RELAZIONE NAVIGATION 5G SECURITY

I. INTRODUZIONE

Le reti 5G sono ormai considerate un'infrastruttura critica nazionale. Assieme alla potenza, velocità e capacità della rete, sono aumentate anche le minacce e la loro complessità.
Con l'aumentare delle opzioni di implementazione (come SA e NSA) e degli attori in gioco (stakeholder, operatori delle comunicazioni, utilizzatori, …) è aumentata la complessità dell'ecosistema, e quindi la difficoltà nel proteggerlo. Quindi, è facile capire come anche strumenti e misure di protezione devono evolversi.
In questo paper vengono quindi proposti tre contributi volti a promuovere l'implementazione di metodologie di garanzia e valutazione della sicurezza che coprano diverse fasi del ciclo di vita del 5G

II. EU CYBERSECURITY PERSPECTIVE

La sicurezza delle reti 5G è considerata essenziale per garantire l'autonomia strategica dell'Unione quindi affrontarla richiede più che gli sforzi dei singoli Stati. In questo scenario, ha un ruolo primario l'Agenzia dell'Unione Europea per la sicurezza informatica (ENISA). Negli ultimi anni, l'ENISA e il gruppo di cooperazione NIS [7] hanno pubblicato diversi documenti e relazioni, tra cui:
• La valutazione coordinata dei rischi per la sicurezza informatica delle reti 5G a livello UE
• Il pacchetto di strumenti UE per la sicurezza informatica delle reti 5G
• La matrice dei controlli di sicurezza 5G
ENISA sta inoltre sviluppando un sistema candidato di certificazione per la sicurezza informatica sul 5G, denominato schema EU5G, la cui base è probabilmente NESAS. Il NESAS, sviluppato congiuntamente da 3GPP e GSMA, è uno schema volontario immediatamente applicabile alle apparecchiature di rete mobile, che opera attraverso i seguenti due approcci:
• Valutazione della sicurezza relativa ai processi di sviluppo e al ciclo di vita del prodotto del fornitore.
• Valutazione della sicurezza delle apparecchiature di rete tramite test di sicurezza standardizzati (test SCAS) condotti da un laboratorio accreditato.
Con NESAS come base di riferimento, sarebbero comunque necessari ulteriori sforzi per allineare EU5G ai requisiti del Cybersecurity Act. In conformità con il framework NESAS, i test delle specifiche di garanzia della sicurezza (SCAS) sono progettati da 3GPP per valutare la sicurezza dei prodotti di rete e sono pubblicati nella serie TS 33, che contiene test sia per prodotti di rete generici che specifici per il 5G. Anche questi test hanno bisogno di essere aggiornati per far fronte alle nuove esigenze.

III. Risultati

A. ScasDK: un framework per i test SCAS

ScasDK è un framework che consente ai laboratori di test di terze parti di progettare, sviluppare ed eseguire test SCAS su infrastrutture core 5G virtualizzate con funzioni di rete closed-source multi-vendor. I test SCAS hanno lo scopo di verificare se le implementazioni delle funzioni di rete soddisfano gli scenari limite specificati nello standard 3GPP. Ciò si ottiene innescando comportamenti anomali in diversi punti della rete e verificando se la reazione della funzione di rete sottoposta a test sia conforme alle specifiche di sicurezza. Per affrontare le sfide del 5G, è stato sviluppato un nuovo modello con funzioni di rete closed-source. Utilizza componenti standard con comunicazioni intercettate da proxy ad hoc che consentono la modifica dinamica dei messaggi e un facile adattamento agli aggiornamenti.

Questo modello supporta l'attivazione di comportamenti anomali, il coordinamento dei componenti e il monitoraggio delle comunicazioni, essenziali per supportare test SCAS più complessi rispetto allo scenario di base.
Diversi tipi di proxy soddisfano protocolli specifici cruciali per le operazioni 5G:
• Protocollo NGAP/NAS: per la comunicazione tra EU/gNB e AMF.
• Protocollo HTTP: per la comunicazione all'interno delle funzioni di rete del piano di controllo dell'architettura basata sui servizi.
• Protocollo PFCP: per la comunicazione tra SMF e UPF.
La prima versione del framework offre due di questi tre proxy, quello per NGAP/NAS e quello per HTTP. ScasDK è stato validato sviluppando un sottoinsieme di test SCAS, eseguendoli su tre implementazioni open source di reti core.

B. Test crittografici
Le pratiche di sicurezza 5G incorporano molti principi allineati al concetto di zero trust. Qui, le funzioni di autenticazione assumono un'importanza primaria e, di conseguenza, le funzioni crittografiche su cui si basano. Queste ultime sono il fondamento della protezione delle informazioni sensibili nelle reti 5G e del funzionamento senza interruzioni di vari servizi.
a) Test della corretta implementazione degli algoritmi crittografici
I processi di valutazione della sicurezza includono attività volte a verificare la corretta implementazione delle funzioni e dei protocolli crittografici. Queste attività consistono in test funzionali (black box) dell'implementazione, integrati o sostituiti con l'ispezione (grey/white box) delle porzioni SW/FW/HW pertinenti.
Per testare la corretta implementazione delle funzioni crittografiche ci sono due approcci: diretto o indiretto. Il test diretto richiede l'accesso alle interfacce di input e output della funzione e la disponibilità di vettori di test opportunamente definiti. I vettori di test sono specificati nell'ambito del 3GPP per varie funzionalità crittografiche richieste per specifici componenti della rete 5G, tra cui le funzioni di autenticazione e generazione di chiavi utilizzate nel protocollo 5G Authentication and Key Agreement (5G AKA) e altri. In genere, le interfacce necessarie per i test diretti non sono più accessibili una volta che la funzionalità crittografica è stata integrata in un componente della rete 5G. L'idea del test indiretto delle funzioni crittografiche si basa sul presupposto che la prova della corretta implementazione di una funzione crittografica possa essere ottenuta da test definiti per altri scopi, in particolare da test SCAS la cui esecuzione richiede al componente di invocare funzioni crittografiche.
b) Test della configurazione dei protocolli di rete in relazione al supporto degli algoritmi crittografici
Nel mondo delle reti cellulari, le vulnerabilità di sicurezza derivano spesso da configurazioni errate all'interno dei loro meccanismi di protezione. Errori di configurazione possono verificarsi inaspettatamente e possono derivare da varie fonti, come errori umani, interpretazioni errate delle linee guida sulla sicurezza o semplicemente l'applicazione impropria delle regole standard 3GPP che, in alcuni casi, sono influenzate da un significativo grado di labilità e opzionalità, come evidenziato da un recente rapporto approfondito dell'ENISA. 5GMap è uno strumento per valutare i parametri di sicurezza all'interno delle reti cellulari operative (LTE e 5G) e individuare casi di configurazione errata. 5GMap estrae gli algoritmi di sicurezza supportati dalle stazioni base e dalle reti core e determina gli algoritmi predefiniti scelti da queste entità. Inoltre, il comportamento del sistema è stato esaminato in alcuni casi limite:
• Se una connessione viene stabilita o meno quando solo l'algoritmo di crittografia o integrità nullo è incluso nelle capacità.
• Se una connessione viene stabilita o meno quando le capacità includono l'algoritmo di crittografia (o integrità) nullo insieme a un algoritmo che sembra non essere supportato dalla stazione base e/o dalla rete core.

L'obiettivo è verificare se la rete stabilisce una connessione anche quando non è in grado di supportare la sicurezza richiesta dall'utente.
I test hanno rivelato differenze nelle scelte algoritmiche tra i vari operatori esaminati: due su tre non supportano nemmeno alcun livello di crittografia NAS. Per quanto riguarda le differenze di configurazione tra le diverse celle fisiche, l'esperimento ha dimostrato che le celle analizzate sono configurate con gli stessi parametri di sicurezza.

C. Approccio basato su ontologie per la base di conoscenza sulla sicurezza informatica
Il processo di valutazione del rischio richiede un'identificazione iniziale degli asset rilevanti all'interno dell'architettura. Successivamente, assegnando i controlli di sicurezza alle vulnerabilità sfruttabili, si riduce la superficie di minaccia degli asset. Tuttavia, l'applicazione di questa metodologia al contesto di un servizio 5G non è semplice: i servizi 5G si basano su un'infrastruttura sottostante che include hardware, software e processi, con le loro minacce e vulnerabilità altamente specifiche. In tale scenario virtualizzato, le minacce alla sicurezza associate sono un mix di minacce relative alle reti fisiche e alle tecnologie di virtualizzazione. Di conseguenza, l'attenzione è stata rivolta all'utilizzo di ontologie, tecnologie utili per la standardizzazione e la rappresentazione della conoscenza, con particolare attenzione all'automazione.
Uno studio introduce una nuova prospettiva per delineare l'ambiente operativo attraverso un'analisi della sicurezza basata su ontologie all'interno di un'architettura 5G complessa. In primo luogo, viene presentato un modello architetturale che integra framework standardizzati. In secondo luogo, viene proposto un nuovo metamodello ontologico fondamentale che incorpora elementi di sicurezza informatica per l'analisi dei servizi 5G forniti su un'architettura di rete basata sui servizi.
L'ontologia è suddivisa in 6 sotto-ontologie: 3 sono relative alla definizione del servizio, all'implementazione dello slice e alla gestione degli elementi; le restanti introducono 3 pilastri concettuali per la valutazione della sicurezza: le minacce, le vulnerabilità e il meccanismo di sicurezza.

IV. CONCLUSIONI

L'evoluzione del 5G verso un'architettura dinamica e cloud-native richiede un approccio avanzato alla sicurezza, con solide misure di garanzia e valutazioni dei rischi. Pur offrendo miglioramenti rispetto alle reti precedenti (crittografia più forte, privacy potenziata, autenticazione unificata), la sicurezza del 5G va oltre gli standard, coinvolgendo tutte le fasi del ciclo di vita della rete. Il documento analizza il contesto europeo e propone strumenti e metodologie per garantire la sicurezza 5G, con l'obiettivo di supportare le decisioni strategiche e sviluppare soluzioni di monitoraggio e valutazione dei rischi.