


Thinking like a 5G attacker

Leverage attack graphs to illuminate 5G network vulnerabilities


The protection of ever-expanding attack surfaces is a constant challenge, particularly with the adoption of 5G and edge computing technologies. Industries are being transformed through the combination of increased reliable connectivity, drastically faster speeds, and a significant reduction in network latency. In addition, the software-defined nature of 5G allows for the implementation of new paradigms such as network slicing.

Network slicing offers added flexibility around infrastructure deployment and it minimizes the need for additional hardware while strengthening cybersecurity measures. However, as companies look toward network slicing to capture the benefits of 5G technology, additional considerations should be taken to secure their respective "slices" against potential vulnerabilities.


OVERVIEW OF NETWORK SLICING




Multiple distinct slices may be created to allow unique network access for several enterprises and applications across common Radio Access Network (RAN) resources



Unique authentication is required for each individual slice to preserve data and security isolation



Proper network slice management is necessary to prevent malicious actors from accessing data from different slices

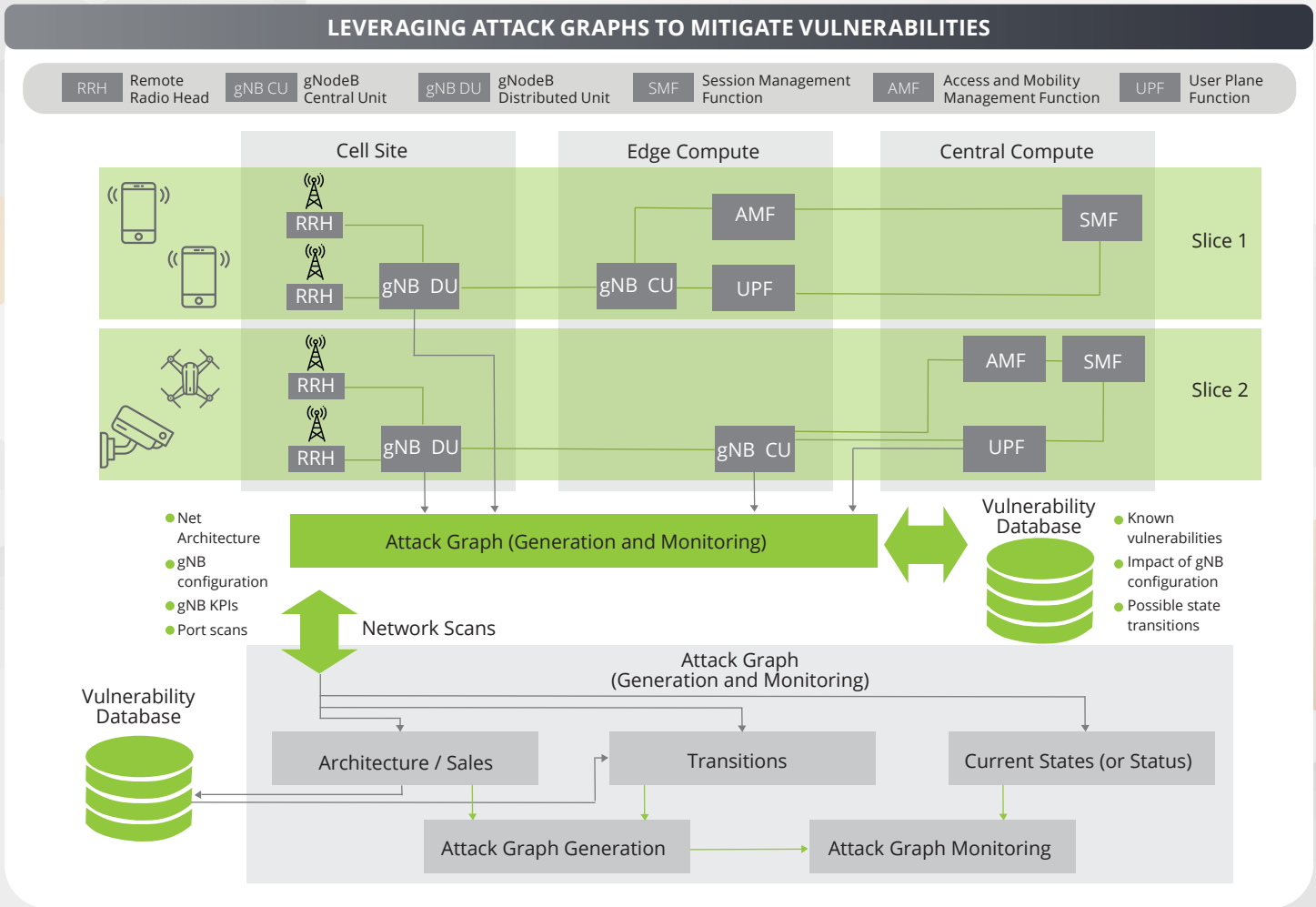


Based on deployment type (e.g., hybrid, private), slices can be used to separate individual organizations or individual applications within an organization

There are established standards that provide specifications to build 5G networks. However, specifications for the development and implementation of security for network slicing are still in development. 5G networks consist of complex, changing layers and infrastructure. Therefore, multiple tools are needed to identify vulnerabilities within the environment.

Some of the most pressing vulnerabilities in 5G network security include data leakage, network disruption (unavailability), and device spoofing. Tools like attack graphs provide a simpler way to represent the interconnection of devices within networks; capture additional metadata associated with the services, protocols, ports, and applications on each node; and "think like a 5G attacker" to explore and identify complex paths of attack.

This provides the ability to determine the current state of hosts within a network and support up-to-date analyses of network weaknesses and points of exploitation.



For over a year, Deloitte's Cyber 5G/Edge team has worked with Virginia Tech and its Commonwealth Cyber Initiative (CCI) team to provide innovative research and develop specific insights regarding 5G communications and vulnerabilities, using a specific lens of how threat actors could attack 5G networks. Ventures like these amongst the business, scientific, and academic communities help bring impactful research, results, and recommendations in emerging technologies such as 5G. This article highlights one of the specific research areas related to identifying 5G's attack graphs in rapidly-changing, vendor-specific and enterprise-specific network implementations.

5G networks are expected to serve as the communications infrastructure for mission-critical services such as emergency and natural disaster rescue, public safety, and military services. As a result, cyber attacks to these 5G networks may pose significant risk to public health/safety as well as national security risks. Additionally, 5G also has broad commercial applications (e.g., smart manufacturing, Internet of Things (IoT) deployment), so enterprises interested in rolling out 5G networks should understand the protocol's vulnerabilities and ways to secure it. While researchers have studied the "intra-layer" security of 5G networks extensively over the past several years, research regarding "inter-layer" security has not been as robust. This specific research by Deloitte and Virginia Tech focuses on "inter-layer" security by analyzing four different kinds of attacks (denial of service– DoS/distributed denial of service – DDoS; eavesdropping; data exfiltration; malware deployment) and creating attack graphs to illustrate challenges and vulnerabilities between 5G network layers and identify the paths an adversary may take to do the most damage to a 5G network.

The attack graphs show how an attack on one 5G network slice could affect another 5G network slice, given that 5G network slices share some of the same infrastructure. For example, with slicing, user data traffic of slice 1 may be carried through a virtual user plane function 1 (UPF1) while UPF2 traffic carries separate traffic from slice 2.

DENIAL OF SERVICE USE CASE THREAT VECTORS SUMMARY

Policy Updates

For this use case, two threat vectors were considered: (1) the air interface of the RAN, and (2) the shared edge compute resources supporting RAN as well as the Core and mobile edge compute (MEC) functions.

	Air Interface of the RAN	Shared Edge Compute Resources
Attack origination	<ul style="list-style-type: none"><li>Malware is deployed on vulnerable Internet of Things (IoT) devices in Slice 2</li><li>Compromised devices jam or flood the air interface</li></ul>	<ul style="list-style-type: none"><li>A malicious MEC application is instantiated on Slice 2 (e.g., a graphics processing application for security cameras is infected with malware)</li><li>Malware is leveraged to circumvent compute resource segmentation policy</li></ul>
Implications	<ul style="list-style-type: none"><li>Services in Slice 1 are denied or, at a minimum, degraded because Slice 1 shares physical resources (e.g., RF spectrum) with Slice 2</li></ul>	<ul style="list-style-type: none"><li>Edge compute resources are monopolized by generating "fake" computationally intensive processing tasks</li><li>RAN and Core functions are degraded in Slice 1 because Slice 1 and Slice 2 share edge compute resources</li></ul>

KEY NEXT STEPS FOR HOW TO LEVERAGE ATTACK GRAPHS

Because 5G networks consist of complex, changing layers and infrastructure, multiple tools are needed to identify vulnerabilities in this environment.

As companies look forward to network slicing as a way to harness 5G connectivity/speed, this research reveals additional steps companies should consider when securing their slices through means such as network segmentation, access controls, and security assessments.

1

DO NOW:

- Assess the level of visibility for devices on the network
- Characterize the attack surface in the network across both devices and network slices
- Determine location of crown jewels in all network slices

2

DO NEXT:

- Identify ingress and egress points for crown jewels and build a threat model
- Define an appropriate governance model, security policies, and detection mechanisms for crown jewels

3

DO LATER:

- Automate monitoring of attack vectors to drive proactive detection and response
- Drive security enhancement initiatives to protect critical databases and equipment in alignment with security controls and industry standards such as 3GPP and NIST

Contact us:



Wendy Frank  
Principal  
Deloitte & Touche LLP  
wfrank@deloitte.com



Abdul Rahman, Ph.D.  
Associate Vice President  
Deloitte & Touche LLP  
abdulrahman@deloitte.com



Shehadi Dayekh, Ph.D.  
Specialist Leader  
Deloitte & Touche LLP  
sdayekh@deloitte.com



James Lee  
Senior Manager  
Deloitte & Touche LLP  
jjlee@deloitte.com