FEBBRAIO 2025

Rete 5G:
Sicurezza, Innovazione e Sfide Future

Autori:
Stefano Savo
Stefano Cangiano

www.ictsecuritymagazine.com

Indice

L'EVOLUZIONE DELLE RETI MOBILI E L'AVVENTO DEL 5G 4

ARCHITETTURA E INNOVAZIONI TECNOLOGICHE DEL 5G 4

5G: SFIDE PER LA SICUREZZA 8

VULNERABILITÀ E SICUREZZA NELLE RETI 5G: ANALISI PRATICA DEGLI IMSI E SUCI CATCHER 13

IL FUTURO DELLA SICUREZZA NELLE RETI 5G 26

Autori

Stefano Savo

Security & Intelligence Specialist & Co-Founder della società ISK

Dottore in Scienze e Tecnologie Informatiche presso l'Università di Roma "Tor Vergata", ha esperienza decennale nel settore dell'Intelligence Militare e Privato. Ha svolto diverse operazioni come ausiliario di polizia giudiziaria. Ricopre ruolo di Security Specialist Consultant proponendo servizi mirati per la Security, Intelligence, Cyber Security & Digital Forensics. Esperto in attività di TSCM (Technical Surveillance Countermeasures) a supporto del controspionaggio industriale. Nel 2019 è CO-Founder della società ISK (isksecurity.it) partner strategico ed esterno per attività di TSCM, Cyber Security & Digital Forensics.

Stefano Cangiano

Cyber Security Specialist & Founder/CEO della società ISK

Titolare delle licenze EJPT e ECPPT (Professional Penetration Tester) della società eLearnSecurity. Svolge attività di Network Security in particolare Penetration Test & VA – Vulnerability Assessment.
Nel 2019 fonda la società ISK (www.isksecurity.it), partner strategico ed esterno per attività di Security specializzata. Svolge attività di bonifiche ambientali da microspie, attività di Security Assessment e Mobile Security.

L'Evoluzione delle Reti Mobili e l'Avvento del 5G

L'evoluzione delle reti mobili ha seguito una progressione storica marcata da innovazioni tecnologiche significative che hanno trasformato il modo in cui comunichiamo e accediamo alle informazioni. L'architettura hardware del 5G è progettata per supportare la trasmissione di dati ad alta velocità, una bassa latenza, e una maggiore capacità di connessione simultanea rispetto alle generazioni precedenti. Questa architettura è composta da diversi componenti chiave che lavorano insieme per garantire la funzionalità e le prestazioni della rete 5G.

Secondo l'Unione Internazionale delle Telecomunicazioni (ITU), l'introduzione del 5G, la quinta generazione di tecnologia cellulare, promette di rivoluzionare non solo le comunicazioni personali, ma interi settori industriali, offrendo velocità di trasmissione dati fino a 20 Gbps, latenza inferiore a 1 ms e una densità di connessione di 1 milione di dispositivi per km^2.

Architettura e Innovazioni Tecnologiche del 5G

Architettura Hardware del 5G

Di seguito, descriviamo i principali componenti hardware e le loro funzioni:

1. Stazioni Base (Base Stations)

gNodeB (gNB): È la stazione base 5G che fornisce la connettività radio agli utenti. Sostituisce l'eNodeB della rete LTE e gestisce la comunicazione tra i dispositivi mobili e la rete centrale. La gNB è responsabile della gestione delle risorse radio, della codifica/decodifica dei segnali e dell'instradamento dei dati.

2. Antenne

- Massive MIMO (Multiple Input Multiple Output): Utilizza un grande numero di antenne per trasmettere e ricevere più segnali simultaneamente. Questo migliora significativamente la capacità e l'efficienza spettrale della rete 5G.

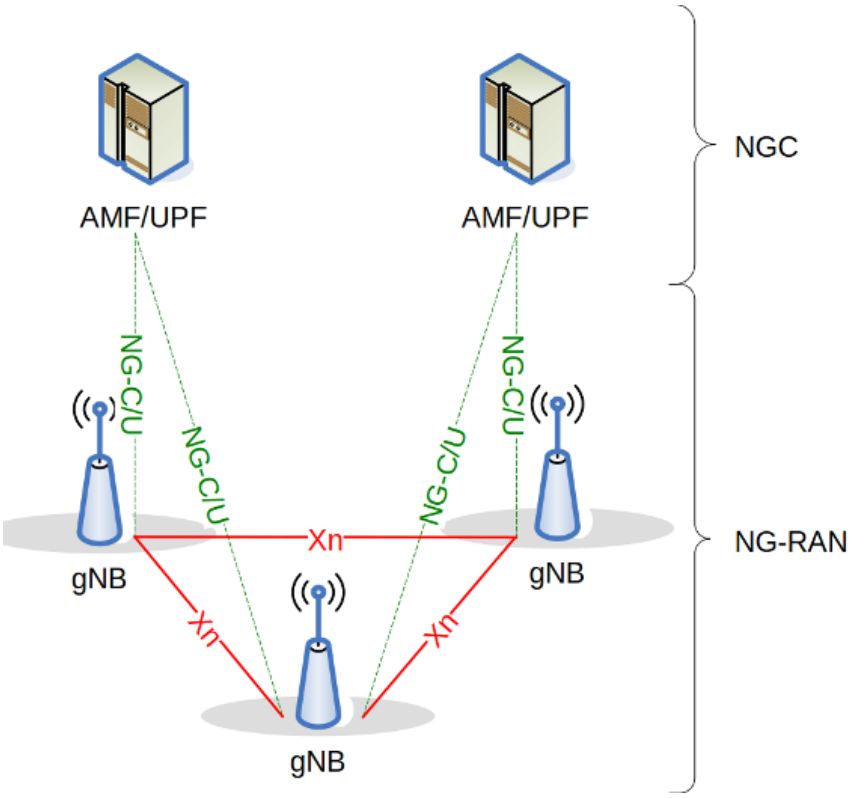


Figura 1 Architettura Rete 5g

- Beamforming: Tecnica che consente di dirigere i segnali radio direttamente verso specifici dispositivi mobili, migliorando la qualità del segnale e riducendo le interferenze.

3. Core Network (Rete Centrale)

NG Core (Next Generation Core): È la rete centrale 5G, responsabile della gestione del traffico dati e delle connessioni. È composta da diversi componenti, tra cui:

AMF (Access and Mobility Management Function): Gestisce la registrazione degli utenti e la loro mobilità.

SMF (Session Management Function): Gestisce le sessioni dati e la loro qualità.

UPF (User Plane Function): Instrada i dati tra la rete e gli utenti finali.

NSSF (Network Slice Selection Function): Gestisce la selezione delle slice di rete, permettendo la creazione di reti virtuali personalizzate per diverse applicazioni.

4. Dispositivi Utente (User Equipment, UE)

- Smartphone e Dispositivi Mobili: Dotati di modem 5G in grado di connettersi alla rete e supportare velocità di trasmissione elevate.
- IoT Devices: Dispositivi connessi utilizzati in vari settori come l'automazione industriale, la smart home e la sanità.

Il 5G come Catalizzatore di un Futuro Interconnesso

L'avvento del 5G segna un punto di svolta nell'evoluzione delle tecnologie di comunicazione, promettendo di ridefinire il tessuto stesso della nostra società digitale. Mentre ci avventuriamo in questa nuova era, è evidente che il potenziale del 5G va ben oltre il mero incremento delle velocità di connessione. Secondo un rapporto del MIT Technology Review Insights, il 5G fungerà da spina dorsale per l'Internet of Everything, facilitando l'integrazione seamless di tecnologie emergenti come l'intelligenza artificiale, la blockchain e l'edge computing. Questa convergenza tecnologica non solo accelererà l'innovazione in settori critici come la sanità, i trasporti e l'energia, ma aprirà anche la strada a modelli di business rivoluzionari e a nuove forme di interazione uomo-macchina. Tuttavia, con queste opportunità senza precedenti emergono anche sfide complesse che richiederanno una collaborazione globale tra governi, industria e accademia. La gestione responsabile di questa transizione tecnologica sarà cruciale per garantire che i benefici del 5G siano distribuiti equamente, minimizzando al contempo i rischi potenziali per la privacy e la sicurezza. In definitiva, il successo del 5G non sarà misurato solo in termini di prestazioni tecniche, ma anche dal suo impatto positivo sulla società, sull'economia e sull'ambiente, plasmando un futuro più connesso, efficiente e sostenibile per le generazioni a venire.

Verso un Ecosistema 5G Sicuro: Sfide e Strategie Emergenti

Mentre esploriamo le potenzialità rivoluzionarie del 5G, è imperativo affrontare le complesse sfide di sicurezza che questa tecnologia comporta. Il prossimo capitolo approfondirà le implicazioni critiche per la cybersecurity nell'era del 5G, analizzando le vulnerabilità uniche introdotte dall'architettura distribuita e dall'iperconnettività. Esamineremo le strategie all'avanguardia sviluppate da esperti del settore e organizzazioni come il National Institute of Standards and Technology (NIST) per contrastare minacce emergenti. Dall'implementazione di protocolli di crittografia quantistica alla realizzazione di architetture Zero Trust, scopriremo come l'industria sta evolvendo per garantire l'integrità, la confidenzialità e la disponibilità dei dati in un ecosi-

stema 5G. Inoltre, esploreremo il ruolo cruciale dell'intelligenza artificiale e del machine learning nel rilevamento e nella mitigazione proattiva delle minacce, nonché le implicazioni geopolitiche della sicurezza delle infrastrutture 5G. Questo approfondimento fornirà agli stakeholder una comprensione essenziale delle misure necessarie per navigare in sicurezza nel panorama in rapida evoluzione del 5G, bilanciando innovazione e protezione in un mondo sempre più interconnesso.

5G: sfide per la sicurezza

Sicurezza e Vulnerabilità nell'Era del 5G: La sfida alla cybersecurity

L'avvento del 5G rappresenta un salto quantico nelle tecnologie di comunicazione, promettendo velocità senza precedenti, latenza minima e connettività ubiqua. Tuttavia, questa rivoluzione tecnologica porta con sé una serie di sfide critiche per la cybersecurity. In questo capitolo, esploreremo le vulnerabilità emergenti e le minacce sofisticate che accompagnano l'implementazione delle reti 5G. Dall'espansione della superficie di attacco dovuta alla proliferazione di dispositivi IoT, alle complessità introdotte dal network slicing e dalla virtualizzazione, esamineremo le molteplici sfaccettature della sicurezza 5G. Particolare attenzione sarà dedicata all'analisi degli IMSI Catcher, strumenti di intercettazione che sollevano questioni cruciali sulla privacy e la sicurezza delle comunicazioni nell'era 5G. Attraverso un'indagine tecnica e un approccio pratico, sveleremo le implicazioni di queste tecnologie per le forze dell'ordine, la sicurezza nazionale e la protezione dei dati personali.

Gli 8 problemi di sicurezza associati alle reti 5G:

1. Maggiore Superficie di Attacco

Con l'aumento del numero di dispositivi connessi (grazie all'Internet of Things, IoT), la superficie di attacco si espande notevolmente. Ogni dispositivo connesso può diventare un potenziale punto di ingresso per attacchi informatici. Inoltre, molti dispositivi IoT hanno capacità di sicurezza limitate, rendendoli vulnerabili.

2. Virtualizzazione e Slicing di Rete

Il 5G utilizza ampiamente tecnologie di virtualizzazione e network slicing, che permettono di creare reti virtuali indipendenti per diversi tipi di servizi. Sebbene ciò offra flessibilità e efficienza, introduce anche nuovi rischi. Se un attaccante riesce a compromettere uno slice, potrebbe avere accesso a dati sensibili o compromettere la funzionalità dell'intera rete.

3. Interfacce e Protocollo Nuovi

L'adozione di nuove interfacce e protocolli nel 5G comporta rischi inerenti alle vulnerabilità sconosciute. Le nuove tecnologie possono avere bug o falle di sicurezza non ancora identificate e sfruttate dagli hacker.

4. Maggiore Complessità della Rete

Le reti 5G sono significativamente più complesse rispetto alle generazioni precedenti. Questa complessità aggiuntiva può rendere più difficile la gestione della sicurezza e aumentare le possibilità di configurazioni errate, che possono essere sfruttate dagli attaccanti.

5. Problemi di Privacy

Il 5G può raccogliere e trasmettere enormi quantità di dati, compresi dati personali sensibili. La gestione e la protezione di questi dati rappresentano una sfida significativa. Esiste il rischio che i dati vengano intercettati, manipolati o utilizzati senza il consenso degli utenti.

6. Minacce da Stati Nazionali

La sicurezza delle reti 5G è diventata una questione geopolitica, con timori che attori statali possano sfruttare vulnerabilità nelle reti per spionaggio o attacchi. La dipendenza da fornitori di infrastrutture 5G di specifici paesi ha sollevato preoccupazioni su possibili backdoor e accessi non autorizzati.

7. Attacchi alle Infrastrutture Critiche

Le reti 5G supporteranno infrastrutture critiche come la sanità, i trasporti e l'energia. Gli attacchi contro queste reti possono avere conseguenze devastanti. Ad esempio, un attacco ai sistemi di controllo industriale collegati tramite 5G potrebbe interrompere servizi essenziali.

8. Sicurezza delle Comunicazioni V2X (Vehicle-to-Everything)

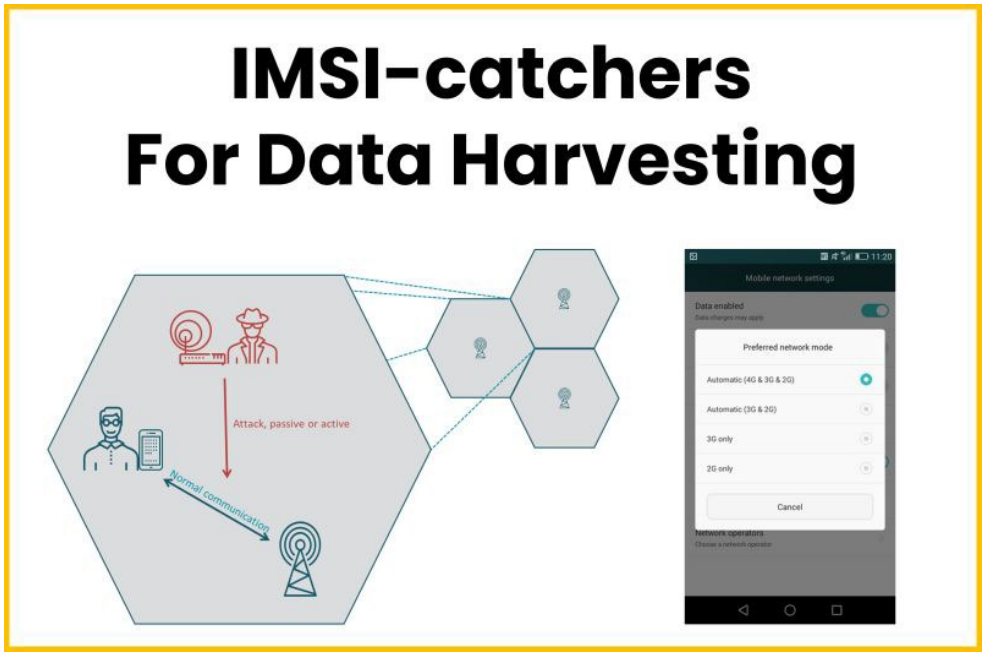
Con il 5G, le comunicazioni tra veicoli e tra veicoli e infrastrutture (V2X) diventeranno comuni. Garantire la sicurezza di queste comunicazioni è cruciale per prevenire attacchi che potrebbero causare incidenti o interrompere il traffico.

Tra le tante problematiche citate abbiamo toccato con mano quella riguardante la privacy degli utenti e cosa sia possibile ottenere da un attacco basato su strumento **IMSI Catcher**. Per far questo abbiamo "vestito" i panni di un attaccante dopo aver ricostruito tramite progetti libe-

ramente disponibili sul web (open-source) un IMSI Catcher adatto per un test da laboratorio. L'ambiente risultava perfettamente schermato dall'esterno affinchè le comunicazioni esterne (reti cellulari) non venissero intralciate.

Per meglio comprendere gli studi e i comportamenti degli smartphone in una rete di nuova generazione dobbiamo descrivere cos'è un IMSI catcher e quali sono le sue funzionalità.

Cos'è un IMSI catcher?



Un IMSI Catcher funziona simulando una torre cellulare legittima, inducendo i telefoni cellulari nelle vicinanze a connettersi ad esso piuttosto che a una vera torre cellulare. Ecco come avviene questo processo:

- **Simulazione della Torre Cellulare**: L'IMSI Catcher trasmette segnali radio che imitano quelli di una torre cellulare autentica, utilizzando frequenze e protocolli di comunicazione standard delle reti mobili (GSM, UMTS, LTE, 5g).

- **Connessione dei Dispositivi**: Quando un telefono cellulare rileva il segnale dell'IMSI Catcher, lo considera una torre cellulare valida e tenta di connettersi ad essa. Il dispositivo mobile fornisce il proprio IMSI all'IMSI Catcher per l'autenticazione.

- **Intercettazione del Traffico**: Una volta che il telefono è connesso all'IMSI Catcher, il dispositivo può intercettare e monitorare varie forme di comunicazione, inclusi SMS, chiamate vocali e dati di rete. In alcuni casi, l'IMSI Catcher può anche eseguire un attacco "man-in-the-

middle," dove il traffico è intercettato e poi instradato alla vera torre cellulare, consentendo all'utente di continuare a usare i servizi senza sapere che sono sotto sorveglianza.

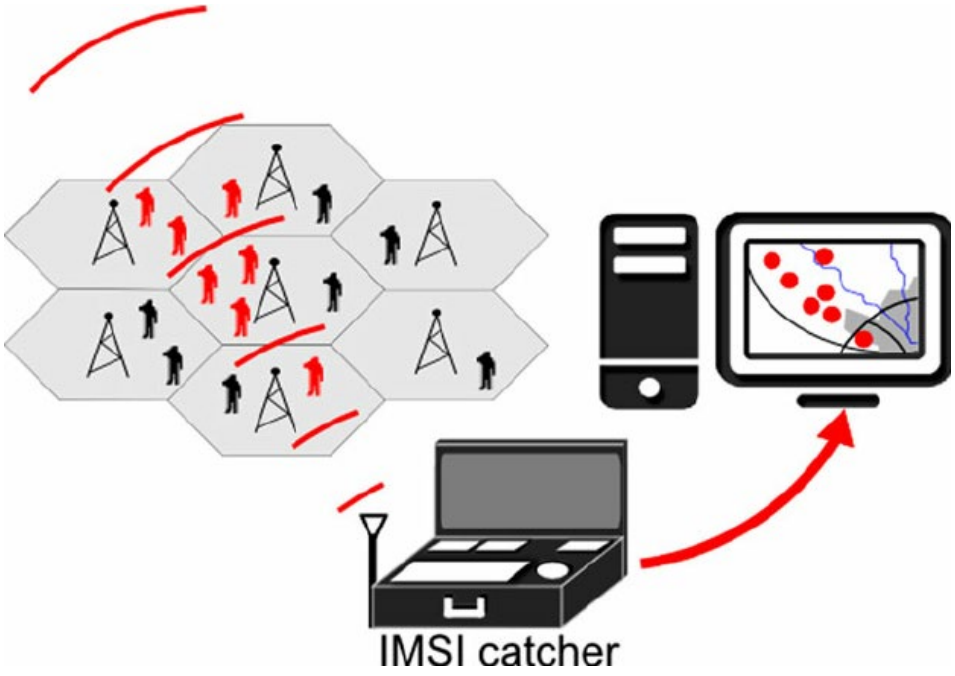


Figura 2 Funzionalità di un IMSI Catcher

Quali sono gli usi e le applicazioni di un IMSI Catcher?

Gli usi e le applicazioni di un IMSI Catcher possono essere molteplici. Facciamo qualche esempio:

1. Applicazioni delle Forze dell'Ordine

Le forze dell'ordine utilizzano gli IMSI Catcher per:

- **Localizzazione di Sospetti**: Tracciare la posizione di sospetti in tempo reale utilizzando l'IMSI del loro telefono cellulare.
- **Intercettazione delle Comunicazioni**: Ascoltare chiamate e leggere messaggi SMS per raccogliere informazioni su attività criminali.
- **Raccolta di Dati di Massa**: In situazioni come manifestazioni pubbliche, un IMSI Catcher può essere usato per raccogliere dati su tutti i telefoni presenti nell'area.

2. Applicazioni Militari e di Sicurezza Nazionale

Le agenzie di intelligence e militari possono usare gli IMSI Catcher per:

- **Sorveglianza delle Comunicazioni**: Monitorare le comunicazioni in zone di conflitto o di interesse strategico.
- **Raccolta di Informazioni**: Raccogliere dati di intelligence su gruppi terroristici o altre minacce alla sicurezza nazionale.

3. Abusi da Parte di Attori Malintenzionati

Attori malintenzionati possono utilizzare gli IMSI Catcher per:

- **Spionaggio**: Intercettare comunicazioni private e raccogliere informazioni sensibili.
- **Furto di Identità**: Ottenere informazioni personali che possono essere usate per furti di identità o altre attività fraudolente.

Verso un Futuro 5G Sicuro: Bilanciare Innovazione e Protezione

L'analisi delle sfide di sicurezza del 5G e l'esplorazione degli IMSI Catcher evidenziano la complessità del panorama della cybersecurity nell'era delle comunicazioni ultra-veloci. Mentre le potenzialità del 5G sono innegabili, è imperativo adottare un approccio proattivo e multidimensionale alla sicurezza. La collaborazione tra fornitori di tecnologia, enti regolatori e esperti di sicurezza sarà cruciale per sviluppare soluzioni robuste che proteggano l'integrità delle reti 5G e la privacy degli utenti. L'implementazione di tecnologie come la crittografia quantistica, l'intelligenza artificiale per il rilevamento delle anomalie e architetture di rete Zero Trust rappresentano passi promettenti verso un ecosistema 5G più sicuro. Tuttavia, la vigilanza continua e l'adattamento alle minacce emergenti rimarranno essenziali. Solo attraverso un impegno costante nell'innovazione della sicurezza possiamo realizzare appieno il potenziale trasformativo del 5G, garantendo al contempo la fiducia e la protezione degli utenti in un mondo sempre più interconnesso.

Vulnerabilità e Sicurezza nelle Reti 5G: Analisi Pratica degli IMSI e SUCI Catcher

Nel panorama in rapida evoluzione delle telecomunicazioni, l'avvento del 5G promette una rivoluzione nelle capacità di connettività e trasmissione dati. Tuttavia, questa innovazione porta con sé nuove sfide in termini di sicurezza e privacy. Questo capitolo esplora in profondità le vulnerabilità delle reti 5G, con particolare attenzione alle tecniche di intercettazione come gli IMSI e SUCI Catcher. Attraverso un'analisi tecnica e un caso studio pratico condotto in laboratorio, esamineremo le implicazioni di queste tecnologie per la privacy degli utenti e la sicurezza delle reti. Dalla simulazione di una torre cellulare 4G per indurre connessioni da dispositivi 5G NSA, alle sfide poste dal 5G SA con l'introduzione del SUCI, questo articolo offre una panoramica completa delle attuali minacce e delle contromisure in sviluppo. Esploreremo inoltre le differenze cruciali tra le architetture 5G NSA e SA, evidenziando come queste influenzino la sicurezza delle comunicazioni mobili. Questa analisi è essenziale per professionisti della sicurezza informatica, sviluppatori di reti mobili e decisori politici impegnati nella regolamentazione delle tecnologie di comunicazione di nuova generazione.

Caso reale di un test effettuato in laboratorio

1. Problemi di Privacy

Gli IMSI Catcher sollevano gravi preoccupazioni per la privacy:

- **Senza Consenso**: La maggior parte degli utenti non è consapevole di essere sorvegliata e non ha dato il consenso per la raccolta dei propri dati.
- **Dati Sensibili**: Gli IMSI Catcher possono intercettare dati sensibili come messaggi privati, dettagli di contatti e informazioni di localizzazione.

2. Implicazioni Legali

L'uso degli IMSI Catcher è regolamentato in molti paesi, ma le leggi variano notevolmente:

- **Autorizzazione Legale**: In alcune giurisdizioni, le forze dell'ordine devono ottenere un mandato per usare un IMSI Catcher.
- **Regolamentazione**: Alcuni paesi hanno regolamenti specifici per limitare l'uso e prevenire gli abusi di questi dispositivi.

Il nostro test è stato quello di simulare la creazione di una torre cellulare (nel nostro caso impostata su frequenze portanti 4g) per indurre il telefono vittima (connesso a rete 5G NSA) a rivelare il suo identificativo. L'architettura della nostra torre cellulare è stata costruita seguendo progetti liberamente disponibili come Srsran utilizzando schede SDR Ettus b200 per l'elaborazione e la gestione dei segnali delle comunicazioni in digitale attraverso il PC.

Figura 3 Hardware utilizzato per il test

Di seguito mostriamo come in termini di segnale viene vista la nostra torre cellulare.

Figura 5 Come viene vista la nostra torre cellulare di test da un dispositivo mobile

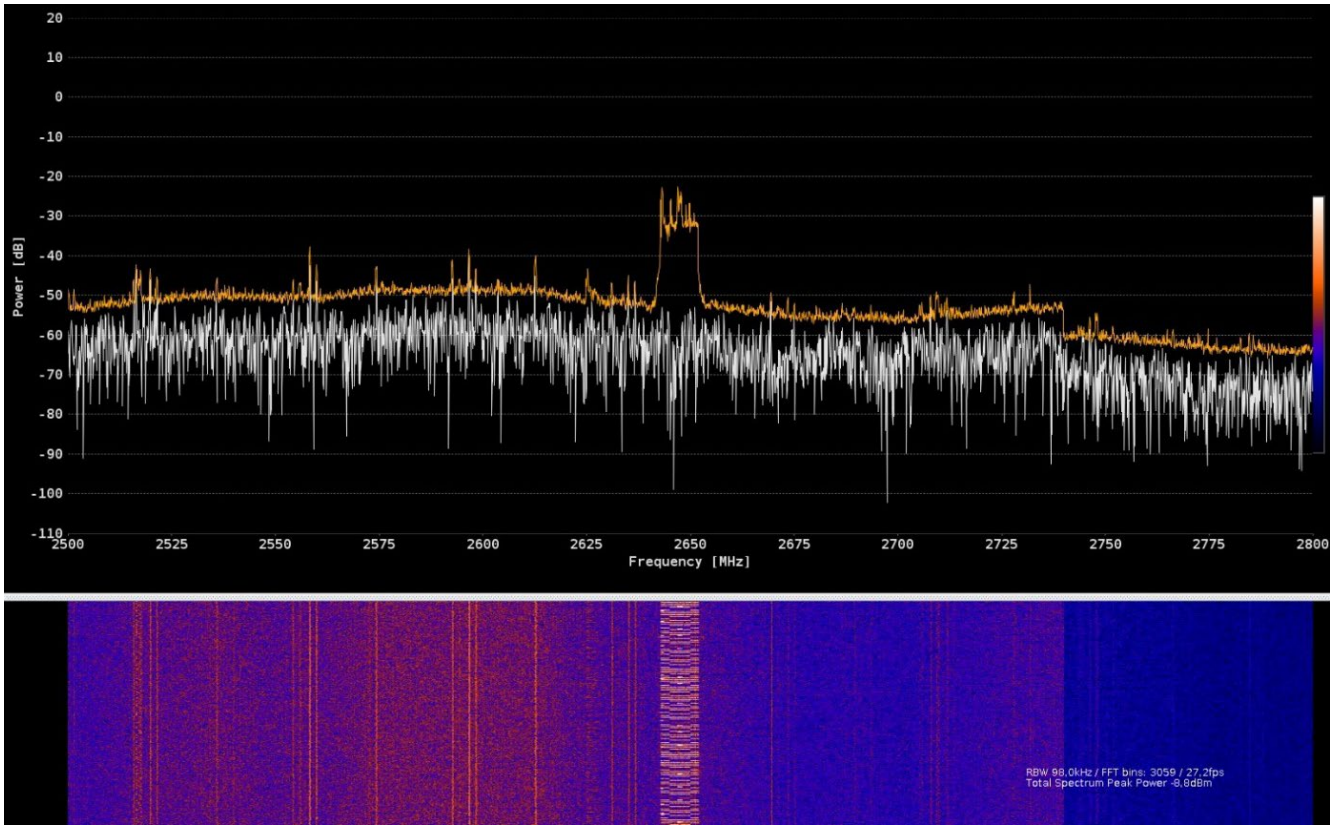


Figura 4 Analisi dello spettro relativa alla frequenza portante della nostra torre cellulare di test

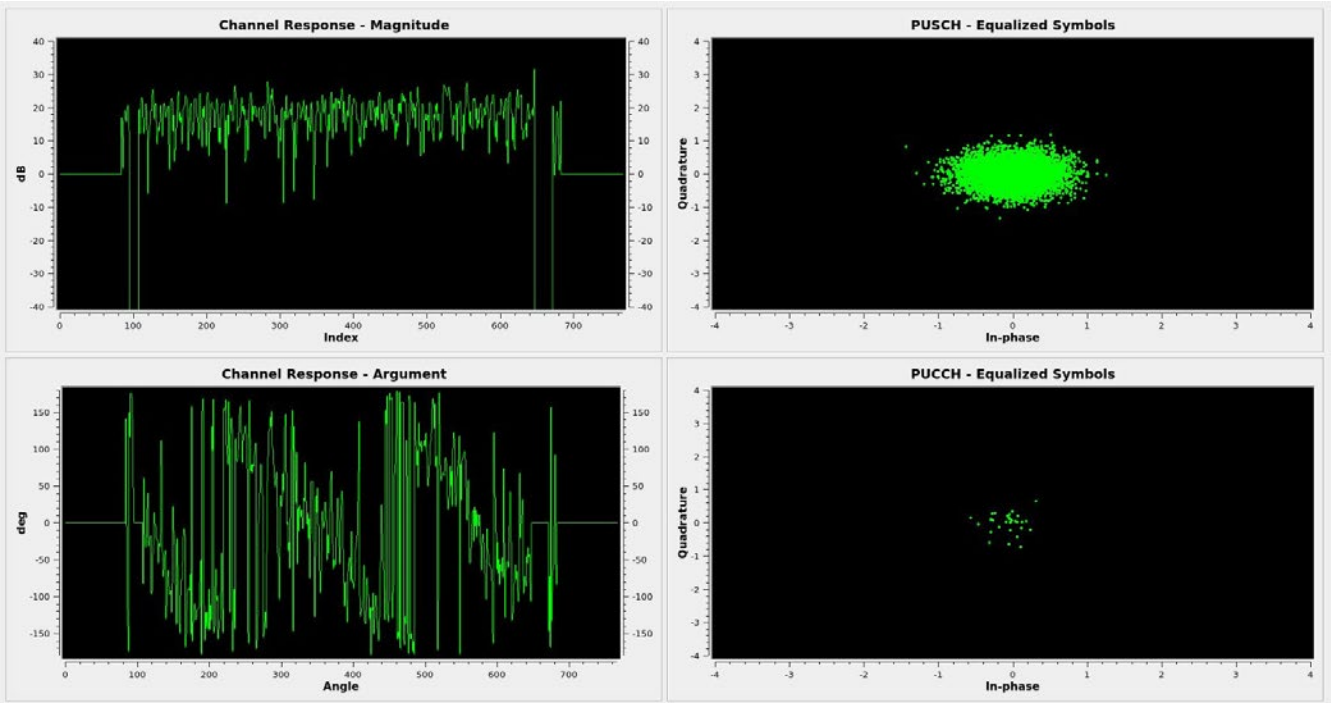


Figura 6 Attività sulle frequenze impostate

Come descritto in precedenza quando il telefono ha rilevato il segnale della nostra rete cellulare ha tentato la connessione alla BTS rivelando in chiaro il suo IMSI (identificativo SIM).

```
Initial UE message: LIBLTE_MME_MSG_TYPE_ATTACH_REQUEST
Received Initial UE message -- Attach Request
Attach request -- M-TMSI: 0xdff[redacted]
Attach request -- eNB-UE S1AP Id: 1
Attach request -- Attach type: 2
Attach Request -- UE Network Capabilities EEA: 11110000
Attach Request -- UE Network Capabilities EIA: 01110000
Attach Request -- MS Network Capabilities Present: true
PDN Connectivity Request -- EPS Bearer Identity requested: 0
PDN Connectivity Request -- Procedure Transaction Id: 144
PDN Connectivity Request -- ESM Information Transfer requested: false
UL NAS: Received Identity Response
ID Response -- IMSI: 22210[redacted]
```

Figura 7 Log che descrive il tentativo di aggancio alla nostra torre del dispositivo vittima. IMSI è rivelato in chiaro

Nel caso in cui il telefono mobile vittima (UE) sia connesso tramite rete 5g SA (nuova generazione) la tecnologia "protegge" l'utente dal rivelare identificativo della SIM. Questo è stato possibile con l'introduzione del SUCI. Una delle principali innovazioni del 5G è l'uso di identità temporanee (SUCI - Subscription Concealed Identifier) al posto degli IMSI (International Mobile

Subscriber Identity) durante la comunicazione iniziale. Questo significa che l'IMSI effettivo non viene mai trasmesso in chiaro, rendendo più difficile per un IMSI catcher identificare e tracciare gli utenti.

Gli attacchi ad una rete di nuova generazione sono sempre possibili attraverso il jamming.

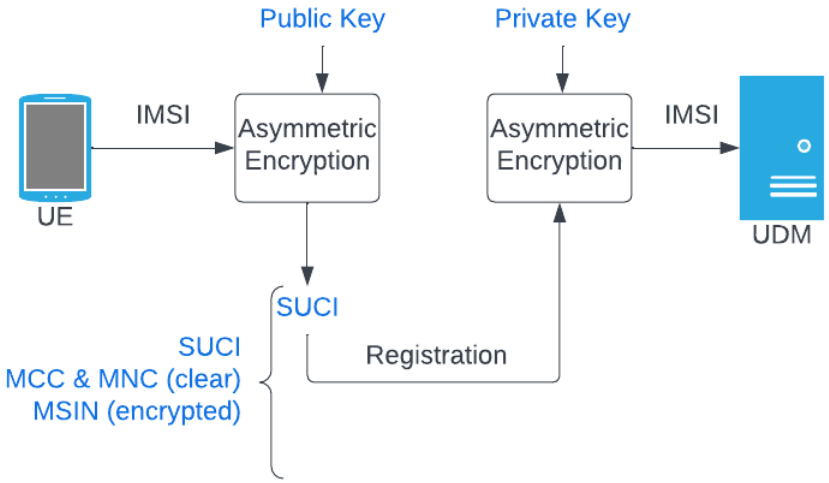


Figura 8 Crittografia dell'identificativo nelle nuove reti con tecnologia 5g SA

Il jamming è una tecnica utilizzata per interferire con le comunicazioni radio, e può essere sfruttata per forzare un dispositivo a passare da una rete più sicura (come il 5G) a una meno sicura (come il 2G o il 3G), dove è più facile utilizzare un IMSI catcher. Questa tecnica è nota come "downgrade attack". Ecco come funziona:

Come Funziona un Downgrade Attack con Jamming

Interferenza del Segnale 5G:

L'attaccante utilizza un dispositivo di jamming per disturbare il segnale 5G in un'area specifica. Questo rende difficile, se non impossibile, per i dispositivi connettersi alla rete 5G.

Connessione Forzata a Reti Legacy:

Con il segnale 5G disturbato, i dispositivi tenteranno di connettersi a reti di fallback come 4G,

3G o addirittura 2G, che sono meno sicure e più vulnerabili agli attacchi IMSI catcher.

Intercettazione delle Comunicazioni:

Una volta che il dispositivo si è connesso a una rete meno sicura, l'attaccante può utilizzare un IMSI catcher per intercettare le comunicazioni, raccogliere dati e identificare l'utente.

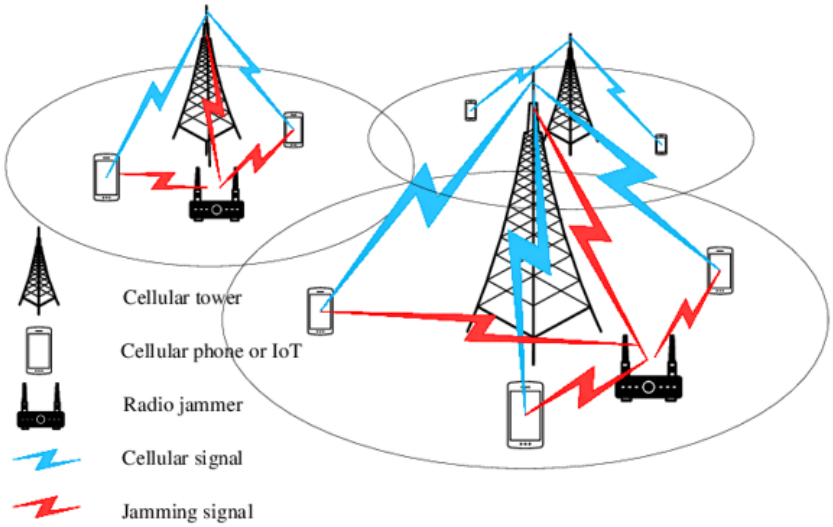


Figura 9 Descrizione del principio di funzionamento di un attacco jamming su una rete a nuova tecnologia

Nel nostro caso abbiamo potuto mettere in atto l'attacco attraverso l'utilizzo di un jammer software liberamente reperibile su Github (https://github.com/PentHertz/Modmobjam)

DIFFERENZA 5g SA-NSA

5G NSA (Non-Standalone)

Il 5G Non-Standalone è un'architettura che utilizza l'infrastruttura di rete 4G LTE esistente per gestire la maggior parte delle funzioni di controllo, mentre la nuova tecnologia 5G è utilizzata principalmente per migliorare la capacità e la velocità della trasmissione dati. In pratica, il 5G NSA combina le risorse del 4G e del 5G per fornire un'esperienza migliorata agli utenti.

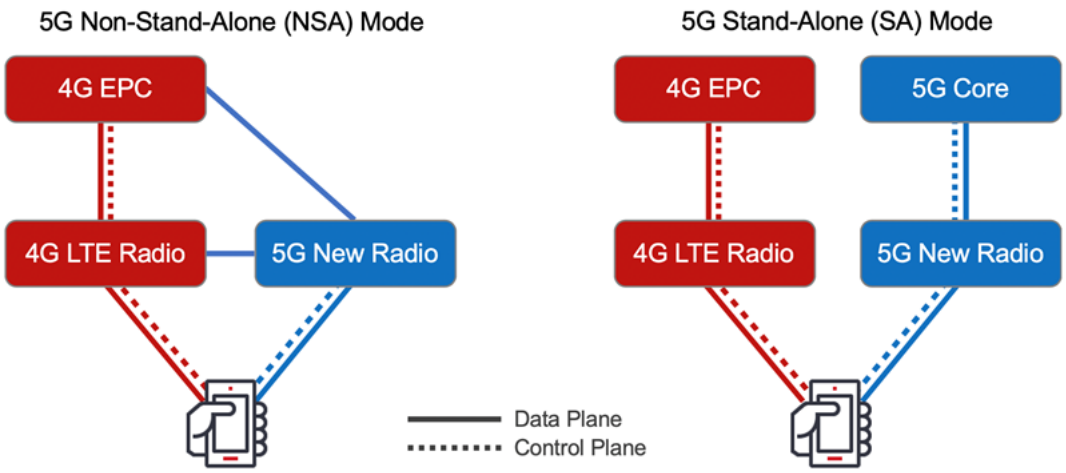
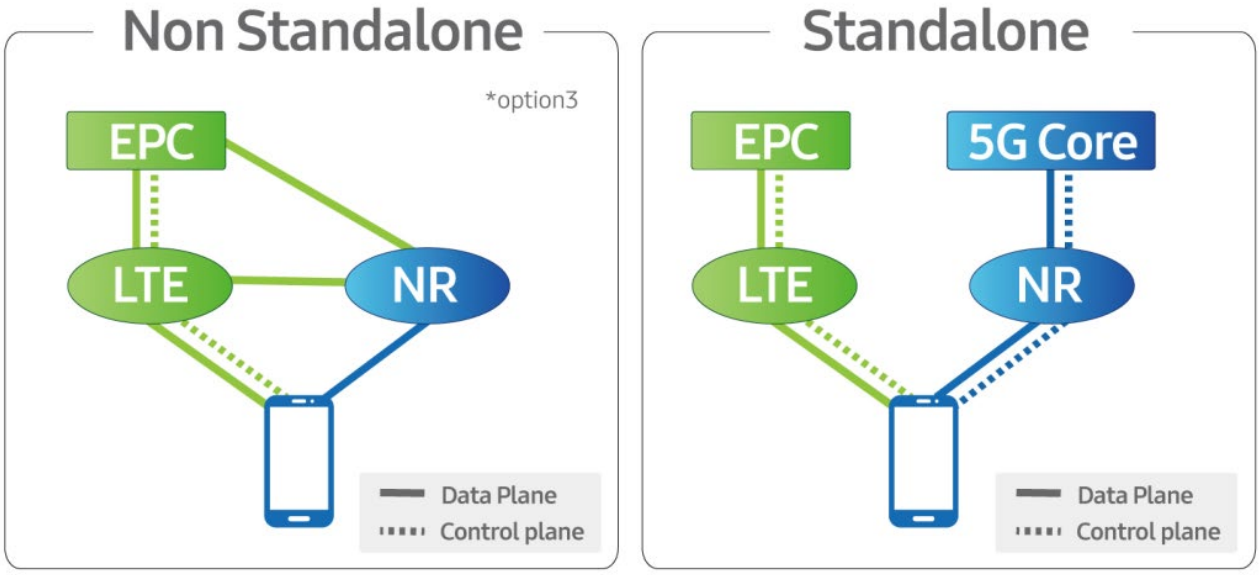


Figura 10 Differenze reti 5g NSA - SA

Caratteristiche:

- **Dipendenza dal 4G**: La rete 4G LTE gestisce il controllo della rete (segnalazione), mentre il 5G viene utilizzato per il traffico dati.



- **Implementazione Rapida**: Le reti 5G NSA possono essere implementate più rapidamente e con costi inferiori rispetto al 5G SA, poiché sfruttano l'infrastruttura 4G esistente.

5G SA (Standalone)

Descrizione:

Il 5G Standalone è un'architettura di rete completamente indipendente che utilizza un'infrastruttura 5G end-to-end, senza dipendere dalla rete 4G LTE. Questo approccio consente di sfruttare appieno tutte le funzionalità e i vantaggi della tecnologia 5G.

Caratteristiche:

- **Indipendenza dal 4G**: La rete 5G gestisce sia il controllo della rete (segnalazione) che il traffico dati, senza necessità di appoggiarsi al 4G.
- **Nuova Infrastruttura**: Richiede un'infrastruttura di rete completamente nuova, inclusi nuovi core network, stazioni base e dispositivi compatibili con il 5G SA.

Nonostante i progressi in termini di sviluppo nella diffusione della nuova tecnologia 5g SA (i provider stanno investendo già dal 2019 nell'aggiornamento dell'infrastruttura) ancora oggi sono presenti problematiche in termini di sicurezza e privacy per gli utenti connessi alla rete telefonica, questo perché le vecchie tecnologie devono coesistere con le nuove rendendo quindi la rete più vulnerabile. Il SUCI ha introdotto sicuramente un grado di protezione maggiore riguardo la privacy degli utenti ma non ha escluso del tutto gli attacchi.

Cosa significano i termini "SUPI" e "SUCI" e a cosa servono

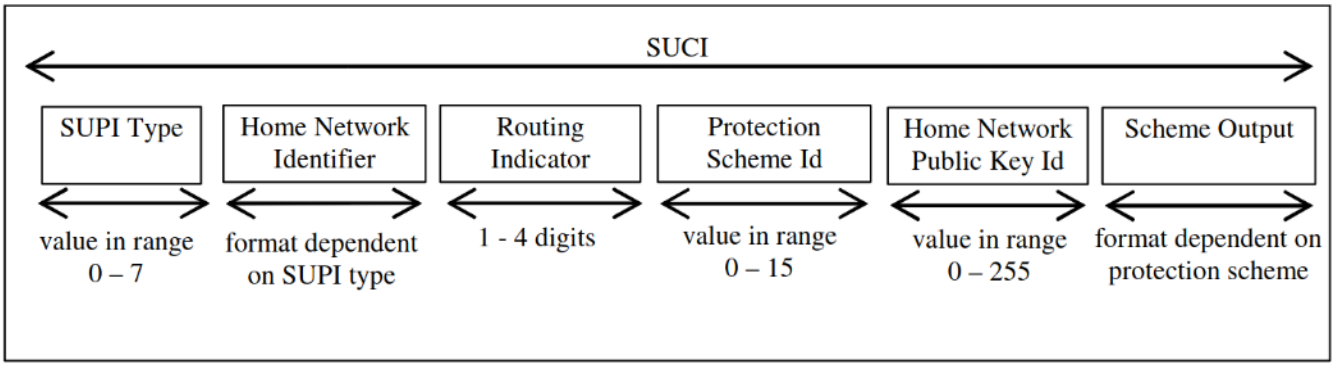
Nella tecnologia 5G, i termini "SUPI" e "SUCI" sono importanti concetti legati all'identificazione degli utenti e alla protezione della loro privacy.

Ecco una spiegazione delle loro differenze e dei loro usi:

SUPI (Subscription Permanent Identifier)

Il SUPI è un identificatore permanente e unico assegnato a ciascun utente di un servizio 5G. Funziona in modo simile all'IMSI (International Mobile Subscriber Identity) utilizzato nelle reti 4G e precedenti. Il SUPI viene utilizzato principalmente per identificare in modo univoco l'abbonato nel database dell'operatore di rete.

Caratteristiche del SUPI:



- **Unicità**: Ogni SUPI è unico per ogni utente.
- **Permanenza**: Non cambia durante la durata dell'abbonamento dell'utente.
- **Formato**: Solitamente, il SUPI è un numero molto lungo che include il Mobile Network Code (MNC) e il Mobile Country Code (MCC), tra le altre informazioni.

SUCI (Subscription Concealed Identifier)

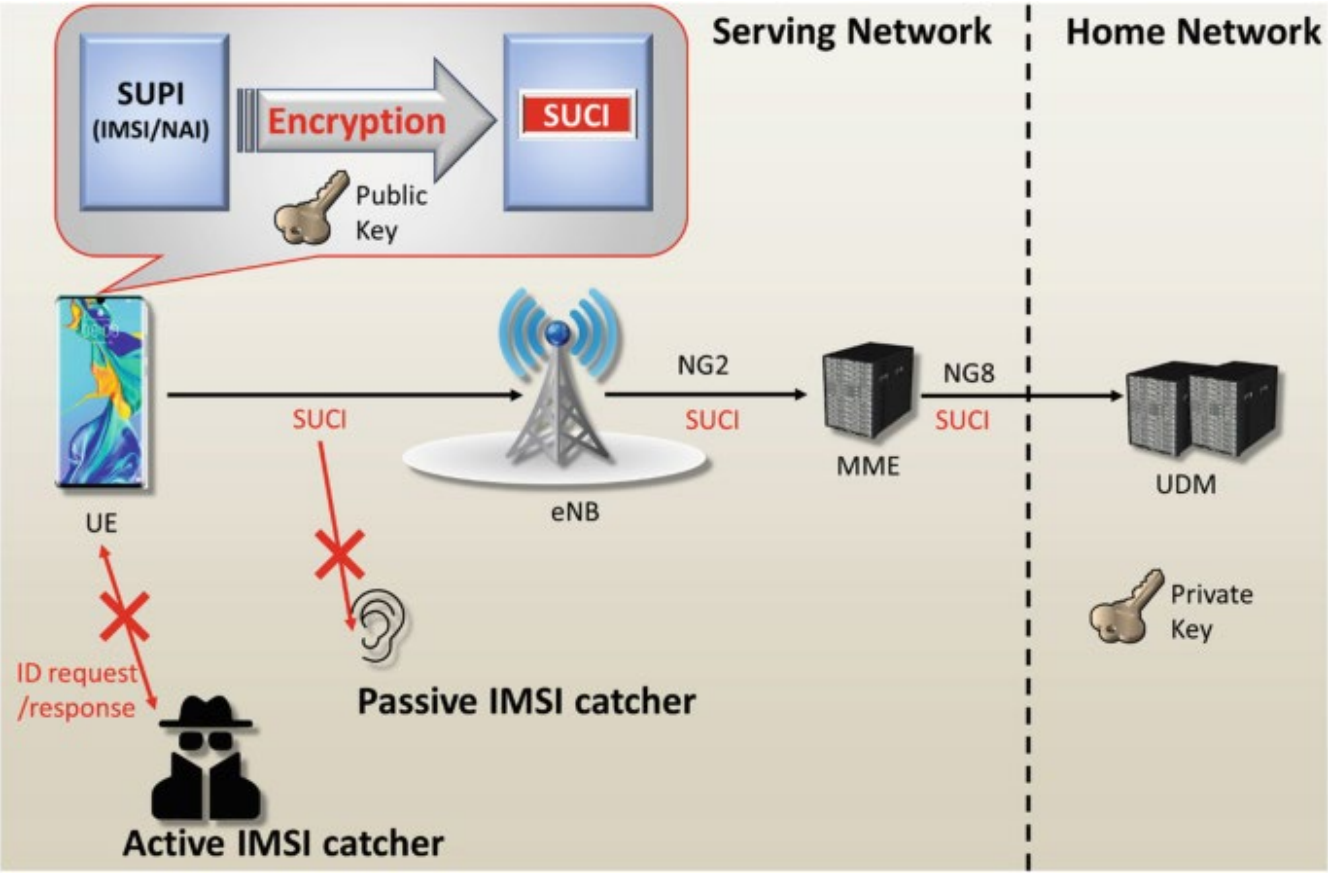
Il SUCI è una versione criptata del SUPI, utilizzata per proteggere la privacy degli utenti quando i dati vengono trasmessi sulla rete. L'idea alla base del SUCI è di evitare che il SUPI venga trasmesso in chiaro sulla rete, prevenendo così il tracciamento e la sorveglianza non autorizzati.

Caratteristiche del SUCI:

- **Protezione della privacy**: Cripta il SUPI per garantire che non possa essere facilmente intercettato e utilizzato per scopi malevoli.
- **Uso temporaneo**: Il SUCI viene generato e utilizzato solo temporaneamente durante la trasmissione dei dati.
- **Generazione**: Il SUCI è generato utilizzando algoritmi di crittografia, combinando il SUPI con una chiave pubblica dell'operatore di rete.

Differenze principali tra SUPI e SUCI:

- **Permanenza**: Il SUPI è un identificatore permanente e unico, mentre il SUCI è una versione temporanea e criptata del SUPI.



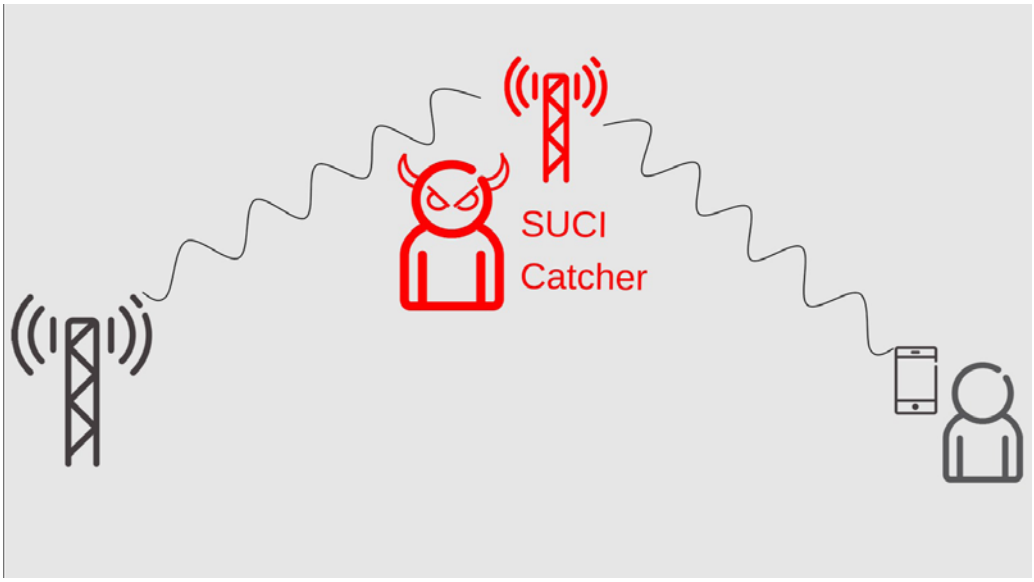
- **Utilizzo**: Il SUPI viene utilizzato internamente dall'operatore per identificare l'utente, mentre il SUCI viene utilizzato per proteggere l'identità dell'utente durante le comunicazioni di rete.
- **Privacy**: Il SUPI, se trasmesso in chiaro, può compromettere la privacy dell'utente, mentre il SUCI protegge la privacy criptando il SUPI.

Che succede se un attaccante riproduce quello che viene ridefinito come SUCI Catcher (IMSI Catcher 5g)?

Informazioni Potenzialmente Ottenibili da un SUCI Catcher

SUCI (Subscription Concealed Identifier):

Il SUCI è una versione criptata dell'IMSI (International Mobile Subscriber Identity). Intercettando il SUCI, un attaccante potrebbe tentare di decifrarlo per ottenere l'IMSI reale.



Metadati della Comunicazione:

Anche se il contenuto della comunicazione è criptato, un SUCI Catcher potrebbe raccogliere metadati come la frequenza delle comunicazioni, i tempi di trasmissione, la durata delle connessioni, e i pattern di traffico.

Informazioni di Posizionamento:

Un SUCI Catcher può essere utilizzato per triangolare la posizione di un dispositivo basandosi sulla potenza del segnale e sulla direzione delle comunicazioni. Questo può rivelare la posizione fisica dell'utente.

Tipi di Dispositivi e Modelli di Utilizzo:

Analizzando i SUCI e i metadati associati, un attaccante potrebbe dedurre il tipo di dispositivo utilizzato (ad esempio, marca e modello) e i modelli di utilizzo dell'utente.

Potenziali Utilizzi delle Informazioni Ottenute

Tracciamento e Sorveglianza:

Ottenere il SUCI e i metadati associati può permettere agli attaccanti di tracciare i movimenti e

le attività degli utenti. Questo è particolarmente rilevante per la sorveglianza di individui specifici.

Profilazione degli Utenti:

Raccolta di informazioni dettagliate sui modelli di utilizzo e sui dispositivi può essere utilizzata per creare profili degli utenti. Questi profili possono includere informazioni su comportamenti, preferenze e routine.

Intercettazione di Comunicazioni Future:

Se un attaccante riesce a decifrare il SUCI e ottenere l'IMSI, potrebbe utilizzare queste informazioni per future intercettazioni di comunicazioni o per eseguire attacchi di spoofing o di frode.

Abusi di Sicurezza e Frodi:

Le informazioni ottenute potrebbero essere utilizzate per impersonare l'utente o per eseguire altre forme di frode, come il furto di identità o l'accesso non autorizzato ai servizi mobili dell'utente.

Conclusioni

La nostra analisi dettagliata delle vulnerabilità nelle reti 5G, con particolare focus sugli IMSI e SUCI Catcher, rivela un panorama di sicurezza complesso e in continua evoluzione. Mentre l'introduzione del SUCI nel 5G SA rappresenta un significativo passo avanti nella protezione della privacy degli utenti, la coesistenza con tecnologie legacy mantiene aperte alcune vulnerabilità. Gli attacchi di downgrade e le tecniche di jamming dimostrano che la sicurezza delle reti 5G richiede un approccio olistico e multistrato.

Le implicazioni di questa ricerca sono profonde per l'industria delle telecomunicazioni, i regolatori e gli utenti finali. È evidente che la transizione completa alle reti 5G SA e l'implementazione universale di protocolli di sicurezza avanzati sono cruciali per mitigare le vulnerabilità attuali. Tuttavia, questo processo richiederà tempo e investimenti significativi.

Guardando al futuro, è imperativo che lo sviluppo delle tecnologie di comunicazione mobile proceda di pari passo con l'evoluzione delle strategie di sicurezza. Ciò include non solo miglioramenti tecnici, ma anche una maggiore consapevolezza e formazione degli utenti, nonché quadri normativi aggiornati per affrontare le nuove sfide di privacy e sicurezza.

In ultima analisi, la sicurezza nel 5G è un obiettivo in movimento, che richiede una collaborazione continua tra ricercatori, sviluppatori e autorità di regolamentazione. Solo attraverso questo sforzo congiunto possiamo sperare di realizzare il pieno potenziale del 5G, garantendo al contempo la protezione dei dati e la privacy degli utenti in un mondo sempre più connesso.

Il Futuro della Sicurezza nelle Reti 5G

L'evoluzione delle reti 5G porta con sé non solo innovazioni tecnologiche senza precedenti, ma anche nuove sfide per la sicurezza e la privacy. Mentre ci addentriamo in questa nuova era di connettività, è fondamentale adottare un approccio olistico e proattivo per affrontare le vulnerabilità emergenti.

Sicurezza 5G come priorità nazionale e internazionale

Secondo un rapporto del World Economic Forum, entro il 2025 si prevede che il 5G supporterà 1,2 miliardi di connessioni a livello globale. Questa crescita esponenziale amplifica l'importanza di implementare robuste misure di sicurezza. Come evidenziato dall'Agenzia dell'Unione Europea per la Cybersecurity (ENISA), la sicurezza del 5G deve essere considerata una priorità nazionale e internazionale.

Alcuni esempi di strategie per il contrasto delle minacce nel 5G

Le aziende leader nel settore stanno sviluppando soluzioni innovative per contrastare le minacce.

Ericsson, ad esempio, ha introdotto il concetto di "Security Reliability Model" per il 5G, che integra la sicurezza in ogni fase dello sviluppo e dell'implementazione della rete. Questo modello enfatizza l'importanza di una "security by design" nell'architettura 5G.

Nokia, d'altra parte, sta puntando sull'intelligenza artificiale e il machine learning per potenziare la sicurezza delle reti 5G. Il loro sistema di "Network Operations Master" utilizza algoritmi avanzati per rilevare e mitigare le minacce in tempo reale, dimostrando come l'AI possa essere un alleato cruciale nella difesa cibernetica.

Un aspetto particolarmente promettente è l'applicazione della crittografia quantistica nelle reti 5G. Ricercatori dell'Università di Bristol, in collaborazione con Toshiba, hanno recentemente dimostrato la fattibilità di integrare la distribuzione quantistica di chiavi (QKD) nelle reti 5G, promettendo un livello di sicurezza senza precedenti per le comunicazioni future.

Sicurezza 5G e Geopolitica, non è solo una questione tecnologica

Tuttavia, la sicurezza del 5G non è solo una questione tecnologica, ma anche geopolitica. Il National Cyber Security Centre del Regno Unito sottolinea l'importanza di una supply chain diversificata e affidabile per l'infrastruttura 5G, evidenziando come la sicurezza nazionale sia intrinsecamente legata alla resilienza delle reti di telecomunicazione.

Per quanto riguarda la privacy degli utenti, l'introduzione del SUCI (Subscription Concealed Identifier) rappresenta un significativo passo avanti, ma è necessario continuare a sviluppare e implementare protocolli di autenticazione ancora più robusti per proteggere l›identità degli utenti da attacchi sofisticati.

Sicurezza nelle Reti 5G, uno sguardo al futuro

Guardando al futuro, la convergenza tra 5G e tecnologie emergenti come l'edge computing e l'Internet of Things (IoT) aprirà nuove frontiere per l'innovazione, ma anche nuove sfide per la sicurezza. Secondo Gartner, entro il 2025, il 75% dei dati aziendali sarà creato ed elaborato al di fuori dei data center tradizionali. Questa decentralizzazione richiederà un ripensamento fondamentale delle strategie di sicurezza.

In conclusione, mentre ci muoviamo verso un mondo iperconnesso, la sicurezza delle reti 5G deve evolversi da una considerazione secondaria a un pilastro fondamentale dell'architettura di rete. La collaborazione tra governi, industria e ricerca accademica sarà cruciale per sviluppare standard e best practices che possano tenere il passo con la rapida evoluzione della tecnologia e delle minacce.

Solo attraverso un impegno collettivo e una visione lungimirante potremo garantire che il potenziale rivoluzionario del 5G si realizzi pienamente, creando un ecosistema digitale sicuro, resiliente e affidabile per le generazioni future.

CYBER CRIME CONFERENCE

16-17 APRILE 2025

AUDITORIUM DELLA TECNICA, ROMA

Iscriviti alla newsletter di ICT Security Magazine
per conoscere l'agenda e partecipare alla
13ª Edizione della Cyber Crime Conference