SecurityGen
Telecom Security. Transcending Generations.

DoS (Denial-of-Service): A Rising Concern For Telcos

The very nature of the Telecom industry, where critical infrastructure is used to store and transmit sizeable sensitive data, makes it a soft target for cyberattacks. Additionally, with the adoption of 5G and the rising integration of technologies, interoperability and virtualisation security has become even more challenging and complex for the MNOs.

We have seen how hackers have been taking advantage of this complex telco landscape and executing advanced attacks recently. And marking the first cyberattack of the year, 2022 came the news of Vodafone Portugal just a few days back. As per initial industry reports, Vodafone Portugal was hit by a "deliberate and malicious" cyberattack on Feb 7, 2022. The attack suspended 4G and 5G networks for customers and digital TV and SMS services.

This brings to light how the telecommunications industry faces an increased threat of DoS attacks, which was highlighted in a recent study by Cloudflare in the latter half of 2021. With DoS becoming a preferred network attack technique, let's look at how a bad actor can execute DoS attacks on the telecom network.

DoS attacks on SS7 networks, which may affect 2G/3G networks:

- **MSRN (Mobile Station Roaming Number) pool exhausting:** During this attack, an intruder needs to send many messages 'ProvideRoamingNumber' to allocate all MSRN pool numbers. As soon as the intruder assigns all the MSRN numbers, no incoming voice calls are available for the subscribers registered on the attacked mobile switch. In this case, the network gets restored immediately once the attacker stops sending 'ProvideRoamingNumber' messages.

- **Subscriber registration storm:** The network denial-of-service attack can also be executed via the MAP Reset signalling message. In such a scenario, the message informs a visited subscriber databasem – VLR – node that a home subscriber database – HLR – for one or a set of subscribers was restarted for some reason. And all the subscribers from that HLR need to update their location information initiating new registration procedures. If the intruder spoofs an HLR with many subscribers, the simultaneous registrations of all of them can lead to a signalling storm from the affected VLR to the affected HLR, overloading the equipment CPUs and signalling channels on all involved interfaces. This resulting storm can impact a significant network segment.

- **Illegitimate subsystem prohibition:** Another type of SS7 attack is connected with the routing protocol SCCP, more precisely with the node management mechanism on the SCCP layer – SCCPMG. A network element can inform the network environment that a particular subsystem has witnessed a failure. After receiving such instruction, a network element should stop communicating with the indicated subsystem until the system is fully restored. The SCCPMG protocol messages should be working within the dedicated network segment only. However, if the configuration errors allow the network to receive this kind of message routed globally, the intruders can send fake information about network element failures. Thus, prohibiting the network environment from communicating between essential functions.

DoS attacks that could affect 4G and 5G:

- **Subscriber DoS via S6a CLR to random IMSI numbers:** During this attack, the malefactor sends S6a Cancel Location Requests to all target MNO's MME nodes. Each request targets random IMSI in the operator's range to affect as many different subscribers as possible. Once MME receives such a message, the

subscriber's UE is disconnected from the 4G network. Usually, this also affects internet connection; even in cases, 3G may still be available. The period during which services remain suspended depends on the Network and UE in question. For example, some phones may start reconnecting in a matter of seconds and thus, not get impacted by the attacks, while the 4G modems may continue to be disconnected until a restart or a relatively long time (ranging from 30 mins to an hour). Restarting UE usually helps to reconnect the network and fix internet access.

- **Network Equipment DoS via S6a CLR:** This attack is similar to the previous one, but each S6a CLRs contains flags to reconnect immediately instead. As a result, all targeted subscribers will disconnect and reconnect again. This reconnection traffic may cause a signalling storm which, in turn, may lead to Denial of Service for Evolved Packet Core nodes (MME and HSS specifically).

- **Network Equipment DoS via S6a RSR:** This attack also aims to create a signalling storm. Here the idea is to send S6a Reset requests towards all operators' MME. These messages are targeted using IMSI prefixes instead of full IMSIs. S6a RSRs indicate that HSS was restarted, and target subscribers may need to reconnect. As a result, it is possible to target all MNO subscribers using only a handful of requests – one to each MNO's MME. While, theoretically, all affected subscribers should reconnect, generating much internal signalling, we are yet to see this effect in practice. Even though this attack looks unfeasible, it is still reported in FS.19.

- **Removal or alteration subscriber information in HSS:** A vendor-specific attack. FS.19 mentions that some nodes parse all incoming Diameter requests without checking for any constraints on which Diameter AVPs may be present in which requests. As a result, it may be possible to create an S6a Update-Location Request (S6a ULR) that includes additional S6a Insert Subscriber Data Request (S6a IDR) AVPs or even AVPs from messages of other interfaces that HSS will parse. This may lead to alteration of subscriber's data in the HSS. So, each malformed S6a ULR sent from the external Network by malefactor using a random IMSI may lead to breaking one subscriber configuration within the HSS. The attack continues while such S6a ULR are coming towards the Network, as, even in case of proper backups of subscriber database being restored, new subscribers continue to get affected.

- **Internal nodes start a Diameter DoS attack by sending a high volume of packets:** Here, the internal malefactor reconfigures the nodes to generate high volumes of signalling traffic, e.g. by installing additional software. The result may be signalling storm or DDoS of a single Evolved Packet Core entity, e.g. HSS.

- **Internal malefactor starting a Diameter DoS attack by sending a high volume of malformed packets targeting Vendor-specific issues:** During our assessments, we often found that internal malefactor can discover a specific malformed packet that can affect EPC node ability to handle incoming signalling. For example, we were able to find a packet that, when sent repeatedly, led to the restart of the MME node of a particular vendor. If the malefactor keeps sending such packets, the node keeps rebooting, resulting in a network element DoS attack.

- Attacks to the 5G Core elements using rogue Network Elements and abusing SBI interface messages created to allow flexible and resilient networks.

- Attacks to the Virtual Infrastructure, which is the norm for modern 4G and 5G networks and, depending on the Security Posture and policies, may take much time to recover.

Security practices to prevent DoS attacks

- Monitor your environment, especially the assets that deliver customer service. Segregate these assets from the remaining infrastructure, including the authentication systems.

- Virtualisation and dynamic networks make this task hard on any SOC; Mobile Operators should ensure that security must follow the same approach while going for a hyperscale approach and automation on Network.

- Ensure MFA, logging and close automatic monitoring for any access to telecom assets. It's crucial to avoid compromise through the same methods used against companies worldwide.

- Implement NG Firewall to block malicious messages coming from the IPX network.

- Perform regular signalling security assessments to see if there are new ways to bypass current protection measures.

Apart from our comprehensive Telecom Security Assessments, we also provide Next-Generation Firewalls and IDS for Signalling protocols SS7, Diameter and GTP. Given the modern complex network systems, we recently launched our SecurityGen Breach and Attack Simulation Platform. This innovative AI-enabled platform provides network owners with an automated system that can continuously perform network assessments and provide remediation guidance to address existing threats in the network according to priority. Thus, ensuing proactive security coverage and strengthening the security posture of network owners.

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 | India | South Korea | Japan | Malaysia | UAE