ONELAYER

Enterprise Grade Security for Private LTE/5G

Private Mobile Networks: The New Enterprise Security Battleground

How IoT is driving cellular and enterprise network convergence and creating new risks and attack vectors

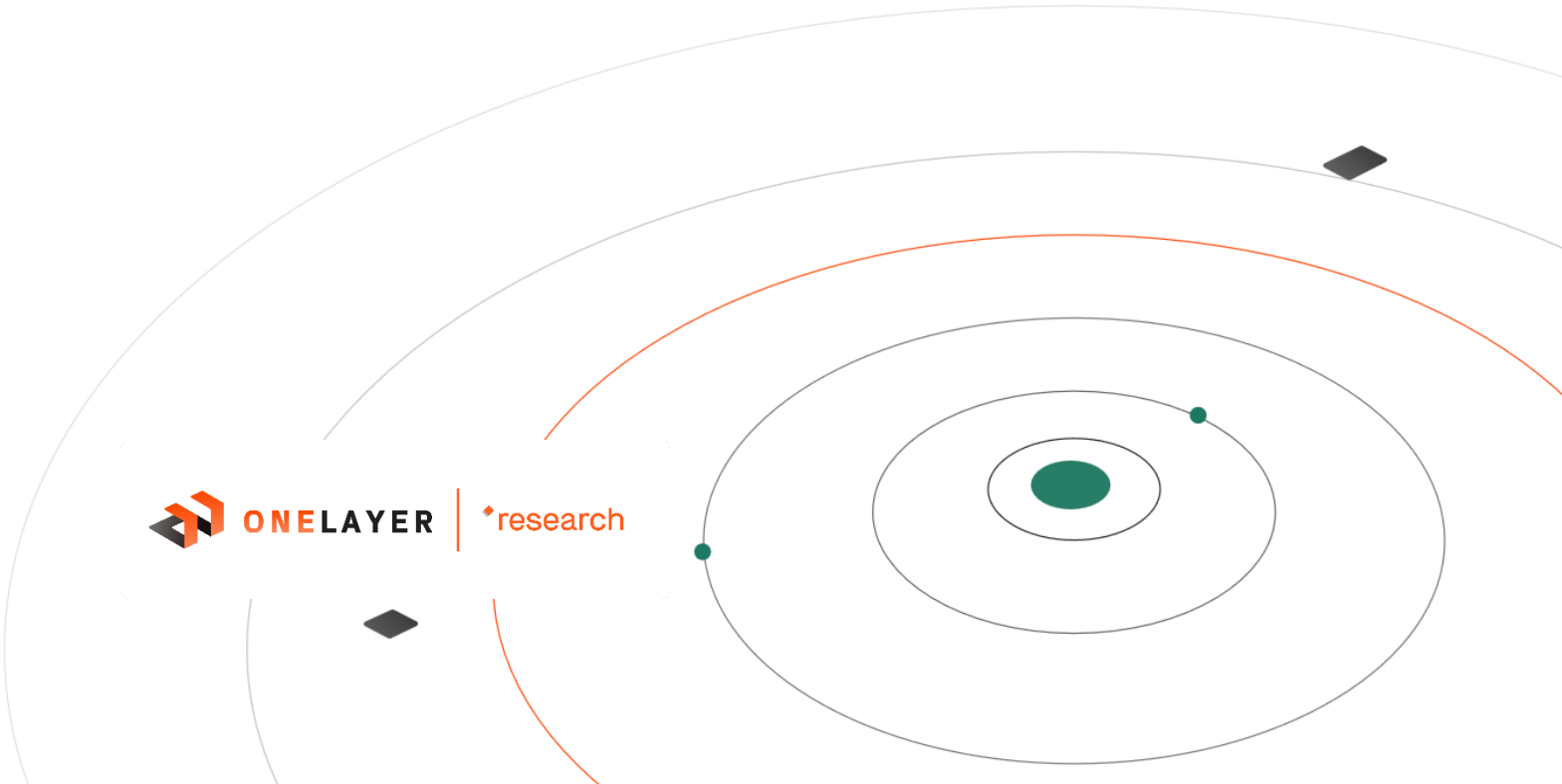


Table of Contents

Abstract

Historically, cellular networks have been operated by a relatively small number of organizations. Most are major telecommunications providers delivering general-purpose mobile communications services. More recently, however, emerging technologies like Internet of Things (IoT) devices and 5G cellular networks make it increasingly attractive for enterprises to design and deploy private cellular networks to enable new business innovations and overcome the limitations of traditional enterprise wireless networks.

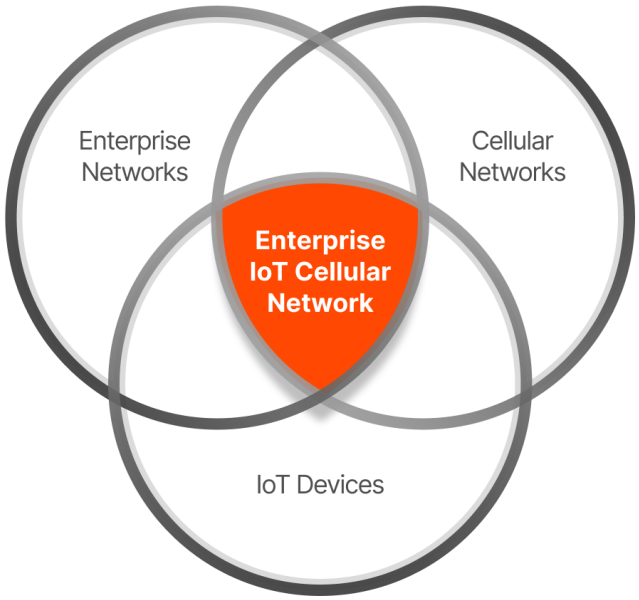
This paper is intended to help security executives understand the unique security risks that private cellular networks present and develop strategies for extending existing enterprise security tools and practices into these highly unique environments.

Convergence is Creating New Opportunities – and New Risks

IoT is Driving Cellular and Enterprise Network Convergence

Accelerating adoption of IoT devices is driving a convergence between cellular and enterprise networks. As enterprises pursue new applications of IoT devices, they often encounter limitations with traditional enterprise wireless networks and public mobile network operator (MNO) network capabilities. This is leading many enterprises to implement their own private cellular networks.

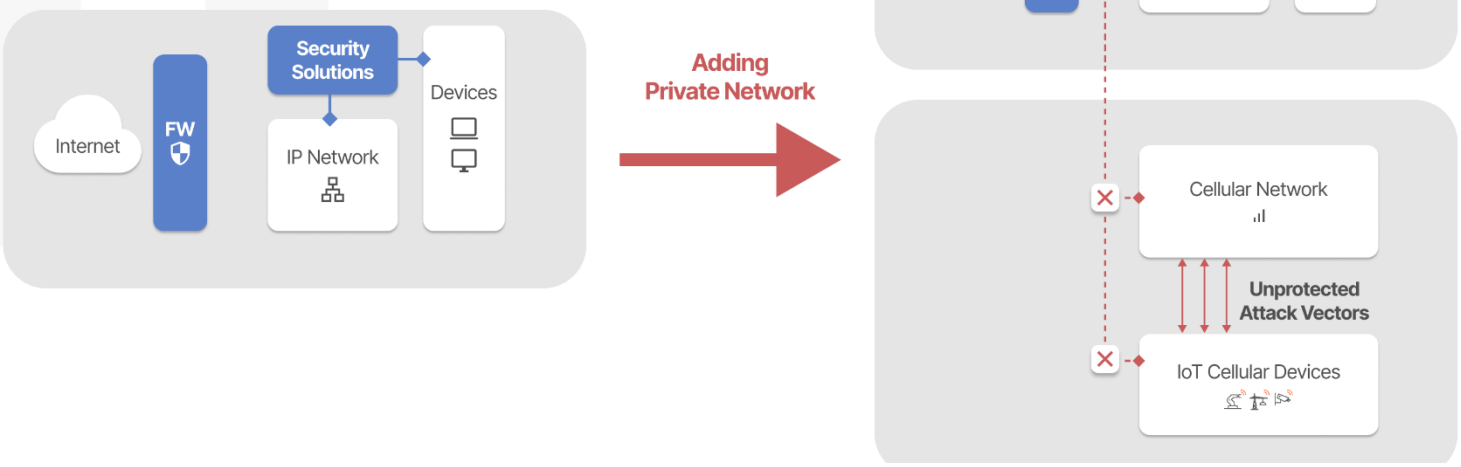
As enterprises deploy models that include IoT device connections to both cellular and enterprise networks, it creates new enterprise security challenges at the intersection between these distinct domains.



Traditional Enterprise Security Frameworks Now Have a Critical Gap

The concept of mobile network security isn't new. MNOs have been targeted by attackers since their inception. However, MNOs have a much different set of security incentives than a typical enterprise. They focus primarily on the protection of the network core and generally do not take responsibility for the security of individual devices. In contrast, enterprises must protect their network infrastructure and ensure that all activities on every endpoint are secure and compliant.

As enterprises adopt private cellular networks, they must complement their existing enterprise security tools with new capabilities that address the unique challenges and protocols found in cellular infrastructure.



How Attackers Will Operate in Converged Environments

Change and complexity always create opportunities for potential attackers, and many are now turning their attention to private cellular networks. Most follow a familiar cyberattack sequence:

1. Identifying an **attack vector**, or a weak point that exposes an initial entry point into a protected network.
2. Initiating **lateral movement** by advancing beyond their initial entry point towards higher-value assets such as important databases, possible points of failure, devices with confidential information, etc.
3. Launching an attack that creates a specific **impact**, such as denial of service, data exfiltration, etc.

While this overall attack methodology will likely continue as private cellular networks are adopted, each specific phase will be affected in very significant ways. For example, the inter-connectivity of private networks is much different from how public cellular networks function. This creates new attack vectors that attackers can exploit to gain access to private networks.

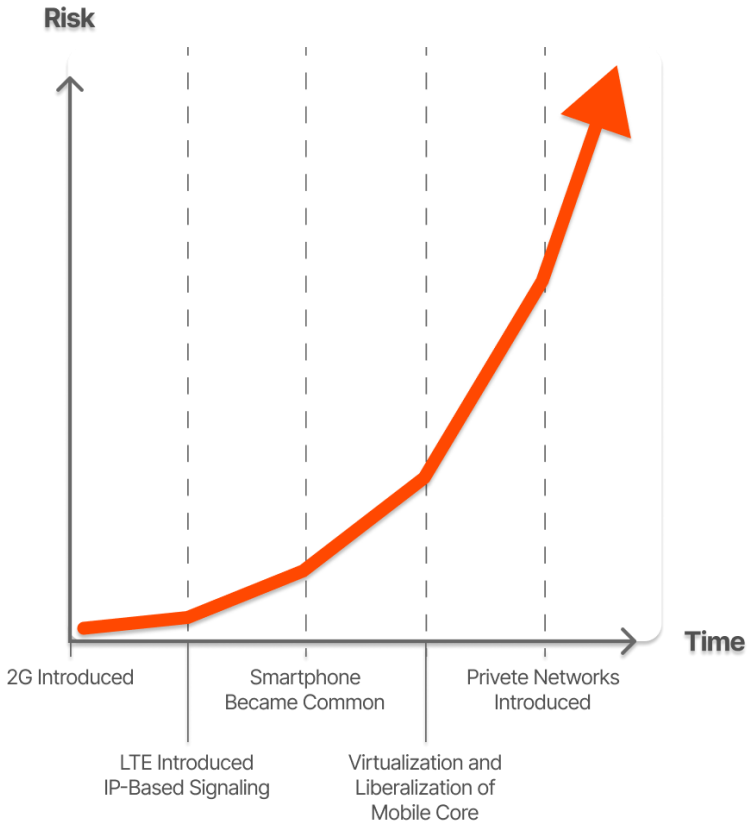
Once an attacker gains access, lateral movement can also advance in new ways that are unfamiliar to enterprise security teams. While these attack methods may have been possible on MNO infrastructure, the new use cases found on private networks will likely increase their cost-effectiveness and popularity. Evolution of wireless technologies, including new vendor entrants and increasing use of virtualization technology in mobile infrastructure, will also increase the number of possible attack vectors.

Enterprises are embracing cellular technologies just as the overall cost for an attacker to launch an attack on cellular infrastructure is decreasing.

An Expanded Universe of Enterprise Attack Vectors

An attack vector is a path an attacker manipulates to gain access to a target. Through this access, the attacker can make some type of impact on the target, such as injecting malicious code to manipulate enterprise devices. An attacker generally needs to impact the enterprise network and devices, with or without the enterprise's awareness, to realize value from an attack. Examples include denying or degrading enterprise network services, stealing data, blocking access to data, and more.

Just like a house has many doors and windows through which a malicious individual could gain entry, a typical enterprise has many possible attack vectors. Mapping and understanding them is a critical activity for security teams.



Attackers have an unfair advantage when it comes to attack vectors. They only need to exploit one to be successful, while security teams' success depends on understanding and protecting them all.

Enterprises Now Have Three Distinct Security Domains

As noted above, enterprises adopting private cellular networks must develop a security strategy that addresses three intersecting domains.

1. The IoT Domain

IoT devices are common targets for threat actors for a variety of reasons. They are often deployed in large numbers, and there have been numerous examples of poor software vulnerability management by IoT device vendors. Any successful attempts to exploit these vulnerabilities will private a possible launch point for a broader attack against the enterprise.

2. The Cellular Domain

The cellular protocol that private mobile networks are based on defines the network's architecture and operational aspects. Although cellular protocols are generally considered more secure than other protocols, they are nonetheless vulnerable to specific types of attacks. A successful attack at the cellular protocol level could enable an attacker to initiate or end certain network services and cause other types of disruptive impacts.

3. The Enterprise Domain

The fact that the private cellular network is acting as an enterprise network means that the architecture of the network, its connectivity model, and the types of activities that could cause severe impact are very different from traditional MNO deployments. This affects how organizations must think about their attack surface and the types of attacks their network is likely to be targeted by.

It’s more important than ever for enterprise security teams to understand the unique risks that exist across the IoT, cellular, and enterprise domains and how to defend against them holistically.

IoT Devices Have Inherent Risks

As IoT device adoption accelerates, many enterprise and device vendors are playing catch-up with security protections. This is particularly relevant for enterprises adopting private cellular networks since IoT device risks will often extend across both traditional enterprise networks and private cellular networks. The following are some specific IoT device attack vectors that enterprises should factor into their security strategy.

1. IoT and OT Device Vulnerabilities

In the race for IoT device market share, device security often takes a back seat to factors like cost. Many devices have very few integrated protection mechanisms, and software quality tends to be very low. Many IoT devices are not subjected to established device security best practices like code testing and penetration testing. As a result, software vulnerabilities, including many with high criticality, are a common occurrence. The story isn't much better for legacy operational technology (OT) networks, which often contain aging technologies that weren't designed with broadscale network connectivity in mind.

2. Remote Management Requirements

Given the specialized nature of industrial IoT and OT devices, they will likely require remote connectivity by experts for configuration, updates, and maintenance. This can be a net positive in some ways since regular updates may reduce device vulnerability risks. However, the connectivity used for remote management may also be a possible attack vector. An attacker may attempt to hijack the service provider's connection or worse, compromise their internal network.

3. Device Roaming Across Networks

Many of the techniques used to secure individual devices are tied to a specific type of network. However, IoT or OT devices may need to roam between different networks. For example, certain devices may move between an enterprise WiFi network and a private cellular network in different situations. Since many security tools protecting IoT and OT devices operate at the network level, gaps in protection are likely as devices roam between distinct networks.

4. Supply Chain Compromises

Supply chain compromises are an increasing concern in the wake of numerous high-profile incidents that have affected enterprises worldwide. Even organizations that have invested in state-of-the-art security technologies and highly skilled teams can be blindsided if a downstream vendor ships hardware or software that has been compromised in advance. Supply chain compromises can be exploited in many ways, jeopardizing the integrity of networks where IoT and OT devices operate. Risks may range from vulnerabilities to hidden backdoors that stand ready for attackers to use at will.

While IoT devices are powerful tools for innovation, they also present a variety of serious risks that enterprises must defend against.

Using Private Cellular Networks for IoT Adds Possible Attack Vectors

In addition to the inherent IoT risks described above, the use of private cellular networks creates an additional set of attack vectors that must be considered.

1. Slicing Manipulation and Lateral Movement

Slicing is a feature in 5G networks that allows the operator to manage several different networks using the same cellular packet core. This enables dedicated allocation of radio resources, quality of service (QoS) management, and other network operations functions. Some enterprises building private cellular networks take advantage of this technology, leasing a slice of a public cellular core rather than creating a standalone private network.

In these situations, the slicing technology is a vector that an attacker might use to gain access to the private cellular core. Since sliced private networks are part of a public core, attackers could attempt to locate a weakness in the slicing mechanism to gain initial access to a private network. For example, an attacker could potentially find a misconfiguration in the slicing implementation, allowing them to initiate lateral movement between the public and private slices or disrupt the network.

2. Roaming Connectivity

Roaming is a familiar feature to users of public cellular networks. This functionality is provided through an interconnection model known as an IP exchange (IPX). To support roaming, the cellular cores of different carriers are connected to a common IPX. The IPX network allows the cores to communicate with signals that make roaming between networks possible.

Roaming in a private cellular network setting will likely have different characteristics than a traditional MNO scenario. However, there will be roaming applications in private networks. For example, some

organizations may wish to deploy hybrid models that allow devices to roam between private and public networks as they move between enterprise locations or are deployed in areas that lack private network coverage. In these scenarios, the roaming interconnection is another potential vector an attacker can exploit. Hijacking the connection to the IPX, impersonating another core connected to the IPX, or compromising another trusted core are just a few ways that an attacker may gain a foothold through a weakness in the roaming implementation.

Radio Access

Cellular networks offer significantly wider coverage than WiFi networks, providing enterprises and their users much more flexibility to use connectivity in innovative ways. However, the extended range of cellular signals gives enterprise IT and security teams less control over network reach. Since the range of cellular networks will likely extend well beyond the physical boundaries of the enterprise, the difficulty for an attacker to access the cellular network from easily accessible locations is much lower.

1. Stolen SIM

While Ethernet networks require a physical connection and WiFi networks often rely on passwords for access, cellular technology operates differently. Access is granted by the presence of a SIM. A SIM is a physical card that contains the key to connect to the cellular network while also allowing the network to identify precisely who is using the device. The original purpose of SIMs was to enable the carrier to measure usage accurately for billing purposes. In private networks, the SIM is generally managed by the enterprise, a third-party carrier, integrator, or an IT services partner.

Private network operators need to control SIM distribution tightly since a valid SIM can be used to grant any device access to the network, likely without the enterprise's knowledge. As private cellular networks become more common, we can expect to see an increase in SIM theft through techniques such as theft of SIM-enabled enterprise devices, social engineering, or breaches of third-party partners involved in SIM

distribution and management. In any of these scenarios, an acquired enterprise SIM would allow an attacker to access the enterprise network with ease.

2. N6 Exploitation

All interfaces between entities in a cellular network have a name. N6 is the name assigned to the interface at the gateway between the cellular core and the network users gain access to via the cellular infrastructure. In the case of a public cellular network, this would most often be the internet. A private network may also connect to the internet. However, it's more likely that the private cellular network will connect to a more sensitive internal network, such as an IoT network, an operational technology (OT) network, an IT network, or another segment of the enterprise local area network.

If an attacker is somehow able to access the network that the cellular network is connected to – or if the network is connected directly to the internet – a savvy attacker may try to use this vector to attack the cellular core through the N6 gateway. This is a complicated vector to utilize since the attacker must successfully identify a vulnerability in the core component. Nonetheless, it is an attack vector that enterprises should have a strategy for defending.

Cellular networks introduce an expansive new set of potential vulnerabilities that are unfamiliar to many enterprise security teams and inadequately addressed by existing security tools.

Existing Enterprise Attack Vectors Now Also Extend to Cellular Networks

The challenge of attack vectors on converged networks works both ways. In addition to the new mobile-specific attack vectors described above, there are also risks that existing enterprise attack vectors will extend to private cellular networks.

The following are some high-level examples that enterprise security teams should consider:

Cloud Lateral Movement	Now that it is more common for cellular cores to run in virtualized or cloud environments, there is a greater risk that lateral movement in compromised cloud environments can advance into the private cellular network.
Drive-By Compromise	While many IoT devices are autonomous, some may still be susceptible to the same types of human factor risks that affect workstations on the enterprise network.
Exploitation of Public-Facing Applications	Not every private cellular network will have public-facing applications, but those that do may see the same types of vulnerability exploit attempts frequently seen in the enterprise domain.
External Remote Services and Trusted Relationships	In a converged environment, a breach of third-party partners providing support for the enterprise domain could serve as an attack vector for the private cellular network

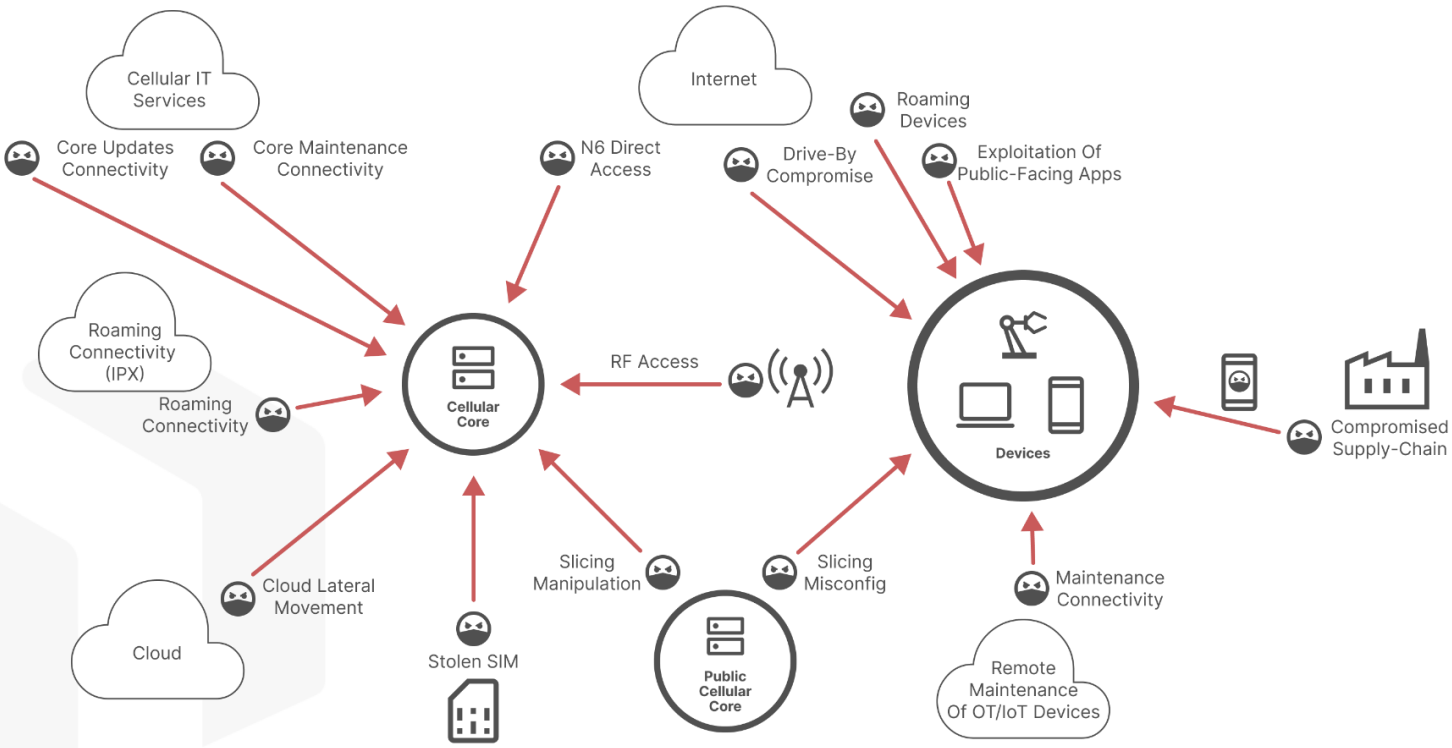
These topics are likely familiar to many enterprise security teams, but it's important to re-examine them through a wider lens once private networks are deployed.

Traditional enterprise security challenges and risks are amplified when private cellular technologies are added to the enterprise environment.

For a more in-depth overview of enterprise attack vectors and how they apply in converged environments, see the Appendix at the end of the document.

How Attackers Target Converged Enterprise Networks

In the section above, we've identified an extensive set of attack vectors that can be used to access private networks, as summarized in the figure below.



Now, let's turn our attention to the attack methods that threat actors may use to take advantage of these possible paths into the enterprise and cause a specific negative impact. The following is a summary of possible attack types that are particularly relevant to private cellular networks, grouped by their common techniques.

Denial of Service and Signaling Storm

Denial of service (DoS) is a well-known and highly effective attack technique since it requires low effort but can have a high impact. It is also a very scalable attack method that doesn't require significant customization to target different networks. Therefore, one advanced hacker can develop a DoS tool that any attacker with baseline technical aptitude can use.

Like traditional enterprise networks, cellular networks are also susceptible to DoS attacks. One example is a core signaling storm. In these types of scenarios, the cellular core is communicating via cellular signals as described by the 3rd Generation Partnership Project (3GPP) standards. Even though extensive steps are taken to keep the cellular protocol as secure as possible, there are still many protocol vulnerabilities that can be exploited to generate a signaling storm – or a DoS on a core entity via signaling. For example, a malicious signal may be sent to a core entity commanding it to release all contexts (the user "sessions" in the cellular network) using GTP-C spoofed messages[1] [2]. This could cause the entire network to drop.

A second type of cellular DoS attack method is a radio signaling storm[3] [4] [5]. Radio protocols, while very advanced from a bandwidth perspective, are quite vulnerable from a security perspective. A very low-cost and low-effort attack technique is simply blocking radio channels used for control purposes. This could cause new connections to be blocked, existing connections to be dropped, and other adverse outcomes depending on the specific methods used.

Radio signaling storm attacks have existed for decades. However, increasing use of private cellular networks changes the value/cost equation for attackers. While public cellular networks are generally capable of handling a signaling storm of a specific cell, private networks

1 FS.20 GPRS Tunnelling Protocol (GTP) Security v4.0

2 GTP-C is used in LTE and 5G NSA, while 5G SA replaced it with HTTP/2. It doesn't mean there are no Signaling Storms in 5G SA, only the attack would look differently and apply other methods.

3 https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8399903/

4 https://ieeexplore.ieee.org/document/7004004

5 https://arxiv.org/pdf/1312.3681.pdf

will likely be much more sensitive to one or several malfunctioning cells. In most cases, these scenarios will disrupt the entire network, potentially causing significant financial harm to the affected enterprise. As a result, radio signaling storms will likely increase in frequency as more private cellular networks are deployed.

A third attack technique that enterprises should be aware of is SMS DoS[6]. This technique exploits vulnerabilities in a cellular modem's parser to send a large volume of specifically crafted SMS messages that can overwhelm the cellular modem and disrupt service.

Code Execution

Code execution is a technique that involves the discovery of a vulnerability that allows remote code execution on a device, server, or other critical piece of equipment. These attacks require significant expertise and extensive research on the target device to deliver a payload capable of exploiting a vulnerability correctly. However, if successful, this technique can be devastating since it often gives the attacker a great deal of flexibility to initiate attacks on other devices on the network, prevent the device from functioning, leak sensitive data, and more.

Given the IoT device vulnerabilities risks described above, the potential for code execution is quite high. In addition, unlike enterprise endpoints like personal computers, IoT and OT devices have low-to-no defense mechanisms against code execution[7]. This makes the task of developing a payload to exploit an existing vulnerability much easier. The combination of limited protection measures and low-quality code often found on these devices is a potential recipe for disaster for enterprises. After all, these types of incidents are both high-impact and relatively likely. For example, the well-known Mirai botnet exploited the low security standards of IoT devices by targeting known code execution vulnerabilities[8].

6 https://documents.trendmicro.com/assets/white_papers/wp-attacks-from-4G-5G-core-networks.pdf

7 E.g., https://blog.morphisec.com/aslr-what-it-is-and-what-it-isnt/

8 For example: https://www.fortinet.com/blog/threat-research/the-ghosts-of-mirai, https://www.trendmicro.com/en_us/research/20/g/new-mirai-variant-expands-arsenal-exploits-cve-2020-10173.html, https://www.fortinet.com/blog/threat-research/the-ghosts-of-mirai , https://github.com/kernelsmith/about/blob/master/pubs/realtek_sdk.md

Firmware modification is another code execution method that targets IoT or OT devices[9]. Cellular equipment is proven to be susceptible to these types of vulnerabilities, including known code execution vulnerabilities in cellular basebands[10] [11], cells, and even in some cellular cores[12].

Core Manipulation

The core is the brain of a cellular network, supporting critical capabilities like mobility, session, and authentication management. It has complete control over the cellular network. The cellular core is comprised of several different entities, which communicate based on the 3GPP specifications. These specifications articulate cellular standards, which most recognize as "generations" such as LTE and 5G. These standards include security elements, but like most standards and protocols, they have security flaws as well.

Manipulating the configuration of core entities or spoofing of core traffic by an attacker can harm the entire network. The core manipulation risks that private cellular networks face are very similar to those targeting carriers. As with a private network, the carrier core is a single point of failure. Therefore, MNOs go to great lengths to protect themselves from various core manipulation risks.

For example, malicious signaling coming from the roaming network[13] [14] is a well-known attack method, and MNOs use numerous security solutions to defend against it. There are more advanced types of core manipulation as well. For example, one of the most important networking protocols in the mobile core is GPRS Tunnelling Protocol (GTP). GTP is used to tunnel both user-plane traffic and control-plane signaling between core entities. Attackers sometimes attempt to target

9 https://documents.trendmicro.com/assets/white_papers/wp-attacks-from-4G-5G-core-networks.pdf

10 https://i.blackhat.com/USA21/Wednesday-Handouts/us-21-Over-The-Air-Baseband-Exploit-Gaining-Remote-Code-Execution-On-5G-Smartphones.pdf

11 https://www.usenix.org/system/files/conference/woot12/woot12-final24.pdf&lang=en

12 https://research.nccgroup.com/2021/11/16/exploit-the-fuzz-exploiting-vulnerabilities-in-5g-core-networks/

13 https://aaltodoc.aalto.fi/bitstream/handle/123456789/37914/master_Singh_Isha_2019.pdf?sequence=1&isAllowed=y

14 https://www.blackhat.com/docs/eu-16/materials/eu-16-Holtmanns-Detach-Me-Not.pdf

this protocol through use of a GTP-in-GTP vulnerability[15]. This entails hiding a control-plane packet inside a GTP user-plane packet with the aim of tricking the core into executing it.

Another example is packet injection inside a GTP tunnel[16], which allows a malicious piece of user equipment (UE) to impersonate a different UE, perhaps bypassing policies in the process. Attackers may also attempt to transmit a spoofed GTP-C packet to command core entities to misbehave[17].

Session Hijacking and Man-in-the-Middle

Session hijacking is a technique that involves stealing a session between a target and another benign entity. After hijacking the session, the attacker can act as a man-in-the-middle, reading sensitive data or manipulating the packets that are sent between the victim and the other entity. The attacker can also attempt to send spoofed packets, which the user may trust.

These risks apply to private cellular networks as well. For example, a private network tells the UE which DNS server it should be using when it connects to the network. When this connection occurs, there is a procedure called PDP attach, during which the UE gets an IP allocation on the networks and a DNS server for DNS translation. A sophisticated attacker could manipulate or spoof this packet and inject a malicious IP into the device. After that point, every time the device attempts to browse a new domain, it would query the malicious IP to translate the domain into an IP address. This gives the attacker complete control over the IP addresses that the device communicates with and trusts.

There are other forms of hijacking that are unique to certain types of networks and devices. MQ Telemetry Transport (MQTT) hijacking and Modbus hijacking are two examples that relate to IoT and OT devices specifically[18].

15 https://www.gsma.com/membership/wp-content/uploads/2017/09/Positive-Technologies-White-Paper.pdf

16 https://documents.trendmicro.com/assets/white_papers/wp-attacks-from-4G-5G-core-networks.pdf

17 FS.20 GPRS Tunnelling Protocol (GTP) Security v4.0

18 https://documents.trendmicro.com/assets/white_papers/wp-attacks-from-4G-5G-core-networks.pdf

Another example of a man-in-the-middle attack is the manipulation of the Non-Access Stratum **(**NAS) attach request of the UE. Using this technique, an attacker could turn off integrity protection and ciphering for the session[19]. They could also disable the power saving mode of the device, which can increase the amount of power waste by more than five times[20].

Brute Force

Brute force is another popular attack technique that can be targeted at private cellular networks. Brute forcing involves trying to take a specific action, such as logging in to a specific service, on a continuous basis to gain the privileges of a specific user or set of users. Brute force attacks can be simplistic, such as trying all possible combinations, or more intelligent dictionary attacks that include data elements such as common number sequences, birth dates, names, etc.

In a private cellular network environment, brute force can be attempted against critical infrastructure components. For example, industrial routers have backup communication channels based on SMS. An attacker could attempt to brute force this SMS channel in an attempt to gain control of these routers. This is not a common scenario that carriers are targeted with, so security tools are not designed to monitor for it. Enterprise security tools would be equally ineffective at detecting this technique. There are many other cellular network elements that can be targeted with brute force attacks as well, such as the administrator interface of the core and radio access network entities.

Attackers have a variety of attack techniques at their disposal, and the new use cases introduced by private cellular networks will likely give new life to known attack methods that are not widely used against MNOs.

19 https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8399903/

20 https://i.blackhat.com/USA-19/Wednesday/us-19-Shaik-New-Vulnerabilities-In-5G-Networks-wp.pdf

Securing Your Journey to Network Modernization and Convergence

As this paper illustrates, the convergence between the IoT, cellular, and enterprise domains creates a complex set of risks and challenges for enterprise security teams. The wide range of attack vectors introduced by IoT devices and private cellular networks – and the myriad of possible attack methods that can be used to target them – makes extending existing enterprise security tools and practices into these converged environments extremely challenging.

OneLayer's mission is to help enterprise network and security teams, including those with limited prior experience with cellular technologies, extend their enterprise security tools and strategies to private cellular networks.

OneLayer provides a software-based solution to secure private 5g networks. The OneLayer platform provides asset management, visibility, policy creation and threat prevention, which enable organizations to leverage the full potential of private cellular networks by extending and adopting existing security methodologies to this new type of network.

Appendix

Since many enterprise security professionals are familiar with the common traditional attack vectors in enterprise environments, the sections above focus primarily on the new risks presented by IoT and private cellular networks. However, a more in-depth exploration of enterprise attack vectors and their relevance in converged environments is included below.

Cloud Lateral Movement

Virtualization and cloud computing have transformed enterprise IT by replacing costly and inefficient on-premises hardware deployment approaches with more dynamic and scalable virtual resources. These technologies have now made their way into cellular infrastructure as well. A decade ago, most cellular infrastructure was based on complex dedicated hardware. Now, many of these functions can be virtualized and run in the cloud. The flexibility and cost advantages of this type of approach are disrupting the entire telecommunications market and driving the growth of private cellular network usage. Today, most cellular cores support virtualization or are in the process of enabling it. Most private cellular networks will likely be cloud-based as well.

While cloud enablement brings many advantages, it is also another attack vector that security teams must defend. When a cellular network core runs in the cloud, any cloud infrastructure vulnerabilities that an attacker can exploit for lateral movement could expose a cloud-hosted cellular network core to new types of risks.

Drive-By Compromise

Many of the most successful cyberattacks exploit human factors. While user productivity is the reason that many networks exist, the wide range of actions that users may take while connected to the network presents a significant risk. Drive-by compromise is a well-known risk in the enterprise that exploits human factors to cause a specific malicious action to occur. Often, this is done by driving a user to a particular website and using various methods to mislead or coerce them into

taking a specific set of steps. This often culminates in the injection of malicious code into the browser, exploiting a vulnerability to execute the code on the target device.

Private cellular networks may include both user-based and autonomous devices. Nonetheless, drive-by compromise is a significant risk that security teams must consider, particularly since devices connecting to private cellular networks may be protected by less diligent endpoint protection and vulnerability management practices, making them easier to exploit under the right conditions.

Exploitation of Public-Facing Applications

Public-facing applications are one of the best-known methods of attacking enterprises – and often the easiest to execute. For many years, public-facing applications were so poorly protected that even low-skill attackers could exploit them using basic techniques like SQL injection, probing SSH connections with obvious credentials, etc. More recently, enterprises have developed better awareness and protection methods for public-facing applications. However, attackers still regularly gain access to enterprise networks by exploiting application vulnerabilities.

While not every private cellular network will have public-facing applications, those that do will be susceptible to the same risks. When private network use cases include public-facing applications, attackers may use the same tactics described above – or more sophisticated techniques like exploitation of buffer overflow vulnerabilities – to execute remote code on the server as a means of connecting to the private cellular networks.

External Remote Services and Trusted Relationships

Remote services by trusted third-party partnerships are a common attack vector used against enterprise networks. Many enterprises have trusted relationships with third parties, who are granted the ability to communicate with the enterprise network. For example, many organizations engage remote IT services firms to assist with enterprise network management and other IT functions. After several high-profile

cases of these trusted relationships being exploited by attackers, many enterprises have reduced third-party access to must-have functions and deployed specialized protection tools to secure this attack vector. However, these types of attacks remain a significant risk for enterprises.

It's also a risk that is likely to increase with the introduction of private cellular networks. The cellular core of these networks must be managed by network administrators, including ongoing monitoring of network hygiene and resolution of any detected operational issues. However, unlike with traditional enterprise network management, the skills required to manage cellular networks are quite scarce, and the learning curve is steep. Therefore, many enterprises will likely choose to outsource the management of their cellular core to third-party specialists. In these cases, remote connectivity will be required to support day-to-day administration and regular updates to the cellular core software.

A sophisticated attacker could utilize this connectivity to break into the core, possibly even with high-level administrative privileges. This could be executed through a hijacking of the connection or even an advance compromise of the trusted partner's network. In fact, any service provider performing this function for multiple enterprises would be an attractive target since one successful breach could enable access to many different organizations using private cellular networks. Moreover, attack vectors that provide access to the core are among the most important to defend against since with relatively low expertise and effort, an attacker could launch an attack with severe impact.