SecurityGen

Telecom Security. Transcending Generations.

More than 50% of networks are vulnerable to VoLTE hacking, potentially resulting in revenue leakages

This is because many VoLTE networks are launched with weak security setups. This oversight leaves them vulnerable to hackers, who can penetrate the IMS network, engage in fraud, and disrupt service availability. What's more, as VoLTE networks expand their reach for roaming, these vulnerabilities are no longer confined to one country but expose VoLTE services at global scale.

Why the VoLTE Rush?

As we move away from 2G/3G networks across the globe the number of VoLTE networks is rapidly increasing.

96% of MNO and MVNO companies have bumped up the priority of VoLTE roaming for 2023.

However, this quick transition also exposes security challenges, as rapid growth underscores the urgency to protect VoLTE networks against a diverse array of security threats.

With around 250 VoLTE networks in operation and more on the way, the risk of security breaches and subsequent data, revenue and other leakages is a growing concern.

The SecurityGen Promise

Quick launch of VoLTE services is an important business objective. And VoLTE roaming testing is the top challenge for operators to validate roaming scenarios.

So, if you're in a hurry to get VoLTE in place and roaming available off the ground, SecurityGen will take care about security part of it:

- Conduct a security audit for your VoLTE network to identify potential vulnerabilities.
- Address those weak spots with existing protection measures—there are always options.
- Plan for the future with more robust, forward-looking security solutions.

We will explore the best option to balance business objective and sufficient threat mitigation techniques, ensuring the security of connections, safety of subscriber data and protection of revenue streams against VoLTE hacks.

Key obstacles and how we will help you to overcome them

Key vulnerabilities persist in mobile networks, allowing adversaries to exploit VoLTE/VoWiFi, especially during roaming scenarios.

Some notorious attacks include:

Call Spoofing and Interception

Charging Abuse via tunneling mechanisms

Denial of Service (DoS) attacks on IMS nodes like I-CSP, S-CSCF

Kaleido Intelligence estimates that operator losses from fraud and security incidents reached over **$35 billion in 2022,** and anticipates that this will increase towards 2025, reaching **$45 billion** that year.

This means hacker and fraudsters will continue to challenge VoLTE/VoWiFi and other VoIP implementation's security measure as exploitation of these technologies provides a surefire way for monetisation, like - **Flash calls, Robocall, Wangiri** etc.

Efficient protection demands not only the deployment of security best practices but also ongoing learning and adapting to new adversary tactics and techniques. And there is no one-size-fits-all solution that could be deployed to instantly solve all problems. SecurityGen offering combines decades of hands-on experience in LTE/5G and legacy networks with cybersecurity best practices backed by telecom threat intelligence. With this expertise, we deliver the shortest path to efficient protection for our customers.

Why SecurityGen?

SecurityGen doesn't simply act according to rules. We continuously challenge cyber-security status quo, doing research and verifying how it is applied in real work telecoms scenarios. This helps to be one step ahead of adversaries and fraudsters.

- Over the last 12 months SecurityGen team conducted more than 150 security audits for MNOs across the globe – we know how networks operate and which deficiencies may be exploited by adversaries.
- Our intrusion detection systems are placed in multiple mobile networks from the Americas to Asia, we continuously collect and analyse information about suspicious, illegitimate and fraudulent activities generating useful threat intelligence.
- Cybersecurity research conducted in our LTE and 5G cybersecurity lab provides a critically important perspective on developing threats. This information allows us to share proactive protection measures with our customers.

The lessons learned from securing VoLTE networks will be instrumental as we go through the **5G evolution, with VoNR (Voice over New Radio)** adoption for mobile voice services. The dynamics of VoLTE security will shape the security blueprint for emerging **5G and VoNR infrastructures** and will definitely pay off.

About SecurityGen

SecurityGen is a global company focused on cybersecurity for 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

UK | Italy | Czech Republic | Brazil | Egypt | Lebanon
India | South Korea | Japan | Malaysia | UAE