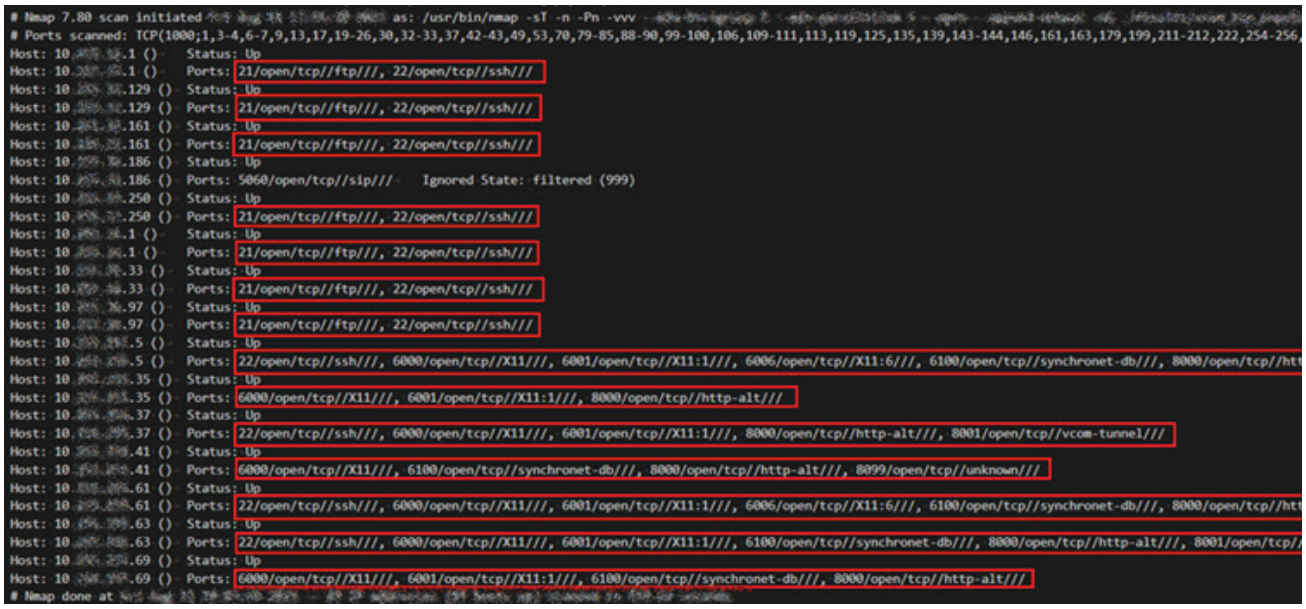
SecurityGen
Telecom Security. Transcending Generations.

What's Wrong With Fast VoLTE Deployments?

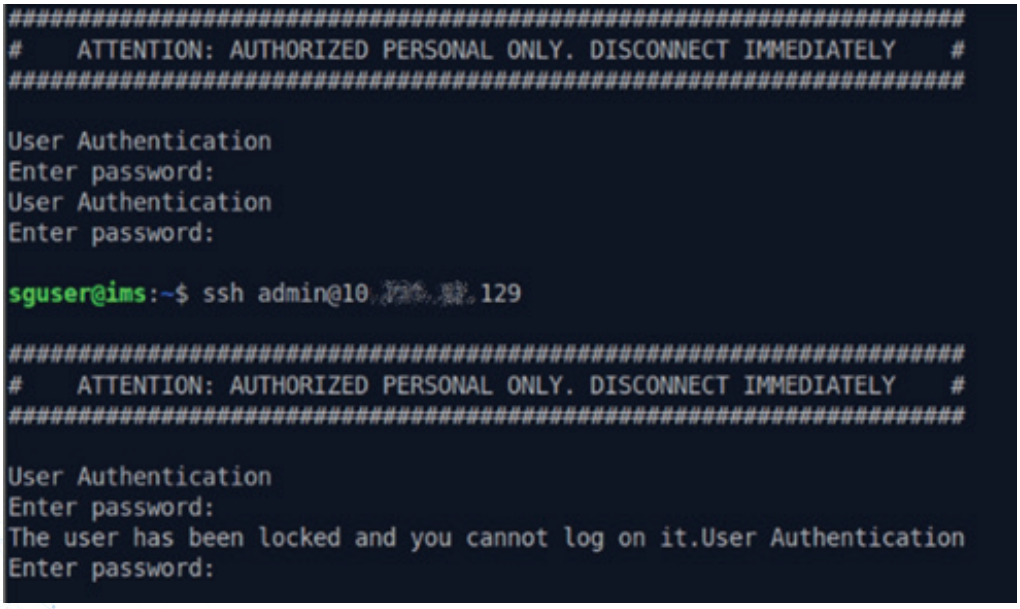
We have already published the conditions of VoLTE deployment **(Volte roaming and the security implications)** in many Mobile Network Operators (MNOs) around the world. Now, we will showcase examples of potentially risky misconfigurations.

Due to the legacy of mobile networks, operators often assume their infrastructure is isolated from subscribers, the internet, and the broader external environment – the wild world. Consequently, they may neglect proper segmentation, firewalls, and Access Control Lists (ACLs). This is because their traditional infrastructure is typically hidden away from prying eyes, leading them to deploy VoLTE infrastructure in a manner similar to other telecom subsystems.

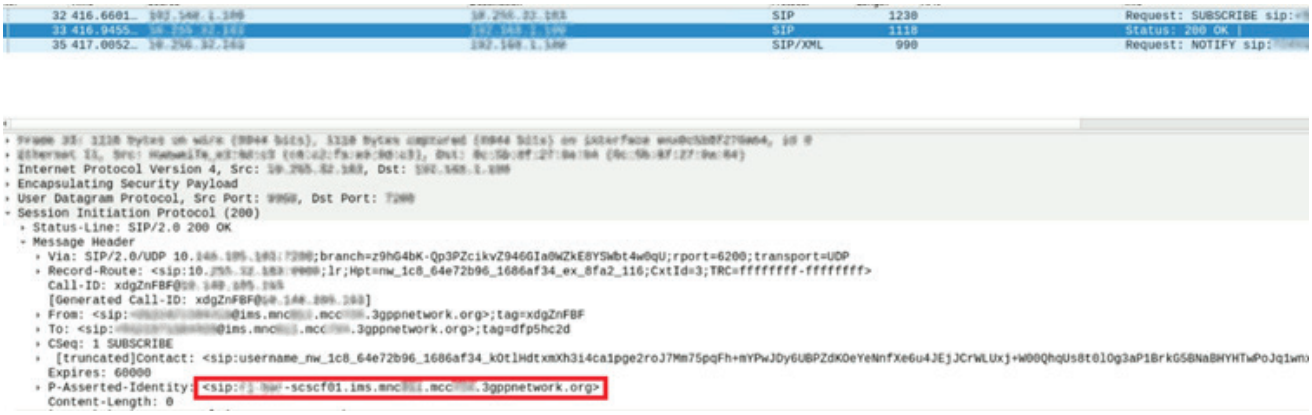
However, operators fail to consider that VoLTE infrastructure is accessible to subscribers just like any other IT infrastructure. Through various VoLTE Security Assessments, we have observed a common scenario where **management interfaces and unnecessary services are exposed/accessible to regular subscribers of VoLTE networks.**



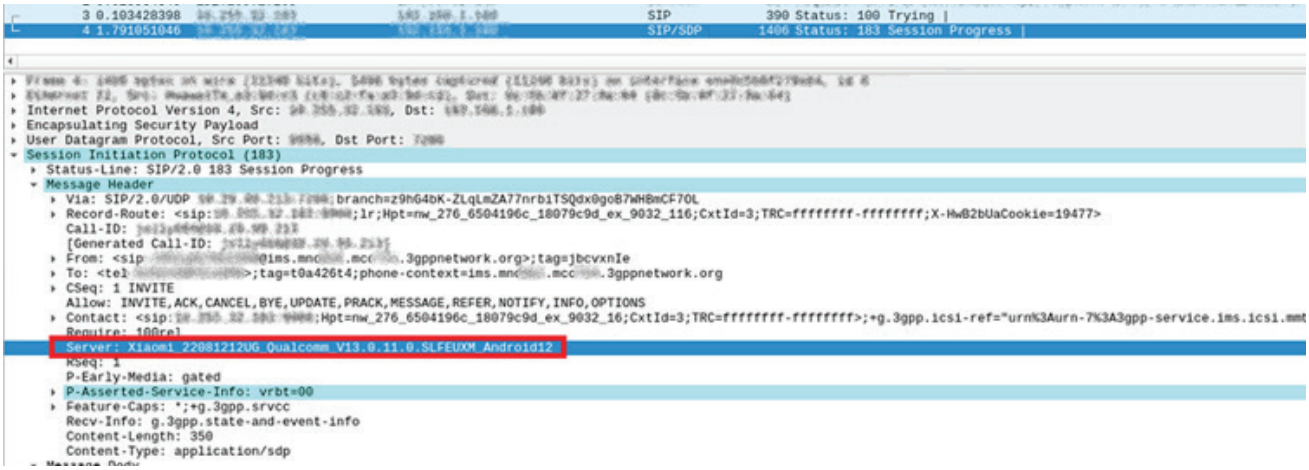
As a telecom security company, we have conducted scans of VoLTE infrastructure, revealing **numerous nodes with open SSH, FTP, X11, and web-management interfaces, all accessible to regular subscribers.**



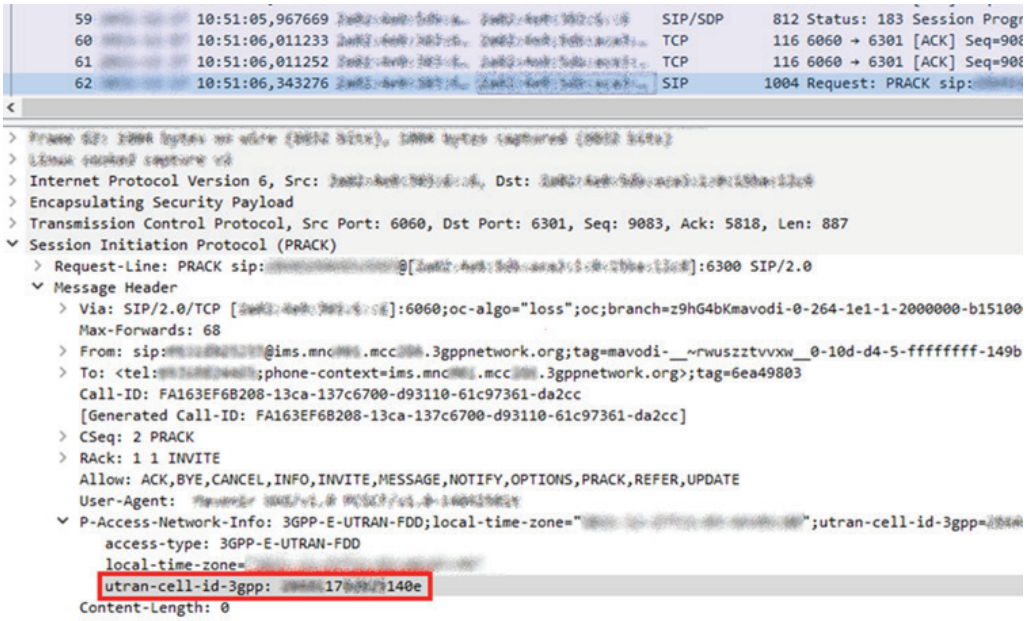
This improper segmentation of the VoLTE network is immediately apparent, but delving deeper reveals issues such **as improper P-CSCF configuration and a lack of encryption.** Consequently, subscribers may be able to view the identities of internal nodes during the registration process.



It's not just the internal infrastructure that's at risk; **there's also the potential exposure of other subscribers' information.** For instance, during a call, it's possible to obtain details such as the calling subscriber's phone model and even their firmware version.



Additionally, the location of the calling subscriber using Cell-ID information.



This list of significant issues doesn't demand a sophisticated hacker; one can acquire this information by simply conducting a **basic nmap-scan and passively analyzing the flow of packets from the subscriber's side.**

In conclusion, the prevailing mindset among many Mobile Network Operators (MNOs) remains rooted in the belief of isolation. This perspective contributes to the persistence of elementary IT-related security issues within VoLTE networks.