www.pipelinepub.com
Volume 20, Issue 1

Six 5G Security Threats to Prepare For

By: Miguel Carames

From the onset, 5G technology created high expectations, spanning from improved energy efficiency to accommodating a high density of IoT devices. Moreover, it promises to provide substantially higher data speeds and lower latencies compared to earlier generations. However, amid all these advancements, one element of 5G in particular has really stirred excitement: network slicing. This technology offers an unprecedented level of flexibility in the way we design, manage, and utilize our networks. Advances such as this, however, often carry hidden elements of risk. This article addresses both the opportunities and the risks operators should consider when offering network slicing.

Tailoring 5G Networks for Slicing

Network slicing is made possible by the introduction of 5G Standalone (5G SA), which enables the creation of virtualized, isolated logical networks, each tailored to specific needs and requirements. One of the most exciting features that network slicing enables is the ability to allocate resources dynamically and to place applications within network slices with appropriate service level requirements. For instance, a gaming platform can be offered through a low-latency, high-bandwidth slice, while a smart factory may prioritize reliability and stability over speed. This granular control over resources ensures that the network is optimized for a diverse range of concurrent applications, from augmented reality experiences to critical IoT services.

The Technical Framework Behind Network Slicing

Digging into the technical specifics of network slicing unveils a complex yet highly adaptive framework that crosses over multiple domains within Communication Service Provider (CSP) networks. These domains can encompass core, transport, edge, and radio access networks (RAN), each playing a distinct role in delivering seamless, highly customized services. To bring this level of flexibility to life, requirements must be seamlessly translated into policies across these sub-domains. This process ensures that the network is not only aware of what is required for each slice, but can also dynamically allocate resources and adapt configurations to meet changing conditions in real time.

It’s worth highlighting that transitioning to 5G SA core requires the adoption of a service-based architecture (SBA). This shift is important because it equips service providers with a framework for modularizing network functions and exposing them through standardized IT-like interfaces, making it possible to not only implement network slicing but also to develop new products through the use of Application Programming Interfaces (APIs).

Key enabling technologies, such as Network Function Virtualization (NFV), cloud-native principles, and orchestration, underpin network slicing. NFV allows for the virtualization of network functions, making it easier to deploy and scale services rapidly. Cloud-native principles enable the development of applications that are designed to run efficiently in the cloud, optimizing resource utilization and enhancing scalability. Orchestration, on the other hand, acts as the conductor of this “symphony” of technologies, coordinating the allocation of resources and ensuring that policies are consistently enforced across various network domains.

Network slicing is a significant technical leap forward, empowering CSPs to provide tailored, high-quality services to their customers, all while optimizing network resources and performance across the multiple domains that make up today's intricate telecommunications landscape. But, as with every significant technological evolution, there are new risk elements that must be accounted for.

Security Considerations for 5G Network Slicing

As we embrace the transformative capabilities of network slicing, it is crucial to address the pressing security concerns that come hand-in-hand with this technological evolution. A recent joint report from the National Security Agency (NSA), Cybersecurity and Infrastructure Security Agency (CISA), and the Office of the Director of National Intelligence (ODNI) sounded an alarm about potential threats associated with network slicing, underscoring several specific security challenges that must be carefully navigated:

- ***Denial of Service (DoS) Attacks*** are disruptive threats that can wreak havoc on network services and slice functionality, affecting both providers and end-users.
- ***Man-in-the-Middle (MitM) Attacks*** pose significant risks by potentially compromising the confidentiality and integrity of data flowing through network slices.
- ***Configuration Attacks*** present the risk of unauthorized changes to network slice settings, potentially exposing vulnerabilities and affecting the performance of connected applications.

These attacks are fueled by specific vulnerabilities and flaws within the network that can compromised. The goal is to identify and eliminate these as quickly and efficiently as possible. Six 5G vulnerabilities to watch for:

1. ***OAuth2.0 security risks.*** ”Open Authorization” is a standard designed to allow a website or application to access resources hosted by other web apps on behalf of a user. These threats are primarily token-based, particularly on the client/server side, and are already well-known to the industry, but IT and network teams still need to be on the lookout for them.
2. ***API-based weaknesses*** can create a whole host of security threats, including injection flaws. This is where an attacker can trick the ”interpreter” into executing unintended commands or accessing data without proper authorization.
3. ***JSON Web Token (JWT)-based vulnerabilities*** have a similar effect as API weaknesses. Risks include JWT tokens being stolen, along with ”fuzzing” of data in the header or payload section, token tampering, and a few other potential risk areas.
4. ***Slow read DDoS attacks*** involve an attacker sending a legitimate HTTP request to a server but then reading the response as slow as one byte at a time. This prevents the server from getting an idle connection timeout, thus holding resources unnecessarily.

5. ***HPACK bombs*** are where an attacker uses seemingly small messages that drastically expand and force the target to allocate gigabytes of memory, slowing down response times.
6. ***Stream multiplexing abuse*** is where attackers leverage flaws in how servers implement stream multiplexing to trigger denial of service attacks.

The serious nature of these threats and vulnerabilities emphasizes the importance of maintaining a secure infrastructure to successfully deliver network slicing-based solutions. Implementing robust security measures, such as encryption, authentication protocols, and continuous monitoring, becomes non-negotiable. Only through a steadfast commitment to security can we harness the immense potential of network slicing while mitigating the risks associated with these advanced network technologies.

Mitigating Risk in Network Slicing

In the constantly changing field of network security, strict policies and rules-based access controls have become indispensable safeguards against myriad threats. These measures establish clear guidelines for controlling access to network slices, regulate what resources can be utilized, and govern how data is to be transferred. While many threats and their potentional impacts are still being assessed, organizations can proactively mitigate likely vulnerabilities and unauthorized access attempts by implementing such policies.

Modern security solutions play a pivotal role in protecting slicing-enabled networks. These solutions are designed to detect and prevent a wide range of security threats, from the subtlest anomalies to the most overt breaches. With advanced threat detection algorithms and real-time monitoring capabilities, they act as vigilant gatekeepers, ensuring that network slices remain resilient and secure.

The importance of continuously monitoring, testing, and analyzing the network cannot be overstated. These practices enable organizations to identify and resolve network vulnerabilities quickly, minimizing any potential window of opportunity for bad actors. By closely monitoring network traffic, running penetration tests, and leveraging analytical tools, security teams can stay one step ahead of potential threats and maintain the integrity and reliability of network slicing environments.

Looking ahead, 5G network slicing holds immense promise. As the technology matures and security measures become more refined, we can anticipate a world where connectivity is seamlessly customized to meet the unique needs of diverse users and applications. This evolution promises to accelerate the growth of the IoT, augmented reality, and countless other innovative applications that we haven't even considered yet. In this rapidly evolving environment, with a digital landscape more versatile and interconnected than ever before, network slicing is poised to be at the forefront, shaping how we experience the power of 5G connectivity. But to fully harness its potential, a comprehensive security strategy is essential. A proactive approach combining strict policies, robust security solutions, and vigilant monitoring, is the key to safeguarding our digital future.