WHITE PAPER

End-to-End Security Considerations in Mobile Networks and Services

Defending Today's Evolving Infrastructure and Expanding Attack Surface

Executive Summary

The requisite complexity of mobile network infrastructure and services creates layers of vulnerability for operators—from exposures stemming from backward compatibility to common IT risks to those stemming from human errors like misconfigurations. With the increasing use of newer technologies such as cloud and virtualization, the mobile network attack surface will continue to evolve and expand.

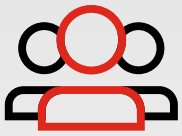
This document discusses today's end-to-end security needs for mobile network operators (MNOs) and provides some general guidance that can be applied to each of the operator's domains.

Complexity and Digitalization Expose New Mobile Network Risks

Mobile network operators have highly complex, interconnected, and distributed deployments of infrastructure and tools that enable the delivery of various services and use cases. This can range from standard voice and data to more complex use cases targeting enterprises and involving partner ecosystems. Mobile operators may also have different generations of networks that may need to interwork with one another.

To assess the security considerations for these kinds of diverse environments, it is important to understand the network's various parts; respective use cases, data, and components; and the overall management and operations.

In general, an operator's mobile network can be divided into access, core, service edge, interconnection points, and operations and maintenance domains and networks. These can be built in physical, virtual, or cloud-native environments; on fully owned data centers; or on a combination of public-private cloud service platforms—depending on the maturity level and the respective 3rd Generation Partnership Project (3GPP) deployment stage. All of the above-mentioned parameters can have significant impact on the operator's security posture.



Mobile operators store huge amounts of personal data and are responsible for the stability of the communications services they provide. A data breach or service failure as a result of a cyberattack can lead to severe financial and reputational damage or impact on customers.[1]

If an operator's service is compromised, attackers can gain access to the entire infrastructure of their customers.[2]

Sources of Vulnerabilities in MNO Networks

At a high-level, vulnerabilities identified within an MNO environment can be attributed to one of three categories. Understanding these categories can help set clear mitigation strategies for each using a layered approach.

- Vulnerabilities caused by backward compatibility requirements, such as bidding down attacks. These vulnerabilities are less common and are relatively difficult to exploit.
- IT vulnerabilities, such as remote code execution and information disclosure. These vulnerabilities are similar to those identified in enterprise IT environments. As MNOs adopt software-based and virtualized deployments, these types of vulnerabilities are being seen in greater numbers.
- Misconfigurations and noncompliance with established recommendations, for example, GSMA FS.19,[3] FS.20.[4] Traditionally, these have been the most common vulnerabilities, leading to exposure of services, visibility into internal MNO infrastructure, and attacks from roaming and external interconnects.

As MNOs move toward virtualization and cloud-native deployments, the volume and weight of these vulnerabilities are changing. There have been an increasing number of vulnerabilities introduced due to software weakness, virtualization, and containerization technologies. Going forward, MNOs will become more exposed to IT-based attacks, akin to those experienced by large enterprises. Similar observations have been made in recent research on Open RAN (radio access network) environments, which are relevant to other telecom domains using virtualization and container technologies.[5]

Backward compatibility-driven vulnerabilities

MNOs must maintain backward compatibility and the ability to interoperate with previous generations of cellular networks to provide coverage for older devices. They also need to interconnect with other operators that have not yet transitioned to 5G. One such instance is the 5G non-standalone architecture (NSA), which leverages the new 5G radio while interworking with the 4G core network.

But this kind of hybrid situation can lead to attackers exploiting vulnerabilities in previous generation technologies to bypass security controls of the newer generation networks. For example, 5G standalone (SA) roaming includes strict controls to ensure trust and integrity between roaming MNOs and all the intermediaries within the roaming control plane. However, due to interworking with the 4G core in NSA, MNOs could be subject to well-known 4G roaming attacks.

Last year, threat actors tried to exploit old vulnerabilities found in the unpatched devices of a few manufacturers in an attempt to access a telecom provider's network.[6]

IT vulnerabilities

These vulnerabilities are not specific to MNOs and may apply to any IT system—from underlying infrastructure component vulnerabilities to application-identified vulnerabilities. Whether they are known, new, or zero-day vulnerabilities, their presence may result in a range of security issues, including information disclosure on exposure points, unauthorized access, or complete compromise of a system or application.

From 3GPP Release 16 onward, the rapid adoption of IT technologies in MNO environments—such as cloud computing technologies, "internet-based" protocols, and API communications—resulted in these types of vulnerabilities becoming the most dangerous and commonly found category. MNOs need to anticipate constant changes within the IT threat landscape and adapt accordingly.

Misconfiguration and noncompliance with established recommendations

A large proportion of vulnerabilities in MNO networks are a result of either misconfiguration or (more generally) noncompliance with security requirements recommended by GSMA and telecom regulatory bodies. Examples may include misconfigured roaming interfaces that allow and process malicious requests; misconfigured N6/SGi interfaces that expose internal services; or the absence of encryption, integrity checks, and replay protection in the RAN and core networks.

Usually, these vulnerabilities are more straightforward to address, as they are directly connected to an MNO's security policies and depend on the effectiveness of hardening standards, adherence to recommendations, and best practice guidelines.

Expected Evolution of Vulnerabilities

Although these general categories are not ranked in terms of volume or severity, clear trends can be derived in parallel with the evolution of MNO networks. In previous generations of mobile networks, the most severe vulnerabilities would have likely been attributed to misconfigurations and noncompliance with industry best practices or vendor security recommendations. Additionally, attacks on mobile networks were mostly possible only from within the trust boundaries of the operator (except for roaming-based attacks, where trust boundaries were extended to partner networks).

With the introduction of IT and the expansion of internet-based technologies in MNO environments, the number of IT-based vulnerabilities will grow in volume and the overall attack surface will significantly expand. Increasing use of cloud and virtualization technologies, additional interconnections (edge cloud, multi-access edge computing [MEC], hyperscalers), and the adoption of open/standard API communications could all expose MNOs to attacks on applications and services from both inside and outside their trust domains. Understanding the overall different categories of vulnerabilities can help frame effective security enforcement policies in MNO networks and ecosystems.

Foundational Principles for End-to-End Cybersecurity

As previously discussed, virtualization and cloud native-driven risks and attack vectors would far surpass existing protocol-based vulnerabilities in telecom networks, such as SS7, Diameter, GTP. It is therefore essential for operators to move from traditional "bolt-on" security approaches to a more holistic, end-to-end security architecture. Such an architecture should be built around four foundational pillars:

- In-depth defense
- Zero trust
- Secure by design
- Real-time security monitoring and response

The overall goal is to reduce the overall attack surface (both internal and external) and to increase the effort and associated cost required by threat actors to mount potential attacks.

Services such as 5G are susceptible to cyberattacks because everything—including the core networks—is software designed. That means all the risks associated with software technologies will manifest on carrier networks as well.[7]

In-depth defense

In-depth defense ensures that cybersecurity is present at all layers of the MNO's networks, services, and overall environment and ecosystem. It dictates vertical and horizontal cybersecurity integration from the underlying physical infrastructure via the virtualization layer—including overall network function (NF) life-cycle management—and onto the applications, services, and value ecosystems provided by the MNO.

In-depth defense principles should also be implemented at various levels within a given layer. For example, in-depth defense within the virtualized infrastructure layer ensures that security follows the entire life cycle of components, including image security verification, virtualization infrastructure hardening, or enforcement of traffic bound for and between the NFs.

Zero trust

Virtualization, openness and exposure, distributed architectures, hybrid clouds, edge computing sites, and the creation of value ecosystems—these all contribute to the disappearance of a traditional network perimeter. To provide cybersecurity for an increasingly perimeter-less world, the basis of the zero-trust principle is never trust, always verify. This means that entities—regardless of their location and connections to trust boundaries—are always considered "rogue" unless they are authenticated (or mutually authenticated, in the case of mobile networks) and authorized (allowed to send a particular request to any particular entity), regardless of their previously authenticated status.

This principle assumes that an attacker is already inside the network. A zero-trust model enhances security by blocking unauthorized access to network resources and preventing internal lateral movement. Zero-trust principles should be implemented across various trust domains, including but not limited to:

- RAN: mutual authentication of various RAN nodes
- Core network: mTLS-based mutual authentication; X.509 certificates for mutual authentication supported by OAuth servers to facilitate authorization for NFs to make requests to other NFs
- Multitenant edge compute environments

Secure by design

In keeping with the secure-by-design recommendations ratified by 3GPP (TS-33.501),[8] operators can enhance the security of communications between NFs in the same trust domain and different trust domains. There are various mandatory and recommended security capabilities that an operator can deploy, including but not limited to enforcing confidentiality; integrity and replay protection within various communication reference points; or the deployment of centralized and federated Certificate Authority to ensure communications are first authenticated and authorized before any target resources are called, from within or out of a particular trust domain. For example, a security gateway (SecGW) ensures secure transport of control, user, and management plane data from the RAN to the core, or between two operators in different trust domains via the inter-PLMN user plane security (IPUPS) function.

The end goal of 5G MNOs is to provide a set of secure services and use cases to consumers and enterprises, ensuring they consume as many services within the MNO domain for the longest possible time. To do so, additional cybersecurity visibility and enforcement points need to be introduced for comprehensive application security—not just in the application runtime but throughout its entire life cycle.

Continuous cybersecurity monitoring and response

This final principle ensures all relevant security events are monitored, correlated, and acted upon in relation to a mobile operator's business and operational logic. For this to be effective, security log monitoring and correlation capabilities must be deployed on all layers, including underlying physical infrastructure, virtualization infrastructure, virtual network functions (VNFs) and cloud-native network functions (CNFs), management and orchestration (MANO) layers, and associated operations support system (OSS) and business support system (BSS) functions.

The monitoring system should be able to detect breaches in all layers and all connected domains. It should also permit the addition of custom correlation rules to detect various attack chains that need to be alerted and responded to with high priority. Additionally, certain correlations should be able to trigger automated responses for rapid threat mitigation.

Conclusion

Cybersecurity is becoming a mandatory enabler for MNO evolution and growth. Security will play a growing role in protecting MNO networks, services, and data; meeting compliance requirements of both operators and their customers; safeguarding sensitive data; and providing high-value, secured use cases for enterprise verticals.

Fortinet empowers MNOs to design and implement end-to-end cybersecurity based on the foundational principles discussed above to ensure an adaptive, agile, and comprehensive security posture in support of sustainable growth and success.

[1] "Why the Telecom Industry Must Prioritize Cybersecurity," Security Boulevard, September 8, 2022.

[2] Ibid.

[3] "FS.19 Diameter Interconnect Security," GSMA, accessed February 27, 2023.

[4] "FS.20 GPRS Tunnelling Protocol (GTP) Security," GSMA, accessed February 27, 2023.

[5] "OpenRAN – 5G hacking just got a lot more interesting," media.ccc.de, July 24, 2022.

[6] "Why the Telecom Industry Must Prioritize Cybersecurity," Security Boulevard, September 8, 2022.

[7] "Cybercriminals Target Telecom Provider Networks," Dark Reading, January 19, 2023.

[8] "Security architecture and procedures for 5G System (3GPP TS 33.501 version 16.3.0 Release 16)," ETSI, August 2020.

March 15, 2023 8:57 AM

1998966-0-0-EN