SecurityGen
Telecom Security. Transcending Generations.

Navigating Present Telecom Threats

Essential Security for 4G & 5G Networks

With the rise of sophisticated cyber threats, telecom operators are increasingly at risk. The rapid 5G rollout has broadened the attack landscape, making the security of core networks paramount. The telecom infrastructure is a prime target for various types of attacks, ranging from those seeking monetization by misusing networks and services to attackers stealing subscriber information, as well as advanced threats aimed at causing disruptions and network outages. Mitigating these threats is a priority to maintain business continuity, brand reputation, customer trust, and regulatory compliance.

SecurityGen's ongoing research and assessments into telecom network vulnerabilities offers critical insights and actionable strategies for telecom leaders to proactively address emerging threats. Below are key areas that telecom leaders should prioritize to stay ahead of evolving adversarial tactics.

Core Network Vulnerabilities

Static Security Protection

Many operators rely solely on rule-based signaling security solutions, assuming they provide adequate protection. **However, our study found that 90% of operators** were vulnerable demonstrating incomplete protection due to inadequate configuration and lack of continuous monitoring. Security protection keeps changing and can degrade over time due to equipment migrations, vendor swaps, and configuration changes.

Legacy Protocols as Backdoor Vulnerabilities

Legacy mobile technologies like SS7 (Signalling System No. 7), nearly 50 years old, remain widespread yet highly vulnerable. **Our research has identified serious backdoor vulnerabilities within SS7**. Its outdated nature makes it a prime target for attackers, impacting even newer 4G infrastructure. New exploitation techniques—such as **Variable Length XUDT Segmentation** and **Parameter Tag Manipulation**—allow attackers to bypass firewalls, posing a critical risk. As operators transition away from 2G/3G, urgent action is needed to close these backdoor vulnerabilities.

Critical Technologies for LTE and 5G

Our assessment found 23% of networks vulnerable to GTP (GPRS Tunnelling Protocol)protocol attacks. This vulnerability stems from gaps in real-time location verification and a lack of border devices with advanced built-in protections. Current security systems, operating primarily as simple whitelists or blacklists, often lack control plane visibility to detect advanced threats targeting the telecom core.

Challenges with Equipment Vendor Security

As operators expand services like VoLTE and VoNR, many rely heavily on equipment vendors for network security. However, these equipment vendors may lack the specialized security expertise to detect complex telecom-specific vulnerabilities, increasing the potential for overlooked threats.

Strategies to Protect Core Telecom Networks

To secure telecom networks effectively, operators need a dynamic, threat-informed defense that evolves with emerging risks rather than relying on static or single-point solutions. Prioritizing threat verification is another essential element, enabling operators to identify and address the most pressing security concerns while avoiding wasted resources on low-impact vulnerabilities.

Adopting a comprehensive security approach backed by telecom-specific threat intelligence enables operators to conduct regular security inspections, actively detect intrusion attempts, and implement robust protections against a range of threats, from general to advanced. This balanced approach, combining proactive threat management with intelligence-led security measures, empowers telecom operators to maintain customer trust, protect brand reputation, and ensure regulatory compliance.

For more details on SecurityGen's latest threat intelligence findings and how our threat-informed defence approach can help secure 4G/LTE and 5G networks: ***contact@secgen.com***

About SecurityGen

Founded in 2022, SecurityGen is a global company focused on telecom security. We deliver a solid security foundation to drive secure telecom digital transformations and ensure safe and robust network operations. Our extensive product and service portfolio provides complete protection against existing and advanced telecom security threats.

Connect With Us

✉ Email: **contact@secgen.com**

Website: **www.secgen.com**

in /company/securitygen/

UK | Italy | Czech Republic | Brazil | Mexico | India | Malaysia | UAE | Egypt | Lebanon