrità del piano utente	*L'integrità del traffico del piano utente tra il dispositivo e la rete non era protetta nelle generazioni precedenti. Ad esempio, in un noto attacco LTE denominato aLTEr, un attore malintenzionato può modificare il payload del messaggio e può reindirizzare le richieste DNS e quindi eseguire un attacco di spoofing DNS.*	*Nel 5G, la protezione dell'integrità del piano utente tra il dispositivo e la rete è stata introdotta come nuova funzionalità, a complemento della protezione della riservatezza esistente del traffico del piano utente. L'abilitazione della protezione dell'integrità del piano utente previene questo tipo di minaccia. Il supporto di questa funzionalità è obbligatorio sia per il dispositivo che per la rete, mentre l'utilizzo è facoltativo e sotto il controllo dell'operatore.*
5GSC-2.3, Pratica consigliata per algoritmi crittografici	*Un operatore di rete è limitato agli algoritmi crittografici supportati nelle apparecchiature distribuite nelle sue reti. Se gli algoritmi configurati per l'uso dovessero risultare in qualche modo deboli, il sistema potrebbe essere a rischio.*	*Il 5G supporta gli stessi algoritmi crittografici disponibili per l'uso in LTE. Secondo le specifiche 3GPP, le apparecchiature di rete 5G devono supportare un algoritmo basato su Advanced Encryption Standard (AES) e un algoritmo basato su SNOW3G. Il sistema supporta il passaggio tra algoritmi implementati nell'apparecchiatura di rete. Questo interruttore potrebbe essere attivato se l'algoritmo configurato per l'uso in una rete risulta debole. Ciò porta una certa agilità intrinseca dell'algoritmo al sistema 5G.*
AUTHENTICATION ENHANCEMENTS, 5GSC-3		
	Minaccia/Vulnerabilità	**Mitigazione**
GSC-3.1, Native Extensible Authentication Protocol (EAP) Support	*Nelle generazioni precedenti, solo AKA veniva utilizzato per l'autenticazione primaria per autenticare reciprocamente l'UE e la rete. La chiave non era associata al nome della rete di servizio. Pertanto, potrebbero verificarsi vari tipi di problemi di sicurezza, come una rete di servizio compromessa e/o una chiave utilizzata per l'accesso non autorizzato, ad esempio roaming e frodi non in roaming.*	*Gli standard 5G specificano l'uso dell'autenticazione indipendente dall'accesso utilizzando EAP-AKA' per consentire l'autenticazione reciproca tra l'UE e la rete e fornire materiale di codifica che può essere utilizzato tra l'UE e la rete di servizio nelle successive procedure di sicurezza. EAP-AKA' lega il nome della rete di servizio alla chiave, impedendo l'accesso non autorizzato. EAP-AKA' è supportato per le tecnologie di accesso 3GPP e non 3GPP. Si noti che EAP-AKA' impedisce anche di ridurre gli attacchi a versioni precedenti di EAP.*

5GSC-3.2, Accesso non 3GPP	*Gli abbonati alla rete 5G possono accedere ai servizi 5G tramite reti di accesso non 3GPP. Le reti non 3GPP700, come il Wi-Fi, possono essere soggette a vari tipi di attacchi alla sicurezza, inclusi punti di accesso falsi per il dirottamento di sessioni utente legittime e attacchi di intercettazione.*	*Un contesto di sicurezza comune viene mantenuto nella rete principale 5G quando una UE si connette da entrambe le reti 3GPP e non 3GPP. In 5G, la funzione di interlavoro non 3GPP (N3IWF) viene utilizzata per l'accesso da reti non 3GPP non attendibili. Per gli accessi non 3GPP, i tunnel IPsec possono essere utilizzati per proteggere l'abbonato e segnalare il traffico dal punto di accesso non 3GPP all'N3IWF.*
5GSC-3.3, archiviazione delle credenziali basata su hardware	*Gli standard 5G specificano che le chiavi a lungo termine e la chiave pubblica della rete domestica devono essere archiviate nell'Universal Subscriber Identity Module (USIM) nell'UE. L'USIM è un contenitore software in esecuzione su un UICC, spesso indicato come scheda SIM. Per le reti 5G che utilizzano EAP-AKA o 5G-AKA, tutte le chiavi crittografiche eccetto la chiave di crittografia SUCI nei protocolli 3GPP sono derivate dalla chiave a lungo termine precondivisa. Una USIM può essere rimovibile (scheda SIM fisica) o incorporata (eSIM). Le chiavi a lungo termine memorizzate nel dispositivo sono bersagli preziosi per gli avversari. Se le chiavi sono compromesse, il traffico di abbonati 3GPP protetto e il traffico di segnalazione possono essere intercettati dall'avversario. Alcuni esempi di attacchi noti contro le chiavi sono attacchi del canale laterale.*	*La protezione della chiave a lungo termine è importante. La sicurezza fisica dei dispositivi mobili può proteggere le chiavi dagli attacchi del canale laterale. In 5G, agli USIM viene fornita una chiave crittografica a lungo termine e pre-condivisa denominata K. Questa chiave è archiviata all'interno dell'USIM a prova di manomissione e all'interno della rete principale (in Authentication Credential Repository and Processing Function [ARPF]) . La riservatezza della chiave a lungo termine è protetta all'interno dell'USIM e dell'ARPF e la chiave non è mai resa disponibile in chiaro al di fuori di tali posizioni. Si noti che la stessa capacità esiste nelle precedenti generazioni di reti 3GPP come 4G.*
5GSC-3.4, Funzione di ancoraggio di sicurezza (SEAF)	*Nelle precedenti generazioni di reti 3GPP, la componente SEAF (Security Anchor Functions) non era presente. Negli scenari di roaming, la rete di servizio (nella Public Land Mobile Network [PLMN] visitata) potrebbe prendere decisioni sull'autenticazione delle UE. Ciò ha creato una superficie di attacco in cui un avversario potrebbe utilizzare una rete di servizio non attendibile per autorizzare in modo fraudolento le UE.*	• *5G introduce i metodi di autenticazione EAP-AKA' e 5G-AKA utilizzando SEAF che prevengono gli attacchi di cui sopra abilitando il controllo domestico dell'autenticazione UE. La funzione del server di autenticazione (AUSF) nella PLMN domestica prende la decisione finale sull'autenticazione UE.* • *SEAF supporta l'autenticazione primaria dell'UE. SEAF supporta anche la riautenticazione dell'UE quando si sposta tra diverse reti di accesso (RAN nella stessa PLMN) o addirittura serve reti (in scenari di roaming) senza dover rieseguire l'autenticazione completa.* • *SEAF detiene la chiave di ancoraggio o la chiave radice per ciascuna UE in entrambi gli scenari in roaming e non in roaming. La chiave di ancoraggio è associata al nome della rete di servizio. SEAF deve autenticarsi presso l'AUSF della rete domestica. Riceve la chiave di ancoraggio dall'AUSF nella PLMN domestica durante la procedura di autenticazione e riautenticazione primaria dell'UE se l'autenticazione ha esito positivo.*

API SECURITY, 5GSC-5		
	Minaccia/Vulnerabilità	**Mitigazione**
GSC-5.1, Sicurezza API per la funzione di esposizione alla rete (NEF)	• *Nelle precedenti generazioni di reti 3GPP, la sicurezza per un meccanismo di esposizione della rete standardizzato non era definita. Anche se la Service Capability Exposure Function (SCEF) è stata introdotta nelle specifiche 3GPP R13 per standardizzare l'accesso alle API di terze parti, è stata utilizzata principalmente per i servizi relativi ai dispositivi Internet of Things (NB-IoT) a banda stretta.* • *Le informazioni sensibili nella rete come il nome della rete dati (DNN), le informazioni sull'assistenza alla selezione di singole sezioni di rete (S-NSSAI) e i dati degli abbonati come SUPI possono essere involontariamente esposti tramite l'interfaccia N33.*	*NEF funge da gateway sicuro per le funzioni applicative (AF) di terze parti (interne) e non attendibili (esterne) per esporre vari servizi come analisi, instradamento del traffico utente, posizione UE, raggiungibilità e informazioni relative alla mobilità. Autentica e autorizza i servizi richiesti dagli AF. Gli standard 5G impongono l'integrità, la riproduzione e la protezione della riservatezza per la comunicazione tra NEF e AF. Gli standard 5G impongono inoltre la connessione da NEF ad AF per supportare TLS e l'uso dell'autenticazione reciproca basata su certificati tra AF di terze parti e NEF. NEF maschera le informazioni sensibili sulla rete 5G come DNN, S-NSSAI e le informazioni sensibili sugli abbonati come SUPI dagli AF di terze parti.*
APPLICATION SECURITY, 5GSC-7		
	Minaccia/Vulnerabilità	**Mitigazione**
5GSC-7.1, Monitoraggio della sicurezza del traffico degli abbonati	*Sebbene gli operatori di rete mobile e le imprese abbiano visibilità sul loro traffico di mobilità, gli attori malintenzionati possono aggirare i meccanismi di rilevamento di un operatore. Ciò crea vulnerabilità per i centri operativi di rete e di sicurezza (rispettivamente NOC e SOC) incapaci di rilevare l'uso delle risorse di rete da parte di un attore malintenzionato. I dispositivi di rete infetti utilizzano in modo dannoso le risorse di rete per il traffico Command-and-Control (C2), che influisce sulle prestazioni della rete e delle applicazioni. Durante gli eventi di sicurezza come gli attacchi DDoS generati dall'UE, i team di risposta alla sicurezza non sono in grado di correlare il traffico botnet o il traffico correlato agli DDoS ai singoli abbonati o alle apparecchiature.*	*L'ispezione del traffico del piano utente e del piano di controllo consente una visibilità contestuale del traffico di rete. L'ispezione degli eventi Packet Forwarding Control Protocol (PFCP) o dei messaggi SMF (Session Management Function) e la loro correlazione con i tunnel GTP-U (General Packet Radio Service) Tunneling Protocol User (GTP-U) consente di mappare SUPI e PEI al traffico di rete. Quando queste informazioni sono associate ai risultati di C2, gli analisti di SOC e NOC di ispezione di vulnerabilità, antivirus e botnet hanno una visione chiara degli utenti malintenzionati. Una volta che queste informazioni sono state raccolte e analizzate da più fonti e monitorate nel tempo, è possibile stabilire una chiara comprensione di quali tipi di dispositivi e utenti causano problemi e cosa provoca tali problemi. Ciò si traduce in un'analisi della causa principale più rapida per gli incidenti di sicurezza della rete.*
5GSC-7.2, Applicazione della sicurezza del piano utente	• *Il malware può essere distribuito tramite una serie di meccanismi, come download incorporati in e-mail o contenuto SMS (Short Message Service), download da siti Web o applicazioni dannosi o persino da hardware dannoso.* • *Il software dannoso installato su UE può causare una serie di problemi sulla rete. Il software dannoso può utilizzare la rete per comunicare con i server C2, causando*	• *Per interrompere la distribuzione di malware da Internet, il traffico in ingresso deve essere ispezionato da un'appliance di sicurezza in grado di eseguire l'analisi del malware e il controllo dei file. L'utilizzo di metodi di rilevamento basati sulle firme è un modo accurato per rilevare il malware noto. Per identificare rapidamente il malware sconosciuto, l'utilizzo di un approccio multi-metodo è il più accurato, associando l'analisi statica e dinamica all'apprendimento*

	congestione sulla rete mobile. L'apparecchiatura utente infetta può anche essere utilizzata come botnet per causare a801 Attacco DDoS contro il 5G Core o risorse e applicazioni di rete. • *L'UE sulla rete può essere utilizzata per accedere ed esfiltrare dati sensibili. L'UE potrebbe anche essere utilizzata per attaccare o accedere a servizi di rete non autorizzati. Con il traffico controllato, UE può anche essere utilizzata per accedere a siti Web dannosi o utilizzare applicazioni SaaS (Software-as-a-Service) non approvate.*	*automatico per ridurre la latenza e i tempi di elaborazione.* • *Ispezionare il traffico del piano utente e analizzarlo rispetto a firme C2 note, domini dannosi noti e algoritmi di generazione di domini è un ottimo modo per identificare il traffico C2. L'implementazione di un'appliance di sicurezza in grado di rilevare e prevenire questo tipo di traffico aiuta a garantire la continuità della rete.* • *Il modo migliore per proteggere dati, applicazioni, risorse e servizi è rimuovere la fiducia implicita attraverso l'architettura zero trust (ZTA) per le reti 5G. La corretta implementazione di 5G ZTA richiede l'implementazione di politiche di controllo granulari su un Policy Enforcement Point (PEP). Il PEP dovrebbe ispezionare tutto il traffico del piano utente e consentire solo il traffico benigno che supporta i casi d'uso aziendali. Le politiche di controllo granulare sono definite con un soggetto completo di attributi 5G come SUPI, PEI, applicazione o servizio. L'implementazione del PEP in N3 combinato con i dati di N4 o N11 consente di correlare e applicare le politiche che contengono SUPI e PEI.*
INTERNET SECURITY PROTOCOL RECOMMENDED PRACTICE, 5GSC-8		
	Minaccia/Vulnerabilità	**Mitigazione**
5GSC-8.2, IPsec/NDS IP	• *Quando IPsec non viene utilizzato nella rete 5G, i dati sensibili degli abbonati e i dati di segnalazione potrebbero essere vulnerabili alle intercettazioni se inviati non crittografati, ad esempio, connessioni di backhaul e su rete di accesso non 3GPP.* • *Quando IPsec viene utilizzato con una configurazione errata, è possibile creare una connessione non sicura utilizzando protocolli o algoritmi deboli o compromessi. Ad esempio, le chiavi precondivise (PSK) potrebbero consentire a una terza parte di decrittografare il traffico intercettato se una rete è configurata per l'utilizzo di chiavi deboli. Le chiavi potrebbero essere trapelate se inviate tramite connessioni non protette o se archiviate non crittografate. Il protocollo Internet Key Exchange versione 1 (IKEv1) potrebbe essere vulnerabile agli attacchi dei dizionari offline se viene utilizzato un PSK debole. Sia IKEv1 che IKEv2 potrebbero essere vulnerabili agli attacchi di amplificazione DDoS a causa di un'implementazione errata del protocollo.*	• *IPsec è una suite di standard aperti per garantire comunicazioni private su reti pubbliche. Si tratta di un comune controllo di sicurezza a livello di rete generalmente utilizzato per crittografare il traffico IP tra host in una rete e per creare una rete privata virtuale (VPN). I tunnel IPsec vengono utilizzati nelle reti 5G per fornire agli abbonati e al traffico di segnalazione integrità, riservatezza e protezione della riproduzione per la connessione backhaul e altre connessioni, come l'accesso alla rete non 3GPP non attendibile. Gli standard 3GPP impongono l'uso dell'integrità dei dati e della protezione anti-riproduzione per IPsec. La riservatezza è facoltativa per IPsec in determinati scenari. Per un elenco completo delle opzioni di configurazione consigliate per i protocolli IPsec e IKE, fare riferimento alla tabella 1 di "NIST SP 800-77".* • *Gli standard 5G specificano che IPsec potrebbe essere utilizzato per proteggere i non SBI.*

11. DIMOSTRAZIONE DELLE CARATTERISTICHE DI SICUREZZA

Questa sezione descriverà come ogni scenario dimostra la caratteristica/categoria di sicurezza e le capacità/proprietà di sicurezza associate.

Questa sezione sarà scritta per una futura bozza.

PRESUPPOSTI E LIMITAZIONI

Questa sezione sui limiti dello scenario dimostrativo verrà scritta per una bozza futura.

SCENARI DI DIMOSTRAZIONE FUNZIONALE

Questa sezione descriverà brevi scenari di dimostrazione funzionale.

Includerà tutti gli scenari funzionali che sono abilitati dall'attuale architettura del sistema e indicherà quelli aggiuntivi che sono pianificati per dopo.

Il funzionamento di ciascuna funzionalità di sicurezza per la soluzione di esempio sarà verificato nel contesto dello scenario dimostrativo descritto di seguito, nonché per ulteriori scenari da aggiungere a una bozza futura.

SCENARIO 1 - IMPLEMENTAZIONE 5G SA UTILIZZANDO UN'UNICA PLMN

Questa sezione fornirà una breve panoramica delle apparecchiature, dell'architettura e del flusso delle chiamate utilizzati in questo scenario.

La funzionalità di dati, voce e video verrà testata per il caso non in roaming.

Dettagli specifici saranno descritti nel piano dimostrativo funzionale.

DATA CALL

Questa sezione fornirà una breve panoramica dell'impostazione della chiamata dati.

Informazioni dettagliate sulla procedura di test e sui risultati dei test per la chiamata dati 5G saranno descritte nel piano di dimostrazione funzionale.

> ***Nel mondo reale, questo test equivale a un abbonato che naviga in un sito Web su Internet o invia un'e-mail a un altro abbonato.***

VOICE OVER IP CALL

Questa sezione fornirà una breve panoramica dell'impostazione della chiamata VoIP.

Informazioni dettagliate sulla procedura di test e sui risultati dei test per la chiamata 5G VoIP saranno descritte nel piano di dimostrazione funzionale.

> ***Nel mondo reale, questo test equivale a un abbonato che effettua una chiamata VoIP su Internet a un altro abbonato.***

VIDEO STREAMING

Questa sezione fornirà una breve panoramica dello streaming video

Informazioni dettagliate sulla procedura di test e sui risultati dei test per lo streaming video 5G saranno descritte nel piano di dimostrazione funzionale.

Nel mondo reale, questo test equivale a un abbonato che effettua una richiesta di video on demand per un particolare file video a un server di streaming video su Internet.

RISULTATI

Questa sezione evidenzierà in che modo le capacità di sicurezza istanziate nella dimostrazione dell'architettura del sistema affrontano i rischi per la sicurezza che si intendeva supportare.

Questa sezione sarà scritta per una futura bozza.

12. APPENDICE A – SECURITY CONTROL MAP

Questa appendice fornirà tabelle che mappano le capacità di sicurezza informatica delle tecnologie utilizzate per la prima fase della soluzione di esempio alla guida NIST applicabile.

Questa appendice sarà aggiunta a una futura bozza.

13. APPENDICE B – FUTURE CAPABILITIES

Ci sono molte funzionalità di sicurezza aggiuntive che saranno incorporate durante questo progetto.

La sezione Security Capabilities descrive quelli che sono previsti per la prima fase del progetto.

Questa appendice descrive funzionalità di sicurezza aggiuntive pianificate provvisoriamente per la fase successiva.

Security Capability	Subreference	Description
Infrastructure Security		
Hardware Roots of Trust Packet Core, ISC-1		
Network Function Policy Enforcement	ICS-1.6	Technically enforce policies that define the servers in the compute environment where NFs can run based on trust values and asset tags.
5G Standalone Security		
Radio Network Security, 5GSC-2		
CU/DU Split	5GSC-2.2	Split gNB into Central Unit (CU) and Distributed Unit (DU), with the CU performing security functions (confidentiality/integrity) and being located closer to the core.
Security Visibility	5GSC-2.4	Enable applications to check the security being applied to the radio connection.
256-Bit Algorithms	5GSC-2.5	Use stronger cryptographic algorithms on this interface once they are adopted by 3GPP SA3.
Interworking & Roaming Security, 5GSC-4		
Security Edge Protection Proxy (SEPP)	5GSC-4.1	Implement application-layer security for the service layer information exchanged between two PLMNs. Provide security functions for integrity, confidentiality, replay protection, mutual authentication, authorization, negotiation of cipher suites, and key management, as well as the notion of topology hiding and spoofing protection.
5G to LTE Interworking Mobility Within the Same Operator Network	5GSC-4.2	Use secure procedures and security demarcations to secure LTE to 5G interworking as defined in 3GPP 23.501 [18]. Includes protecting the transmission of security keying materials between LTE and 5G.
5G to LTE Interworking Mobility Across Operator Networks	5GSC-4.3	Protects handovers involving 5G to LTE internetworking across two operators' network using N26 because 4G does not offer subscription identities encryption, so a UE moving from 5G to LTE will be subject to IMSI catching attacks. GSMA has not finalized work on 5G SA to LTE roaming across different operators.
API Security, 5GSC-5		
Common API Framework (CAPIF)	5GSC-5.2	Use secure interfaces, such as TLS-PSK, TLS-PKI and TLS-OAuth, provided by a common API interface between internal functions and external functions. Use CAPIF Core Function (CCF) to manage all internal and external APIs.
Network Slicing Security, 5GSC-6		
Network Slice Resource Isolation	5GSC-6.1	Enable the creation of multiple logical networks over the same physical infrastructure. Demonstrate orchestrated deployment and configuration of network functions to provide services that are required for a specific usage scenario. Tie into infrastructure security capabilities to isolate slice resources.
Network Slice Additional Authentication	5GSC-6.2	Perform secondary authentication with Network Slice Specific Authentication and Authorization Function (NSSAAF) to check if the user is authorized to use that slice (3GPP TS 29.526). Do additional authentication of subscriber identity.
Application Security, 5GSC-7		
Application Security Onboarding	5GSC-7.3	Ensure that applications are onboarded securely and that communications between applications are secure. Leverage the zero trust concept.
Internet Security Protocol Recommended Practice, 5GSC-8		
TLS Security	5GSC-8.1	Implement TLS security where possible to protect NF communication at the transport layer via mutual authentication and transport security. Ensure protection of the communication's confidentiality and integrity, and implement anti-replay measures.
DNSSEC	5GSC-8.3	Use DNS Security Extensions (DNSSEC) to protect the integrity of any 5G-related DNS communication.
OAuth for Service-Based Architecture (SBA)	5GSC-8.4	Use the OAuth 2.0 framework at the API layer to ensure that only authorized network functions are permitted access to a service offered by another NF. Use CAPIF with TLS-Oauth for all internal and external APIs.

14. RIFERIMENTI

1) NIST SP 1800-33 - 5G Cybersecurity
2) GSMA Securing 5G Era