# Relazione sulla Sicurezza nelle Reti 4G e 5G

## Introduzione

Le reti di telecomunicazioni di quarta e quinta generazione, note rispettivamente come 4G e 5G, hanno rivoluzionato il modo in cui le persone e le aziende si connettono al mondo digitale. Queste reti forniscono connessioni internet più veloci, affidabili e avanzate, abilitando una vasta gamma di servizi e applicazioni. Tuttavia, con l'aumento della complessità e della portata delle reti, emergono nuove sfide per la sicurezza. Questa relazione esamina i rischi e le misure di sicurezza nelle reti 4G e 5G.

## Rischi nella Sicurezza delle Reti 4G e 5G

1. Intercezione delle Comunicazioni: Le comunicazioni su reti wireless possono essere intercettate, specialmente se non sono crittografate correttamente. Ciò può portare a furti di dati sensibili.
2. Attacchi Man-in-the-Middle (MitM): Gli attacchi MitM consentono a un attaccante di intercettare e manipolare il traffico tra due parti. In reti 4G e 5G, le vulnerabilità MitM possono compromettere la sicurezza dei dati.
3. Attacchi Denial-of-Service (DoS): Gli attacchi DoS possono sopraffare una rete con traffico fittizio, rendendola inutilizzabile per gli utenti legittimi.
4. Smishing e Phishing: Gli attacchi di smishing (phishing via SMS) e phishing possono ingannare gli utenti per ottenere informazioni sensibili.
5. Vulnerabilità Hardware e Software: Le vulnerabilità nel hardware e nel software utilizzati nelle infrastrutture di rete possono essere sfruttate dagli attaccanti.

## Misure di Sicurezza

1. Crittografia: L'utilizzo di crittografia forte per la trasmissione dei dati è fondamentale. Le reti 4G e 5G implementano standard di crittografia avanzati come l'AES (Advanced Encryption Standard) per proteggere le comunicazioni.
2. Integrità dei Dati: L'uso di firme digitali e hash crittografici garantisce l'integrità dei dati trasmessi, impedendo l'alterazione durante la trasmissione.
3. Autenticazione Forte: L'autenticazione a più fattori (MFA) e le procedure di autenticazione robuste riducono il rischio di accessi non autorizzati.
4. Protezione contro gli Attacchi DoS: L'utilizzo di sistemi di rilevamento e mitigazione degli attacchi DoS aiuta a mantenere la disponibilità della rete.
5. Sicurezza a Livello di Dispositivo: Proteggere i dispositivi terminali è essenziale. Le aziende dovrebbero implementare politiche di sicurezza dei dispositivi e fornire regolarmente aggiornamenti di sicurezza.
6. Monitoraggio Costante: L'implementazione di sistemi di monitoraggio della rete consente il rilevamento tempestivo di attività sospette o intrusioni.
7. Consapevolezza e Formazione: L'istruzione degli utenti finali riguardo alle minacce online, insieme a sessioni di formazione sulla sicurezza, è fondamentale per prevenire attacchi di phishing e smishing.

I ricercatori hanno individuato alcune vulnerabilità della rete di telefonia cellulare che consentono ad un criminal hacker di intercettare le telefonate degli utenti, leggere gli SMS e tracciarne gli spostamenti: un problema serio soprattutto per i dirigenti di azienda e gli smart worker.

Durante i lavori dell’NDSS Symposium, un gruppo di ricercatori provenienti dalla Purdue University e dalla University of Iowa hanno svelato una serie di vulnerabilità della rete di telefonia cellulare che potrebbero avere forti impatti sui protocolli LTE 4G e 5G.

Secondo l’articolo “Privacy Attacks to the 4G e 5G Cellular Paging Protocols Using Side Channel Information” pubblicato dai ricercatori stessi, i nuovi attacchi potrebbero consentire ai criminal hacker di aggirare le protezioni di sicurezza implementate nei protocolli 4G e 5G consentendo loro di intercettare le telefonate degli utenti e tracciare la loro posizione.

In particolare, le vulnerabilità appena scoperte consentono di riportare in auge i cosiddetti IMSI catcher come il famoso Stingrays. Si tratta di dispositivi che, anche all’insaputa delle compagnie telefoniche, consentono di “pedinare” i telefoni cellulari nel raggio di diverse centinaia di metri. In questo modo gli hacker possono individuare l’esatta posizione dello smartphone, leggere messaggi e trafugare dati e informazioni memorizzati nella memoria del cellulare.

Indice degli argomenti

* [Vulnerabilità delle reti 4G e 5G: i dettagli tecnici](https://www.cybersecurity360.it/news/vulnerabilita-delle-reti-4g-e-5g-i-pirati-ci-spiano-chi-e-a-rischio/" \l "Vulnerabilita_delle_reti_4G_e_5G_i_dettagli_tecnici)
* [Gli altri attacchi che sfruttano i bug delle reti 4G/5G](https://www.cybersecurity360.it/news/vulnerabilita-delle-reti-4g-e-5g-i-pirati-ci-spiano-chi-e-a-rischio/" \l "Gli_altri_attacchi_che_sfruttano_i_bug_delle_reti_4G5G)
* [Vulnerabilità delle reti 4G e 5G: chi è a rischio](https://www.cybersecurity360.it/news/vulnerabilita-delle-reti-4g-e-5g-i-pirati-ci-spiano-chi-e-a-rischio/" \l "Vulnerabilita_delle_reti_4G_e_5G_chi_e_a_rischio)

## **Vulnerabilità delle reti 4G e 5G: i dettagli tecnici**

Sfruttando le vulnerabilità appena scoperte, i ricercatori sono riusciti a mettere a punto tre diverse tipologie di attacco.

Il più pericoloso è stato nominato di ToRPEDO, acronimo di TRacking via Paging mEssage DistributiOn e sfrutta una vulnerabilità nel protocollo di paging utilizzato tipicamente dagli operatori di telefonia per segnalare ad uno smartphone in stato di inattività l’arrivo di una telefonata o di un messaggio di testo. Questa stessa funzionalità può essere sfruttata da un attaccante per localizzare un dispositivo bersaglio, inviare falsi messaggi di paging e lanciare attacchi di tipo [**Denial-of-Service (DoS)**](https://www.cybersecurity360.it/nuove-minacce/ddos-cosa-sono-questi-attacchi-hacker-e-come-stanno-evolvendo/) verso lo smartphone della vittima fino a saturarne le risorse e mandarlo in blocco.

In pratica, quando uno smartphone in stato di inattività riceve una telefonata o un SMS, il modulo MME (Mobile Management Entity) della rete cellulare chiede alla stazione base più vicina al dispositivo di trasmettere un messaggio di paging per notificare al dispositivo stesso la chiamata o il messaggio in arrivo.

Il messaggio di paging contiene anche il Temporary Mobile Subscriber Identity (TMSI) del dispositivo, cioè un numero univoco che lo smartphone utilizza per interfacciarsi con la rete GSM e garantire la riservatezza degli utenti.

I ricercatori hanno quindi scoperto che se un attaccante inizia e poi interrompe immediatamente un gran numero di chiamate in poco tempo, lo smartphone aggiorna molto frequentemente il valore TMSI. Usando un IMSI catcher, un attaccante può sniffare i messaggi di paging contenenti il TMSI e dedurre se il dispositivo è attivo e si trova in un raggio d’azione utile per intercettarlo. Se l’attaccante conosce i luoghi frequentati dalla vittima, ha gioco facile a localizzare il suo smartphone, intercettarne telefonate ed SMS o mandarlo in crash con un attacco DoS.

## **Gli altri attacchi che sfruttano i bug delle reti 4G/5G**

L’attacco ToRPEDO permette di portare a termine anche altri due tipi di violazioni dei dispositivi mobili: PIERCER e IMSI-Cracking, che consentono ad un attaccante di rubare l’IMSI del dispositivo della vittima.

In particolare, a causa di un difetto di progettazione della rete cellulare, l’attacco PIERCER (acronimo di Persistent Information ExposuRe by the CorE netwoRk) consente all’aggressore di associare l’IMSI univoco del dispositivo della vittima al suo numero di telefono.

A quel punto, con il numero IMSI in mano, gli aggressori possono lanciare attacchi di ogni genere che potrebbero consentire loro di curiosare alla lista delle chiamate della vittima, registrarle, leggere gli SMS in arrivo, individuare la sua esatta posizione e quindi gli spostamenti durante la giornata.

Infine, l’attacco IMSI-Cracking consente di ottenere il numero IMSI univoco associato allo smartphone della vittima mediante un attacco di forza bruta e poi prendere il pieno controllo del dispositivo a sua totale insaputa.

## **Vulnerabilità delle reti 4G e 5G: chi è a rischio**

Come abbiamo visto, utilizzando i “soliti” IMSI catcher come Stingrays e DRTBox un attaccante può intercettare le sue vittime in maniera abbastanza semplice, anche se possiede un dispositivo 5G di nuova generazione.

C’è da dire, comunque, che il reale successo di questi attacchi dipende molto dalle tecnologie mobile e dai protocolli di rete utilizzati dagli operatori telefonici. Gli stessi ricercatori che hanno scoperto le vulnerabilità delle reti 4G e 5G hanno verificato, ad esempio, che negli Stati Uniti d’America i dispositivi sono più vulnerabili a Torpedo. In Europa, invece, non sono stati effettuati al momento test “sul campo”.

“Gli attacchi di cui stiamo parlando”, è il commento di Massimo Carlotti, Sales Engineer Italy and South EMEA di CyberArk, “sono indubbiamente insidiosi perché, come spiegato nell’articolo, sfruttano debolezze intrinseche nei protocolli LTE 4G e 5G che riguardano le prime fasi dell’interazione con i terminali mobili ed al mutuo riconoscimento con la rete in previsione di trasferimento di messaggi e chiamate. Inoltre, cosa ancora più grave, parliamo delle reti mobile più avanzate esistenti e di quelle di nuova generazione”.

Secondo Carlotti, “le dinamiche di autenticazione ed identificazione reciproca tra terminale e rete dovrebbero essere rese più sicure in ogni operazione e non accettare di applicare sistemi di protezione di livello inferiore per alcun tipo di comunicazione proprio per evitare compromissioni di questo tipo, che sfruttano “concessioni” dovute, in alcuni casi, a vecchie esigenze dipendenti da reti e terminali meno performanti o a metodi di comunicazione di base (ad esempio la retrocompatibilità) in cui non si è tenuto conto del concetto di “security by design”. In questo caso un’eventuale correzione potrebbe dipendere, prima ancora che dagli operatori, da una ridefinizione dei meccanismi di base della sicurezza delle reti. Operazione che potrebbe rivelarsi molto complessa per via della molteplicità di attori coinvolti e per l’impatto che potrebbe avere sulle infrastrutture già esistenti”.

Da parte loro, i principali operatori di telefonia e gli stessi ricercatori rassicurano comunque sul fatto che i bug possono essere facilmente corretti. Il problema è che non si sa quanto tempo ci vorrà per farlo e rendere così le reti 4G e 5G completamente sicure e immuni da ogni possibile tentativo di intercettazione.

Le [reti *Long Term Evolution*](https://www.fastweb.it/fastweb-plus/digital-magazine/storia-rete-cellulare/), meglio conosciute come LTE (ovvero le reti [4G](https://www.negozi.fastweb.it/it/4g-cose-e-a-cosa-serve/) e [5G](https://fastweb.it/fastweb-plus/digital-dev-security/la-tecnologia-del-domani-il-5g/)), soffrono di una grave vulnerabilità che potrebbe permettere ad un hacker di rubarci l'identità o di violare i nostri dispositivi mobili. Lo hanno scoperto i ricercatori della Università di Bochum e della New York University di Abu Dhabi, che hanno rivelato questo bug durante il Network Distributed System Security Symposium del 25 febbraio 2020 a San Diego.

Sfruttando questa vulnerabilità, spiegano i ricercatori, è possibile mettere in atto degli attacchi chiamati "IMPersonation Attacks in 4G NeTworks" (INP4GT). Nonostante il nome dell'attacco, però, a rischio sono anche le reti 5G e i device potenzialmente attaccabili non sono solo gli smartphone e i tablet, ma tutti quelli che si connettono alle reti LTE. Quindi anche svariate centinaia di milioni di [**dispositivi** *Internet of Things*](https://www.fastweb.it/fastweb-plus/digital-magazine/iot-5g-vantaggi-e-prospettive-future/) (IoT) già presenti sul mercato.

Questa vulnerabilità è stata già comunicata a maggio 2019 alla GSM Association, l'associazione degli operatori di rete mobile che conta oltre 750 membri nel mondo e più di 400 aziende che sviluppano tecnologie per le reti cellulari.

## **Come funziona IMP4GT**

I ricercatori hanno effettuato gli attacchi IMP4GT utilizzando le cosiddette software-defined radio (SDR), che sono sostanzialmente delle radio "software", emulate su un hardware come un normale PC. Usando una SDR, il team di scienziati è riuscita ad eseguire attacchi "[*man-in-the-middle*](https://www.fastweb.it/fastweb-plus/digital-magazine/cosa-sono-lo-sniffing-e-lo-snooping/)", mettendosi appunto "in mezzo" tra uno smartphone 4G e i ripetitori ai quali era collegato. Duranti questi attacchi i ricercatori sono riusciti a far credere al cellulare che la SDR era il ripetitore e al ripetitore che la SDR era il cellulare.

Tecnicamente, queste due fasi dell'attacco si chiamano "uplink impersonation" e "downlink impersonation". "La uplink impersonation - spiegano i ricercatori dell'Unicersità di Bochum - consente a un utente malintenzionato di stabilire una connessione IP arbitraria verso Internet, ad esempio una connessione TCP a un server HTTP. Mentre con la downlink impersonation l'attaccante può stabilire una connessione TCP con il telefono scavalcando un eventuale firewall della rete LTE".

Alla base di questa falla c'è un mancato controllo di sicurezza nella fase di autenticazione reciproca, cioè quella fase in cui il telefono e la cella telefonica dialogano per stabilire una connessione. In questa fase, usando una SDR, i ricercatori sono riusciti a "mettersi in mezzo" facendo quindi tra tramite tra i due dispositivi, senza che questi si accorgessero di nulla.

## **Cosa si rischia con IMP4GT**

Una volta che questo canale di comunicazione è stato compromesso, la fase successiva dell'attacco consiste nel leggere, registrare ed eventualmente modificare arbitrariamente i pacchetti di dati che vengono scambiati tra telefono e cella telefonica. Manipolando il traffico dati un cracker potrebbe "fingersi" lo smartphone per effettuare acquisti non autorizzati, accedere a siti Web illegali, caricare documenti sensibili utilizzando l'identità della vittima e persino reindirizzare l'utente a un sito dannoso, al fine di veicolare un malware.

Una volta che il firewall dell'operatore telefonico è violato, poi, il telefono può ricevere qualsiasi connessione in entrata. "Tale attacco è un trampolino di lancio per ulteriori attacchi, come la distribuzione di malware", spiegano ancora i ricercatori. Va notato, però, che l'avversario deve trovarsi nel raggio di 2 km dal telefono cellulare della vittima per poter sferrare efficacemente un attacco IMP4GT. Il meccanismo di funzionamento di IMP4GT non è molto diverso da quello usato dagli "intercettatori IMSI", cioè quelli che vengono utilizzati dalle forze dell'ordine per le intercettazioni telefoniche.

## **Il 5G è sicuro?**

La domanda che tutti gli esperti si sono posti dopo aver letto la ricerca sugli attacchi IMP4GT è: funzionano anche con le [**reti 5G**](https://www.fastweb.it/fastweb-plus/digital-dev-security/la-tecnologia-del-domani-il-5g/)? La risposta degli studiosi è stata chiara: "Da un punto di vista strettamente tecnico, è possibile". Secondo i ricercatori, quindi, la [**rete 5G**](https://www.fastweb.it/fastweb-plus/digital-magazine/frequenze-radio-5g/) va rafforzata, e anche parecchio, con ulteriori misure di protezione finalizzate a rendere impossibili attacchi di questo tipo. Il problema, però, è che tali misure di protezione avrebbero un costo elevato, genererebbero un traffico dati maggiore (quindi più congestione della rete 5G) e tutti gli smartphone 5G già venduti andrebbero sostituiti. Gli stessi ricercatori, per tutti questi motivi, ammettono che tutto ciò "è qualcosa che non avverrà nel futuro prossimo".

## Conclusione

Le reti 4G e 5G offrono connettività avanzata, ma anche nuove sfide per la sicurezza. È essenziale implementare misure di sicurezza robuste, comprese crittografia forte, autenticazione sicura e monitoraggio costante, per proteggere le reti e i dati degli utenti. Inoltre, la consapevolezza degli utenti e la formazione sulla sicurezza sono altrettanto cruciali per prevenire attacchi sofisticati. La sicurezza deve rimanere al centro dello sviluppo e dell'implementazione delle reti 4G e 5G per garantire un'esperienza utente sicura e affidabile.