6.0 Global Title Abuse and Interconnect

Signalling systems, such as Signalling System #7 (SS7), are required in some mobile networks to route calls, establish location and access account information and are an evolution of the signalling systems designed for older fixed networks but augmented to facilitate mobility and roaming. Traditionally, the interconnect traffic between mobile operators relied on these underlying signalling protocols for effective operation and utilised an inherent trust model that assumed that only those entities that needed signalling access actually had it. For many years, this trust assumption has not been correct, and operators recognise that attacks can come through their signalling network and their connections to other operators and partners.

The ecosystem[38] supporting the provision of roaming and interconnect services is large, diverse and has complex interactions. Compromised interconnect services have the potential to expose customer data, user data traffic and the intermediaries associated with interconnection and roaming services[39]. The actors involved range from MNOs and MVNOs to transit carriers, GRX/IPX providers, firewall management providers, roaming hubs, roaming Value Add Service providers and messaging aggregators.

In accordance with the recommendations of the International Telecommunications Union (ITU), national numbering plan administrators are responsible for managing their national telecommunications numbering plans. For mobile network signalling purposes, a portion of mobile numbering resources is assigned to a single, unique Global Title (GT) that can then be used for routing signalling messages on telecommunications networks. The practice of leasing GTs (by a "GT lessor" to a "GT lessee") has enabled additional entities (GT lessees) to gain access to the global SS7 network and to exchange signalling messages using GTs associated with the GT lessor. This reduces routing transparency and has led to concerns that such GT leasing practices can introduce security risks for MNOs and their customers.

During the past year, there have been several reports of GT leasing attacks[40]. It was identified that[41] Fink Telecom was linked to over 100 GTs used to undertake a range of attacks and data compromises, such as those in south east Asia and Israel where the systems were used to take over Telegram messaging accounts and other accounts by redirecting SMS traffic.

[38] More fully described in the earlier Attacks on Operators section
[39] https://citizenlab.ca/2023/10/finding-you-teleco-vulnerabilities-for-location-disclosure/
[40] Finding You: The Network Effect of Telecommunications Vulnerabilities for Location Disclosure - The Citizen Lab
[41] https://www.lighthousereports.com/investigation/ghost-in-the-network/

Analysis

The broader signalling and interconnect security topics (including examples of GT abuse), discussed in the previous edition of the GSMA security landscape report[42], remain very important. Abuse of GTs can also result in the generation of fraudulent artificially inflated traffic (AIT) and the interception of messages used as part of two factor authentication (2FA) to access online accounts. Rather than directly targeting network infrastructure, these attacks can focus on security weaknesses that can compromise end-user privacy.

As part of their efforts to close off routes for attack, GSMA members have developed a GSMA GT Leasing Code of Conduct[43] that describes expected practices from GT lessors. The code is accompanied by explanatory materials to aid understanding[44]. GT lessors and transit carriers involved in GT leasing arrangements are encouraged to voluntarily declare to their partners that they adhere to the GT Leasing Code of Conduct, as evidence of their commitment to routing transparency and to reduce the risks for MNOs and their customers. Operators and carriers that do not lease GTs are also encouraged to publicly declare their support for the Code of Conduct and request compliance by their suppliers and partners (including certain sub-leasing scenarios that are explicitly expected to be prohibited).

[42] GSMA | GSMA Mobile Telecommunications Security Landscape 2023 - Security, pp 23-24
[43] https://www.gsma.com/newsroom/wp-content/uploads//FS.52-v1.0.pdf
[44] GSMA | GSMA Global Title Leasing Code of Conduct - Security