Anitec-Assinform

White Paper

La sicurezza cyber delle reti

A cura del
Gruppo di Lavoro Infrastrutture

Aprile 2023

Associazione Italiana per l'Information and Communication Technology (ICT)
Milano, Via San Maurilio 21, 20123
Telefono 02 0063281
segreteria@anitec-assinform.it – anitec-assinform@pec.it – www.anitec-assinform.it
P.IVA: 10053550967 C.F.: 10053550967

Anitec-Assinform

Sommario

INTRODUZIONE

La sicurezza nelle comunicazioni è un elemento fondante della fiducia che riponiamo nelle reti di telecomunicazioni quando ad esse affidiamo la trasmissione e la conservazione dei nostri dati, della nostra identità, del nostro patrimonio o quando da esse dipendendo la sopravvivenza in caso di disastri naturali ed emergenze o, più semplicemente, per mantenere e sviluppare il mondo moderno.

Le reti mobili, più che quelle fisse, stanno evolvendo rapidamente verso capacità di trasmissione dei dati in molti casi superiori all'infrastruttura di rete fissa esistente in molti Paesi. Il 5G in tal senso è una rivoluzione in atto che consentirà nuovi modelli sociali, permetterà di collegare trilioni di dispositivi IoT alla rete, abiliterà operatori mobili virtuali ma anche tanti settori ed utenti industriali, ognuno con il suo slicing, in reti sempre più basate su architetture Cloud ed interconnesse.

Quella della cyberscurity delle reti diventa quindi un argomento molto complesso da gestire proprio perché gli attori coinvolti si moltiplicano notevolmente a partire dagli utenti finali ed i loro use case per passare dai produttori di tecnologie e dai gestori della rete.

Questo White Paper intende dare una visione della complessità da affrontare a livello architetturale e tecnologico, senza avere la pretesa di entrare nei dettagli, per un pubblico non esperto di cybersecurity ma sensibile all'argomento ed alle tecnologie. Vengono passati in rassegna concetti come 5G, layers di rete, gestione delle identità ed autenticazione, minacce alla rete, nuovi standard 3GPP e O-RAN, sistemi IoT ed altri per comprendere meglio quanto, appunto, sia complessa una rete ma ancora di più la sua protezione della sicurezza.

Allo stesso tempo vengono analizzate evoluzioni, standard e nuove architetture di rete che consentono di affrontare meglio e più rapidamente gli aspetti di sicurezza: l'approccio Zero Trust con l'utente e l'organizzazione al centro oltre che la visione attuale su come la blockchain può aiutare oggi mentre avanzano

le sperimentazioni di tecniche basate su quantum computing che rivoluzioneranno nei prossimi decenni l'intero settore.

1. LE POSSIBILI CRITICITÀ IN UNA RETE

Le reti 5G aprono la strada a nuovi e avanzatissimi scenari di utilizzo, ma, nelle proprie scelte di sviluppo, i consumatori e le aziende devono porre primaria attenzione affinché i propri dati, operazioni e transazioni siano al sicuro dalle possibili minacce.

Nel complesso, le minacce considerate più rilevanti sono quelle legate alla compromissione della riservatezza, disponibilità e integrità delle informazioni.

Più in particolare, è stata rilevata una serie di scenari di minaccia rivolti alle reti 5G in particolare per quanto riguarda:

- Interruzione della rete 5G locale o globale (Disponibilità);
- Spionaggio di traffico/dati nell'infrastruttura di rete 5G (Riservatezza);
- Modifica o re-indirizzamento del traffico/dati nell'infrastruttura di rete 5G (Integrità e/o Riservatezza);
- Distruzione o alterazione di altre infrastrutture digitali o sistemi informativi (Integrità e/o Disponibilità).

Considerata la maggiore complessità e la criticità dei servizi e applicazioni rese disponibili dalle nuove reti rispetto a quelle preesistenti, le minacce alla rete 5G presentano differenze importanti, che riguardano anzitutto la natura e l'intensità dei loro potenziali effetti negativi. In particolare, le applicazioni per cui le reti 5G saranno impiegate potrebbero peggiorare significativamente l'impatto negativo dell'attacco.

La gravità di specifici scenari di minaccia per le reti 5G può quindi variare in base a diversi fattori, in particolare:

- il numero e la tipologia di utenti interessati;
- la durata dell'evento prima del rilevamento o della riparazione;
- la tipologia dei servizi interessati (pubblica sicurezza, servizi di emergenza, sanità, attività governative, elettricità, acqua, ecc.)
- l'entità del danno o perdita economica;
- il tipo di informazione violata.

Tutto ciò richiede un nuovo approccio alla sicurezza della rete caratterizzato da operazioni di sicurezza sia predittive che automatizzate.

Le minacce informatiche sono sofisticate e in continua evoluzione. Con il 5G che rappresenta una completa trasformazione della rete, gli attacchi possono avvalersi di migliaia o addirittura milioni di reti interconnesse con nodi che potenzialmente vulnerabili. Quindi, le reti 5G richiedono una sicurezza integrata che va oltre lo standard 3GPP e comprende l'automazione, l'orchestrazione della sicurezza, l'analisi e l'apprendimento automatico degli scenari per rilevare e mitigare ogni possibile minaccia.

I nuovo approccio alla sicurezza richiede quattro capacità chiave: **adattamento, velocità, integrazione e automazione**.

- **Adattamento**
  L'adattamento è necessario per rispondere in modo rapido e appropriato per contrastare le tecniche sempre più sofisticate dei cyber-attacchi. Gli hacker spesso modificano dinamicamente i loro attacchi in tempo reale o quasi; quindi, le difese devono essere almeno altrettanto adattive per rispondere altrettanto rapidamente.
- **Velocità**
  La velocità è un altro requisito fondamentale. Uno dei fattori di successo più importanti nella sicurezza è la riduzione del tempo di permanenza, che è il periodo di tempo in cui un hacker non viene rilevato. Nel 2018 questo tempo era stimato in circa 78 giorni, ma utilizzando concetti di Artificial Intelligence / Machine Learning, orchestrazione e automazione è possibile ridurre il tempo di permanenza fino all'80%.
- **Integrazione**
  Una piattaforma di sicurezza informatica deve integrare il maggior numero possibile di strumenti e sistemi di sicurezza diversi in modo di poter facilmente filtrare i falsi allarmi e rispondere più efficacemente alle minacce reali.
- **Automazione**
  L'automazione riduce il crescente carico di lavoro che deve affrontare i team di sicurezza. La sicurezza informatica 5G utilizza l'automazione per affrontare gli attacchi ricorrenti e intervenire rapidamente e con successo utilizzando risposte automatiche predefinite.

2. IL 5G E I NUOVI SCENARI DI SICUREZZA

La rete 5G promette di essere molto più capace, flessibile, ma è anche più complessa delle precedenti.

Molti elementi di rete tradizionali di 4G sono sostituiti in 5G dalle funzioni di rete virtuale e architetture "Cloud".

Si stima che miliardi di dispositivi saranno collegati alla rete 5G nei prossimi anni. Molti di questi dispositivi saranno sensori a bassa potenza, indossabili e piccoli dispositivi utilizzati nell'industria.

Inoltre, la rete 5G aumenta la capacità wireless di 1000 volte, e collegherà 7 miliardi di persone e 7 trilioni di dispositivi IoT.

La realizzazione della rete come servizio e la diversità dei casi d'uso 5G renderanno la sicurezza della rete più complessa.

Disponibilità, riservatezza e integrità di tutte le funzioni di utente, gestione e controllo devono evolversi per soddisfare reti più dinamiche, un maggior numero di attori coinvolti nella fornitura di servizi, l'ampia varietà di dispositivi (incluso IoT), utenti e applicazioni.

Le caratteristiche delle reti 5G, ovvero il loro modello architetturale, che consente l'erogazione di servizi multipli sfruttando la stessa infrastruttura, con proprietà avanzate di velocità, densità, qualità e bassa latenza delle comunicazioni, favoriranno lo sviluppo di nuovi modelli di business, di nuove applicazioni e servizi, ma comporteranno un aumento della superficie di attacco con impatto sulle necessità di cyber security.

Le applicazioni relative ai settori della Sicurezza Pubblica e Protezione in caso di Disastri (PPDR) e di tutte le infrastrutture critiche vitali per il Paese, inclusi i sistemi delle Amministrazioni Pubbliche, saranno particolarmente impattate.

Le reti 5G apporteranno una forte discontinuità rispetto al passato a fronte del cambiamento della tipologia di utenza - che in minima parte sarà composta da dispositivi o sistemi piuttosto che da persone - e alla larga introduzione di tecnologie di virtualizzazione, che consentirà la creazione di partizioni di rete gestite da differenti operatori. Cambiamenti che avranno impatto sui rischi informatici e sulle modalità di gestione della sicurezza, come quelli relativi alla separazione delle differenti partizioni, specializzate e eterogenee, in cui sarà suddivisa la rete.

Le reti 5G vedranno più di prima operare attori diversi, come gli operatori di reti mobili virtuali (MVNO), i fornitori di servizi di comunicazione (CSP) e i fornitori di infrastrutture di rete.

Gli operatori mobili, che nelle reti delle generazioni precedenti avevano l'accesso diretto e il pieno controllo su tutti le componenti del sistema, potranno dover condividere parte di questa responsabilità con altri soggetti; questo nuovo modello rappresenta pertanto una sfida e impone di riconsiderare i tradizionali meccanismi di governance della sicurezza e di sincronizzare le policy sulla privacy tra i possibili attori coinvolti.

Gli standard 5G ereditano quindi non solo le caratteristiche di sicurezza delle generazioni precedenti ma forniscono nuove e significative funzionalità per rendere il sistema 5G più sicuro e aperto e per soddisfare i requisiti di sistema più stringenti.

I dispositivi connessi e le applicazioni nell'ambiente richiederanno l'accesso alla rete progettato secondo requisiti di resilienza, sicurezza e protezione della privacy.

Nelle successive versioni dello standard 5G verranno fornite funzionalità di sicurezza sempre più avanzate e nuovi schemi di autenticazione e protezione dei dati per l'uso massiccio di dispositivi IoT.

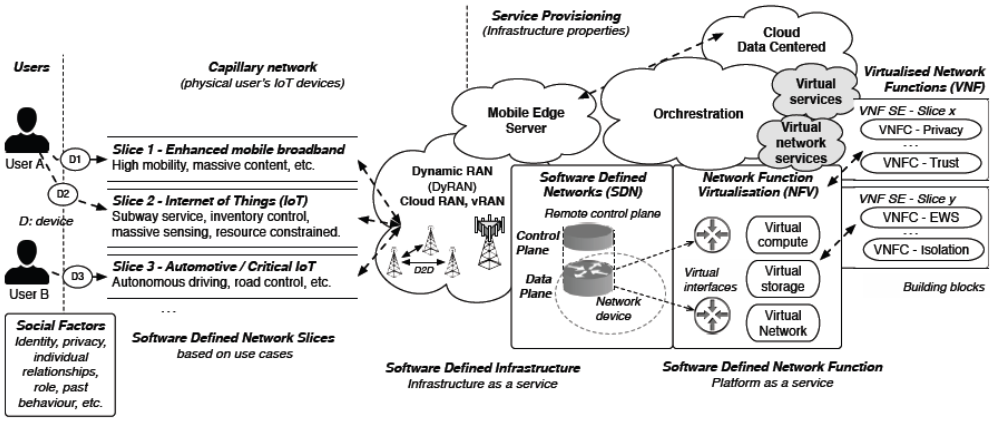

Fig. 1 – Elementi dell'architettura 5G

3. LA SICUREZZA DELLE COMPONENTI DELLA RETE END TO END: I FATTORI DI RISCHIO E I PRESIDI 5G CONTRO LE VULNERABILITÀ

3.1. Fattori di Rischio e vettori di Attacco

I fattori di rischio vengono tipicamente valutati e classificati in base al modo in cui potrebbero influire sui tre aspetti chiave della sicurezza delle informazioni:

- Integrità
- Disponibilità
- Riservatezza

Le seguenti funzioni, considerate criticamente sensibili, richiedono i massimi livelli di protezione perché una loro compromissione potrebbe compromettere seriamente l'integrità, la disponibilità o la riservatezza:

- Infrastruttura di virtualizzazione
- Controllori
- Orchestratori
- Gateway Internet
- Routing e commutazione del traffico IP nel core
- Funzioni di database
- Funzioni di autenticazione, controllo degli accessi e altre funzioni di sicurezza.

3.1.1. Risolvere il compromesso tra sicurezza e prestazioni

Un conflitto mina la sicurezza di alcune reti di telecomunicazione ma, in una visione poco consapevole spesso adottata, molti sottolineano anche che "la sicurezza non paga". L'implementazione può essere infatti costosa e può indurre alla ricerca di un compromesso tra sicurezza e prestazioni.

Poiché dare la priorità alle prestazioni e ai ricavi rispetto alla sicurezza aumenta il rischio ed espone una maggiore superficie di attacco, è probabile che questo compromesso si riveli dannoso nel lungo periodo.

La soluzione è investire maggiormente in infrastrutture che migliorino le prestazioni e la scalabilità, in modo che l'implementazione delle misure di sicurezza non comprometta le prestazioni della rete.

Se ben gestita, la sicurezza può essere un fattore di differenziazione positivo per gli operatori di telecomunicazioni.

Esiste inoltre un effetto correlato che può rendere difficile l'aggiornamento dei sistemi: alcuni operatori di telecomunicazioni fanno funzionare le loro apparecchiature con livelli di utilizzo trasversale così elevati da ostacolare la capacità di applicare gli aggiornamenti in modo continuativo. Anche questo problema può essere affrontato investendo maggiormente in infrastrutture che migliorino le prestazioni.

I rischi principali per il layer di virtualizzazione includono i seguenti:

- Attacchi che consentono a un hacker di aggirare la separazione forzata di un hypervisor per controllare i carichi di lavoro in esecuzione sull'host o per spostarsi lateralmente verso altri host e applicazioni.
- Un attacco riuscito al fabric di virtualizzazione, al sistema di orchestrazione o alle funzioni di gestione della virtualizzazione potrebbe consentire a un aggressore di accedere all'intero sistema di virtualizzazione, compresi tutti i server i carichi di lavoro virtuali, compromettendo potenzialmente l'intera rete e compromettendo la disponibilità e la riservatezza dei servizi critici.

Il piano di segnalazione rischia inoltre di essere il destinatario di dati dannosi, che potrebbero compromettere la disponibilità della rete.

3.1.2. Minacce e fattori di rischio specifici del 5G

Il documento del 5GPPP Security Working Group sul panorama della sicurezza 5G[1] identifica una serie di rischi di sicurezza specifici per il 5G e i relativi requisiti.

In generale, l'architettura orientata ai servizi della rete principale 5G introduce una gamma più ampia di dati e servizi rispetto al 4G, aumentando la superficie di attacco. I protocolli web e le API comuni delle reti 5G aprono ulteriori vettori di attacco.

Ecco alcuni dei rischi identificati dal gruppo di lavoro che sono rilevanti per reti di telecomunicazioni. Questo elenco preliminare richiederà aggiornamenti durante la transizione al 5G:

- Accesso o utilizzo non autorizzato di risorse
- Furto di identità
- Clonazione dell'identità per ottenere l'accesso a risorse sensibili - Uso fraudolento di risorse condivise
- Modifica delle credenziali degli abbonati
- Isolamento debole delle partizioni di rete (slice), che potrebbe esporre dati sensibili ad applicazioni in esecuzione in altre slice attraverso un attacco "side-channel".
- Routing di cattura del traffico a causa di virtualizzazione ricorsiva o additiva
- Mancanza di rilevamento di alterazioni del piano di controllo o del piano utente
- Difficoltà nella gestione dei livelli di servizio verticali e della conformità alle normative.

Inoltre, la mancanza di standard di sicurezza comuni tra più domini potrebbe rendere la gestione complessa e difficile, aumentando il rischio di errori di

[1] https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP_White-Paper_Phase-1-Security-Landscape_June-2017.pdf

configurazione o altre modifiche che espongono vulnerabilità o vettori di attacco.

3.1.3. Imperativi di sicurezza fondamentali per ridurre il rischio

Questi rischi e vettori di attacco necessitano di imperativi di sicurezza fondamentali. In generale, la sicurezza del piano di virtualizzazione e della sua gestione si basa sulla capacità di fare quanto segue:

- Mantenere aggiornati il sistema di virtualizzazione e le macchine virtuali, in modo omogeneo- Applicare rapidamente gli aggiornamenti di sicurezza critici.
- Implementare mitigazioni che neutralizzino i vettori di attacco noti.
- Controllare l'accesso alle risorse e al livello di gestione utilizzando i principi del privilegio minimo e della separazione dei ruoli.
- Isolare gli hypervisor e le macchine virtuali con domini e pool di sicurezza che impediscano gli spostamenti laterali.
- Proteggere i dati sensibili attraverso la segmentazione dei carichi di lavoro e dello storage.
- Crittografare i dati in transito e memorizzati su sistemi di archiviazione (at rest).
- Progettare l'infrastruttura virtualizzata seguendo le best practice e i modelli per il provisioning automatizzato, la gestione automatizzata, l'amministrazione sicura e la micro-segmentazione.
- Progettare la gestione del piano di virtualizzazione per isolarlo da altri sistemi e reti.
- Controllare rigorosamente l'accesso e l'uso del livello di gestione del piano di virtualizzazione.
- Monitorare e verificare il piano di virtualizzazione.
- Tracciare l'accesso e le modifiche al livello di gestione.

3.2. Componenti del sistema interni alla rete mobile

3.2.1. Sicurezza del dialogo tra terminali e infrastruttura

Il dialogo tra i terminali e la rete è una delle componenti che resta sotto il totale controllo del gestore mobile, e quindi il design delle funzionalità di sicurezza segue principi simili a quelli utilizzati nel sistema 4G, ma sviluppato per soddisfare al meglio le esigenze dei nuovi use case.

Le identificazioni degli utenti, che solitamente erano inviate in chiaro, ora sono state protette per evitare attacchi IMSI catcher. Questi attacchi rappresentano una problematica per la rete 4G, ma la protezione degli ID degli utenti aiuta a mitigare questo problema.

L'infrastruttura di rete 5G comprende la protezione contro attacchi di intercettazione e modifica dei dati e delle informazioni e la criptazione del traffico di segnalazione di rete e del terminale; in particolare, la protezione dell'integrità della segnalazione del terminale è adattato per le trasmissioni di dati di piccole dimensioni, ad esempio per i dispositivi IoT.

3.2.2. Gestione dell'identità rispetto alla rete

L'aspetto peculiare delle reti mobili è la gestione sicura delle identità per l'identificazione e l'autenticazione degli abbonati, in roaming o no, che si basa su funzionalità consolidate di criptazione già esistenti nel sistema 4G.

Una delle nuove funzionalità di sicurezza del sistema 5G è la struttura di autenticazione in cui gli operatori possono scegliere in modo flessibile le credenziali di autenticazione, i formati degli identificativi e metodi di autenticazione diversi per gli abbonati e i dispositivi IoT: oltre alle SIM fisiche il sistema 5G consente anche altri tipi di credenziali quali certificati, chiavi precondivise e token (protocolli di autenticazione 5G AKA e EAP - Extensible Authentication Protocol).

Ad esempio, mentre le SIM continueranno a essere utilizzate per gli smartphone, le credenziali non basate su SIM card sarebbero utili per dispositivi IoT molto economici, come piccoli sensori di temperatura, in cui richiedere

l'implementazione e l'implementazione di schede SIM sarebbe non conveniente.

Va comunque evidenziato il fatto che per le reti 5G la fase di autenticazione degli utenti rimane sotto il pieno controllo della Home Network dell'operatore, che, anche in condizioni di roaming, può essere assicurato attraverso l'introduzione di un Security Proxy.

3.2.3. Riservatezza

Nei sistemi 5G, la protezione della privacy degli abbonati è compresa nei requisiti della fase progetto (privacy by design).

I rischi derivanti da possibili debolezze del Sistema Operativo degli smartphone sono rappresentati dalla possibilità che un attaccante localizzi un dispositivo inviando falsi messaggi di paging e quindi intercetti e registri telefonate e SMS e lanci attacchi di tipo Denial-of-Service (DoS) verso lo smartphone della vittima fino a saturarne le risorse e mandarlo in blocco.

L'architettura 5G rende pressoché impossibile, a una parte non autorizzata, decodificare e leggere informazioni comunicate in modalità wireless, protette utilizzando un sistema crittografico che permette ai dispositivi e alla rete di autenticarsi reciprocamente.

Inoltre, il sistema 5G è anche in grado di rilevare false stazioni radio base che potrebbero essere utilizzate per localizzare e intercettare i dispositivi e di occultare l'identificativo del terminale anche in situazioni di roaming.

3.2.4. Valutazione di sicurezza dei dispositivi di rete mobile

Nel contesto delle reti 5G, è fondamentale stabilire quali requisiti di sicurezza debbano soddisfare gli apparati di rete e che questi siano implementati nei processi di sviluppo e nel ciclo di vita del prodotto.

3GPP e GSMA hanno creato un sistema di assicurazione della sicurezza denominato NESAS (Network Assurance Security Assurance Scheme), che si applica e si implementa al ciclo di vita delle apparecchiature di telecomunicazione che mira a soddisfare le esigenze di molte normative

nazionali e internazionali sulla sicurezza informatica, come il quadro di certificazione UE sulla sicurezza informatica.

NESAS comprende due componenti principali:

- I requisiti di sicurezza, definiti congiuntamente da operatori e fornitori in ambito 3GPP. Questi requisiti sono al momento definiti su base nodo e raccolti nelle cosiddette SeCurity Assurance Specifications (SCAS). Esistono vari tipi di requisiti, tra cui l'uso di una politica di sicurezza generale, la lunghezza minima delle password di gestione, ma anche requisiti di test di solidità e resistenza agli attacchi.

- Una infrastruttura di auditing governata dal GSMA, che certifica (o revoca) i fornitori nominando le società di revisione che eseguono gli audit dei processi di sviluppo e i test di conformità.

3.3. Componenti del sistema esterni alla rete

3.3.1. Terminali: sistemi operativi, applicazioni, configurazioni dei dati

Le applicazioni installate sugli smartphone possono veicolare, quando prelevate da fonti non affidabili, dei malware (virus, worm, Trojan, rootkit, botnet) progettati per utilizzare un dispositivo senza il consenso del proprietario. Gli obiettivi dell'attacco possono essere, ad esempio, la violazione della privacy, lo sniffing, il blocco del servizio (DoS: Denial of Service), l'"overbilling".

Gli smartphone sono spesso il principale repository di dati personali dell'utente perché vengono trasportati in ogni momento e sono sempre disponibili. Se i dati sulla memoria dello smartphone o sul suo supporto rimovibile non sono sufficientemente protetti (tramite crittografia), un utente malintenzionato può accedere a tali dati.

3.3.2. Componenti IoT

La rete 5G può comprendere capillarmente moltissimi dispositivi IoT [massive Machine Type Communication (mMTC)], che si connettono ai componenti fisici dell'infrastruttura di rete utilizzando le tecnologie di accesso radio disponibili; alcuni dispositivi IoT sono anche in grado di connettersi ad altri dispositivi in modalità Device to Device. Per i servizi real time, come alcune applicazioni automotive o particolari processi industriali, si parla di Ultrareliable MTC (uMTC).

Per aumentare la copertura ed evitare eventuali ostacoli nella propagazione del segnale, alcuni componenti IoT possono funzionare come "ripetitori" o nodi di accesso temporaneo.

Questa parte dell'ecosistema 5G può essere vulnerabile, perché se i "ripetitori" sono sottoposti ad attacchi, si interrompe la comunicazione tra i dispositivi IoT di un'area specifica e i Service Provider. L'attacco può avvenire, ad esempio, attraverso Internet, interferendo con il sistema di controllo remoto del service provider che gestisce i terminali IoT che fungono da nodo ripetitore. Se i dispositivi IoT sono protetti da userid e password predefiniti in fabbrica, un malware può ad esempio ottenere l'accesso ai dispositivi connessi.

La difesa da questo tipo di attacco può essere difficile perché i sistemi di controllo dei sistemi di gestione dei dispositivi IoT possono non essere dotati di funzionalità di riconfigurazione dei nodi o anche perché non sono disponibili le informazioni sull'attaccante (ad esempio, la sua posizione e il raggio di trasmissione).

Alcuni prodotti IoT possono infatti incorporare le password nel firmware che controlla le funzioni di base di un particolare dispositivo.

Mentre gli smartphone e i computer dispongono di sistemi operativi in grado di gestire gli accessi e difendersi dagli attacchi, il firmware dei dispositivi senza sistemi operativi integrati, come router e dispositivi IoT, non è facilmente riconfigurabile e gli stessi produttori non forniscono modi semplici per aggiornare il firmware utilizzato nei propri dispositivi IoT.

Per annullare (o minimizzare) eventuali minacce derivanti da tali possibili vulnerabilità, sarà pertanto importante porre particolare attenzione a questo tipo di dispositivi, prevedendo ad esempio adeguati test di sicurezza.

3.3.3. Edge computing

Le architetture Mobile Edge Computing comprendono tecnologie complementari che interagiscono in un ecosistema aperto in cui la virtualizzazione e il calcolo distribuito sono sfruttati dai fornitori di servizi per distribuire e fornire applicazioni agli utenti finali.

L'Edge Computing è indispensabile per sviluppare applicazioni che richiedono un calcolo molto rapido per elaborazioni che comprendono insiemi di dati limitati e una bassa o bassissima latenza (ad esempio una applicazione che percepisca la chiusura degli occhi di un guidatore e attivi un segnale sonoro per risvegliarlo).

Nella guida autonoma dei veicoli, l'elaborazione periferica all'interno di ogni veicolo sarà responsabile, ad esempio, del comportamento agli incroci, mentre le decisioni di navigazione e la pianificazione del percorso probabilmente avranno origine nel cloud centrale.

I componenti che generano le funzionalità di edge computing (hardware, software, firmware) saranno basati su un modello di deployment ibrido che comprenderà produttori fornitori e sviluppatori provenienti da ambienti e mercati diversi (nell'esempio dei veicoli a guida autonoma, software di navigazione, hardware e firmware di attuazione dei servocomandi, monitoraggio delle prestazioni e del consumo delle componenti meccaniche, diagnostica, eccetera).

Qualsiasi sistema di cloud computing, quindi anche le architetture MEC, possono potenzialmente veicolare flussi di dati malevoli che degradano le prestazioni dell'intero sistema provocando un anomalo consumo di risorse o accessi non autorizzati alle risorse di altri utenti.

Poiché MEC estende le funzionalità di cloud computing alla periferia delle reti mobili, il livello di protezione che può essere offerto dagli host periferici è basso rispetto a quello ottenibile nei tradizionali data center di grandi dimensioni.

Inoltre, le architetture MEC sono per lo più in una fase iniziale e possono basarsi su una molteplicità di tecnologie e fornitori, elementi che amplificano il potenziale rischio di attacchi e problemi di privacy.

3.3.4. Gestione dell'identità rispetto alle applicazioni

Nell'architettura 5G coesisteranno più modelli di autenticazione a seconda degli attori coinvolti nella gestione:

- **Autenticazione solo da parte dell'operatore di rete**
  L'autenticazione del servizio comporta una notevole quantità di costi per i fornitori di servizi. I fornitori di servizi potrebbero delegare al gestore di rete il servizio autenticazione, in modo che gli utenti possano accedere a più servizi una volta completata una singola autenticazione, sollevandoli da ripetute operazioni di autenticazione.

- **Autenticazione solo da parte dei fornitori di servizi (sia industrie sia operatori nel ruolo di fornitori di servizi)**
  Specularmente, il gestore di rete, per ridurre i costi operativi, potrebbe fare affidamento sulle capacità di autenticazione delle industrie attraverso dispositivi esenti da autenticazione di accesso alla rete radio.

- **Autenticazione da parte di entrambe le reti e dei fornitori di servizi**
  Per alcuni dei servizi potrebbe essere adottato i modello tradizionale in cui la rete si occupa dell'accesso alla rete (attraverso la SIM) e i fornitori di servizi gestiscono l'accesso al servizio attraverso una procedura di autenticazione basata su userid e password, riconoscimento biometrico eccetera.

Il problema dell'autenticazione sarà particolarmente rilevante per gli aspetti di sicurezza e privacy, dato il gran numero di dispositivi IoT che raccolgono dati da infrastrutture come smart cities, sistemi ospedalieri o uffici e case intelligenti.

Il rischio principale nei processi di autenticazione è il possibile furto delle credenziali di accesso o la presenza di malware progettati per prendere il controllo e fornire una "backdoor", ad esempio nel software di autenticazione dei sistemi di controllo dei dispositivi IoT o delle componenti di edge computing.

Inoltre, è da supervisionare l'aggiornamento dei i parametri di sicurezza dell'utente con il roaming da una rete di operatori a un'altra, per evitare a utenti malintenzionati di accedere a una rete e ai suoi servizi fingendo di essere un

utente legittimo, usufruire di servizi, tempo di trasmissione dati o costi di accesso a spese altro account utente.

3.3.5. User Privacy Protection

A valle della fase di autenticazione resta il problema dell'identificazione di chi può accedere a quali dati e con quale grado di delega sulla loro lettura, scrittura o modifica.

In una rete eterogenea in cui vengono utilizzate tecnologie di accesso multiple, la protezione della privacy delle informazioni dell'utente dipende dalla robustezza della filiera alla tecnologia di accesso (si paragoni la tenacia agli attacchi di una rete mobile su frequenze "proprietarie" da quella di una rete basata su frequenze condivise come WiFi, SRDs eccetera.

I dati dell'utente possono attraversare reti di accesso e entità funzionali di rete fornite da diversi operatori o service provider ed essere presenti su segmenti di rete diversi.

Le reti dovranno anche essere in grado di rilevare il tipo di servizio che un utente sta utilizzando, ma è da sottolineare che lo stesso rilevamento del tipo di servizio e di accesso ricade di per sé nella sfera della privacy degli utenti.

3.3.6. Mobile Cloud Computing

Il cosiddetto Mobile Cloud Computing (MCC) migra i concetti di cloud computing negli ecosistemi 5G, cui sono associati una serie di nuovi aspetti relativi alla vulnerabilità di sicurezza legati alla nuova infrastruttura e architettura delle reti 5G.

Queste minacce possono essere classificate in base ai segmenti di rete, vale a dire:

- "front-end", visibile al cliente, che comprende l'interfaccia utente e il sistema o la rete di computer dei client utilizzati per accedere al sistema cloud;

- "cloud based delivery", attraverso i quali gli utenti sottoscrivono la possibilità di utilizzare dei pacchetti applicativi (Software-as-a-Service o

SaaS) i cui provider possono a loro volta sottoscrivere servizi cloud di tipo Platform-as-a-Service (PaaS), Infrastructure-as-a-Service (IaaS) e altro;

- "back end computing", il segmento utilizzato dal fornitore di servizi che include server, sistemi di archiviazione dati, macchine virtuali e software che costituiscono il cloud dei servizi. Il back-end fornisce le procedure di sicurezza, il controllo del flusso dei dati e i protocolli tra i nodi per l'interoperabilità.

Le infrastrutture del cloud condivise tra più operatori mobili virtuali richiederà una rigorosa separazione nei diversi segmenti per evitare uso scorretto delle risorse e l'integrità delle informazioni dei vari operatori. Ad esempio, l'architettura basata su Network Slicing necessità dell'isolamento delle "slice" di rete e l'implementazione di protocolli di sicurezza del dialogo tra le diverse "slice".

Le architetture di rete programmabili prevedono interfacce aperte, modelli comuni e "pubblici", in cui le applicazioni possano essere fornite da qualsiasi fornitore di SW e l'elaborazione possa essere interamente decentralizzata. Di conseguenza, le architetture basate su SDN richiedono procedure robuste di autenticazione e autorizzazione delle applicazioni e delle diverse componenti, per evitare l'attacco alle risorse di rete, ad esempio, attraverso l'accesso non autorizzato alle informazioni relative all'instradamento dei dati, la saturazione malevola delle applicazioni centralizzate di controllo del traffico, o la contaminazione da virus delle interfacce di programmazione delle applicazioni critiche.

Allo stesso modo, l'errata configurazione delle funzioni di rete virtuale (Virtual Network Functions) può portare a conflitti che possono provocare ostacoli al funzionamento della rete. Attraverso le funzionalità VNF, gli operatori possono fornire servizi su misura e applicazioni ad altri operatori di rete sulla stessa infrastruttura e devono assicurare le adeguate misure di sicurezza e separazione dei domini amministrativi. Per loro natura, infatti, le VNF sono soggette ai tipici attacchi quali spoofing (la falsificazione dell'identità per lanciare attacchi di phishing), sniffing e DoS, oltre ad alcune minacce tipiche della virtualizzazione delle funzionalità quali violazioni della chiave di criptazione (side-channel attack), saturazione del controllo della segnalazione (flooding attack), attacchi al monitor delle macchine virtuali (Hyperjacking

attack), o malware inserito direttamente da amministratori fraudolenti di funzioni virtualizzate.

4. Standard Europeo, situazione italiana, raccomandazioni O-RAN, 3GPP

Con il passaggio al 5G, le dimensioni della rete di accesso radio si stanno espandendo in modo significativo. Con il 5G, la RAN diventa più densa, con siti e sistemi di diversi fornitori. Con l'aumento delle postazioni edge, delle stazioni base e delle antenne, aumentano anche il numero di interfacce, i vettori di attacco e i rischi.

La necessità di proteggere la RAN per il 5G diventa fondamentale e i nuovi casi d'uso accentuano la necessità di migliorare la sicurezza.

I servizi personalizzati su richiesta, la banda larga mobile potenziata (eMBB), le comunicazioni massive di tipo macchina (mMTC) e le comunicazioni ultra-affidabili a bassa latenza (URLLC) richiedono tutte capacità di sicurezza nuove o ampliate.

Questi cambiamenti nelle dimensioni, nell'accesso, nei casi d'uso e nella distribuzione delle responsabilità contribuiscono a creare una serie di problemi di sicurezza per le reti di accesso radio per il 5G.

Open RAN, l'iniziativa di disaggregazione e apertura della RAN guidata da O-RAN Alliance, sposta ulteriormente la responsabilità della sicurezza agli operatori di telecomunicazioni, che potrebbero a loro volta dover distribuire le responsabilità della sicurezza tra più fornitori, segmenti e possibilmente cloud. Di conseguenza, il numero di tecnici, appaltatori e amministratori di sistema che necessitano di accesso, in remoto, in loco o in entrambi i modi, è destinato ad aumentare di pari passo con la crescita della RAN. Nuovi approcci e componenti richiedono uno spostamento dell'attenzione.

4.1. 5G, virtualizzazione e il percorso verso la sicurezza dell'Open RAN

Una rete di accesso radio aperta cerca di adottare la traiettoria del settore verso la virtualizzazione e il software-defined networking. Gli standard per il 5G puntano a un futuro cloud-native e parte di questo futuro risiede in una visione di disaggregazione della RAN.

La virtualizzazione e Il software-defined networking consente agli operatori di telecomunicazioni di sostituire l'hardware RAN, costoso e appositamente costruito, con server comuni e di base. Virtualizzando e disaggregando le funzioni RAN, gli operatori possono ridurre i costi, distribuire le funzioni di rete per la RAN nelle loro posizioni ottimali, gestire le funzioni su scala da una postazione centrale e automatizzare aspetti quali l'elasticità e la sicurezza.

La Open RAN Policy Coalition collega l'O-RAN al miglioramento della sicurezza:

"L'O-RAN ha il potenziale per basarsi sui miglioramenti della sicurezza già consentiti dal 5G e permettere all'operatore di controllare completamente la sicurezza della rete, migliorando in ultima analisi la sicurezza operativa della propria rete. Uno dei vantaggi è la maggiore visibilità degli eventi di sicurezza: Un operatore di rete avrà accesso diretto a un maggior numero di dati sulle prestazioni della rete perché i componenti sono disaggregati e collegati attraverso interfacce aperte"[2].

Grazie a questa visibilità, gli operatori possono individuare e mitigare più rapidamente gli attacchi e altri problemi di sicurezza.

La visibilità che accompagna una Open RAN migliora la valutazione e la gestione dei rischi per la sicurezza. La virtualizzazione e il software-defined networking consentono di proteggere la RAN con le seguenti tecniche di sicurezza avanzate:

- containerizzazione
- micro-segmentazione e isolamento della rete
- automazione e orchestrazione
- catena di fiducia, dai repository di immagini dei container fino all'implementazione su hardware con root of trust e processori potenziati per la sicurezza
- Network Slicing
- Spostamento di un maggior numero di funzionalità di sicurezza dalle reti core più vicine all'edge 5G e ai punti di accesso della RAN.

[2] https://www.openranpolicy.org/wp-content/uploads/2021/04/Open-RAN-Security-in-5G-4.29.21.pdf

- Crittografia end-to-end più forte

Oltre a portare nuove tecniche e capacità di sicurezza, un'architettura Open RAN diversifica l'ecosistema dei fornitori e promuove l'interoperabilità con interfacce aperte.

4.2. Standard emergenti di sicurezza delle telecomunicazioni

Per identificare le soluzioni ai principali rischi e requisiti di sicurezza di una Open RAN, ci si basa su diversi documenti e organizzazioni che definiscono gli standard:

1. Analisi della sicurezza per il settore delle telecomunicazioni: Summary of Findings, del National Cyber Security Centre del Regno Unito, pubblicato nel gennaio 2020[3].
2. 5G PPP Phase 1 Security Landscape, pubblicato dal 5GPPP Security Working Group nel giugno 2017[4].
3. Cybersecurity of 5G Networks EU Toolbox of Risk Mitigating Measures, pubblicato dalla Commissione europea nel gennaio 2020[5].
4. L'O-RAN Alliance, la sua architettura e le pubblicazioni del suo gruppo di lavoro sulla sicurezza[6].
5. Le pubblicazioni della Open RAN Policy Coalition, compreso il documento del 2021 sulla sicurezza della Open RAN nel 5G[7].
6. Pubblicazione speciale 800-207 del NIST statunitense, Architettura a fiducia zero[8].

[3] https://www.ncsc.gov.uk/files/Summary%20of%20the%20NCSCs%20security%20analysis%20for%20the%20UK%20telecoms%20sector.pdf
[4] https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP_White-Paper_Phase-1-Security-Landscape_June-2017.pdf
[5] https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64468
[6] https://orandownloadsweb.azurewebsites.net/specifications
[7] https://www.openranpolicy.org/wp-content/uploads/2021/04/Open-RAN-Security-in-5G-4.29.21.pdf
[8] https://csrc.nist.gov/publications/detail/sp/800-207/final

7. National Strategy to Secure 5G Implementation Plan della National Telecommunications and Information Administration[9] (NTIA) del Dipartimento del Commercio degli Stati Uniti.

Anche altre organizzazioni di standard di telecomunicazione, tra cui 3GPP, GSMA, ETSI e Telecom Infrastructure Project (TIP), forniscono standard, quadri e linee guida per aiutare gli operatori di telecomunicazioni a garantire la sicurezza del 5G.

Gli standard di sicurezza stabiliscono le basi per l'architettura delle reti e dei processi di accesso radio da parte degli operatori di telecomunicazioni, in grado di proteggere in modo proattivo e di rispondere rapidamente a minacce, vulnerabilità ed exploit.

4.3. Protezione dei sistemi aperti vs. protezione dei sistemi chiusi

Alcuni fornitori di hardware proprietario RAN continuano ad alimentare l'idea errata che le interfacce aperte introducano rischi per la sicurezza, idea che viene presumibilmente promossa per creare la percezione di una barriera all'ingresso nei mercati RAN e per bloccare i clienti nella loro unica soluzione.

Gli stack verticali chiusi di hardware appositamente costruito sono un problema enorme per gli operatori di telecomunicazioni e, in ultima analisi, per i consumatori. Gli operatori potrebbero non avere visibilità sulle vulnerabilità e sui rischi di un sistema chiuso e devono fidarsi del fatto che l'intero stack verticale sia aggiornato, incluse le patch di sicurezza, bloccato e privo di vulnerabilità.

L'Open RAN adotta l'approccio opposto: cerca cioè di definire interfacce aperte attraverso specifiche tecniche per "fornire una base e un'architettura per migliorare la sicurezza".

L'Open RAN Policy Coalition sottolinea che "gli standard aperti aiutano gli utenti e gli operatori di rete a comprendere meglio, ad allinearsi e a dimostrare la corretta implementazione dei requisiti di sicurezza".

[9] https://ntia.gov/other-publication/national-strategy-secure-5g-implementation-plan

Questo fa crescere efficacemente il mercato dei fornitori di soluzioni 5G, in quanto gli operatori di rete hanno la possibilità di scegliere tra una varietà di fornitori e provider per offrire soluzioni interoperabili standardizzate.

Inoltre, quando le interfacce aperte standardizzate si combinano con l'immediata condivisione pubblica delle informazioni sulle vulnerabilità e sugli exploit, i fornitori e gli operatori possono intervenire per applicare patch ai sistemi, mitigare i danni e prevenire la diffusione o il movimento laterale in una rete.

Quando il team operativo di sicurezza di un operatore di telecomunicazioni sa cosa c'è all'interno dei sistemi che sta eseguendo, di cosa sono composti questi sistemi e quali sono le loro interfacce, può proteggerli meglio prima di un attacco e rispondere con visibilità e conoscenza durante un attacco o quando viene alla luce una vulnerabilità.

Secondo le osservazioni della Open RAN Policy Coalition presentate all'NTIA, una RAN aperta e interoperabile fornisce una rete sicura.

- Gli standard favoriscono la sicurezza, l'interoperabilità e la fiducia trasparenti e verificate
- L'architettura cloud garantisce resilienza, scalabilità e segmentazione e consente l'introduzione del Multi-Access Edge Computing (MEC).
- La segmentazione, la containerizzazione e la virtualizzazione garantiscono una maggiore sicurezza e isolamento dall'hardware in su.

Nel suo paper intitolato 5G and Open RAN Security: Next Generation Trust[10], la Open RAN Policy Coalition sostiene che poiché una Open RAN è un'architettura fondamentalmente aperta, essa apre l'ecosistema a nuovi fornitori, aumentando la diversità delle soluzioni RAN virtualizzate.

[10] https://www.openranpolicy.org/wp-content/uploads/2021/04/Open-RAN-Security-in-5G-4.29.21.pdf

4.4. Intervento governativo per proteggere le reti richiedendo più fornitori

Uno stack RAN e una rete multivendor sono fondamentali per la sicurezza. I problemi di sicurezza legati all'utilizzo di stack RAN di un solo fornitore si aggravano se i componenti sono sistemi chiusi senza trasparenza del software per l'operatore e senza un rapido annuncio pubblico delle vulnerabilità di sicurezza scoperte e delle relative patch.

Gli ambienti multi-vendor che fioriscono grazie all'adozione di interfacce aperte standardizzate e alla conseguente interoperabilità portano ad ambienti più protetti e a infrastrutture di telecomunicazione più sicure, tanto che alcuni governi stanno iniziando a richiedere o a supportare ambienti multi-vendor.

Ad esempio, gli standard di sicurezza 5G emergenti, come i requisiti di sicurezza delle telecomunicazioni (TSR) del National Cyber Security Center (NCSC) del Regno Unito, richiedono l'uso di più fornitori. Negli Stati Uniti, la Cybersecurity and Infrastructure Security Agency (CISA) ha condotto un'analisi economica del mercato della RAN 5G[11] per determinare se alcune politiche sarebbero in grado di sostenere l'innovazione della catena di fornitura, i nuovi operatori e il sostegno ai fornitori di RAN affidabili. Il CISA ha stabilito che l'istituzione di sovvenzioni alla R&S per l'innovazione farebbe progredire le strategie per migliorare la fornitura di apparecchiature RAN affidabili, tra le altre opzioni.

4.5. Rischi, minacce e vulnerabilità di una Open RAN

I rischi e i requisiti di sicurezza stanno cambiando con la transizione degli operatori di telecomunicazioni alle reti 5G. In generale, l'architettura orientata ai servizi della rete principale 5G introduce una gamma più ampia di dati e servizi rispetto al 4G, aumentando la superficie di attacco. I protocolli web e le API comuni delle reti 5G espongono un maggior numero di vettori di attacco

Come qualsiasi altro sistema di telecomunicazione, una O-RAN deve affrontare sfide di sicurezza, comprese quelle simili a quelle affrontate dai sistemi RAN

[11] https://www.ntia.gov/files/ntia/publications/2021-1-12_115445_national_strategy_to_secure_5g_implementation_plan_and_annexes_a_f_final.pdf

esistenti. Con un numero maggiore di dispositivi in grado di connettersi a una rete 5G attraverso la RAN, vi è una maggiore necessità di contrastare gli attacchi "denial of service" e i tentativi di eludere i sistemi di autenticazione.

Con un sistema 5G autonomo, anche il modello di fiducia si è evoluto. Il 3GPP ha osservato che la fiducia all'interno della rete per un sistema 5G autonomo può diminuire man mano che gli aspetti del sistema si allontanano dal nucleo centrale, e questo cambiamento nel modello di fiducia può influire sul profilo di rischio per la RAN, in particolare per i DU distribuiti nel dominio pubblico.

Con un sistema 5G non standalone che supporta anche diverse reti di accesso, comprese le generazioni precedenti come il 4G, il sistema non standalone erediterà molti dei rischi di queste generazioni precedenti.

Per questo motivo, i gruppi industriali che creano le specifiche, come la O-RAN Alliance, e gli operatori di telecomunicazioni che implementano le reti di accesso radio per il 5G dovranno effettuare una rigorosa modellazione delle minacce e un'analisi dei rischi per la RAN.

4.5.1. Rischi e vettori di attacco in una Open RAN

Di seguito alcuni rischi e vettori di attacco che meritano particolare attenzione in una O-RAN.

- I principali attacchi alla catena di fornitura software commerciale degli ultimi due anni rendono ancora più necessario che i fornitori e gli operatori di telecomunicazioni utilizzino processi di sviluppo sicuri, provenienza del codice firmato e altre forme di protezione.
- L'utilizzo nella RAN di tecnologie emergenti come l'intelligenza artificiale può introdurre nuovi rischi ed esporre nuovi vettori di attacco.
- L'aumento dell'IoT e la proliferazione dei dispositivi connessi aumenta il rischio di attacchi da parte di dispositivi compromessi.

4.6. La sicurezza nella standardizzazione 3GPP e O-RAN Alliance

In tempi recenti il problema della sicurezza nelle reti mobili è stato affrontato prima dall'ente di standardizzazione 3GPP, a partire dallo standard 3G e in misura maggiore nell'ambito delle specifiche 5G NR, e poi anche da O-RAN Alliance che ha voluto una forte enfasi sugli aspetti di security e di come dare evidenza che questa sia stata progettata all'interno di una rete O-RAN.

4.6.1. La security negli standard 3GPP

Analogamente alla sicurezza delle comunicazioni su rete internet, 3GPP ha affrontato i problemi di sicurezza anche per la rete radio.

La sicurezza su rete internet utilizza algoritmi e protocolli che hanno lo scopo di garantire la confidenzialità e l'integrità delle comunicazioni, oggi tutti noi siamo abituati a lavorare utilizzando una VPN per connetterci alla rete aziendale, in modo da rispettare criteri di sicurezza di livello enterprise.

La sicurezza sulle reti mobili viene affrontata da 3GPP ormai a partire dagli standard 3G utilizzando algoritmi di cifratura e di firma digitale ("integrity signing") su tutta la comunicazione che passa per l'interfaccia radio, sia essa legata allo user plane che al control plane. In questo modo è possibile mettere in sicurezza la comunicazione tra terminale e rete evitando che lo sniffing sulla radio dia accesso ai dati scambiati sulla rete mobile. In particolare, a firma digitale assicura che non sia realizzabile un attacco del tipo "man in the middle".

Gli algoritmi di cifratura si sono poi evoluti nel corso degli passando dallo standard 3G al 4G e poi con il 5G per evitare attacchi di forza bruta.

Per quanto riguarda le connessioni tra gli elementi di rete mobile che avvengono sulle interfacce di midhaul e di backhaul, vengono utilizzati protocolli sicuri del tipo IPSec e comunque utilizzando VPN che rafforzano la sicurezza della comunicazione su interfacce che di solito sono basate su standard IP (IETF) e su fibra.

Con lo sviluppo degli standard 3GPP relativi al 5G NR, sono state realizzate due specifiche che normano anche i test da effettuare su una rete per garantire

che i requisiti di sicurezza siano rispettati, e i principali costruttori di strumentazione hanno realizzato delle suite di test che consentono in modo automatico di validare la sicurezza.

All'interno delle specifiche 3GPP, la famiglia 33.XXX tratta gli aspetti di sicurezza definiti come SCAS ("SeCurity Assurance Specification"). In particolare, la specifica TS 33.511 "Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class" descrive I test da effettuare su una rete radio per garantirne la sicurezza.

I test riguardano la verifica degli aspetti di cifratura e di firma digitale, e contemplano sia casi positivi (cifratura e firma digitale implementati correttamente) che negativi (la cifratura non viene realizzata e la rete mobile blocca la comunicazione, oppure cosa succede se la firma digitale non è corretta). Particolare enfasi è dedicata agli algoritmi di negoziazione delle chiavi e relativa validazione della corretta esecuzione.

In conclusione, la sicurezza è stata progettata come aspetto peculiare delle reti mobili a partire dagli standard 3G, ma con l'avvento del 5G la sicurezza è stata normata anche a livello di test minimi che vanno effettuati dai costruttori e dagli operatori sugli apparati e sulle reti per garantirne l'efficacia.

Sarebbe auspicabile che gli standard 3GPP venissero recepiti a livello nazionale come livello normativo e che tutti gli apparati utilizzati per la realizzazione di reti mobili e le reti realizzate utilizzando tali apparati siano certificate utilizzando questi standard.

4.6.2. Sicurezza e O-RAN Alliance

Le reti mobili di accesso radio O-RAN sono basate sugli standard 3GPP e su altri standard, e sono fondate su 3 principi fondamentali:

- disaccoppiamento tra HW e SW
- infrastruttura cloud
- interfacce standardizzate e aperte tra le funzioni di rete (Network Function – NF)

O-RAN Alliance, l'ente di standardizzazione per le reti di accesso radio O-RAN, ha recepito le ultime normative 3GPP e quindi ha stabilito che sono parte dei requisiti per la realizzazione di una rete O-RAN.

Oltre alle normative 3GPP, O-RAN Alliance aggiunge altre specifiche che servono a garantire l'integrità e la confidenzialità sulle interfacce O-RAN, mediante l'utilizzo di algoritmi di trasporto sicuri come IPsec e TLS e facendo uso di certificati basati sull'autenticazione X.509.

L'architettura O-RAN è completamente cloud native, la stessa che viene utilizzata per la realizzazione dei cloud pubblici e privati. O-RAN Alliance specifica anche i test da realizzare sull'infrastrutture per garantire che sia sicura.

Anche nel caso di reti O-RAN è auspicabile che gli standard O-RAN vengano correttamente recepiti a livello nazionale normativo e che tutti gli apparati utilizzati per la realizzazione di reti mobili e le reti realizzate utilizzando tali apparati siano certificate utilizzando questi standard.

5. SCENARI E SOLUZIONI DI SICUREZZA END TO END

5.1. Sicurezza nelle Infrastrutture Critiche (reti pubbliche / trasporti / energia / data center / cloud security, ...)

La creazione di un ambiente collaborativo per i fornitori di infrastrutture critiche europee in cui possono scambiare informazioni su vulnerabilità e minacce in modo sicuro e protetto è requisito importante per la gestione delle reti mission-critical.

Poiché i fornitori di infrastrutture critiche hanno a che fare con sistemi spesso grandi e complessi, hanno messo in atto sistemi per coprire una miriade di casi d'uso come il rilevamento delle perdite, la gestione della qualità del servizio, il rilevamento delle problematiche, la misurazione del servizio, la videosorveglianza, l'accesso controllo e molti altri.

Tutti questi diversi casi d'uso coinvolgono risorse diverse provenienti da vari fornitori; tuttavia, queste risorse spesso sono anche dotate di sistemi di gestione, database e strumenti per controllare il funzionamento e la manutenzione dell'infrastruttura. Oltre ai fornitori di elementi dell'infrastruttura, ci sono altre parti interessate o partecipanti all'infrastruttura critica come regolatori, consulenti/appaltatori, agenzie ambientali, meteorologiche e altre agenzie governative che possono influenzare il funzionamento e la sicurezza dell'infrastruttura critica.

Di conseguenza ci sono molte fonti di dati disponibili all'interno del fornitore dell'infrastruttura critica sullo stato e le prestazioni dei diversi asset. Con i progressi nelle tecniche di ML e IA è possibile creare più approfondimenti da dati storici e in tempo reale per aiutare a prevedere guasti o eventi che possono essere presi in considerazione per il funzionamento e la pianificazione dell'infrastruttura critica.

Gli algoritmi di rilevamento delle anomalie possono correlare diversi punti dati da domini o casi d'uso diversi, il che può anche portare a informazioni dettagliate su vulnerabilità della infrastruttura critica, minacce, potenziali vettori di attacco o attacchi in corso.

Rendere disponibili tali informazioni sulla vulnerabilità ad altri fornitori di infrastrutture critiche e possibilmente ad altre parti interessate o partecipanti all'ecosistema può portare a una preparazione molto migliore in un contesto dell'UE contro possibili interruzioni delle infrastrutture critiche.

5.1.1. Reti Mission – Critical

Per loro natura, le reti e i sistemi di comunicazione mission-critical devono essere caratterizzate da elevata disponibilità/affidabilità e tempi di reazione estremamente ridotti. Questo perché le organizzazioni pubbliche (forze di polizia, operatori dell'emergenza, operatori sanitari, …) e private (es. operatori di infrastrutture critiche, grandi industrie, trasporti, …) che le impiegano devono affrontare situazioni operative nelle quali anche pochi secondi di ritardo possono avere impatti in termini di vite umane e/o danni al business incalcolabili.

Il 5G è la tecnologia pensata per supportare i sistemi mission-critical in tre modi principali.

1. È caratterizzata da una latenza molto bassa, metà della latenza del 4G, che assicura estrema reattività
2. Può gestire richieste di banda molto elevate, da quattro a cinque volte quella del 4G, garantendo la possibilità di servizi dati estremamente sofisticati
3. È pensata per garantire un'elevata disponibilità (99,999%) assicurando il servizio anche in scenari estremamente complessi di "fail" degli elementi di rete (IOPS, PROSE).

Mission Critical Communications (MCC) è uno degli elementi chiave delle reti 5G. Con la standardizzazione di MCC avviata con la Release 13 del 3GPP, le comunicazioni mission-critical vengono fornite come servizio di rete che consente agli operatori dell'emergenza - polizia, vigili del fuoco e personale medico di emergenza - di aggiungere ai servizi di una radio tradizionale le moderne capacità di comunicazione che sono oggi disponibili per qualsiasi utente di rete commerciale dotato di uno smartphone.

Nelle reti 5G, i First Responder MCC possono integrare i servizi voce Push-to-Talk con Push-to-Video, e sevizi dati multimediali per condivisione di video, chat

di gruppo, condivisione di file, condivisione della posizione, il tutto supportato da una completa gestione delle priorità e della qualità del servizio sulla Rete.

Grazie ai servizi MCC in uno scenario di disastro naturale o incidente primi soccorritori possono condividere un video in diretta dal luogo del disastro tra i membri del team, nonché ricevere video da droni, telecamere di sorveglianza, aerei e satelliti in tempo reale. Possono anche condividere la loro posizione, migliorando notevolmente il lavoro di squadra e la comunicazione di gruppo.

Le reti 5G permettono di includere anche automobili e "cose" nel flusso di comunicazione: servizi come V2X (vehicle to any) e MTC (Machine Type Communications) sono supportati nativamente, il che consente agli operatori Mission Critical di creare tipi di soluzioni che prima non si pensava nemmeno possibili. Sensori di temperatura, sensori di umidità, sensori di velocità e direzione del vento, sensori termici e molti altri, possono diventare un "elemento salvavita", nell'ambito di una missione. Senza considerare la possibilità di integrare robot (UGV, UAV, …) ed automi ad esempio per operazioni di ricerca e salvataggio.

Altre tecnologie abilitate dalle reti 5G che possono avere un impatto significativo per gli operatori mission critical sono la Realtà Aumentata (AR) e la Realtà Virtuale (VR). Ad esempio, un primo soccorritore potrebbe indossare occhiali speciali o un casco, dove tutte le immagini vengono visualizzate direttamente sullo schermo della maschera, inclusi video, identificazione dell'oggetto, mappa, posizione dei membri del team e altro.

Il valore della rete sta nei servizi che può fornire. Con l'avvento dell'era 5G, quei servizi saranno più avanzati, fluidi e dinamici che mai e spesso sviluppato in collaborazione con terze parti / partner e in continua evoluzione per supportare le nuove esigenze del cliente.

Questa flessibilità senza precedenti fatta di enormi quantità di dispositivi collegati e applicazioni fornite, porterà a rivedere il tradizionale perimetro di rete. Se la sicurezza attuale ha dei requisiti già abbastanza difficili da gestire, i prossimi anni porteranno dei livelli di complessità completamente nuovi.

Il cloud, le reti software-defined (SDN) e l'evoluzione del 5G richiedono tutti un cambiamento nelle operazioni di sicurezza, in particolare l'uso dell'automazione a supporto di nuovi casi d'uso per garantire la sicurezza e l'erogazione del servizio.

È pertanto importante capire come integrare gli apparati nell'ambiente globale tenendo conto delle metodologie e processi presenti ma anche delle future evoluzioni e delle operazioni che verranno implementate.

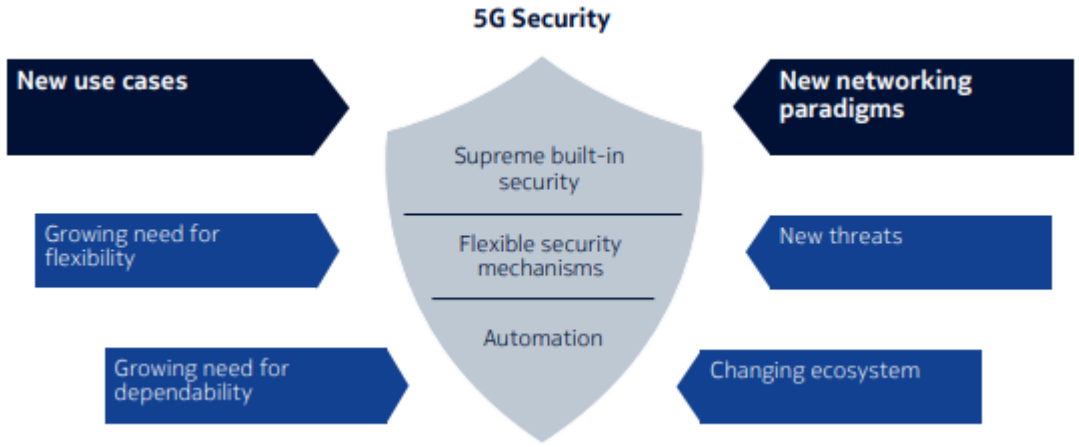

Fig. 3 – Scenario Cybersecurity 5G

5.1.2. Operazioni di sicurezza con orchestrazione, analisi e Automazione

Il mondo del 5G richiede ai CSP di ampliare il loro approccio alla sicurezza per comprendere altre tecnologie, come il cloud e l'IoT. Ciò richiede la raccolta di dati relativi al servizio dalla rete – prestazioni, Syslog, informazioni da eventi di sicurezza.

Questi dati devono quindi essere correlati in tempo reale per creare un quadro più dettagliato di ciò che accade nella rete. Le reti 5G abbracciano molti domini infrastrutturali, possibilmente indipendenti, e contengono numerose funzioni virtuali ma anche apparati fisici. Questa complessità richiede flussi di lavoro automatizzati per ridurre il tempo e lo sforzo per fornire servizi e la sicurezza, la gestione e l'orchestrazione adattando automaticamente le funzioni di sicurezza per una gestione più efficace dei vari cambiamenti.

Operazioni di sicurezza efficaci si basano su strumenti che soddisfano le richieste di prestazioni delle reti virtuali e supportare altri requisiti, come la scalabilità della rete stessa e dei servizi offerti.

I principi chiave di Security Orchestration, Analytics e Response/Reporting (SOAR) includono:

- Misura costante dello stato della sicurezza e dei livelli di rischio.
- Controllo e limitazione dell'accesso ai principali sistemi operativi e risorse in aggiunte alla usuale sicurezza perimetrale per la governance e la gestione degli accessi fino al livello di esecuzione dei comandi.
- Rilevamento delle minacce all'inizio della catena di mitigazione. Il rilevamento precoce richiede analisi multidimensionali tra sistemi e risorse per identificare le minacce che altrimenti potrebbero non essere rilevate. Lo scopo è identificare anomalie dal comportamento normale e identificare in modo proattivo gli attori dannosi, aiutare gli analisti della sicurezza a dare priorità al rischio e avviare la risposta rapida appropriata.
- Risposta rapida per ridurre al minimo l'impatto degli attacchi informatici: il tempo che intercorre tra il rilevamento e la mitigazione deve essere quasi eliminato. È qui che l'automazione dei processi di sicurezza gioca un ruolo chiave.

5.1.3. Operazione nel CyberSpazio

Nell'ambito della trasformazione del cyberspazio, la sperimentazione svolge un ruolo chiave per testare ed esplorare soluzioni esistenti e in via di sviluppo, accelerando così la fornitura di soluzioni critiche applicabili agli scenari del cyberspazio.

I fornitori delle tecnologie chiave per le reti mission-critical in tutto il mondo propongono diverse funzionalità relative al Cyberspazio, in particolare in relazione a:

- Consapevolezza dei possibili scenari operativi
- Soluzioni di intelligenza artificiale/machine learning
- Sistemi di supporto alle decisioni
- Automazione per la gestione delle minacce informatiche.

Si devono prevenire le intrusioni di soggetti non autorizzati, e proteggersi dagli attacchi interni. Si devono prevenire l'esfiltrazione dei dati, il danneggiamento dei sistemi o dei loro componenti. Devono proteggersi dal denial-of-service e garantire che i sistemi non vengano utilizzati per attacchi denial-of-service.

Ci si deve anche assicurare che i dati utilizzati da questi sistemi siano corretti e di buona qualità e sviluppare nuove capacità.

Uno degli argomenti principali è rendere più semplici le attività di sicurezza perché se ne possano automatizzare molte, perché si possano sfruttare tecniche uniche per cercare, rilevare e agire.

Se si è in grado di prevedere cosa è probabile che venga attaccato e come, se si possono definire delle risposte automatiche per mitigare l'impatto e l'attacco, se si può controllare e testare il modello predittivo per vedere se è danneggiato da input non validi, allora ci si può affidare a questi sistemi.

Le cosiddette Emerging and Disruptive Technologies (EDT), come l'Intelligenza Artificiale o l'Analisi dei Big Data, rappresentano una sfida importante ma anche un'opportunità. L'effetto dirompente del loro sviluppo e delle loro applicazioni specifiche avrà ramificazioni in ciascuno dei domini operativi, ma può anche presentare sfide di nuovo tipo.

5.2. Attacchi alla supply-chain

Gli attacchi alla supply chain sono in costante aumento. Gli effetti devastanti e a catena (non siamo davanti a un gioco di parole, purtroppo) provocati da questo genere di minacce si sono manifestati in tutta la loro forza e distruttività con il caso SolarWinds, piattaforma di gestione software vittima di uno spietato hackeraggio in grado di evadere le difese dell'azienda texana riuscendo a raggiungere i suoi clienti in tutto il mondo.

Purtroppo, la drammaticità di questo evento non ci deve sorprendere se pensiamo che, anche nell'ambito della cybersecurity, il concetto di supply chain coinvolge davvero un'ampissima gamma di risorse: hardware, software, cloud, storage, applicazioni. E non solo: a ben vedere, un attacco alla supply chain non è altro che una combinazione di almeno due attacchi. Il primo attacco coinvolge un fornitore che a sua volta viene poi utilizzato per attaccare

l'obiettivo finale (tipicamente il cliente, o un altro fornitore) e ottenere l'accesso alle sue risorse.

Pertanto, affinché un attacco sia classificato come attacco alla supply chain, sia il fornitore che il cliente devono essere obiettivi. Interessante, dal punto di vista tassonomico, osservare come le tecniche di attacco e gli asset colpiti varino a seconda dell'obiettivo prescelto.

Secondo i dati prodotti da Enisa nel report "Threat Landscape For supply chain Attacks"[12], si è infatti osservato come, dal punto di vista del fornitore, le tecniche di attacco più diffuse siano costituite da infezione da malware, social engineering, attacchi brute-force, prendendo di mira asset quali librerie e software preesistenti, codice e configurazioni.

Al contrario, le variabili in gioco degli attacchi che coinvolgono i clienti sono diverse, con una predilezione per il phishing ad esempio, e compromettendo asset quali dati (personali, di pagamento e finanziari, email, proprietà intellettuale, etc.).

5.3. Approccio Zero-Trust

Dall'indagine svolta da Enisa è emerso inoltre che il 66% dei vettori di attacco utilizzati sui fornitori rimane ancora sconosciuto, mentre per il 16% sono state sfruttate delle vulnerabilità software. Dati, questi, che portano a una riflessione profonda sulla capacità di indagine di molte aziende e su un livello di "fiducia" diffuso presente all'interno della stessa supply chain. In molti casi, infatti, il servizio del fornitore diventa, agli occhi del cliente, automaticamente sicuro, privo di minacce: in poche parole, "trusted". Per questo, si rende (purtroppo) necessario eliminare completamente il concetto di fiducia secondo il quale se un fornitore è affidabile, lo saranno automaticamente anche i servizi offerti. Per affrontare un panorama in costante evoluzione, con minacce sempre più sofisticate, è fondamentale introdurre un approccio Zero Trust.

Questo tipo di approccio - ben riassunto in "non fidarsi mai, verificare sempre"- presuppone l'assenza di un perimetro di rete affidabile, secondo il quale ogni transazione deve essere autenticata prima che possa concretizzarsi.

[12] https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

Grazie a un rigoroso controllo e una verifica serrata di ogni singolo elemento dell'infrastruttura - reti, applicazioni, utenti, cloud pubblici e privati - è possibile osservare tutte le anomalie - spesso inaspettate, come quelle che coinvolgono i servizi dei propri fornitori, per definizione affidabili(!) - che, se maligne, sono prontamente rilevate e bloccate.

Questo principio deve essere applicato in maniera olistica su tutta la catena di fornitura, sia da chi produce i beni e i servizi, sia da chi li riceve, con la sicurezza a costituire un elemento intrinseco e radicato fin dagli esordi della produzione del software stesso. Limitare quel 16% di attacchi che utilizzano vulnerabilità software dei fornitori è oggi possibile con una gestione Shift-left e un approccio DevSecOps: se i controlli si spostano sempre più verso l'origine del software e le verifiche del codice saranno continue, verrà certamente garantita una miglior sicurezza e resilienza.

Di fatto quindi, oggi, qualsiasi organizzazione produce software e qualsiasi soggetto coinvolto nella catena di fornitura può essere a sua volta considerato cliente o fornitore.

Zero Trust e sviluppo sicuro del software sono le chiavi per proteggere questo vastissimo ecosistema di processi, persone, organizzazioni che ogni giorno sono coinvolti nella creazione e nella consegna di beni e servizi.

5.3.1. Costruire una strategia Zero-Trust

Quando non seguono le strategie Zero Trust, le aziende devono affrontare un'ampia gamma di sfide associate alla protezione degli ambienti distribuiti. Il modello Zero Trust di Forrester per la sicurezza delle informazioni è un modello concettuale e architettonico che spiega come i team di sicurezza dovrebbero:

1. riprogettare le reti in microperimetri sicuri;
2. utilizzare l'offuscamento per rafforzare la sicurezza dei dati;
3. limitare i rischi associati ai privilegi eccessivi degli utenti;
4. utilizzare l'analisi e l'automazione per migliorare drasticamente il rilevamento e la risposta alla sicurezza.

I pilastri del modello Zero Trust di Forrester sono sette (vedi Figura sotto):

Fig. 3 - Forrester Zero Trust eXtended (ZTX) Framework

Zero-Trust per i dati. La protezione e la gestione dei dati, la categorizzazione e lo sviluppo di schemi di classificazione dei dati e la crittografia dei dati a riposo e in transito sono fondamentali per qualsiasi approccio Zero Trust.

Zero-Trust per gli Utenti. La limitazione e l'applicazione dell'accesso degli utenti e la protezione degli utenti che interagiscono con Internet, attraverso il monitoraggio continuo e la gestione degli accessi e dei privilegi, sono una componente fondamentale di Zero Trust.

Zero-Trust per le Applicazioni. I carichi di lavoro sono i sistemi front-end e back-end che gestiscono l'azienda e la aiutano a conquistare, servire e fidelizzare i clienti. Come per qualsiasi altra area di Zero Trust, queste connessioni, applicazioni e componenti devono essere trattate come un vettore di minacce e devono essere dotate di controlli Zero Trust come l'ispezione e il controllo delle API basati su policy, la protezione dei file e della memoria attiva dei container e il firewall dell'host guest. Particolarmente preoccupanti sono i carichi di lavoro eseguiti nei cloud pubblici.

Zero-Trust per le Reti. La capacità di segmentare, isolare e controllare la rete è un punto di controllo importante per lo Zero Trust. La segmentazione e l'isolamento aiutano a proteggere meglio le reti.

Zero-Trust per i Dispositivi. La scoperta, l'isolamento e la gestione dei dispositivi sono fondamentali per controllare i rischi associati all'hardware del dispositivo, al comportamento dell'utente, alle app e ai dati a cui si accede dal dispositivo.

Visibilità e analisi. L'analista di sicurezza deve avere la capacità di osservare con precisione le minacce presenti e orientare le difese in modo più intelligente.

Automazione e orchestrazione. Le organizzazioni e la leadership della sicurezza devono utilizzare strumenti e tecnologie che consentano l'automazione e l'orchestrazione della sicurezza (SAO) in tutta l'azienda, per ridurre i tempi di risposta agli incidenti e integrare soluzioni di sicurezza diverse. L'orchestrazione estende i criteri di sicurezza agli ambienti cloud.

5.3.2. Come ottenere il successo di Zero Trust

Per migliorare l'efficacia dei vostri sforzi di Zero Trust, sono necessarie due azioni:

1. implementare soluzioni con sicurezza intrinseca
2. alleviare i problemi organizzativi e culturali che ostacolano la collaborazione tra i team IT e di sicurezza.

Una recente ricerca condotta da Forrester Consulting ha rilevato quanto segue:

- **La sicurezza intrinseca riduce al minimo il rischio residuo di problemi tecnici**. Le soluzioni di sicurezza intrinseca sono soluzioni software integrate che aiutano le aziende a ridurre i vettori di minacce grazie al fatto che sono integrate anziché integrate, unificando gli strumenti e i team per migliorare la visibilità e utilizzando il contesto in tempo reale per rilevare e rispondere meglio alle minacce.
- **La sicurezza intrinseca riduce la complessità e i costi.** Un'indagine e una riparazione più rapide e una riduzione della

complessità grazie alla sicurezza intrinseca si traducono in una riduzione delle spese di capitale e operative.

- **Le possibilità di successo aumentano rendendo la Zero-Trust un'attività collaborativa**. Il successo di Zero Trust dipende dal fatto che l'intera organizzazione si concentri sullo stesso obiettivo, con i professionisti dell'IT e della sicurezza che lavorano in collaborazione. Abbattete i silos dell'IT e della sicurezza riunendo i team per stabilire obiettivi, traguardi e misure di successo concordati.

6. NUOVI TREND NELLA SICUREZZA: BLOCKCHAIN & QUANTUM

6.1. Blockchain e Cybersecurity

La Blockchain è notoriamente la tecnologia sottostante il mondo delle criptovalute, ma negli ultimi anni è stata reinterpretata e utilizzata come una tecnologia efficiente e robusta per governare le interazioni tra diversi attori o *devices* in modalità sicura, affidabile e decentralizzata.

Le transazioni della Blockchain sono immagazzinate in una *catena di blocchi* non modificabile. Questi blocchi sono validati, in gergo *minati* (dal processo di *mining*, caratteristica tipica di ogni Blockchain) da nodi certificatori, in modalità *permisionless* su reti pubbliche come nel caso di BitCoin o Ethereum, oppure su reti private *permissioned* come nel caso di Hyperledger.

In ambito Telco e in particolare per le reti 5G, la modalità *permissioned* Blockchain risulta quella più indicata, per ottimizzare i costi, per assicurare un ulteriore livello di sicurezza per la privacy dei dati degli utenti finali e degli operatori e per evitare qualsiasi violazione del GDPR.

Vediamo alcuni casi di cybersecurity abilitati dalla tecnologia Blockchain sulle infrastrutture di rete:

- **Condivisione delle infrastrutture di rete 5G**: la gestione delle reti di telecomunicazioni sta diventando sempre più complessa anche a causa di una frammentazione degli attori in gioco. In ambito mobile, ad esempio, gli standard prevedono la possibilità di una condivisione di elementi attivi, quali quelli della RAN (modello MOCN o MORAN) o della Core Network (modello GWCN) o degli elementi passivi quali la condivisione di siti di celle, torri e infrastruttura passiva in generale. Grazie all'uso della tecnologia Blockchain e in particolare degli smart contracts, da essa abilitati, è possibile gestire in modalità automatica, sicura e dinamica la condivisione di elementi di rete senza la necessità di intermediari e secondo il modello decentralizzato introdotto da Blockchain.
- **Gestione e autenticazione di dispositivi IoT per il mondo 5G**: molti degli use case del 5G sono basati su comunicazioni a bassa

latenza per dispositivi IoT in scenari ad alta densità (Massive Machine-Type Communications, mMTC, e Ultra Reliable Low Latency Communications, uRLLC). La gestione di un numero così elevato di dispositivi in scenari a bassa latenza, con diversi attori coinvolti, usando un modello centralizzato in cui un'unica identità gestisca sia l'autenticazione dei dispositivi che le relative applicazioni, potrebbe risultare poco efficiente. La Blockchain invece, con il suo modello decentralizzato e l'abilitazione degli smart contracts, permette di assicurare un maggiore livello di sicurezza, una migliore tracciabilità, una riduzione dei costi di gestione dovuta alla condivisione dei dati.

- **Fraud Prevention per International Roaming**: nelle procedure di Roaming Internazionale, le frodi avvengono quando un utente accede alle risorse della propria rete mobile di provenienza (home network) attraverso la rete mobile visitata in un altro paese (visited network). L'operatore della home network non può addebitare in tempo reale il costo dei servizi offerti all'utente ed è comunque obbligato a pagare il servizio di roaming all'operatore della visited network. In questo caso l'utente fraudolento sfrutta i tempi lunghi di verifica e risposta tra le due entità di rete coinvolte. Grazie alla Blockchain è possibile applicare procedure di Real Time Data Clearing, ovvero tutte le entità coinvolte nella procedura di roaming costituiscono una Permissioned Blockchain attraverso uno smart contract basato sui dati di CDR (charging data record) inseriti nella rete Blockchain: la procedura di riconciliazione è ora real-time e utente fraudolento può essere bloccato immediatamente.
- **Blockchain per Number Portability**: Fenomeni di subscription identity fraud, che si verificano quando un utente accede ai servizi della rete mediante falsa identità, possono essere arginati dalla Blockchain, soprattutto in uno scenario di collaborazione tra gli operatori: sostituendo database indipendenti (e non necessariamente aggiornati) con un modello di Blockchain comune, sicuro, condiviso e distribuito, portando ripercussioni sia sui costi che sulla sicurezza della rete. Un esempio è sicuramente la Number Portability, un sistema attualmente piuttosto complesso sia per l'assenza di uno standard internazionale condiviso, sia poiché basato su un modello centralizzato inadatto a gestire più di un certo quantitativo di richieste nell'unità di tempo. Blockchain, offrendo a tutti gli operatori un modello fondato sulla trasparenza, sempre aggiornato e sicuro, permetterebbe transazioni e

cambi operatore in tempi ridottissimi, con in più tutta la sicurezza e la trasparenza che sono insite in un registro condiviso abilitato dalla stessa tecnologia Blockchain.

- **BlockChain per combattere il Calling Line Identity Spoofing**: Il CLI Spoofing è una tecnica fraudolenta che consiste nella sostituzione del vero calling line identity con un altro numero prima della consegna della chiamata al destinatario. Nei paesi anglosassoni attualmente per combattere il fenomeno è usata la modalità STIR/SHAKEN, un meccanismo di sicurezza nei protocolli di rete in grado di eliminare la vulnerabilità. Un metodo alternativo è quello di utilizzare la tecnologia blockchain all'interno di un consorzio di operatori a livello internazionale, in grado di certificare l'identità dell'utente chiamante attraverso un registro condiviso abilitato proprio dalla Blockchain.

6.2. Quantum Key Distribution

La Quantum Key Distribution (QKD) è una tecnica di distribuzione sicura di chiavi di crittografia che si basa su fenomeni fisici di tipo quantistico. Le chiavi scambiate con questa tecnica possono essere utilizzate da qualsiasi sistema di crittografia simmetrico. La bassa velocità di trasmissione impiegata rende la QKD adatta soltanto allo scambio delle chiavi e non alla comunicazione di altri tipi di informazioni.

Il principio alla base della QKD è l'impiego di un canale di comunicazione non sicuro per lo scambio delle chiavi sul quale viene utilizzato un protocollo che sfrutta lo stato quantistico di particelle elementari. Tipicamente si utilizzano fotoni poiché questi interagiscono poco con la materia circostante e possono essere trasmessi su distanze relativamente lunghe senza una alterazione eccesiva del loro stato quantistico.

Mediante l'impiego di un ricevitore a singolo fotone è possibile rilevare lo stato quantistico dei fotoni e da questi ricavare la chiave trasmessa.

La sicurezza della QKD si basa direttamente sulle leggi fondamentali della meccanica quantistica secondo le quali non è possibile rivelare o copiare lo stato quantistico di una particella senza modificarlo. Questo consente al sistema di ricezione di rivelare eventuali intrusioni sul canale di scambio delle chiavi.

Il canale fisico sul quale vengono trasmessi i fotoni può essere costituito dallo spazio libero (ad es. per comunicazioni satellitari) oppure da una fibra ottica. Le tecniche di QKD su fibra ottica sono particolarmente interessanti perché utilizzano lo stesso mezzo fisico comunemente impiegato nelle reti di telecomunicazioni terrestri.

I primi sistemi commerciali di trasmissione di chiavi crittografiche mediante QKD utilizzano come stato quantistico la polarizzazione dei fotoni e sono in grado di raggiungere distanze massime di alcune decine di km.

La principale limitazione di questi sistemi è la loro incompatibilità con gli amplificatori ottici e con i sistemi di multiplazione WDM attualmente impiegati nelle reti di telecomunicazioni. Il canale di comunicazione per lo scambio di chiavi deve quindi essere realizzato con una coppia di fibre dedicate e, nel caso la distanza da raggiungere sia superiore a quella massima consentita dal sistema QKD, occorre inserire lungo il percorso dei "trusted node" che siano in grado di rigenerare il protocollo quantistico.

Per superare queste limitazioni e per ridurre i costi ancora elevati di queste soluzioni sono in corso sperimentazioni in molti paesi del mondo. In particolare, la Comunità Europea all'interno dei suoi programmi di finanziamento della ricerca sta promuovendo la progettazione di una rete europea basata su QKD.

www.anitec-assinform.it