**Comprehensive Research on SS7 and Its Impact on 5G Network Slicing**

Signaling System No. 7 (SS7) is a crucial **telecommunications signaling protocol** that plays a key role in traditional mobile networks. However, its **inherent security vulnerabilities** pose a major risk when **5G networks interoperate with older 2G, 3G, and 4G networks**. Attackers can exploit SS7 flaws to **track users, intercept SMS messages, hijack calls, and launch DoS attacks**, which could significantly **impact 5G network slices**.

**1. What is SS7 and Why is it Still Relevant in 5G?**

**Overview of SS7**

SS7 (Signaling System No. 7) is a **telecommunication signaling protocol suite** used for: **Call setup & routing**  
 **SMS delivery**  
 **Mobile network authentication**  
 **Location tracking services**

It was **designed for trusted networks**, meaning **security was not a major concern** in its original development. Today, as telecom networks have evolved to **5G**, the **legacy dependence on SS7 remains a critical security issue**.

**SS7’s Role in 5G Networks**

Modern **5G networks use more secure protocols** such as:

* **Diameter** (for authentication and routing)
* **HTTP/2** (for communication in 5G Core)
* **SBI (Service-Based Interfaces)** for service-oriented communication

However, **5G still needs to interoperate with older networks** (4G, 3G, and 2G). **This legacy interconnection keeps SS7 relevant** and creates a backdoor for attackers to compromise 5G slices.

**Why SS7 Vulnerabilities Matter for 5G**

* **5G devices may still rely on SS7-based authentication** when communicating with 3G/4G networks.
* Attackers can **exploit weaknesses in older networks** to infiltrate 5G slices.
* **Sensitive 5G services (e.g., financial transactions, smart cities, military communications) are at risk** if SS7 is left unprotected.

**2. SS7 Security Vulnerabilities & Their Impact on 5G Network Slicing**

**A. Location Tracking Attacks**

**Threat:**

Attackers can exploit SS7 vulnerabilities to **request a mobile device’s real-time location** without the user's knowledge.

**Impact on 5G:**

**Tracking sensitive users:** Attackers can monitor the location of **VIPs, government officials, military personnel, or corporate executives** within **high-security 5G slices**.  
 **Targeted cyberattacks:** Location data can be used to **launch phishing or hacking attacks** against users in sensitive slices.

**Example Attack:**

* A hacker **exploits SS7’s MAP (Mobile Application Part) messages** to track **a CEO’s movements** while they communicate over a secure corporate 5G slice.

**Countermeasures:**

**Deploy SS7 Firewalls:** Block unauthorized location requests.  
 **Encrypt Location Requests & Responses:** Prevent location data interception.

**B. SMS Interception (Bypassing Two-Factor Authentication)**

**Threat:**

Attackers can use SS7 vulnerabilities to **reroute SMS messages** (including OTPs for Two-Factor Authentication).

**Impact on 5G:**

**Bypassing 2FA:** If **5G network slices use SMS for authentication**, an attacker can intercept OTPs and gain **unauthorized access** to critical applications.  
 **IoT & Enterprise Security Risks:** IoT slices that rely on **SMS-based authentication** are vulnerable to SS7-based OTP hijacking.

**Example Attack:**

* A hacker **exploits the SRISM (SendRoutingInfoForSM) SS7 command** to intercept **a 2FA SMS meant for a banking slice user**, allowing unauthorized financial transactions.

**Countermeasures:**

**Adopt App-Based MFA or FIDO2 Authentication:** Replace SMS-based authentication.  
 **Use AI-Driven Fraud Detection:** Detect unusual SMS rerouting patterns.

**C. Call Hijacking & Eavesdropping**

**Threat:**

Attackers can **reroute phone calls** and listen in on conversations by manipulating SS7 signaling messages.

**Impact on 5G:**

**Intercepting critical communications:** If a **5G slice is used for emergency response, banking transactions, or corporate meetings**, attackers can **listen in or manipulate conversations**.  
 **Financial fraud & identity theft:** Call hijacking allows **social engineering attacks** where attackers **impersonate a CEO or banking representative**.

**Example Attack:**

* A hacker **exploits SS7’s Call Forwarding function** to redirect a **VIP’s corporate 5G slice calls to an attacker-controlled number**.

**Countermeasures:**

**Use End-to-End Encryption for Calls:** Ensure voice communication security.  
 **Monitor & Log Unusual Call Forwarding Requests:** Detect hijacking attempts.

**D. SS7-Based Denial-of-Service (DoS) Attacks on 5G Interconnections**

**Threat:**

Attackers **flood SS7 networks with fake signaling messages**, causing service outages and authentication failures.

**Impact on 5G:**

**Spillover effects on 5G slices:** A **DoS attack on a 4G authentication system** can **disrupt connected 5G slices**.  
 **Identity spoofing & service downtime:** Attackers can **disable authentication**, making it easier to impersonate users.

**Example Attack:**

* A hacker **floods a 4G intermediate node with fake SS7 UpdateLocation messages**, **overloading the 5G Authentication System (AUSF)**.

**Countermeasures:**

**Rate-Limit SS7 Requests:** Prevent excessive signaling traffic.  
 **Use AI-Driven Anomaly Detection:** Identify unusual traffic spikes.

**3. How SS7 Attacks Can Be Used to Compromise 5G Network Slices**

The table below summarizes the impact of SS7 attacks on 5G slices and the required mitigation strategies.

|  |  |  |
| --- | --- | --- |
| SS7 Attack | Impact on 5G Network Slices | Mitigation Strategies |
| Location Tracking | Tracks users in sensitive slices (e.g., corporate, military). | SS7 Firewalls, encrypted location requests. |
| SMS Interception | Bypasses OTP security for access to 5G slices. | Non-SMS authentication (app-based MFA). |
| Call Hijacking | Intercepts critical 5G slice communications. | End-to-end encryption, anomaly detection. |
| SS7 DoS Attacks | Causes authentication failures in 5G slices. | AI-driven monitoring, rate-limiting. |

**4. Solutions: How to Secure SS7 for 5G Network Slicing**

**1. Deploy SS7 Firewalls**

Detect & block unauthorized SS7 requests in real time.  
 Prevent location tracking, SMS interception, and call hijacking.

**2. Implement AI-Based Threat Detection**

Use **machine learning** to analyze signaling traffic for anomalies.  
 Identify & prevent **SS7-based fraud and cyberattacks**.

**3. Migrate to Secure Diameter & HTTP/2 Protocols**

**Reduce reliance on SS7** for inter-network authentication.  
 Enable **stronger encryption and security policies** in 5G signaling.

**4. Adopt End-to-End Encryption**

Encrypt voice calls & messages to prevent **interception attacks**.  
 Ensure **highly sensitive 5G slices (e.g., government, finance) are protected**.

**Conclusion**

🔹 **SS7 vulnerabilities remain a major threat to 5G network slicing due to legacy interconnections with older networks.**  
🔹 **Attackers can exploit SS7 flaws to track users, intercept messages, hijack calls, or launch DoS attacks on 5G slices.**  
🔹 **Telecom providers must implement SS7 firewalls, AI-driven threat detection, and secure alternative protocols to mitigate risks.**

Here are several real-world case studies that illustrate the exploitation of SS7 vulnerabilities:

**1. German Bank Account Thefts (2017)**

**Incident:** Attackers exploited SS7 vulnerabilities to intercept two-factor authentication (2FA) codes sent via SMS to online banking customers in Germany. By redirecting these SMS messages, the attackers were able to complete unauthorized bank transfers, effectively draining the victims' accounts.

**Method:**

* Attackers first infected victims' computers with malware to obtain online banking credentials.
* Using SS7 vulnerabilities, they redirected the victims' mobile communications to devices controlled by the attackers.
* When the bank sent an SMS with a transaction authentication number (TAN) for 2FA, the attackers intercepted it and completed the fraudulent transactions.

**Impact:** Multiple bank customers suffered financial losses due to unauthorized withdrawals.

**Source:**

[The Hacker News](https://thehackernews.com/2017/05/ss7-vulnerability-bank-hacking.html?utm_source=chatgpt.com)

**2. Bitcoin Theft via SS7 Exploitation (2017)**

**Incident:** Researchers demonstrated how SS7 vulnerabilities could be used to take control of a victim's Gmail account and subsequently access their Bitcoin wallet, resulting in the theft of over $4,000 worth of cryptocurrency.

**Method:**

* By exploiting SS7 flaws, the researchers intercepted SMS messages intended for the victim.
* They used this access to reset the victim's Gmail password by receiving the SMS-based verification code.
* With control over the Gmail account, they reset the password for the victim's Bitcoin wallet and transferred the funds.

**Impact:** This proof-of-concept attack highlighted the potential for significant financial theft through SS7 vulnerabilities.

**Source:**

[CyberScoop](https://cyberscoop.com/ss7-bitcoin-hack-positive-technologies/?utm_source=chatgpt.com)

**3. Location Tracking and Eavesdropping (2014)**

**Incident:** Security researchers revealed that SS7 vulnerabilities allowed attackers to track the movements of mobile phone users and intercept their calls and messages without their knowledge.

**Method:**

* By sending specific requests through the SS7 network, attackers could obtain the location information of targeted mobile devices.
* They could also redirect calls and SMS messages to devices under their control, enabling eavesdropping and data interception.

**Impact:** This vulnerability posed significant privacy risks, allowing unauthorized parties to monitor individuals' locations and communications.

**Source:**

[Wikipedia, the free encyclopedia](https://en.wikipedia.org/wiki/Signalling_System_No._7?utm_source=chatgpt.com)

**4. U.S. Congressman Phone Hack Demonstration (2016)**

**Incident:** In a controlled demonstration, researchers exploited SS7 vulnerabilities to intercept and record phone calls made by U.S. Congressman Ted Lieu, highlighting the ease with which such attacks could be carried out.

**Method:**

* With the Congressman's consent, researchers used SS7 exploits to track his phone's location and intercept calls.
* They demonstrated the ability to listen to and record conversations without any physical access to the device.

**Impact:** This demonstration underscored the critical security flaws in the SS7 protocol and the potential risks to high-profile individuals.

**Source:**

[Congressman Ted Lieu](https://lieu.house.gov/media-center/in-the-news/what-ss7-and-china-using-it-spy-trump-s-cell-phone?utm_source=chatgpt.com)

**5. Global Surveillance Exploitation (2018)**

**Incident:** Investigations revealed that various entities were exploiting SS7 vulnerabilities to conduct global surveillance, tracking individuals' movements and intercepting communications across different countries.

**Method:**

* By leveraging SS7 flaws, attackers could access location data and communication content of mobile users worldwide.
* This was often done without the knowledge or consent of the individuals or their service providers.

**Impact:** The exploitation of these vulnerabilities raised significant concerns about privacy and the potential for unauthorized surveillance on a global scale.

**Source:**

[Enea](https://www.enea.com/location-tracking-attacks-exploiting-the-ss7-network/?utm_source=chatgpt.com)

References

* **Articles & Research Papers**
* [SS7 Security Overview (ENISA)](https://www.enisa.europa.eu/)
* [SS7 Vulnerabilities Report by AdaptiveMobile](https://www.adaptivemobile.com/)
* IEEE Paper: "SS7 Security Threats and Impact on 5G"
* **Videos & Webinars**
* YouTube: **"How SS7 Attacks Work and How to Prevent Them"**
* Webinar: **"5G Security Risks from Legacy Networks"**