Palindrome Technologies

Emerging Communications Networking Trends & Cybersecurity Challenges

Communication networking technologies are going through a dramatic transformation for service providers, suppliers, application developers, and consumers. Emerging network technologies provide greater bandwidth, low latency, better coverage and support for existing and emerging multimedia applications and services. Service providers, enterprises, and government organizations must adopt new software and network architectures to support connectivity, mobility and use cases. The primary wireless technologies (Wi-Fi, 5G and Citizen Broadband Radio Service [CBRS]) are building upon previous wireless generations and will interwork with each other to support user roaming across both private and public network domains.

This paper describes the current trends in wireless technologies and architectures, focusing on:

- **Security threats** and risks stakeholders need to consider to protect their users, data and infrastructure.
- **Key issues** and efforts that industry stakeholders, standards forums and government entities must continue to address to enable secure deployments countering the evolving threat environment.
- Examples of **security research** that is needed to advance the state-of-the-art in holistic security approaches.

Table of Contents

The Emerging Wireless Network Technology Landscape

The public telecommunications infrastructure is going through a dramatic transformation. Widely deployed 4G Long-Term Evolution (LTE) technology is incapable of supporting the formidable bandwidth, latency and scalability requirements of many growing and emerging technologies. Increasing demand created by consumer multi-media and Internet of Things (IoT) devices and the media-rich applications they support have pushed network requirements to new limits. These applications include streaming video, virtual reality/augmented reality (VR/AR), videoconferencing, telemedicine, vehicle to everything (V2X), and demanding enterprise applications. In order to facilitate the evolution and expansive growth of these emerging technologies, the Fifth Generation ("5G") of mobile technology has been deployed. In addition to supporting the traditional telecom services (e.g., voice and data), 5G is designed to facilitate a much larger ecosystem of applications and services. This ecosystem is leveraging disruptive technologies such as high-speed mobile connectivity, distributed cloud environments, virtualized network and computing functions, open-source software components, and machine-learning algorithms to automate service and operations management.

The primary goals of 5G are:

1. Greater system capacity
2. Higher data rates (gigabits per second)
3. Reduced latency (targeting sub-10 ms)
4. Massive device connectivity
5. Improved security

The interplay of these technologies, architectures and capabilities are reorienting the way people and enterprises interact with multimedia services and devices, including entertainment, home automation, healthcare, social interactions, transportation, work environment and several others.

In addition to Public 5G networks, enterprise organizations are deploying private 5G networks, which they are combining with Wi-Fi and public networks to form network hybrids. Private 5G network deployments are growing rapidly to support commercial enterprise and government use cases, including industrial automation, IoT devices, AR/VR/XR and new communication services. The network elements supporting a private 5G network can be managed by the enterprise organization, or a service provider, and support mission critical and non-critical application requirements including reduced latency, higher speeds, greater coverage and control, tailored performance and reliability. This also includes guaranteed QoS to meet the demand of applications, operational flexibility and enhanced security in terms of identity and access management.

In certain scenarios, such as building automation and maritime operations, the Citizen Broadband Radio Service (CBRS) is leveraged to offer private LTE/5G-NR (New Radio) service in support of commercial and government enterprise applications. CBRS uses band 3550-3700 MHz, a part of the radio spectrum that, per the U.S. Federal Communications Commission (FCC), is used sparingly by the U.S. government and other entities. CBRS has been identified for shared wireless private broadband applications. Currently, LTE and 5G NR are the chosen access technologies to be used in this band. The use cases for CBRS primarily focus on improving in-building or local area connectivity by facilitating private LTE/5G radio networks. This radio access may be used for alternative broadband access, to help increase mobile capacity, to support private LTE/5G services, or in-building cellular services. As such, it is expected that private cellular networks will guarantee network capacity and resiliency for data-intensive applications being transported from one location to another.

Wi-Fi is ubiquitously used to provide connectivity to a myriad of use-case scenarios, including residential LAN, enterprise LAN, public hotspots, smart city applications, and industrial automation. Wi-Fi has become an indispensable part of day-to-day networking and

connectivity. Wi-Fi was initially permitted to operate in the unlicensed Industrial Medical Scientific (ISM) bands of 2.4 GHz and 5 GHz spectrum by the FCC. Through the evolution in the IEEE 802.11 standards and improvements made in the last 20 years, Wi-Fi aims to meet the ever-growing demand on wireless networks, focusing on increased spectral efficiency, throughput, and improved latency. But as Wi-Fi network deployments continue to grow, Wi-Fi networks face many challenges, including congestion, restricted wideband channel availability and legacy device support.

In order to sustain Wi-Fi's rate of growth, the Wi-Fi 6/6E/7 versions have been specified. The use of the 6 GHz band in Wi-Fi 6E and 7 nearly triples the amount of spectrum (i.e., contiguous and wider channels) available to Wi-Fi attached devices. The 6 GHz band enhances the peak data rates and offers favorable propagation characteristics without some of the limitations of the millimeter wave (mmWave) bands. However, while the 6 GHz band's shorter wavelengths support greater data transfer speeds, the effective operating distance is shorter relative to the 5 and 2.4 GHz bands. This makes real Wi-Fi 6E/7 networks likely to use combinations of 6 GHz, 5 GHz, and 2.4 GHz bands to deliver fast, reliable connections throughout an office building. Wi-Fi Protected Access 3 (WPA3) support is mandatory for Wi-Fi 6 and 7 Certified devices by the Wi-Fi Alliance. WPA3-Personal replaces the Pre-Shared Key (PSK) used in WPA2-Personal with Simultaneous Authentication of Equals (SAE), delivering more robust password-based authentication and stronger network traffic protection.

Current Heterogeneous Network Ecosystem

Each of the prevalent and emerging wireless network technologies (5G, Wi-Fi 6/6E/7, CBRS) has defined a coexistence approach in order to support interworking and leverage the capabilities of the different access networks in support of seamless, secure and interoperable services. Both commercial and government enterprise organizations, along with end users, are confronted with the challenge of selecting the right access standard and end-to-end networking technologies to best utilize network conditions and meet application service requirements.

An example of a network coexistence approach is illustrated in the 3GPP specification[1] for an integrated Wireless LAN (WLAN) architecture for untrusted and trusted WLAN integration with the 5G Core (5GC). Figure 1 illustrates 3GPP and Non-3GPP access to the 5G Core.

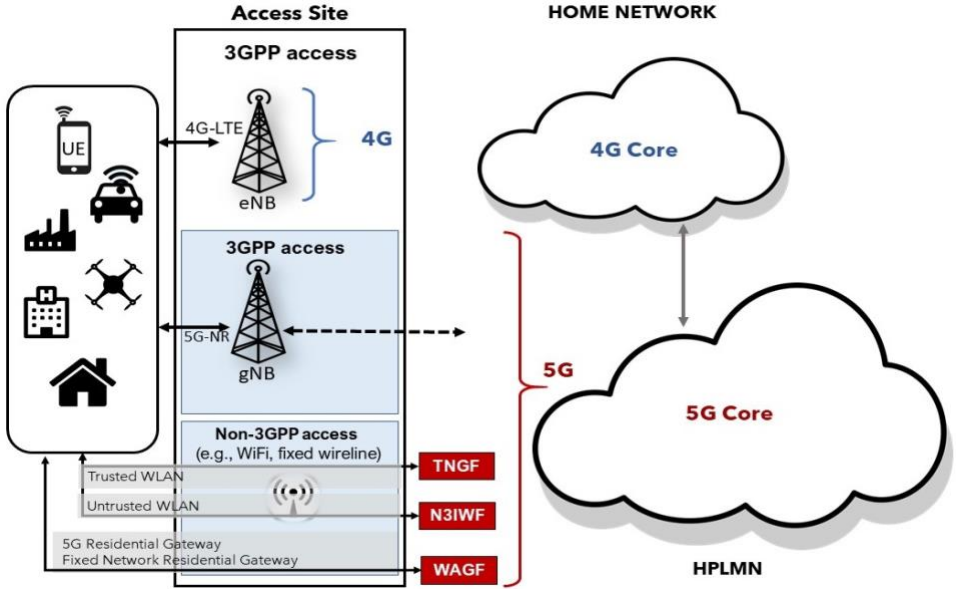


Figure 1: 3GPP vs Non-3GPP access

An untrusted WLAN access network is connected to the 5GC via a non-3GPP Interworking Function (N3IWF) and a trusted access network is connected to the 5GC via a Trusted Non-3GPP Gateway Function (TNGF) or a Trusted WLAN Interworking Function (TWIF). For fixed wireline access the Wireline Access Gateway Function (WAGF) is used. Based on the type of WLAN access offered, an end-user device may, during the discovery process, decide to use untrusted or trusted WLAN access to establish connectivity with the 5GC per organizational policy specifications. This coexistence approach must accommodate 5G network policies for access and route selection, along with applying QoS to the 5G data flows carried over the WLAN access.

[1] 3GPP TS 23.501, System Architecture for the 5G System, Release 17, 2021.

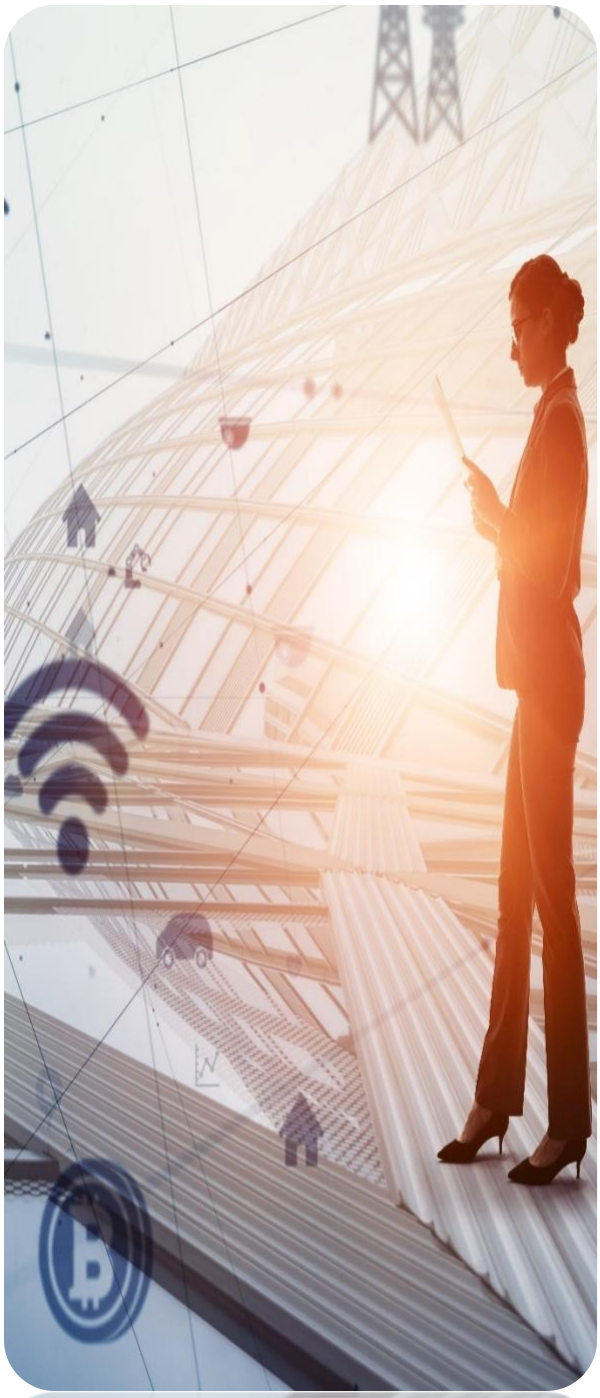
This coexistence introduces several challenges, including technical, architectural and operational, and needs to be addressed by organizations in this converged heterogenous ecosystem. The areas of consideration include:

Transition Architectures: the current 5G architecture is split across two architectures consisting mainly of non-standalone (NSA) 5G (mix of 5G and 4G technology elements) and standalone (SA) 5G (all 5G technology elements). For WiFi and CBRS, there are, for example, new releases of the technologies and architectures covering coexistence approaches. There will be some commonalities of service performance requirements between implementations in commercial and federal organizations but also distinct security requirements that will need to be explored carefully in the design phase, for reliability, authentication, authorization, and confidentiality.

- **Distributed & Complex Service Architectures**: there are several interconnected architectures including private enterprise, carrier network, multi-access edge computing (MEC), far-edge, carrier core network, cloud-based services, and partner networks (e.g., Neutral Host Networks). The implementation complexity and interconnectivity of these distributed architectures raises several challenges for security, including identity-management, network access (e.g., 3GPP vs Non-3GPP), service authorization (i.e., network-slicing), confidentiality and privacy.

- **Diverse Technology Architectures**: the need for robust security has become a continuous challenge as a result of an amalgamation of virtualized and non-virtualized applications, new interfaces and protocol stacks, platforms and network types, a continuing trend towards greater virtualization, and cloud adoption for compute, storage, and cloud-native applications.

- **Multi-Dimensional Domain Interactions**: these different network domains, protocols, interfaces, associated platforms and applications are interacting at different layers to support corresponding network idiosyncrasies and service characteristics.



- **Distributed Security Architecture:** there are various hardware, software, and network-based security mechanisms that are being integrated into the service-based architecture, Radio Access Network, and the associated network elements and functions which may introduce implementation inconsistencies and extend the attack surface beyond the traditional local network boundary. Hence, Zero-Trust architecture (ZTA) and defense in-depth are key concepts that need to be adopted by the stakeholders including, operators, product vendors and enterprise users.
- **"Open Everything"-based Network Infrastructures:** an open-everything initiative with open-source software, hardware and standard interfaces has started to challenge the traditional proprietary approach of using one or two vendors in network implementations. Although this approach has its benefits, it also emphasizes the need for greater due diligence in product security and supply chain integrity. The GSMA NESAS[1] (Network Equipment Security Assurance Scheme) provides the foundation for such due diligence.
- **Software Architecture:** there is increased complexity in maintaining multiple software stacks in various components which are comprised of proprietary code, open-source software, 3rd-party middleware, and firmware, each with different patch and update modes along with network APIs (east-west & north-south interfaces) and cloud native container-based distributed micro-services.
- **Management evolution & orchestration:** the Management and Orchestration (MANO) function has shifted toward a virtualized cloud environment in order to manage various Network Virtualized Function-based platforms, interfaces and infrastructures across different architecture segments. Furthermore, security management continues evolving to improve visibility and constant monitoring, adapt to the new normal and abnormal behavioral patterns, automate responses to events, and simplify patch and update management. Streamlining event-data is crucial in this evolved ecosystem, since large amounts of event-associated data must be accumulated in order for AI/ML functions to perform effective event correlation and response.

- **Shared Operational Responsibilities:** with different network domains, products and business partnerships, the responsibility for managing these different segments falls to different organizations, including mobile network operators, internet and cloud service providers, suppliers, and enterprise organizations. As such, supply chain security and maintaining an integrated operations model becomes a much greater concern in this converged ecosystem.
- **Sundry Device Types:** a wider variety of end-user devices (e.g., 3GPP compliant, Wi-Fi certified) and IoT devices (e.g., sensors, wearables) are interfacing with the private and public infrastructures. Each device has different compute and storage capabilities which dictate the level of security and reliability that can be supported. As such, corresponding security device requirements need to be identified as part of an organization's network strategy.
- **Multiple Supply Chains:** the suppliers of these devices, software, networks and associated operational entities rely on many different supply chains with multiple known and unknown subordinate suppliers. This, in turn, enlarges the attack surface and requires greater due diligence.

Evolved heterogenous networks need to address the following challenges:

- Lack of a comprehensive coexistence network access model that covers discovery, interference, communication, quality of service, and security across all of these technologies. Coexistence interworking specifications and initial products continue to evolve.
- Predictable user network access experience is not guaranteed across 5G, LTE, and Wi-Fi 6/6E/7 wireless technologies that have different strengths and weaknesses around performance, reliability, and security.
- The interfaces between the private and public networks are sometimes inefficient, and lack interoperability and transparency. The user is tasked with the challenge of selecting the best available wireless technology by relying on IT departments, service providers and marketing materials. Organizations need to gain greater insight into the complexity and inter-dependencies of their local and end-to-end implementations in order to implement adequate security controls.
- Security controls at the signalling and transport layers may vary between technologies and service provider implementations. For example, during initial network signalling in a 5G-Non-Standalone configuration, user plane encryption between the user device and the network may or may not be enforced. Similarly, Wi-Fi implementations may optionally enforce security controls (e.g., authentication, encryption, segmentation). Lastly, end-to-end confidentiality and integrity is difficult for end users to verify the security and privacy controls in the current public ecosystem.

The Current Security Landscape

To identify the security implications of 5G and Wi-Fi 6/6E/7 coexistence or convergence, it is necessary to understand the current security standards of these networking technologies (5G/CBRS/ Wi-Fi 6/7), architectures and product features. The identification, categorization, and prioritization of the associated threats within the mobile ecosystem helps define and implement functional controls to mitigate the corresponding threats. The primary threats can be segmented into the following categories: service disruption, traffic analysis, and unauthorized access.

- **Service Disruption** - Denial-of-Service (DoS) attacks aim to disrupt network communications and services, and can affect network nodes, mobility managers, service managers, applications, and users. Disruption attacks can be launched against the radio interfaces (e.g., interference/jamming), network infrastructure interfaces and associated protocols (e.g., signalling, transport, media), network devices and functions and network services. These attacks can propagate across network boundaries and impact other networks.
- **Traffic Analysis and Eavesdropping** – This threat category entails the interception of mobile communications (e.g., signalling messages, user data, traffic patterns) by unauthorized third parties. For example, a device may transition from a 5G New Radio-Unlicensed network to a public Wi-Fi network which may not support adequate protection mechanisms and consequently subject user communications to man-in-the-middle attacks or traffic analysis and disclosure.
- **Unauthorized Access** – This threat is applicable to devices, network elements, network interfaces and network protocol stack layers. Although device and network element security is important, it is considered a critical administrative and management responsibility supported by MANO systems.

The threat actors can be broadly classified into four major categories – criminals, hacktivists, nation states, and insiders. The first three reside outside a network's

operational perimeter. The cyber criminals are primarily interested in monetary incentives. The cyber-hacktivists target specific entities with a goal of data theft or vandalism to tarnish an organization's reputation. The nation-state actors also target specific entities - especially foreign governments and corporations - with the goal of espionage, intellectual property theft, information manipulation, and destruction. The insiders can cause the most damage to a system and organization. The major risk is due to access policies, as these actors can turn rogue anytime. They are mostly employees or third-party contractors who are looking for revenge, profit gains, or are under external pressure. For targeted entities, nation-states can also introduce persistent hardware or software implants via supply chain vulnerabilities that allow zero-day access.

Palindrome Technologies offers a holistic approach to security analysis and verification testing . We use deterministic and non-deterministic security evaluation methods along with a combination of commercial, proprietary, and open-source tools to conduct security analyses at various layers including hardware, firmware, operating system, middleware, application and protocol stacks (i.e., signaling and control plane). To bring realism to the discussion, Figure 2 highlights areas where vulnerabilities are identified during testing various 4G and 5G products and functions. It highlights the need for robust security testing and a strong **Secure Development Lifecycle** program by all stakeholders.

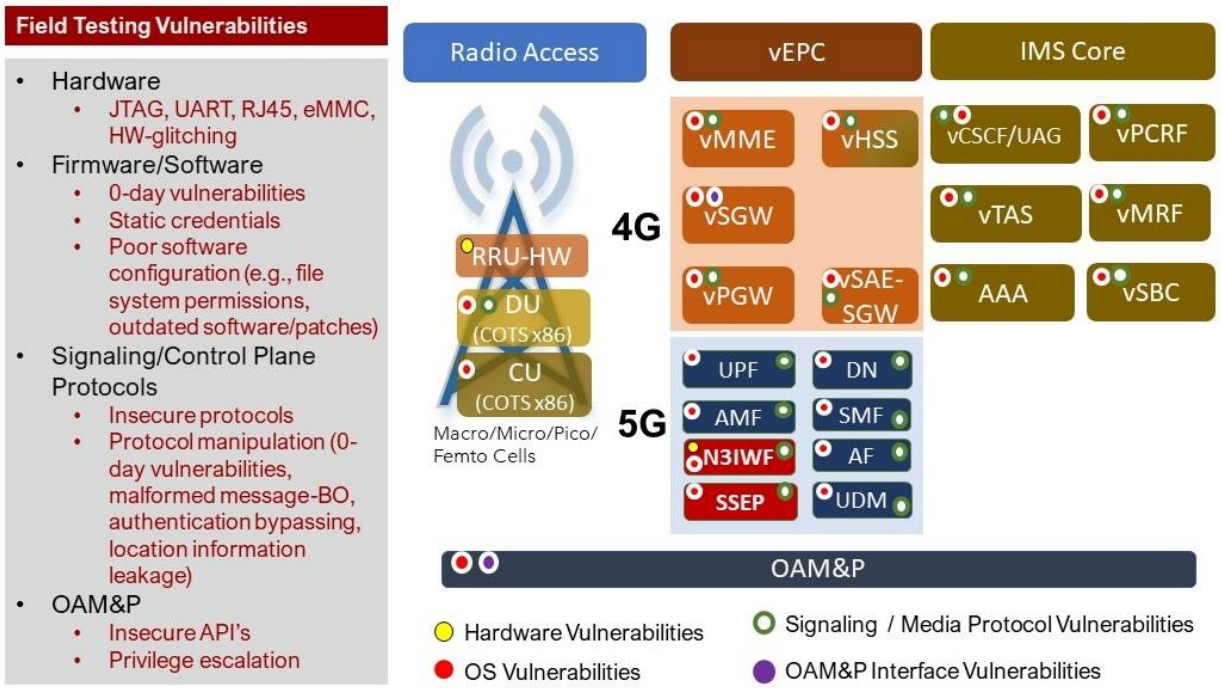


Figure 2: Security vulnerabilities in 4G & 5G Product/Function Testing

Beyond a focus on the individual product components of these technologies, there are many sub-architectures, such as edge and public cloud-based services and radio access network (RAN) elements, that also impact the overall security of the network

infrastructure and services. As an example of scaling up the threat landscape, Figure 3 identifies the major risk areas that require management in the 5G ecosystem, spanning from the UE through external interfaces to other networks and applications. Some of the risk areas are directly related to this work and include security of the UE (i.e., communications stack and supporting functionality) and the interworking functions and interfaces in coexistent networks.

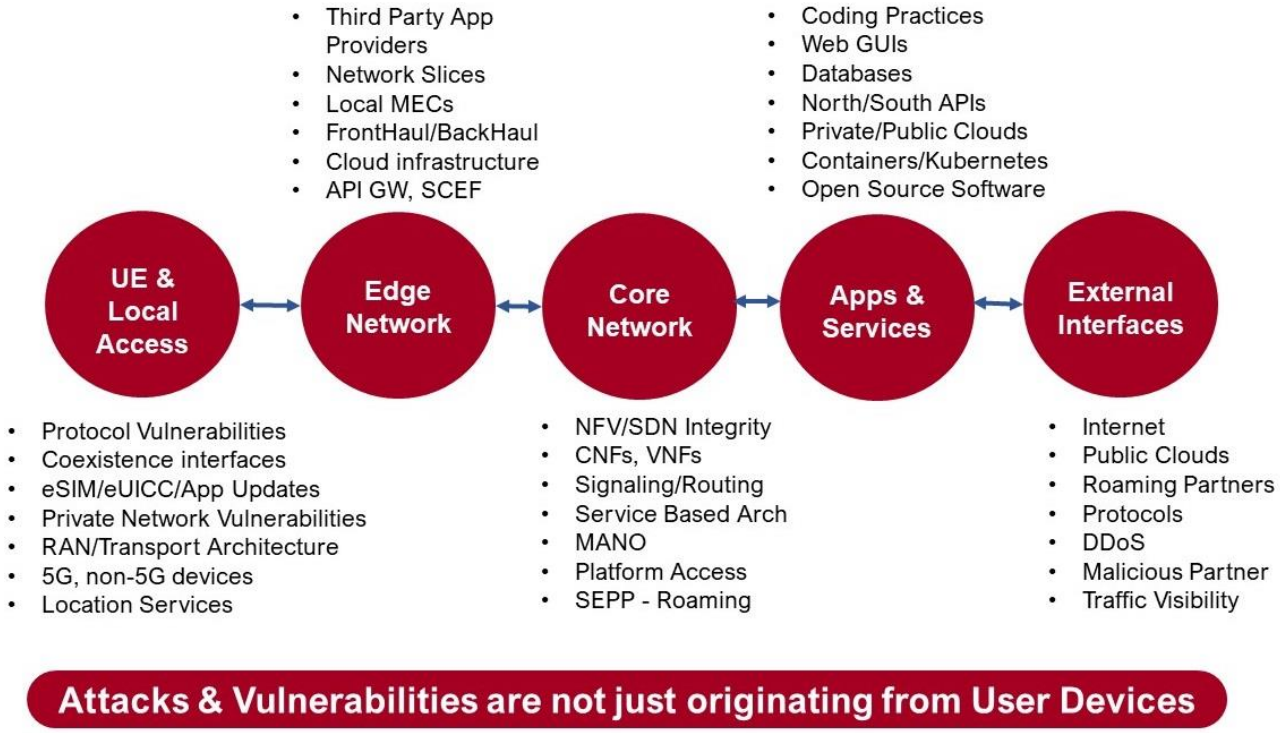


Figure 3: 5G Risk Areas

Holistic View

We need to recognize that considerable work has been completed in developing security architectures and specifications for securing 5G, Wi-Fi 6/6E/7 and CBRS. For example, 3GPP has specified a comprehensive 5G security architecture captured in various principles:

- Use of mutual authentication and authorization confirming that the sender and receiver have established trust and the end-to-end relationship is secured.
- Interworking between 4G functions and databases and 5G functions and databases are segmented, and firewalls provide filtering of service-supporting messaging.

- An open network with available interfaces (e.g., APIs) is presumed and the integration of third-party products and processes will be enabled to increase security.
- Both intra- and inter- network traffic should be encrypted.
- Subscriber identity throughout the different interactions will be provided to prevent location tracking attacks prevalent with previous mobile generations.
- End-to-end isolation and integrity in RAN, transport network and core network to protect users and applications is provided.
- Securing new 5G signaling protocol stacks
- For coexistence approaches, leveraging different authentication and authorization schemes to manage trusted and untrusted users and service requests (e.g., network slicing).

We need to operationalize the security architecture into a holistic framework to address all of the architectures, sub-architectures and components of the heterogeneous environments. Figure 4 provides a list of key focus areas.

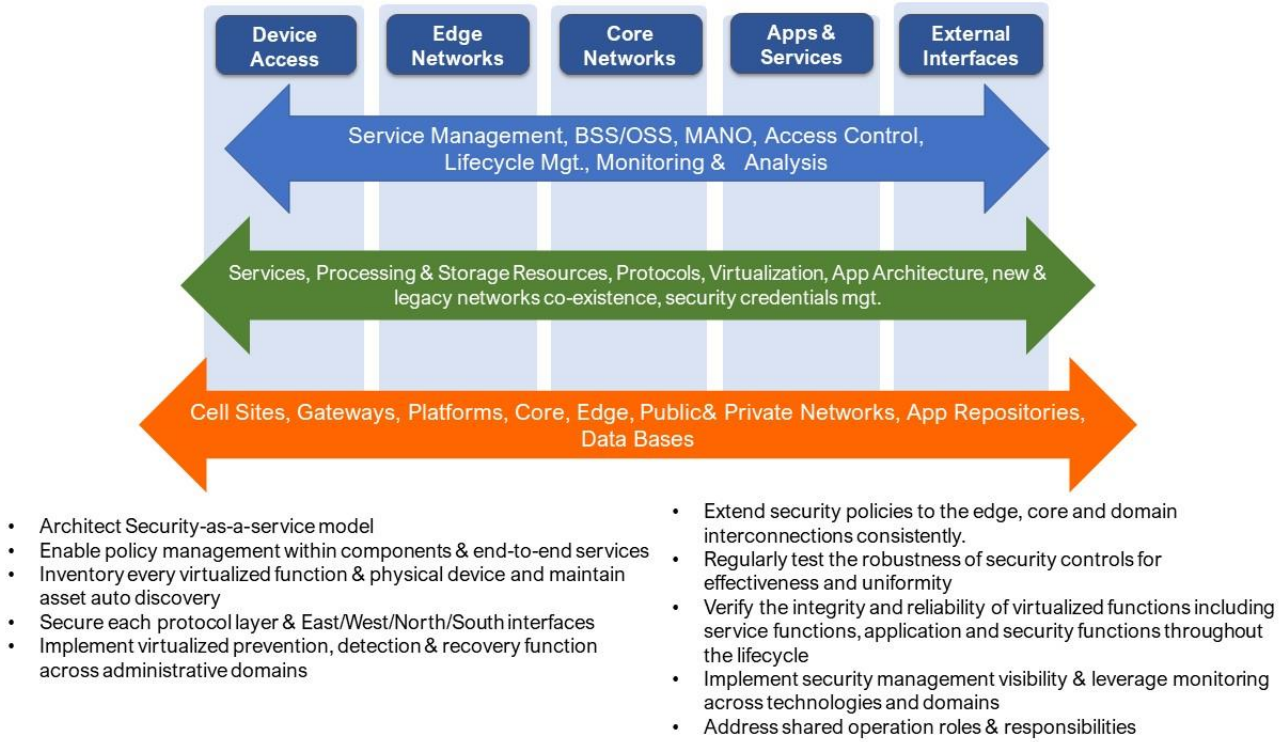
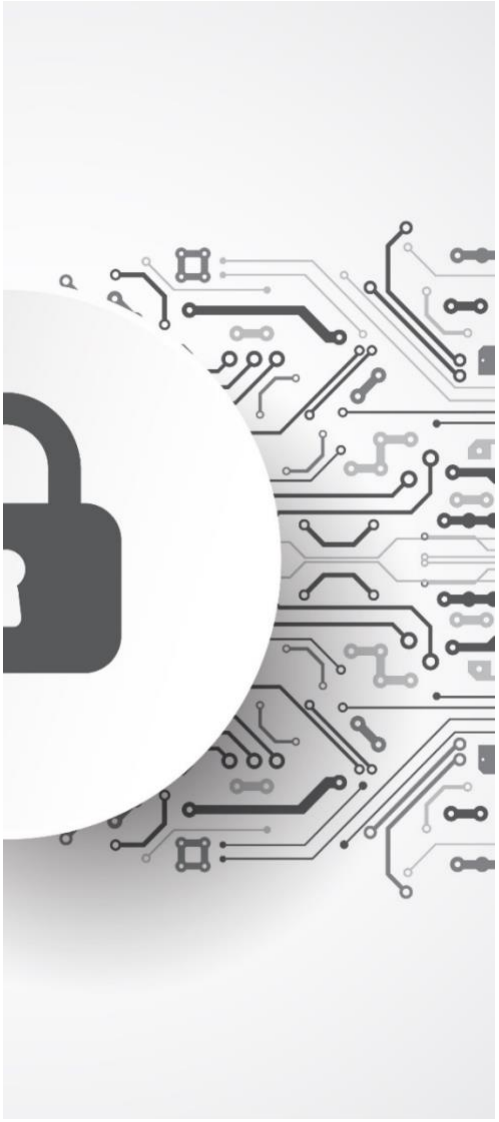


Figure 4: Holistic Security Framework

The Path Forward: Eleven Critical Areas to Address

There are many aspects of these technologies that will have security impact on mobile users, carriers, suppliers, and enterprises. Palindrome Technologies works with partners, customers, and industry groups to extend and enhance existing security approaches, with the goal to address the risks with legacy and new devices, networking, applications and physical facilities supporting the offered services and functionality. To address the challenges discussed in this paper we believe the key focus areas include:

- **Transparency –** Visibility into the security of products, deployments, and user services is required so that risks can be determined and the appropriate security controls implemented.
- **Maturing Threat Modeling –** Applying new frameworks to mobile networks, such as the MITRE ATT&CK™ framework, is a promising start to provide a more complete view of threats.
- **Ongoing Security Research** – New attack vectors and zero-day vulnerabilities are being discovered constantly, and testing and analysis efforts need to continue.
- **Enhanced security testing & processes –** The evolution of the GSMA Network Element Security Assurance Scheme (NESAS), as well as other testing approaches under development, need to be encouraged and implemented.
- **Coexistence Policy Management –** The interworking across private/public domains and among various network technologies needs further research to ensure that consistent security policies are being defined and enforced within local domains and across global connections.
- **Zero Trust Architectures (ZTA) –** the application of ZTA within these communication technology domains requires further study to enable the development of integrated defenses that meet security, business and operational requirements.
- **Software Architectures –** the underlying virtual and containerized applications, open-source components and service mesh middleware are creating complex



security issues where new security approaches are needed.

- **Standards and Specifications –** 3GPP, and industry forums (e.g., OnGo Alliance, GSMA, IETF, IEEE) continue to evolve standards and specifications. Gaps and mandatory/optional requirements need to be adequately identified and addressed.
- **Securing key areas such as Roaming, Interconnection, Slicing –** Ongoing GSMA activities are addressing the security elements of these areas and they need to continue.
- **UE security –** with all of the different applications and profiles that have a bearing on the user's interactions with these different network technologies, the UE security and lifecycle management continues to be of paramount importance.
- **New Technology Vetting –** these heterogeneous networks are very complex to manage and Machine Learning is being touted as a key component of advanced management systems. The ability to test, analyze and secure AI/ML system is in its infancy. More research has to be done before these systems are fully operationalized.

About Palindrome Technologies

Since its inception in 2005, Palindrome Technologies has earned a reputation as a trusted provider of cybersecurity services for top organizations spanning complex telecommunications networks to high assurance environments. Palindrome brings a meticulous discipline to cybersecurity through applied research, scientific analysis, and rigorous testing. With an unwavering commitment to excellence, Palindrome enables clients to operate with confidence in an insecure world. Visit www.palindrometech.com.