Iper-connessi in sicurezza: la sfida del 5G

Contesto di riferimento

Gli attuali processi di trasformazione digitale stanno investendo l'intero pianeta con estrema velocità e pervasività. La commercializzazione di tecnologie *disruptive* crea le condizioni per realizzare concretamente relazioni sociali, casi d'uso e scenari inediti e innovativi.

Le persone, le organizzazioni pubbliche e private e in ultima analisi la prosperità delle società dipendono in maniera crescente dalle ICT e dalle comunicazioni mobili in particolare: secondo la GSMA[1] oggi ci sono al mondo oltre cinque miliardi di utenti di telefonia mobile e più di duemila operatori.

Le telecomunicazioni sono quindi un elemento cruciale: rappresentano la spina dorsale, l'infrastruttura essenziale delle comunicazioni digitali.

Quinta Generazione – 5G

Autorevoli economisti e *think tank* stimano che l'impatto economico globale della quinta generazione di telefonia mobile cellulare (5G) in termini di beni e servizi raggiungerà i 12 trilioni (miliardi di miliardi) di dollari entro il 2035, seguendo una dinamica che dall'interconnessione delle persone con altre persone e con l'informazione si sposterà all'interconnessione delle persone con qualsiasi cosa[2].

In Italia si è da poco conclusa l'asta per i diritti d'uso delle frequenze per il 5G. L'ammontare totale delle offerte per le bande messe a gara ha raggiunto i 6 miliardi e mezzo di euro, superando di oltre 4 miliardi l'introito minimo fissato

nella Legge di Bilancio.[3] I numeri testimoniano le elevatissime aspettative degli operatori di mercato. Un'interessante analisi sulle prospettive di sviluppo del 5G effettuata dall'Autorità per le garanzie nelle comunicazioni Italiana (AGCOM)[4] aiuta sia a delineare il quadro tecnologico delle reti 5G (*small cells[5], network densification, backhauling[6], massive MIMO*[7]) sia a prefigurare lo sviluppo dei principali mercati verticali che trarranno beneficio dalla nuova capacità tecnologica (settore auto e trasporti, energia e *smart grid*, manifattura e industria, media & entertainment, sanità e benessere).

Le previsioni degli analisti suggeriscono che nel 2019 ci saranno circa 24 miliardi di dispositivi collegati in rete e che nel 2020 le connessioni Machine To Machine (M2M) costituiranno circa la metà del totale dei dispositivi e delle connessioni[8]. Dobbiamo immaginare un mondo in cui non solo le persone, ma anche tutte le cose saranno connesse tra loro: le automobili con le strade che solcano, i medici con i dispositivi dei pazienti, i sensori disseminati sul territorio con diverse tipologie di macchine, etc.

Questa visione richiede un salto quantico del livello di connettività ma la posta in gioco è decisamente alta: le reti e i sistemi 5G sono il futuro dell'evoluzione delle comunicazioni e sarà loro richiesto di fornire capacità del tutto nuove.

Alla luce dell'importanza strategica del 5G, la Commissione Europea ha lanciato l'iniziativa 5G Public Private Partnership (5G-PPP)[9] come parte del programma Horizon 2020[10] al fine di favorire la collaborazione tra settori di tipo pubblico e privato per lo sviluppo del 5G. L'iniziativa 5G-PPP deve fornire soluzioni, tecnologie, architetture e standard per la nuova generazione di reti 5G soddisfacendo determinati requisiti.

I requisiti tecnici e funzionali del 5G riguardano

essenzialmente la **latenza**, l'**affidabilità**, la **capacità trasmissiva** e la **mobilità**: saranno necessari servizi caratterizzati da bassa latenza e alta capacità trasmissiva (navigazione su dispositivi mobili, *broadcasting* 4K/8K, etc), servizi a bassissima latenza e altissima mobilità (auto a guida autonoma) e servizi critici a minima latenza ed elevata disponibilità (automazione industriale e chirurgia remota).

In termini generali il 5G dovrà:

- integrare nuove reti di accesso radio in continuità con le tecnologie di rete introdotte dalle generazioni precedenti;
- consentire a miliardi di utenti e oggetti intelligenti nell'*Internet of Things* (IoT) di connettersi alle reti;
- trasmettere quantità enormi di dati in tempi ridottissimi;
- offrire supporto per densità di dispositivi (fino a 100 per metro quadrato);
- garantire ovunque trasmissioni sicure ed affidabili;
- essere altamente efficiente e ridurre il costo per unita` dei dati trasmessi.

Dal punto di vista tecnico, le reti 5G dovranno:

- aumentare significativamente l'attuale capacita` trasmissiva delle reti wireless (fino a 1000 volte);
- connettere 20 miliardi di dispositivi orientati alle persone;
- connettere 1000 miliardi di oggetti nell'IoT;
- risparmiare il 90% di energia utilizzata;
- supportare batterie di durata decennale per dispositivi a bassa potenza dell'IoT;
- assicurare tempi di latenza sotto i 5 millisecondi (ms) e velocita`di upload possibilmente fino a 10Gbps;
- fornire un'affidabilità percepita del 99,999%;
- ridurre il tempo richiesto per creare un servizio di rete da 90 ore a 90 minuti.

La tassonomia delle applicazioni 5G comprende diverse categorie in costante trasformazione quali, ad esempio:

- *Enhanced Mobile Broadband*, che include connettività mobile a banda ultra-larga, presenza virtuale, ologrammi e alta mobilità;
- *Critical Communications*, che include controllo industriale, droni e robot, veicoli ed emergenze;
- *Massive Machine Type Communications* (MMTC), che include il mondo degli oggetti indossabili, di controllo degli inventari, etc;
- *Network Operation*, che include lo *slicing[11]* delle reti, il *routing* e il risparmio energetico.

In termini generali, le precedenti generazioni delle comunicazioni mobili erano costruite per le interazioni umane, ma **la quinta generazione è progettata anche per le macchine**.

Tecnologie mobili e minacce cyber: evoluzioni parallele

Nel corso degli ultimi decenni le tecnologie e gli standard di comunicazione della telefonia mobile cellulare hanno rappresentato uno dei principali fattori abilitanti della *Digital Transformation*: ogni generazione tecnologica ha segnato un periodo di circa 10 anni e si è caratterizzata per l'introduzione di nuovi funzioni, nuovi scenari di utilizzo e nuove minacce di sicurezza:

Figura 1 – Generazioni della telefonia mobile cellulare

I sistemi di comunicazione *wireless* sono stati esposti a vulnerabilità di sicurezza sin dall'inizio: nella prima generazione (1G) i telefoni mobili e i canali *wireless* erano oggetto di attacchi di clonazione e *masquerading[12]*. Nella seconda generazione (2G), lo *spamming[13]* dei messaggi diventò estremamente comune per veicolare false informazioni o

trasmettere informazioni indesiderate. Nella terza generazione (3G) la comunicazione basata su IP ha consentito, di fatto, la migrazione delle vulnerabilità di sicurezza di Internet in un nuovo dominio, quello *wireless*. Con l'aumento della necessità di comunicare tramite IP, la quarta generazione (4G) ha facilitato la proliferazione di dispositivi *smart*, del traffico multimediale e di nuovi servizi. Tale sviluppo ha composto un panorama delle minacce cyber più complicato e dinamico. Con l'avvento della quinta generazione (5G), i vettori delle minacce cyber saranno ancora più importanti e ci sarà una grande attenzione alla tutela della privacy.

Minacce e soluzioni

Nell'interessante lavoro "*5G Security: Analysis of Threats and Solutions*"[14], gli autori individuano gli elementi abilitanti del 5G in tecnologie quali *Cloud Computing*, *Software Defined Networking* (SDN)[15] e *Network Function Virtualization* (NFV)[16]. Dopo aver riassunto le principali sfide di sicurezza (*Flash network traffic*, chiavi di cifratura delle interfacce radio inviate su canali insicuri, mancanza di protezione crittografica dell'integrità dei dati degli utenti, parametri di sicurezza dell'utente non aggiornati con il *roaming* da un operatore di rete all'altro,etc) passano in rassegna le principali minacce con le possibili soluzioni:

Minaccia	**Target**	**Tecnologia interessata**				**Privacy**
		SDN	**NFV**	**Canali**	**Cloud**	
Attacchi DoS[17]	Elementi di controllo centralizzati	X	X		X	
Attacchi Hijacking[18]	Controller SDN, Hypervisor	X	X			
Signaling Storms[19]	Elementi di rete core 5G			X	X	
Furto di risorsa (slice)	Hypervisor, risorse condivise nel cloud		X		X	

Minaccia	Target	Tecnologia interessata				Privacy
		SDN	NFV	Canali	Cloud	
Attacchi alle configurazioni	Virtual switch SDN, router	X	X			
Attacchi di saturazione[20]	Controller SDN e switch	X				
Attacchi di penetrazione	Risorse virtuali, cloud		X		X	
Furto d'identità dell'utente	Database con le informazioni degli utenti				X	X
Attacchi a livello TCP	Comunicazione controller-switch SDN	X		X		
Attacco Man-in-the-middle	Controller SDN	X		X		X
Reset e IP Spoofing	Canali di controllo			X		
Attacchi di scansione	Interfacce aperte			X		X
Esposizione delle chiavi di sicurezza	Canali non cifrati			X		
Attacchi semantici all'informazione	Posizione dell'abbonato			X		X
Timing attack[21]	Posizione dell'abbonato				X	X
Attacchi ai confini	Posizione dell'abbonato					X
Attacchi IMSI catching[22]	Posizione dell'abbonato			X		X

Tabella 1 – Sfide di sicurezza 5G

Oltre a presentare la lista delle principali minacce cyber, gli autori indicano anche le possibili soluzioni tecnologiche:

Tecnologia di sicurezza	Focus principale	Tecnologia interessata				Privacy
		SDN	NFV	Canali	Cloud	
Rilevamento attacchi DoS e DDoS	Sicurezza dei punti di controllo centralizzati	X	X			
Verifica delle configurazioni	Verifica delle regole dei flussi negli switch SDN	X				
Controllo degli accessi	Controllo degli accessi agli elementi SDN e della core network	X	X		X	
Isolamento del traffico	Garantire l'isolamento del traffico per le NFV e per le slice di rete		X			
Sicurezza del collegamento	Fornire sicurezza ai canali di controllo	X		X		
Verifica dell'identità	Verifica dell'identità degli utenti per servizi di roaming e cloud					X
Sicurezza dell'identità	Garantire la sicurezza dell'identità degli utenti					X

Tecnologia di sicurezza	Focus principale	Tecnologia interessata				Privacy
		SDN	NFV	Canali	Cloud	
Sicurezza della posizione	Garantire la sicurezza della posizione degli utenti					X
Sicurezza dell’IMSI	Mettere in sicurezza l’identità dell’abbonato tramite la cifratura					X
Sicurezza del terminale mobile	Tecnologie anti-malware					X
Verifica dell’integrità	Sicurezza dei dati e dei sistemi di storage nel cloud				X	
Mitigazione degli attacchi HX-DOS	Sicurezza per i cloud web service				X	
Controllo dell’accesso ai servizi	Sicurezza del controllo dell’accesso basato su servizi				X	

Tabella 2 – Tecnologie e soluzioni di sicurezza

Vulnerabilità note e incidenti di sicurezza

Nelle telecomunicazioni la parola “segnalazione” (*signalling*) indica l’utilizzo di segnali per controllare le comunicazioni.

I protocolli di segnalazione SS7[23], SIGTRAN[24], GTP[25] e Diameter[26] sono utilizzati dalle reti di telefonia mobile in tutto il mondo: è noto che tali protocolli presentano numerose debolezze di sicurezza che possono essere sfruttate in molti modi diversi. Nonostante non si tratti di attacchi su larga scala, l'impatto per i singoli utenti può essere molto significativo. Le prime generazioni (2G/3G) utilizzavano SS7 e SIGTRAN, protocolli progettati decenni fa. Nessuno all'epoca poteva immaginare la scala che le reti mobili avrebbero raggiunto, quindi il *trust* e la sicurezza non erano un grande problema. Al momento però usiamo ancora questi protocolli *legacy[27]* per assicurare l'interconnessione tra i fornitori di servizi di comunicazione. L'industria e la comunità dei ricercatori di sicurezza hanno iniziato a occuparsi della materia fornendo *good practice* e strumenti necessari, ma c'è ancora molto da fare[28]. Misure basilari di sicurezza sembrano essere state implementate dagli operatori più maturi, ma queste misure assicurano solo un livello di protezione minimo. L'attuale generazione (4G) usa un protocollo di segnalazione leggermente migliore chiamato Diameter: costruito con gli stessi principi di interconnessione ma su base IP, il protocollo è stato dimostrato essere vulnerabile[29]. L'industria sta ancora cercando di capire le implicazioni e identificare possibili *workaround*, ma il livello di minaccia è considerato significativo e degno della massima attenzione[30].

Nell'*"Annual Report Telecom Security Incidents 2017"*[31], ENISA ha analizzato gli incidenti di sicurezza riportati dagli operatori di telecomunicazione di 28 paesi Europei: il quadro normativo di riferimento obbliga gli operatori a notificare alle proprie autorità nazionali gli incidenti di sicurezza significativi. La vista degli incidenti è parziale in quanto, all'interno dell'Articolo 13a della direttiva Framework (2009/140/EC), è richiesto un report nel caso in cui l'incidente di sicurezza abbia causato una "significativa interruzione" dei servizi. L'articolo 40 dell'Electronic

Communications Code intende allargare il perimetro degli eventi da notificare includendo gli incidenti di sicurezza che comportano violazioni della riservatezza (*confidentiality breach*). Dal report emergono alcuni trend:

- la maggior parte degli incidenti ha un impatto sui servizi di telefonia mobile e Internet;
- gli incidenti di sicurezza che hanno impatti sui servizi di telefonia mobile e Internet coinvolgono la maggior parte degli utenti;
- i fallimenti di sistema sono la causa principale degli incidenti di sicurezza (62% dei casi);
- gli errori umani si ripercuotono su un elevato numero di connessioni degli utenti (in media, 1.2 milioni per incidente);
- gli incidenti causati da codice malevolo sono rari;
- i fenomeni naturali stanno causando un numero crescente di incidenti di sicurezza (18% dei casi);
- errori e fallimenti di terze parti rappresentano un quinto del totale degli incidenti di sicurezza.

Conclusioni

La sicurezza delle telecomunicazioni è una priorità assoluta: si tratta di un settore critico che, rispetto ad altri, presenta un livello di maturità in termini di sicurezza delle reti e dell'informazione senza dubbio maggiore. L'economia digitale si fonda su reti e servizi di telecomunicazione sicuri e resilienti ed è chiamata continuamente – in funzione di requisiti dinamici e sfidanti – a rinnovarsi adottando nuove tecnologie in favore di quelle obsolete. Le architetture 5G – *IT-driven* e progettate secondo principi di *multi-tenancy[32]* – aumenteranno la complessità tecnologica e la superficie di attacco: i processi di *softwarizzazione* (SDN) e *virtualizzazione* (NFV) delle reti e delle sue funzioni allargano a dismisura l'impronta del dominio software, con tutti i pro e i contro che ne conseguono. Pensando a Deleuze e

Guattari[33], il *divenire-software* del mondo fisico promuove una forma di nomadismo che trova il proprio climax nella mobilità assoluta: *everybody is everywhere anytime*. Peccato che non esistono attualmente modi di scrivere software intrinsecamente sicuro.

Secondo la visione di Ericsson[34], i *driver* di sicurezza 5G sono quattro: la definizione di nuovi modelli di *trust*, la sicurezza dei nuovi modelli di *delivery* dei servizi, un panorama delle minacce evoluto e l'aumento della preoccupazione per la privacy. Si tratta di *driver* che introducono nuovi requisiti, quindi la sicurezza 5G non potrà essere una copia carbone delle generazioni precedenti.

Le aspettative elevatissime e l'enorme clamore che accompagnano la narrazione relativa al 5G trovano le proprie radici nel fascino esercitato dalla prospettiva di un futuro immediato iper-connesso e velocissimo, in cui le barriere tra umanità e macchine tendono a dissolversi e si sperimentano nuove configurazioni sociali. La possibilità di includere nelle nuove infrastrutture tecnologiche elementi di sicurezza *by design*, facendo tesoro degli errori commessi nel passato, rappresenta un'opportunità da cogliere e da cui ognuno potrà trarre importanti benefici. I fiumi di *big data* – il nuovo petrolio – generati da umani e oggetti perennemente interconnessi, i risultati strabilianti di intelligenze artificiali alimentate da fantastici algoritmi di *Machine Learning*, la velocità crescente negli spostamenti quotidiani, la qualità esagerata di contenuti multimediali creati da produzioni artistiche sempre più raffinate e tanto altro ancora hanno bisogno di infrastrutture di rete capaci, robuste, resilienti, protette, affidabili e sicure.

Note

Articolo a cura di **Andrea Boggio**

Andrea Boggio è Business Development Manager in Fastweb dal 2014 ed è coinvolto in attività di prevendita e progettazione di servizi di Cyber e ICT Security, con particolare attenzione al settore della Pubblica Amministrazione. In precedenza ha lavorato presso multinazionali (HP, NTT Data) e presso aziende italiane focalizzate sulla sicurezza informatica.
Andrea lavora da oltre 15 anni nell'Information Security Arena e si occupa di diverse aree tematiche quali: Governance, Risk & Compliance, SIEM e SOC, Mobile Protection, Threat e Vulnerability Management, Network Security e Cyber Security.
Andrea detiene le certificazioni professionali ISO/IEC 27001:2013 Lead Auditor, CISA, CISM, CGEIT, CRISC, ITIL e diverse altre legate a specifici vendor di sicurezza, è membro del capitolo italiano di ISACA e ha partecipato al Cloud Security and Resilience Expert Group di ENISA.

https://www.ictsecuritymagazine.com/articoli/iper-connessi-in-sicurezza-la-sfida-del-5g/