SecurityGen

Telecom Security. Transcending Generations.

Edition 2, Oct 2022

Some of the security practices to protect your 5G assets

Our earlier edition listed the issues and possible threat vectors to watch while rolling out the 5G networks. And as promised, in this latest edition, we have explained some of the security practices and protocols you can follow to protect against the threat vectors within the 5G ecosystem.

Again, these guidelines are a direct consolidation of the outcomes of our 5G project deployments for MNO customers.
Let's start!

www.secgen.com

I. Business and organisational challenges

Last time we raised the issue of the **False assumptions and the Security paradox along with the numerous theoretical Best practices & guidelines** for 5G security – well, as this involves human elements and perceptions, there can be no straightforward technical solution or guidance. Having said this, it's essential to understand that 5G doesn't come with complete in-built security. There are several areas where you require security expertise specific to telecoms. What we have done here is listed a few approaches that we think could be helpful - as this is what we saw and absorbed while working on projects with our MNO partners over the past 8-9 months.

- **The first step** is understanding your business objectives, as security cannot operate in isolation and must align with the overall organizational goal.

- **Second,** it is essential to communicate and establish with the board and the management (if possible) how cybersecurity is an enabler to business; you can try organizing a cyber-security masterclass for business and leadership.

- **Third,** highlight the importance of understanding and ensuring the security of telecom network assets together with the enterprise IT segment. You can organize a cyber-drill simulating attacks targeting not only enterprise/IT infrastructure but also telecom/core network assets.

- **Remember that strategy without tactics** is the slowest route to victory, and tactics without strategy are the noise before defeat – so don't scare the business with giant strategic plans=cost or tactical turmoil of action items. It would be effective to propose strategic objectives to manage cyber-risks and specific steps for quick wins, demonstrating that you are on the right path.

Additionally, as the 5G networks are still developing across many countries, the information security team can get involved in the development process to ensure that security is well thought-through in the 5G setups. This approach will help break the traditional patch-up and reactive security outlook and offer significant competitive advantages.

II. Technical consideration

2.1 SBA - Threats and security deficiencies original to 5G setup

With 5G security features designed to address the gaps and weak spots in the architecture of previous-generation networks, it has new protection mechanisms based on the following principles:

- **Mutual authentication**
  The sender and recipient must each verify and authenticate each other.
- **Zero-trust model**
  No network component assumes trust in another element, whether inside or outside the MNO.
- **Use of encryption on the transport-level connections**
  To prevent eavesdropping and modification of transmitted data between the endpoints.

Despite the introduction of new security principles in 5G, any new vulnerability like those in SBA is difficult to comprehend and devise an approach plan. We would like to propose some ideas that we tried ourselves and resulted in some interesting outcomes.

- **Get access to the 5G lab created by major vendors as part of solution testing**
  If this is possible, you can potentially assess a smaller twin of future production deployment, which means – information collected about vulnerabilities and configurational deficiencies can be used to overcome similar mistakes during production deployment.

- **Get access to pre-production 5G infrastructure or its pieces**
  As it is quite before the acceptance – so you have time to validate if minimum security controls are in place and ask for remediation in case any issues are identified. In this case, there is a good chance to offload the remediation task to the integrator in charge of deployment or the vendor supplying the solution.

- **If none of the above is an option – why not create your own 5G cyber-lab?**
  It's more than doable nowadays. Many open-source projects are being used as Lego bricks to help you create small but fully operational 5G core networks with SDR-based radio, data and voice services etc. Though this approach would not help to identify vendor-specific vulnerabilities, it will still help to study architectural deficiencies and possible misconfigurations – with this knowledge; you have a better chance to put it right while being ready or in production.

2.2 New and old threats brought to 5G by reused technologies and backward compatibilities

IMS reused in 5G for VoNR

At least here is a straightforward and relatively easy way to resolve it, so here is the exact To Do list for IMS security controls. Since most of the detected threats require that an attacker knows the unique identifiers (a subscriber's IMPI and network element addresses), the most crucial measure is to counteract attacks aimed at obtaining such identifiers.

1)	Using IPsec and TLS with SIP at the Access Layer is necessary. The encryption of SIP signalling helps prevent attacks as the encryption tunnel has to be established before the attack can occur. SIP over IPsec / TLS is a significant security improvement over unencrypted SIP but should be seen as one layer of multiple defences and not relied upon as a single defence.
2)	Filter specific SIP methods if possible (e.g. SIP OPTIONS). If specific SIP methods are not used by the service the network offers, and if these are received, you should strictly not respond to these.
3)	To reduce the likelihood of **denial of service**, you need to implement the interconnect SBC. Consideration must be given to how the I-SBC is protected against DoS attacks that use malformed or suspicious SIP messages. The SBC must be rigorously tested against such messages.

4)	Enable a topology hiding mechanism to reduce the likelihood of **subscriber and network information disclosure.** • SIP requests and responses from the network can be analysed using SIP fingerprinting and used to identify the individual nodes (the manufacturers and sometimes the model and software version) used within the network and, depending on configuration, the actual service provider using the node(s). • Removing specific SIP headers and fields from requests and responses sent towards SIP endpoints on interconnect, network SIP fingerprinting can be made harder for the attacker.
5)	To mitigate fraud risks and subscriber traffic redirection, implement SBC and SIP signalling firewalls.

Apart from the primary defences provided by the I-SBC, several **secondary defences** should also be implemented. These defences must be implemented in case any attack bypasses the defences on the I-SBC.

- It is ideal for defining your security mechanism with the assumption that a malformed or suspicious message will bypass the I-SBC. As such, the core network nodes (e.g. in an IMS network, the I-CSCF, S-CSCF, AS(s), MRFC, MGCF) should be tested to check their capability to withstand such messages.

- SBCs form a vital part of the defence-in-depth layering model, and SBCs protecting core networks provide precious security and often other key functionality such as session management. But we need to be more sophisticated in the approach to signalling security and adopt an in-depth defence approach in which the SBC, while playing an important part, is one of the several defences.

- Monitoring and forensics should be in place to capture and analyse SIP traffic from the attack; this will help improve and enhance future defences. Both the private and public SIP interfaces should be monitored.

SIM and its management – STK vulnerabilities

GSMA has already distributed multiple recommendations for mobile operators, and mobile operators are strongly encouraged to follow these recommendations.

1)	As per GSMA and the SIMalliance, it is critical to analyse and block suspicious messages containing STK commands. This requires that all SMS sent within the mobile network are filtered. It is crucial to ensure that false positives are not introduced and that all the various ingress and egress messaging flows are inspected, including those paths and flows previously thought to be secured or inaccessible.
2)	A regular security assessment is crucial for verifying the effectiveness of security measures. Assessment should be performed quarterly and upon implementation of new equipment or reconfiguration of existing devices whenever such changes have the potential to affect network security.
3)	It is advisable to filter binary SMSs between subscriber and subscriber.
4)	Network equipment vendors provide different types of filtering capability depending on the equipment, vendor and software version. We recommend using a complex approach based on three levels of SMS header and SMS payload filtering that can help to detect or prevent OTA attacks on UICCs. 1. User Data Header (UDH) Filtering 2. UDH + Protocol Identifier (PID) and Data Coding Scheme Filtering 3. UDH + PID/DCS + Payload Filtering

III. General recommendations

Apart from the above ideas and guidance specific to a particular security issue and vulnerability, we think it is imperative to infuse security as a foundational and overarching element in the planning phase. With this in mind, adopting a holistic **IDP (Inspection, Detection, Protection)** based approach to securing networks is helpful.

- **Inspection**
  Security inspection provides the essential visibility to understand the threat landscape of your ever-changing network environment and control actual security posture.

- **Detection**
  Continual real-time monitoring is essential to measure network security efficiency and provide rapid detection of attack and proper response and remediation.

- **Protection**
  Completely secure your network by addressing both generic vulnerabilities and the threats that affect you as an ongoing process.

About SecurityGen

SecurityGen is a global company focused on 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 | Mexico
India | South Korea | Japan | Malaysia | UAE