SecurityGen
Telecom Security. Transcending Generations.

VoLTE Roaming and the Security Implications

Understanding VoLTE roaming

While VoLTE (Voice over LTE) may seem like a novel technology to some, it has been around for over a decade and a half. This begs the question: Why is there a sudden uptick in interest among Mobile Network Operators (MNOs) for VoLTE?

A look back at VoLTE's journey

In the early days of LTE deployment, many operators overlooked VoLTE support. LTE/4G was primarily a data-centric network, devoid of voice capabilities. The majority of operators, especially across many countries, were not deeply concerned about integrating voice due to the widely accepted 2G & 3G fallback method, formally known as **Circuit Switched FallBack (CSFB).** Using CSFB, an LTE device would "fall back" to 3G or 2G networks to complete voice calls. Consequently, LTE was reserved for data, while 3G managed voice, offering a harmonious setup for MNOs and users.

However, as telecommunication technologies evolved, MNOs increasingly gravitated towards advanced technologies like 4G and 5G. These networks promise superior services, reduced latency, and heightened efficiency. This shift has led to a strategic decision to phase out older networks like 2G and 3G to reallocate spectrum for advanced services, such as 5G.

Initially, this didn't set off alarms. With only one of the 2G or 3G networks decommissioned, the fallback mechanism would still operate, ensuring voice continuity. But the landscape began to change, especially in countries like the USA and a few others which either decommissioned both 2G and 3G networks or have plans for a complete shutdown. **VoLTE becomes the sole mode of delivering mobile voice services in these scenarios. The GSMA Intelligence data predicts that more than 55 2G and 3G networks will be closed between 2021 and 2025.** Again, while the two technologies will not necessarily be retired at the same time as can be seen across Europe and Asian countries. There are also few countries like USA who have almost retired both 2G and 3G.

This posed a significant challenge. The shift was smoother for nations like the USA that had the foresight to gear up for this transition. However, others found themselves in a conundrum, especially when ensuring voice services for their citizens traveling to nations without 2G and 3G. The absence of these networks means roaming subscribers from these regions would be isolated, unable to access calls or SMS when in nations that have phased out 2G and 3G—a situation that can have serious implications, especially concerning social security and essential services.

The urgency of the situation triggered a rushed pivot towards VoLTE, occasionally sidelining network security considerations. For roaming calls in countries like the USA, operators had first to stabilize VoLTE for domestic calls. While many MNOs hastened this process, inadvertently introducing security gaps, the next phase is enabling VoLTE in roaming—a daunting challenge. An implementation without detailed security thought process could leave the VoLTE network exposed to threats, particularly from roaming networks.

Security Concerns with VoLTE Roaming

There are a few potential vulnerabilities associated with VoLTE roaming. When combined with the rushed approach to VoLTE implementation, the security vulnerabilities can present potential pitfalls.

- **Data Mining:** Adversaries can collect subscriber details, such as device specifications, iOS versions, and IMEI
- **Illegal Tracking:** Unauthorized location tracking of users
- **Denial of Service:** Potential attacks on network IMS nodes like I-CSP and S-CSCF
- **Charging Policy Bypass:** Allowing users to evade billing structures

Towards a Secure VoLTE Future

We cannot emphasize enough the importance of prioritizing security when venturing into VoLTE. We recommend MNOs to consult **VoIP security standards** and guidelines like **GSMA FS.38**

A well-thought-out approach, with security at its core, is imperative for a seamless, secure and sustainable VoLTE roaming rollout. MNOs need concerted mitigation measures, configurations, and security controls to secure VoLTE roaming. Conducting a security audit of your VoLTE network as a preliminary step is advisable to identify potential vulnerabilities. This proactive measure will help you identify and address the weak spots with requisite protection measures. Further, the audit results will help you plan for more robust, forward-looking security solutions. Below, we have listed a few steps to help you secure VoLTE roaming.

- **Proper network segmentation** is required to prevent subscriber from accessing IMS infrastructure.
- **Encrypt VoIP traffic** to ensure that traffic is secure and cannot be read by anyone who intercepts it.
- **Deploy advanced signalling Firewalls** and proper P-CSCF configuration to protect the IMS network from attacks.
- **Keep software up to date** to prevent known vulnerabilities from being exploited.
- **Regularly monitoring and audit** the IMS network to identify potential vulnerabilities that need to be addressed.