ONELAYER

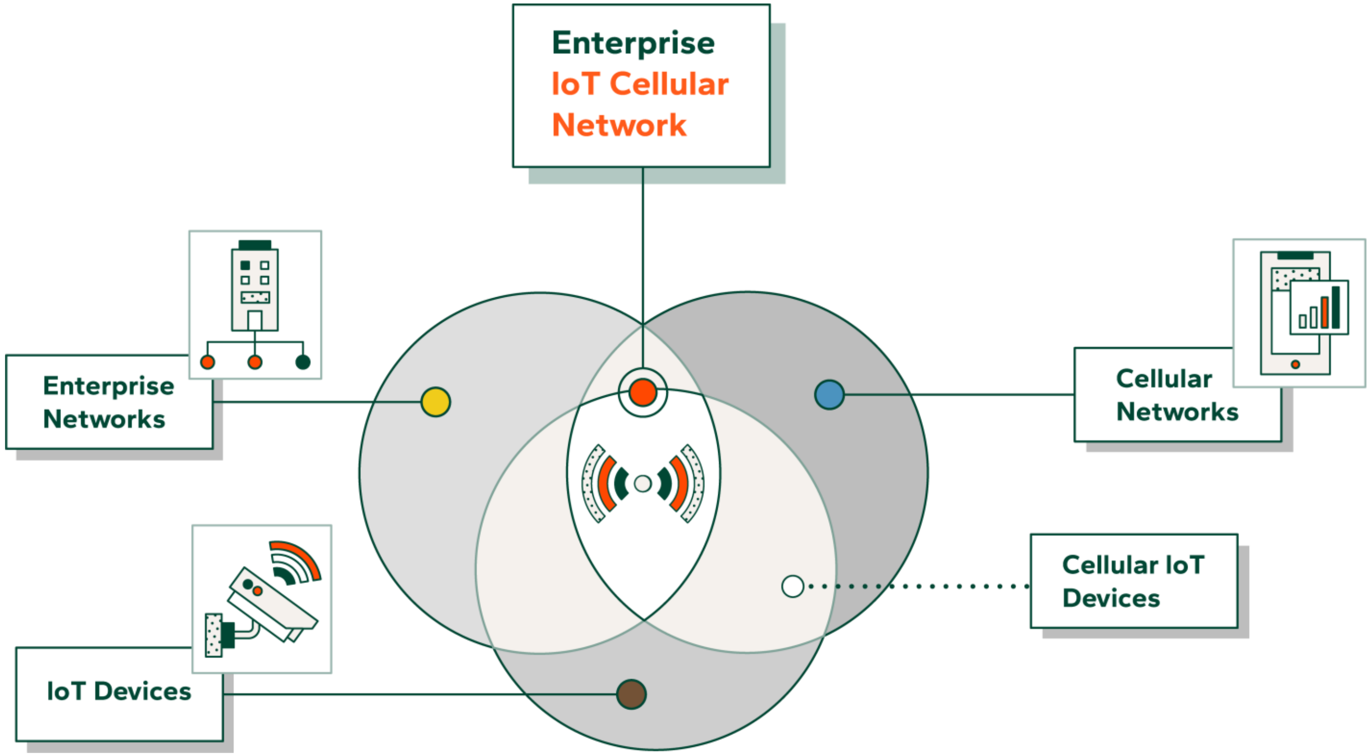
Securing Private Cellular Networks

10 Key Threats and Defense Strategies

Introduction

- Private cellular networks face critical vulnerabilities that can lead to significant security breaches and operational disruptions.
- These attacks can disrupt network functionality, compromise data integrity and confidentiality, and potentially halt company operations, posing severe risks and capital loss.
- Addressing these vulnerabilities is critical for ensuring the security and reliability of the enterprise.

Private Cellular Networks – Attack Vectors



Examples:

- Salt Typhoon Attack
- Sparrow Attack
- Private APNs and Brute Force SMS Attack
- TPC Faking Attack
- Common Search Space Exhaustion Attack
- Combined Uplink Attack
- Re-VoLTE Attack
- MiTM Attacks via Roaming
- Legacy SS7 Protocol Attack
- DoS Attack using IMEI Fraud

- Inter/intra APN movement
- MQTT Hijacking
- Malicious firmware update/ ModBus Hijacking
- Cell signaling storm
- Data DDoS attack (on the core/ device)
- Compromised UE switching networks
- DNS/DHCP hijacking
- CU lateral movement (public-private)
- IP Attack on cellular device
- Cloud lateral movement

Content

1 Salt Typhoon

Identified Attack Vectors

- Chinese state-sponsored cyberattack.
- Compromised eight telecom providers in the U.S., including AT&T and Verizon.
- Critical infrastructure faces severe threats from compromised mobile networks, potentially jeopardizing functions such as water utilities, power grids, etc.
- Exposed a stark reality for enterprises accustomed to trusting MNO infrastructure implicitly.

How Was Salt Typhoon Possible? Identifying Attack Vectors

- Exploitation of Existing Vulnerabilities
- Compromise of Core Network Components
- Infiltration of Lawful Intercept Systems
- Deployment of Advanced Malware and Rootkits
- Targeting of Device Supply Chain
- Potentially Leveraging Additional Methods

Salt Typhoon Alert

Proposed Network Security Actions

Impact on Enterprises: A Call for Enhanced Network Security

Addressing the Expanding Attack Surface:

- Device Security
- Network Segmentation
- Threat Monitoring

Securing the Supply Chain:

- Vendor Assessment
- Firmware Security

Defending Against Advanced Persistent Threats (APTs):

- Rootkit Protection
- Incident Response
- Encryption Standards

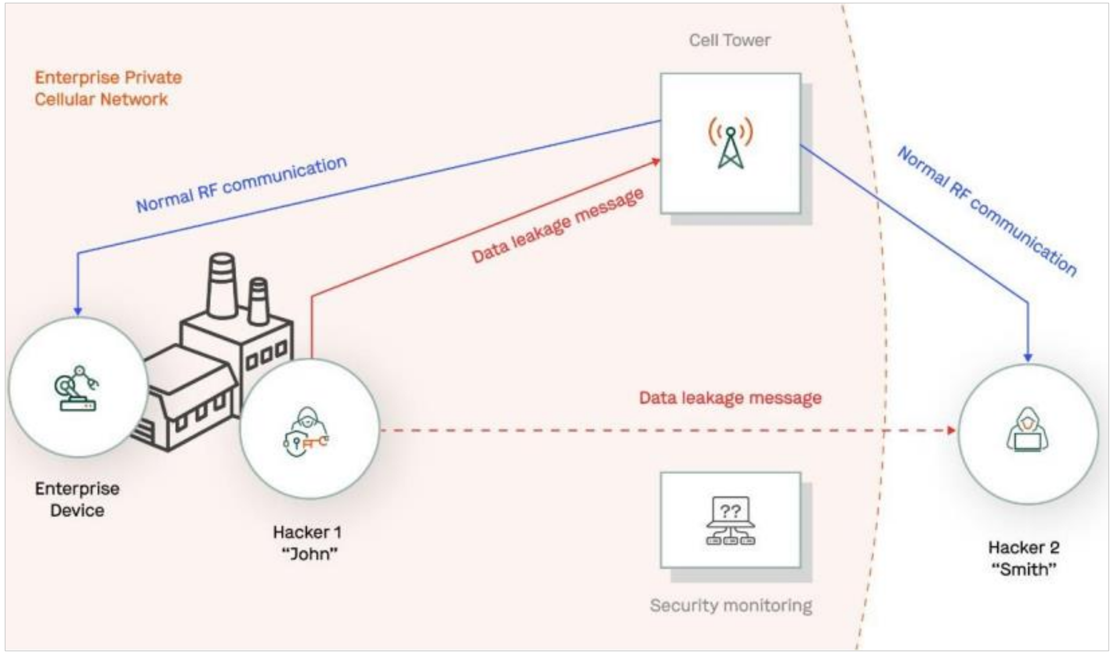
Ensuring Regulatory Compliance and Privacy:

- Regulatory Adaptation
- Cross-Functional Collaboration

2 Sparrow

Identified Attack Vectors

- Exploitation occurs during the unencrypted RF communication phase where messages are transmitted between UE and RAN.
- Allows unauthorized devices to establish hidden channels for data leakage or remote orchestration.
- Focuses on the air interface rather than higher network layers, leveraging wireless communication vulnerabilities.
- **The attack bypasses traditional security measures, enabling anonymous data exfiltration and command/control communications.**



Sparrow

Proposed Network Security Actions

- Implement a layered detection strategy to identify anonymous and suspicious activities.
- Reassess and enhance existing security frameworks to address threats like the Sparrow Attack, safeguarding critical private networks.

3 Private APNs & Brute Force SMS

Identified Attack Vectors

- Bad actors can send SMS to CPEs with public phone numbers even when connected to private APNs, using the SMS channel to disrupt activity.
- Attackers exploit weak default passwords through brute force, bypassing security to control critical infrastructure devices.
- **SMS commands allow attackers to manipulate device settings, leading to privilege escalation and unauthorized access.**

Command	Action	Result
[prefix]enable 0/1	Enable AirLink Management Service (ALMS)	
[prefix]status	Query the status	IP, network status, network type (LTE, UMTS, GPRS), latitude, longitude, timestamp
[prefix]reset	Reset in 30 seconds	
[prefix]relay x y	Set applicable relay x to y	
[prefix]GPS	Get GPS location	Returns a link to a map with device's GPS location

SMS commands supported by several CPE vendors

Private APNs & Brute Force SMS

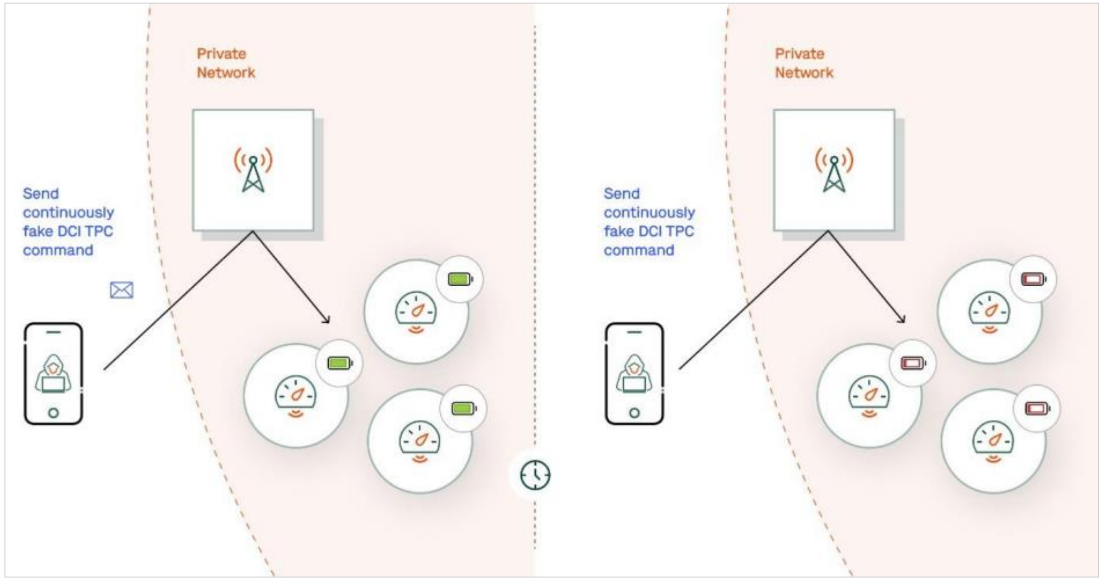
Proposed Network Security Actions

- Monitor CPEs using private APNs rigorously, focusing on access attempts and related security events.
- Enforce stringent security and segmentation policies to restrict device-level communication and limit unauthorized lateral movement.
- Implement mechanisms to block excessive SMS attempts and strengthen password policies to mitigate brute force risks.

4 TPC Faking

Identified Attack Vectors

- Malicious actors inject counterfeit Downlink Control Information (DCI) messages that mimic legitimate Transmission Power Control (TPC) commands, causing continuous elevated power usage in UEs.
- The deception relies on UEs' inherent trust in network directives, allowing these fraudulent commands to blend seamlessly with genuine communication.
- Persistent delivery of fake TPC commands prevents UEs from entering battery-saving modes, exacerbating power drain and network interference.
- **This sophisticated attack targets the unprotected transmission power adjustment process, undermining the operational stability of private networks.**



TPC Faking

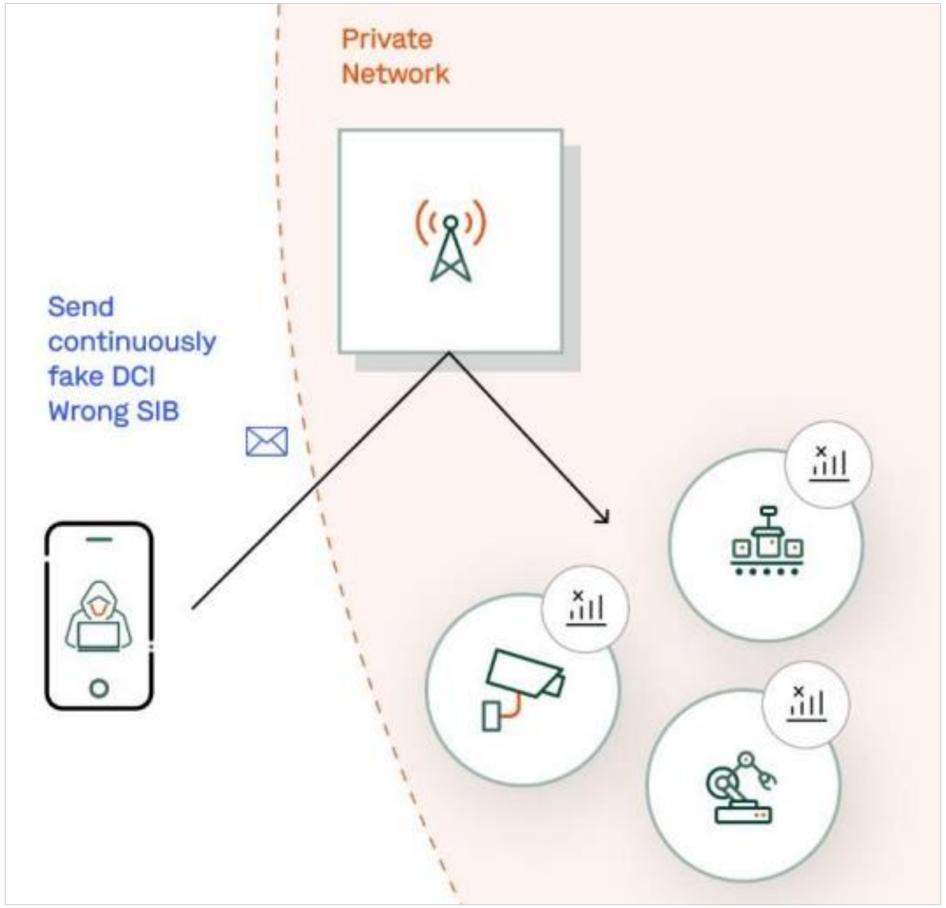
Proposed Network Security Actions

- Implement robust monitoring to detect and identify abnormal DCI message patterns that could indicate TPC manipulation attempts.
- Strengthen authentication and integrity checks for TPC commands to ensure only authorized adjustments to UE transmission power.

5 Common Search Space Exhaustion

Identified Attack Vectors

- The attack disrupts LTE/5G networks by overwhelming the physical downlink control channel (PDCCH) with spurious Downlink Control Information (DCI) messages.
- This attack prevents UEs from receiving essential System Information Blocks (SIBs), crucial for network operations.
- **Private networks, particularly in utilities and manufacturing, face significant disruptions when critical devices are targeted.**



Common Search Space Exhaustion

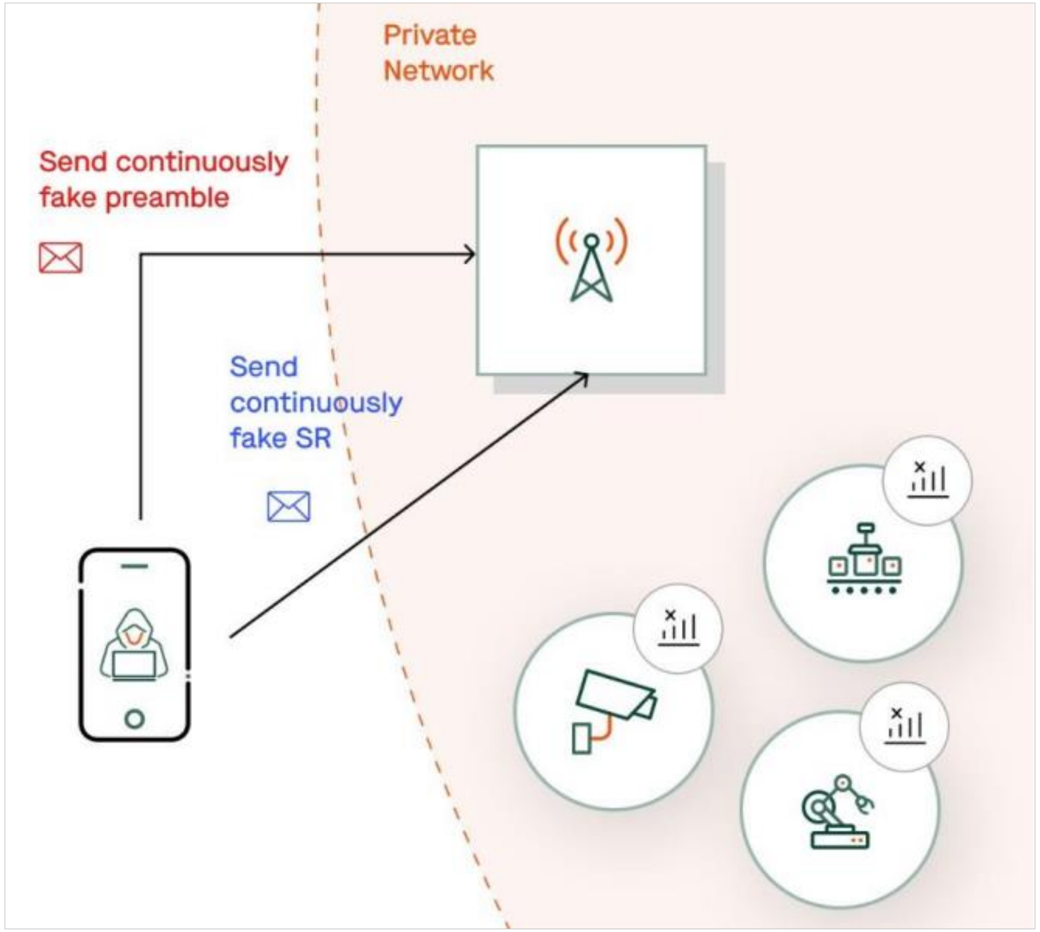
Proposed Network Security Actions

- Implement sophisticated detection systems to identify anomalies in DCI message patterns and mitigate DoS attempts.
- Enhance authentication and validation processes for DCI commands to filter out spurious transmissions.
- Strengthen network defenses, particularly for private sectors, by incorporating robust security protocols to protect each cell against exploitation.

6 Combined Uplink

Identified Attack Vectors

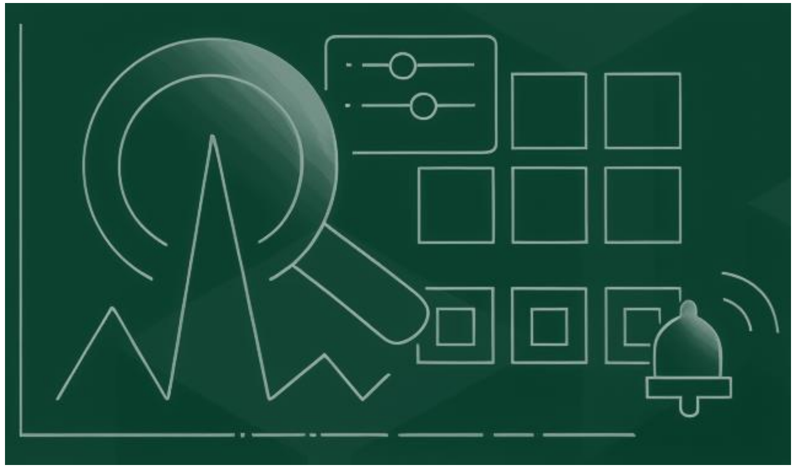
- Physical Random Access Channel (PRACH) Exhaustion floods the network with excessive preamble transmissions, hindering legitimate UEs from establishing connections.
- Segment Routing (SR) Blockage involves either flooding with false scheduling requests or disrupting legitimate SR signals, preventing UEs from acquiring uplink resources.
- This combined attack forces UEs to repeatedly attempt connection, overwhelming the network's resource allocation capabilities.
- **The attack poses significant risks to private networks, particularly those critical to industrial operations.**



Combined Uplink

Proposed Network Security Actions

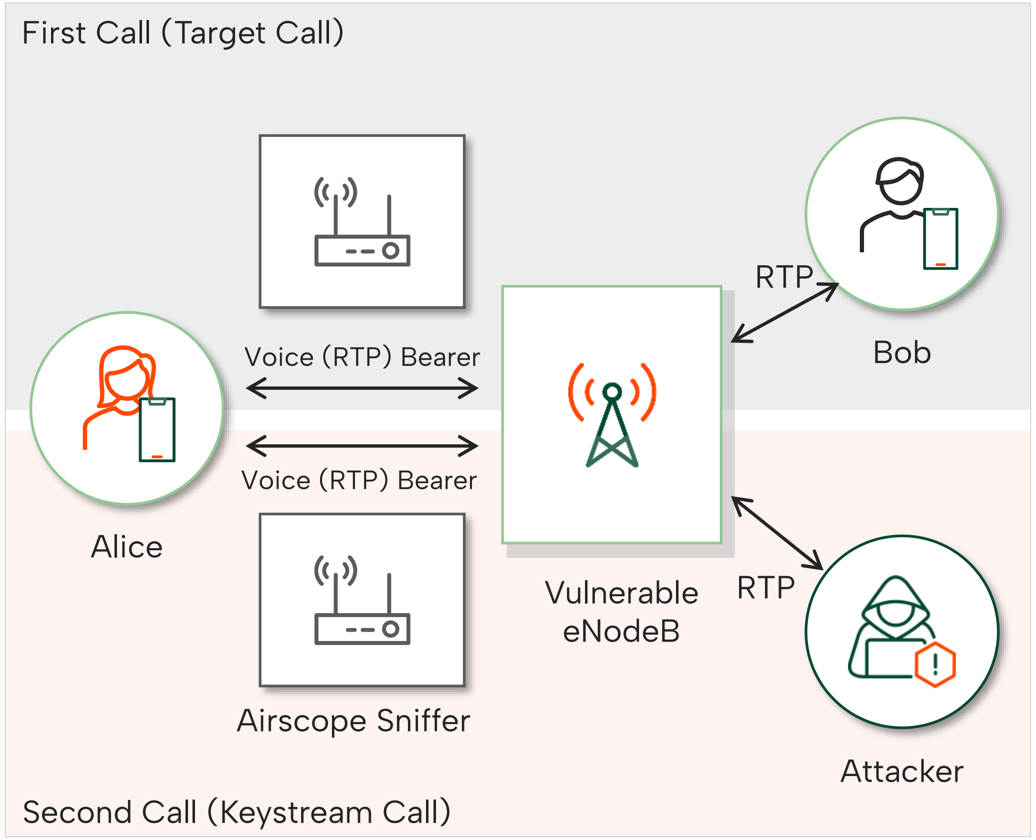
- Implement robust monitoring and anomaly detection systems to identify unusual PRACH and SR patterns, allowing for quick mitigation.
- Enhance resource allocation protocols and introduce protective mechanisms against excessive requests to safeguard network stability.
- Develop contingency plans and rapid response strategies to maintain operational continuity and safety in the event of an attack.



7 Re-VoLTE

Identified Attack Vectors

- Re-VoLTE attack exploits vulnerabilities in the Radio Link Control (RLC) encryption of VoLTE calls by using repeating keystream parameters.
- Back-to-back calls using identical keystreams are targeted, with attackers intercepting communication through Airscope sniffers.
- The exploitable parameters include the static Bearer ID and Keys, which remain unchanged, leading to repeated vulnerabilities.
- **The attack is posing a significant threat to the confidentiality and security of communications in LTE networks.**



Re-VoLTE

Proposed Network Security Actions

- Implement Secure Real-time Transport Protocol (SRTP) to add an additional layer of encryption protection to VoLTE calls.

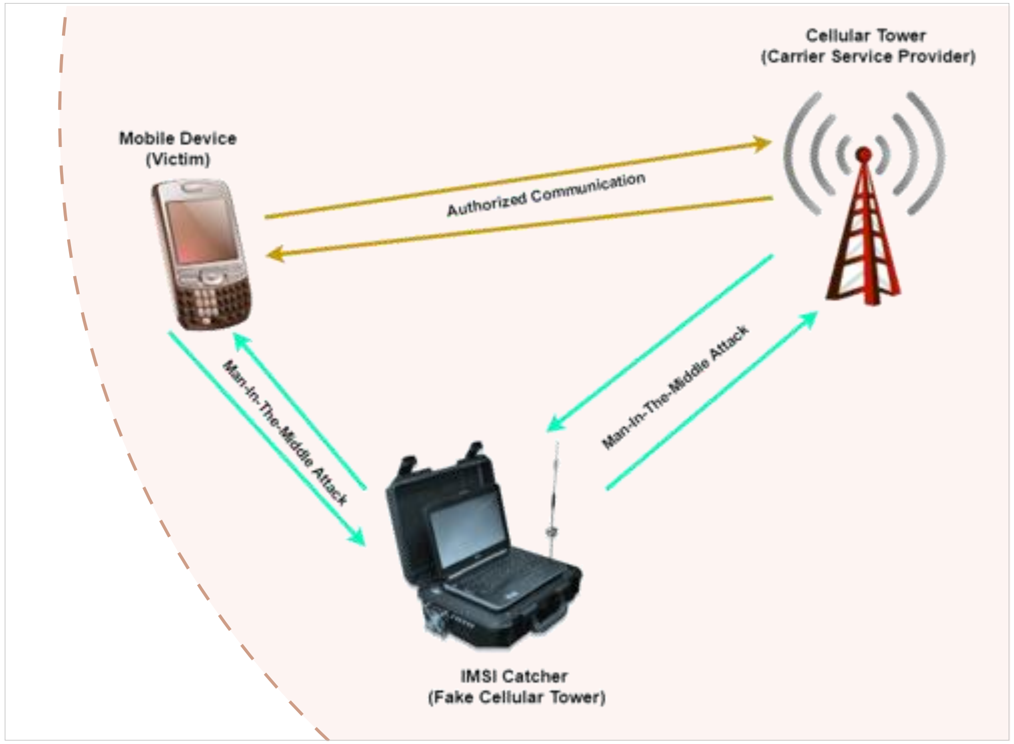
- Modify keystream parameters by either forcing Radio Resource Control (RRC) Reestablishment post-call or randomly changing the Bearer ID after each call.

- While SRTP provides a robust solution, it requires network changes; altering the Bearer ID is simpler but limited by the small number of values, potentially exploitable by repeated attacks.

MiTM Attacks via Roaming

Identified Attack Vectors

- MiTM attacks exploit weaknesses when devices roam between networks, capturing data during these transitions.
- Mixing Up Traffic: Attackers use tricks in HTTP/2 to mess with data streams, intercepting communications
- Redirecting Connections: They can spoof DNS and IP settings to mislead devices and hijack traffic.
- Session Sneaking: Attackers intercept and strip away security layers to listen in on sessions.
- **Data Threat: Sensitive data, like user details, can be captured during roaming, risking privacy breaches.**



MiTM Attacks via Roaming

Proposed Network Security Actions

- Use Strong Encryption: Implement Transport Layer Security (TLS) 1.3 for all communications between networks to keep data secure.

- Enhance Roaming Security Policies: Use Zero Trust Architecture (ZTA) to continuously authenticate and authorize devices, ensuring stringent verification at every connection point.

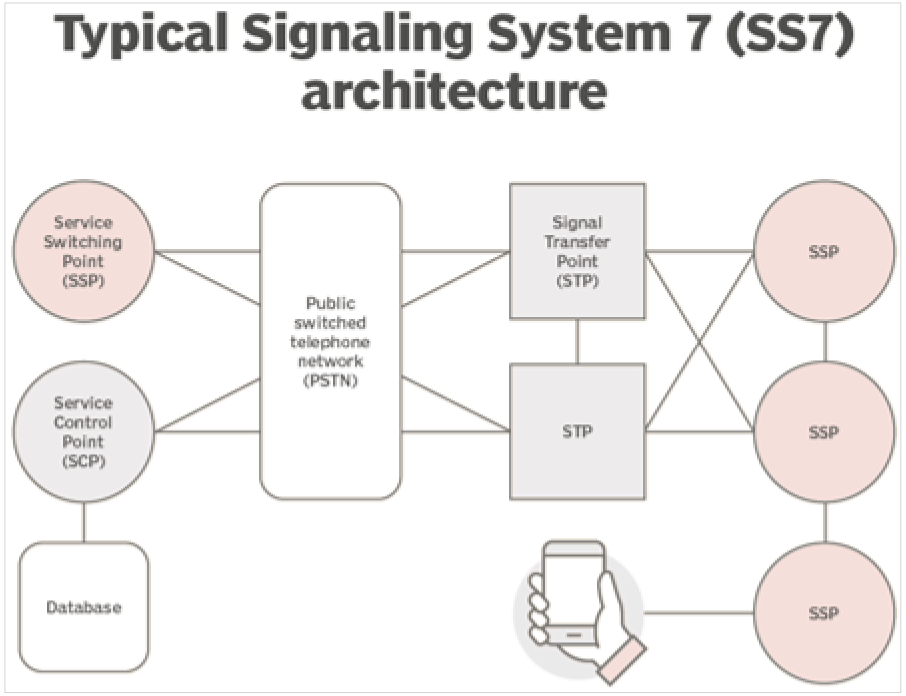
- Encrypt Everything: Use strong encryption to protect data at every step, especially when switching between different networks.

9 Legacy SS7 Protocol

Identified Attack Vectors

- Identity Targeting: Hackers often target IMSI data for identity-based attacks, highlighting the need to secure and scramble this information.
- Roaming Weak Spots: Older network parts are especially vulnerable during international roaming, due to SS7's lack of modern security.
- Firewall Gaps: Even with firewalls, tests show many security holes, stressing the need for ongoing monitoring and fixes.
- Risk: easy for hackers to track, intercept data, and bypass security checks.

The SS7 architecture for landline and mobile phone service can be exploited in an SS7 attack.



Legacy SS7 Protocol

Proposed Network Security Actions

- Deploy SS7 Firewalls: Use firewalls specifically designed to block
  SS7-based attacks.

- Work Together: Encourage sharing of security tips and insights across the telecom industry to combat SS7 vulnerabilities.

- Keep Systems Updated: Regularly test and update firewalls and security settings to stay ahead of new threats.

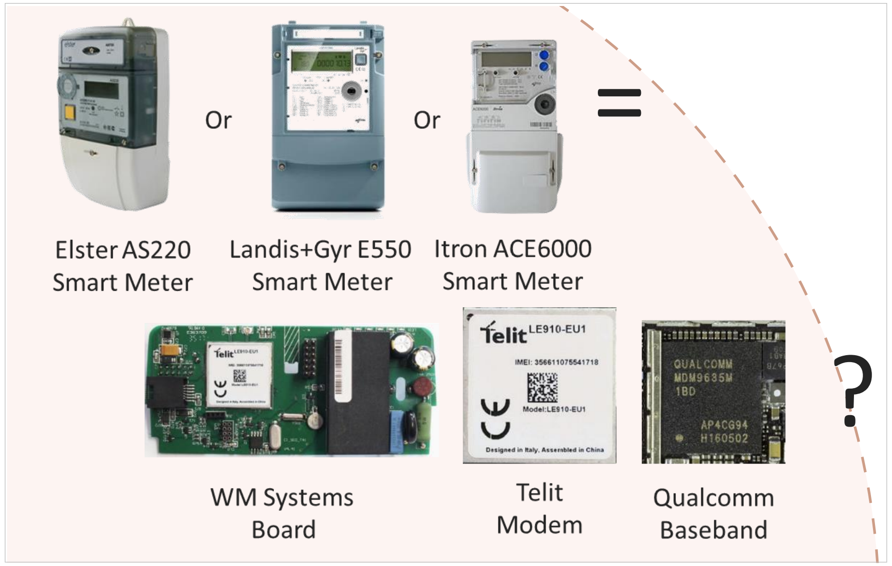
10 DoS Attack using IMEI Fraud

Identified Attack Vectors

- Attackers manipulate IMEI using commands on specific chipsets, (e.g., "AT+EGMR" on Medaitek, and guides for Qualcomm), to alter device identity, bypassing 3GPP authentication and validation controls.

- IMEI fraud combined with a SIM card circumvents the Equipment Identity Register (EIR) checks, enabling network abuse and potential DoS attacks.

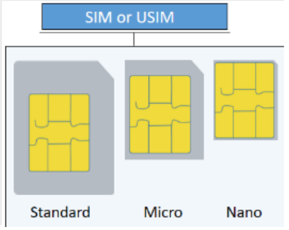
- **This attack vector enables unauthorized access to sensitive systems, such as meters management and monitoring servers.**



Use case analysis – DoS Attack using IMEI Fraud

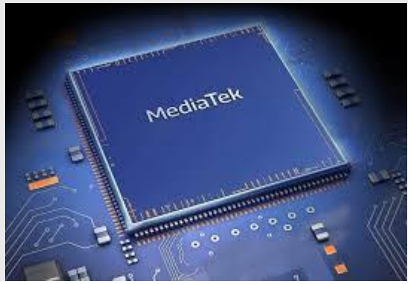
In some cases, IMEI is printed on the device itself.

Some devices are using USIM and it can be extracted from the physical socket.

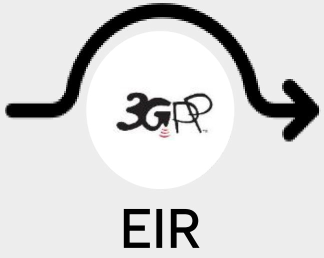


Attacker will be able to **set the IMEI (e.g.: IMEI of the legit meter) over a malicious modem.**

In Mediatek chipset, using “**AT+EGMR**” command will allow the attacker to change the modem IMEI.



Combining the IMEI and the SIM card will allow the attacker to **bypass all the 3GPP authentication and validation (EIR).**



In Qualcomm chipset, using this GIT **guide** will also allow the attacker to change the IMEI.

The attacker will be able to reach, for example, the meters management and monitoring server and will be able to **initiate a DoS attack on this server**

DoS Attack using IMEI Fraud

Proposed Network Security Actions

- Implement anomaly detection mechanisms to identify behavior anomalies, such as DoS and IMEI fraud, by correlating data from multiple sources.
- Use alerts and enforcement measures, like SIM and IMEI deprovisioning, to isolate suspicious activities.
- Employ advanced machine learning models and signaling analysis for proactive detection and enhance operational diagnostics with detailed historical data analysis.
- Integrate a Zero-Trust Approach by collecting extensive data points from the network to take informed and strategic actions against threats.

ONELAYER

To learn more:

www.onelayer.com

in OneLayer