SecurityGen
Telecom Security. Transcending Generations.

MITIGATING RISKS IN TELECOM SUPPLY CHAIN SECURITY – A LONG OVERDUE DISCUSSION

Traditional telecom security solutions redundant

As telecom networks get more sophisticated, digital access and new technologies (5G) emerge, and cyberattacks continue to increase and evolve, posing a threat to telecommunications. Acknowledging this threat is the first step in your efforts to neutralizing it. Identifying, evaluating and managing the overall security posture of telecom supply chains must be an imperative goal not only for security teams, but also for the engineering and operation teams who work together to make seamless mobile communications possible.

Today, however, ensuring telecom supply chain security is becoming more and more challenging. Those who have worked long enough in the telecom engineering space will understand the many reasons why a traditional IT approach to security does not offer enough protection to telecom. Among the many important reasons, some "telecom truths" perdured for years, like the following:

- Traditional IT tools work with standard apps that cannot assess new and evolving risks
- Many functions are isolated from internet access (as if this covered all risks)
- Mobile networks are not data centers – they have their own vulnerabilities
- The general public is unaware of critical telecom security protocols and standards

Most of the above claims did not age well. You still need specialized tools and knowledge to assess Telecom security but with the convergence of Telecom and IT technologies, network devices that used to run on proprietary hardware with limited external connectivity have become a set of virtual machines connected by a collection of message buses that extend across countries. Roaming interconnectivity also connects these core elements to other mobile network operators (MNOs) with equivalent risks. In this scenario, an exposure of assets could result from a single badly typed command or a "temporary configuration" which later becomes part of the network and cannot be touched anymore.

Telecom Supply Chain Regulations

The Cybersecurity & Infrastructure Security Agency (CISA) is a branch of the U.S. government that is focused on improving cybersecurity for the nation's critical infrastructure, which includes telecom, utilities, public health, and logistics. According to CISA, ICT supply chain risks must be evaluated and measured keeping in mind not just the hardware and software but also the services managed by third-party vendors.

This means that telecom companies who play the role of both critical infrastructure owners and service providers must, as part of their safety protocols, actively assess the security of their mobile networks and provide reasonable information and assurance of security standards to their customers.

Similarly, the European Union Agency for Cybersecurity (ENISA) regularly develops and updates its regulations and standards for 5G security. Its stringent risk management guidelines list telecom supply chains as part of critical infrastructure for European countries.

EU ENISA Progress

2019	2020	2021	1H/2022	2H/2022+
• **Threat focus** • **Risk Identification**	• **Threat Focus** • **Risk Management**	• **Guideline** • **Standards** • **Certification Compatability**	• **Risk Management Compatability** • **Standards** • **Virtualization (NVF)** • **ICT Products**	• **Cloud Details** • **Operating Networks** • **Threat intelligence sharing**
ENISA threat landscape for 5G Networks	Update of ENISA threat landscape for 5G Networks Cybersecurity of 5G networks EU Toolbox of risk migrating measures	Guideline on Security Measures under the EECC 5G Supplement Security in 5G Specifications - Controls in 5GPP Methodology of Sectoral Cybersecurity Assessments	Interoperable EU RISK Management Frame-work NVF Security in 5G 5G Cyber Security Standards Risk Management Standards EU ICT Products Common Criteria (draft)	EU Cloud Services (ongoing) EU 5G Networks (ongoing) EU 5G Threat Intelligence Sharing (ongoing)

Apart from the US and European Union, numerous other countries and regions have also created regulations and best practices – influenced by CISA and ENISA - to ensure the highest levels of security for telecom supply chains.

Service Providers in Telecom

While recent supply chain attacks such as Solarwinds, Okta, Log4J gained notoriety within the global cyber-security community after they affected a wide range of ICT Companies, telecom-specific security incidents are not publicized much or investigated.

LightBasin, which we addressed earlier in our article, has already proved the point that roaming interconnection is not as safe as earlier believed. This cluster was able to emulate telecommunication protocols and used packet-capture and scanning tools to gather information by traversing roaming IPX interconnections and taking advantage of the weakest link (equipment at one of the victim's MNOs).

This is why it is becoming increasingly important to take a moment to compare telecom cybersecurity practices with those used in the traditional IT space. While an initial assessment of security policies, frameworks, and safety regulations followed by leading MNO groups will reveal that they are as strong and binding as any other top ICT companies, this may not always be true. There are alarming security vulnerabilities that could prove damaging to the entire system.

To understand the risks better let us examine a recent example of a security breach disclosed by Vodafone. This leading MNO embraced the NIST framework for risk management and cyber-security and included the supply chain as an exposure source to be placed on RM. When Vodafone's recently annual report was published, it contained relevant information on security as part of a very structured way to assess the binding laws and regulations for every market and its impacts on business and actions performed. The document also disclosed information on cyber-attacks, including a relevant third-party supplier attack that the company was made aware of.

On the other hand, a disclosure from the supplier revealed that the attacker had access to information about subscribers using roaming for years before being discovered. Worst of all, due to the associated service being related to roaming, attacker had access to MSISDN and IMSI lists of traveling subscribers. The group's figures are impressive – with 9,000 suppliers and 71 assessments of the supply chain, why is this incident relevant?

Here are a few points to consider:

- MSISDN and IMSI lists are personal data and although they cannot automatically be connected to individuals, they may enable attacks to their privacy
- Traveling subscribers are usually good value subscribers and the list includes government and blue-chip customers
- Vodafone reports the impacts for their subscribers was minimum, but we must consider that other MNOs were affected and total amount of exfiltrated data is not disclosed by the supplier
- Once again, the complexity of the roaming interconnection impacts on security.

Recommendations for MNOs

So, what then can be done to strengthen telecom supply chain security? While limiting services in a highly competitive market is not the answer, neither is reinventing something that took decades to standardize, stabilize and monetize. One option would be to implement stringent security measures on the launch of new roaming services such as:

- VoLTE and Vo5G roaming, rushed by the unplugging of 2G and 3G in some countries
- 5G roaming

As far as ensuring security for networks with legacy protocols, SecurityGen always recommends following the Inspect-Protect-Detect described on the NIST framework to ensure that your risk management is performed in a proactive manner.

An old discussion regarding limitations of filtering on service border elements (STP and DEA) always led to an argument on whether or not "if you keep your IMSI list secret, further attacks are rare". Most of us are aware that IMSI lists are available for sale on the Dark Web. In fact, for those in the telecom supply chain security business, it is now common knowledge that IMSI catchers and rogue NodeBs are built to collect subscriber information. If these developments seem far-fetched, here is another fact that might shock you:

There is strong evidence that MSISDN-IMSI lists were collected on the clearing house between MNOS, meaning that even if you don't use a specific provider, data from your subscribers may have been already collected and sold, depending on the visited network.

This information is both cause for alarm and a call for immediate remedial action. At SecurityGen, we believe that using a NextGen Firewall that identifies and eliminates new and existing threats in addition to IMSI collection is crucial for ensuring security. We must recall that security through obscurity is neither useful nor acceptable in a connected world. Your IMSIs may already have been compromised and mapped, so let's deal with the elephant in the room.

What about future roaming services?

Roaming security is about safely exposing telecom core assets to enable a seamless experience for subscribers around the globe. Today, with many 2G and 3G networks being decommissioned in the US, travelers from abroad may face an unexplainable situation. They may find that while apps and smart functions continue to work, they cannot receive regular phone calls from businesses or relatives that have not yet moved to a fully digital mode.

While technically a VoLTE/Vo5G call in roaming is clearly possible but legacy fallback was the easiest and also, the preferred way while it was available. If you are implementing IMS access from roaming, you should see it as an opportunity of validating its security beforehand.

5G roaming is a new frontier and while roaming providers and MNOs work on the details of implementation and management, there is still time to establish a safe 5G core architecture and assess the strength of its security across network functions. While the costs for later corrections are always higher and some changes would impact a whole distributed core at a single maintenance window, the smartest thing to do at this point would be to act fast.

If 5G seems far from your reality, just consider security starts at the buying process, not excluding any vendors but assuring they will propose and implement secure solutions. The days where 3GPP release compliance were enough are gone. Today, including both Telecom and IT best practices into your process have become an imperative.

References

1 https://www.cisa.gov/supply-chain
2 https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks
3 https://www.secgen.com/articles/SG_Article_LightBasin
4 https://thestack.technology/vodafone-supplier-hacked-syniverse-hack/