Palindrome Technologies

Emerging Communications Networking Trends & Cybersecurity Challenges

Communication networking technologies are going through a dramatic transformation for both 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 (WiFi, 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 need to continue to address to enable secure deployments countering the evolving threat environment.
- Examples of **security research** that needs to continue to improve the state-of-the-art in holistic security approaches.

Palindrome Technologies

Table of Contents

The Emerging Wireless Network Technology Landscape

The public telecommunications infrastructure is going through a dramatic transformation. The existing 4G Long-Term Evolution (LTE) is incapable of supporting the formidable requirements (e.g., bandwidth, speed, scalability) of emerging technologies such as Internet of Things (IoT), Vehicle to everything (V2X), new multi-media devices (e.g., smartphones, tablets), real-time streaming services (e.g., Virtual Reality/Augmented Reality, Telemedicine) and demanding enterprise applications. In order to facilitate the evolution of these emerging technologies the Fifth Generation ("5G") of mobile technology has been introduced. 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) higher system capacity, 2) higher data rates at gigabits per second, 3) reduced latency targeting (under 10 milliseconds), 4) massive device connectivity and 5) improved security. The interplay of these technologies, architectures and capabilities will reorient 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 will adopt private 5G and hybrid (i.e., combination of public and private network resources) deployments and in certain cases WiFi 6/6E. 5G networks, using private network deployment configurations, are going through tremendous growth to support commercial enterprise and government use cases including industry

automation, IoT devices, Augmented Reality/Virtual Reality (AR/VR) and new communication services. The network elements supporting a private 5G network will be managed by the enterprise organization, or a service, and will support mission critical and non-critical application requirements including reduced latency, higher speeds, greater coverage and control, defined 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 the Citizen Broadband Radio Service (CBRS) will be leveraged (e.g., building automation, maritime operations) to offer private LTE/5G-NR in support of commercial and government enterprise applications. CBRS uses band 3550-3700 MHz which is a part of the radio spectrum that the FCC identified as being used sparingly by the U.S. government and other entities. The band was identified as additional frequencies to be used for shared wireless private broadband. 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 for alternative broadband access, to help increase mobile capacity, 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 transporting from one location to another.

WiFi is ubiquitously used to provide connectivity to a myriad of use-case scenarios from residential networking, enterprise environments, public hotspots, smart city applications, industrial and factory automation, etc., and has become an indispensable part of day-to-day networking and connectivity. Wi-Fi was initially permitted to operate in the unlicensed ISM (Industrial Medical

Scientific) bands of 2.4 GHz and 5 GHz spectrum by the FCC (Federal Communications Commission). 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 of wireless networks focusing on increased spectral efficiency, throughput, and improved latency. But as Wi-Fi network deployments continue to grow, Wi-Fi networks faced many challenges including congestion, restricted wideband channel availability and legacy device support.

In order to sustain Wi-Fi's rate of growth, the WiFi 6 and 6E versions were specified. The potential use of the 6 GHz spectrum 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. The 6GHz wireless spectrum uses shorter wavelengths which support faster data transfers but they do not travel long distances. This will make real WiFi 6/6E networks likely to use both 6GHz and 5GHz bands to deliver fast, reliable connections throughout an office building. WiFi Protected Access 3 (WPA3 Support for WPA3 is mandatory for Wi-Fi 6 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 emerging wireless network technologies (i.e., 5G, WiFi 6/6E, CBRS) is defining 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 the 3GPP specification[1] of an emerging Wireless LAN (WLAN) integration architecture for untrusted and trusted WLAN integration with the 5G Core (5GC). Figure 1, illustrates 3GPP and Non-3GPP access to the 5G Core.

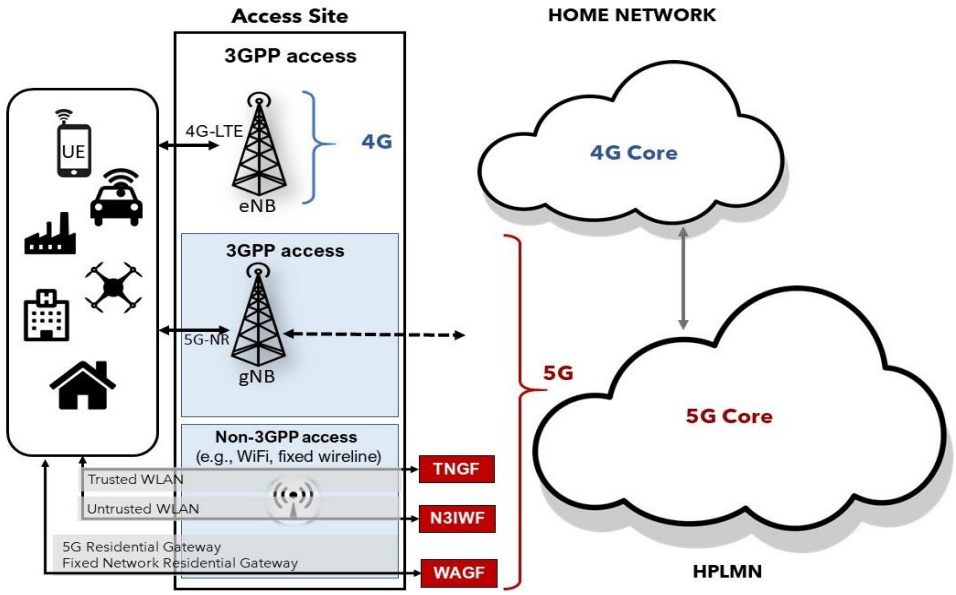
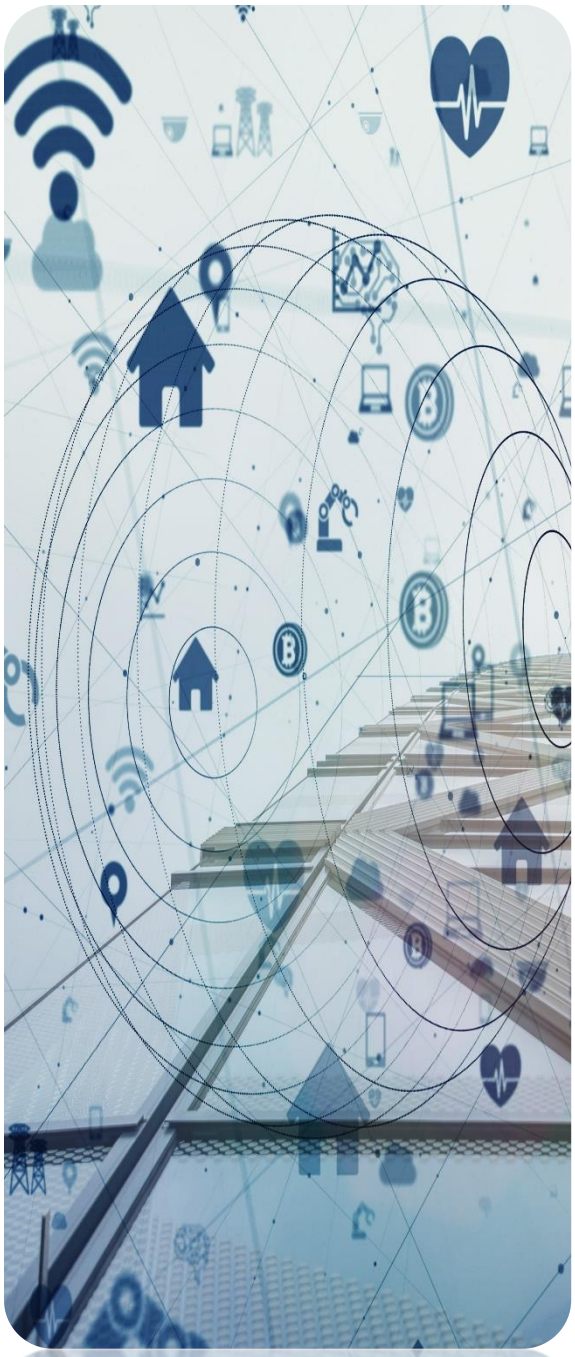


Figure 1 3GPP vs Non-3GPP access

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 discovered, an end-user device may decide to use untrusted or trusted WLAN access to establish connectivity with the 5GC per organizational policy specifications. This coexistence approach has to accommodate 5G network policies for access and route selection, along with applying QoS to the 5G data flows carried over the WLAN access.

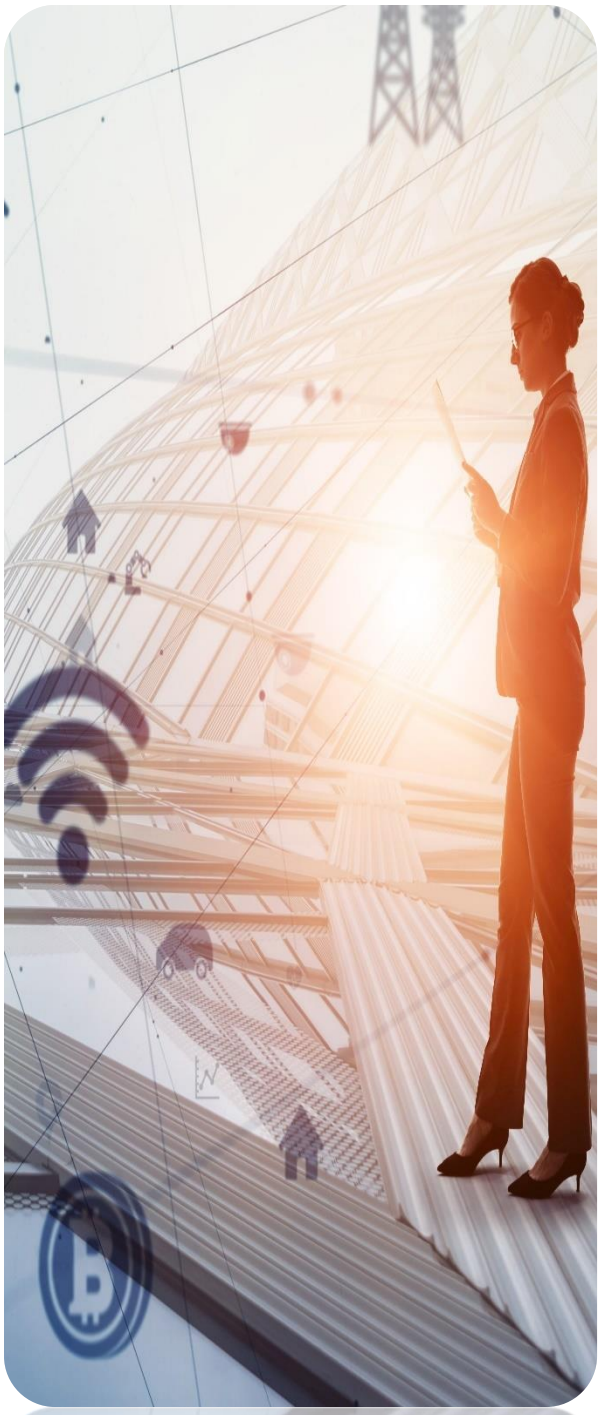
[1] 3GPP TS 23.501, System Architecture for the 5G System, Release 17, 2021.

This coexistence introduces several challenges including technical, architectural and operational and need 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:** there is an amalgamation of virtualized, and non-virtualized applications, platforms and networks with a growing trend (50% to 80% in the next year) towards greater virtualization and cloud (of compute and storage resources), cloud native applications and new protocol stacks and interfaces that need to be secured and sufficiently robust to prevent service disruption.
- **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 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 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:** Management and Orchestration (MANO) functions are moving towards a virtualized cloud environment in order to manage various Network Virtualized Function-based platforms, interfaces and infrastructures across different architecture segments. Furthermore, security management is evolving to improve visibility and constant monitoring, adapt to the new normal and abnormal behavioral patterns, and automate responses to events and patch and update management. Streamlining event-data will be crucial in this evolved ecosystem, since large amounts of events are expected to be accumulated and ultimately machine learning will be paramount in event correlation and response.

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

The challenges in the evolved heterogenous networks that need to be addressed include:

- 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 specification and initial products are still emerging.
- Predictable user network access experience is not guaranteed across various wireless technologies (e.g., 5G, LTE, Wi-Fi 6/6E) that have different strengths and weaknesses around performance, reliability, and security.
- The interfaces between the private and public networks are sometimes inefficient, lack interoperability and not transparent. 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 on 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 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 coexistence or convergence, it is necessary to understand the current security standards of these networking technologies (5G/Wi-Fi 6/CBRS), 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: unauthorized access, traffic analysis and service disruption.

- **Service Disruption** - Denial-of-Service attacks aim to disrupt the services and network communications 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 actors reside outside a network operational perimeter. The cyber criminals are mostly 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 a goal of espionage, intellectual property theft, information manipulation, and destruction. The insider actors can cause the most damage to a system. The major risk is due to access policies, as these actors can turn rogue anytime. They are mostly employees or third-party contractors that 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 multi-dimensional approach to security analysis and verification testing services to carriers, services providers, suppliers and enterprise organizations. We use a combination of commercial, proprietary and open source tools to conduct security analysis and testing at different 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 provides results from 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 of the stakeholders.

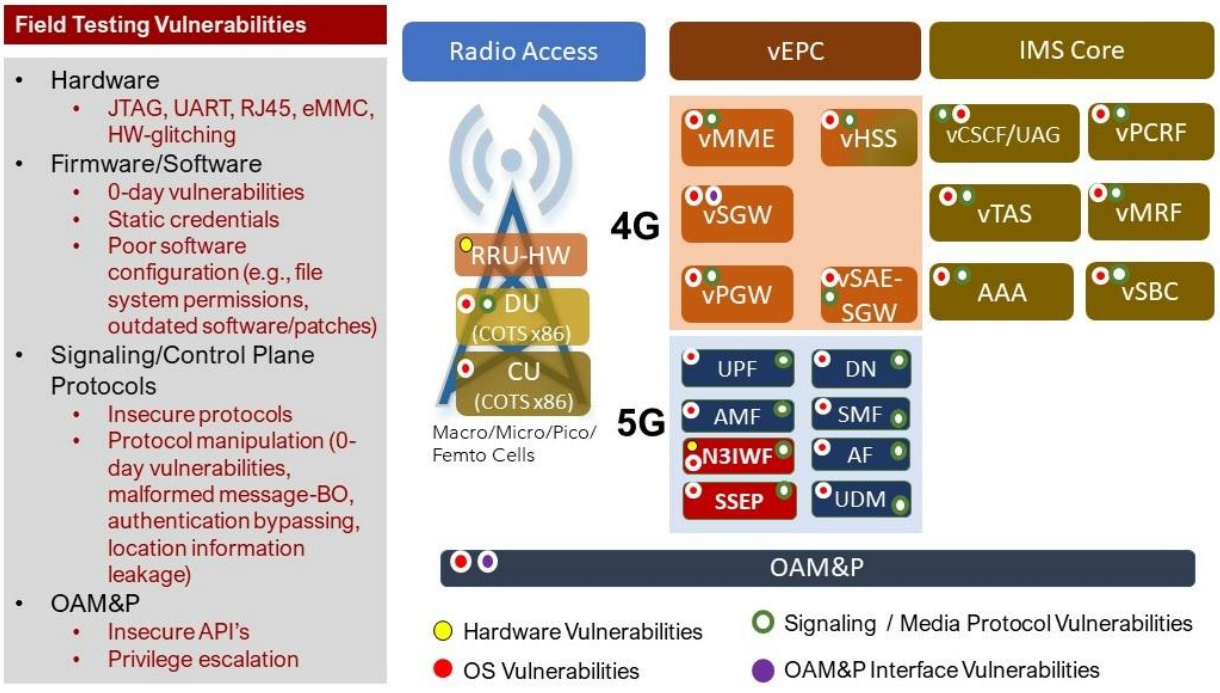


Figure 2 Security Results of 4G & 5G Product/Function Testing

Besides focusing on individual product components of these technologies, there are many sub-architectures (e.g., edge and public cloud-based services, 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 picture, Figure 3 identifies the major risk areas that need to be managed 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.

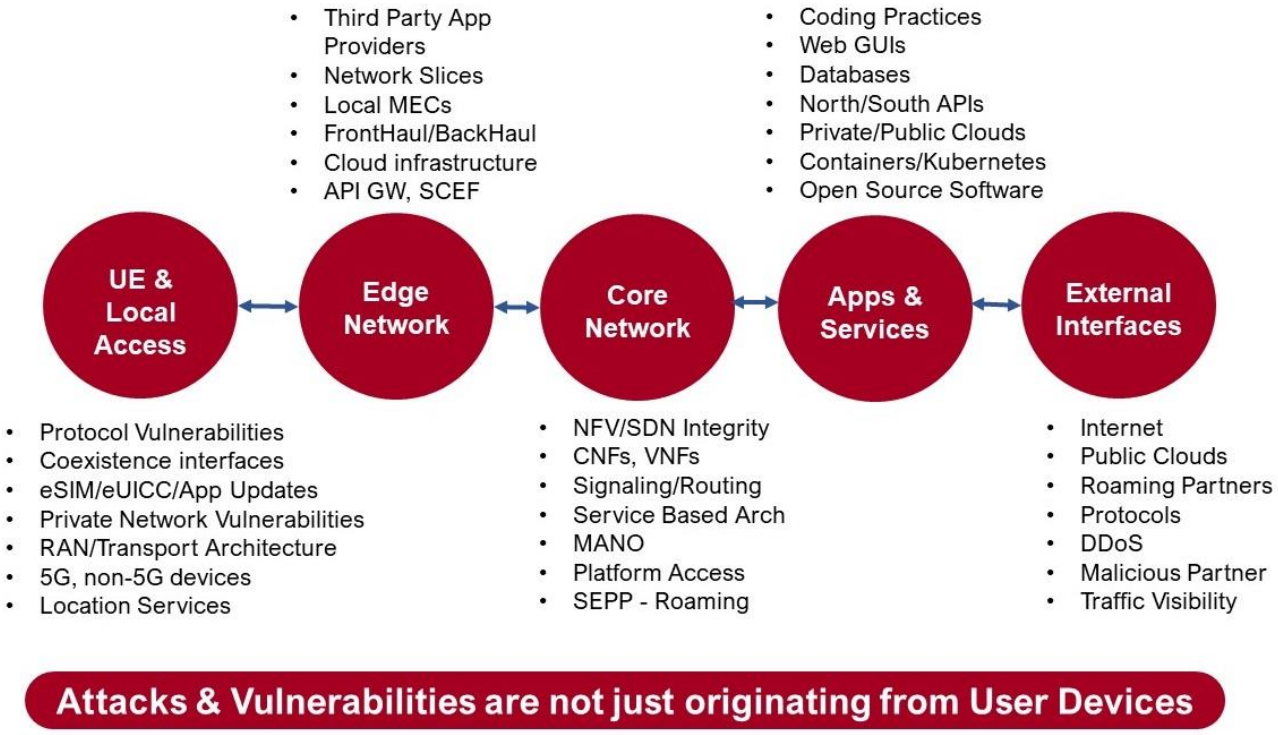


Figure 3 5G Risk Areas

Holistic View

We need to recognize that there has been considerable work in developing security architectures and specifications for securing 5G, WiFi 6/6E and CBRS. For example, the 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 are being implemented
- For coexistence approaches, leveraging different authentication and authorization schemes to manage trusted and untrusted users and service requests (e.g., network slicing) is an evolving requirement.

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.

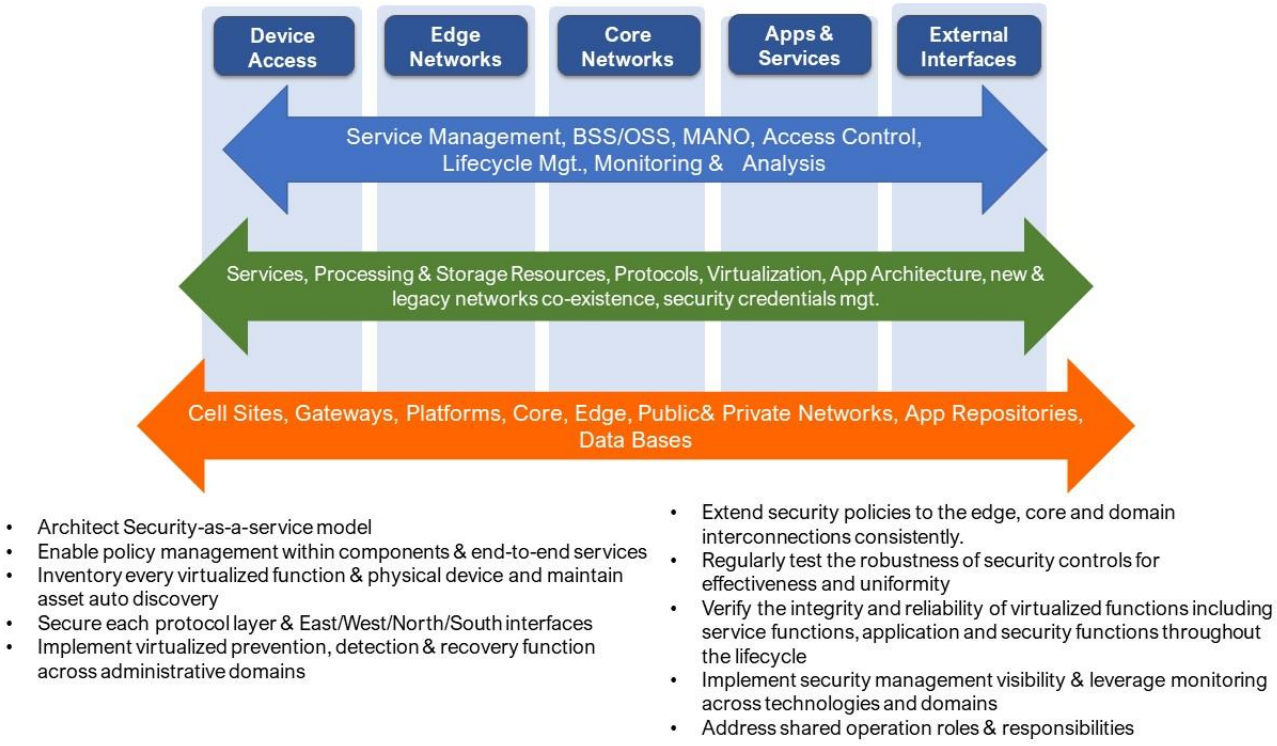
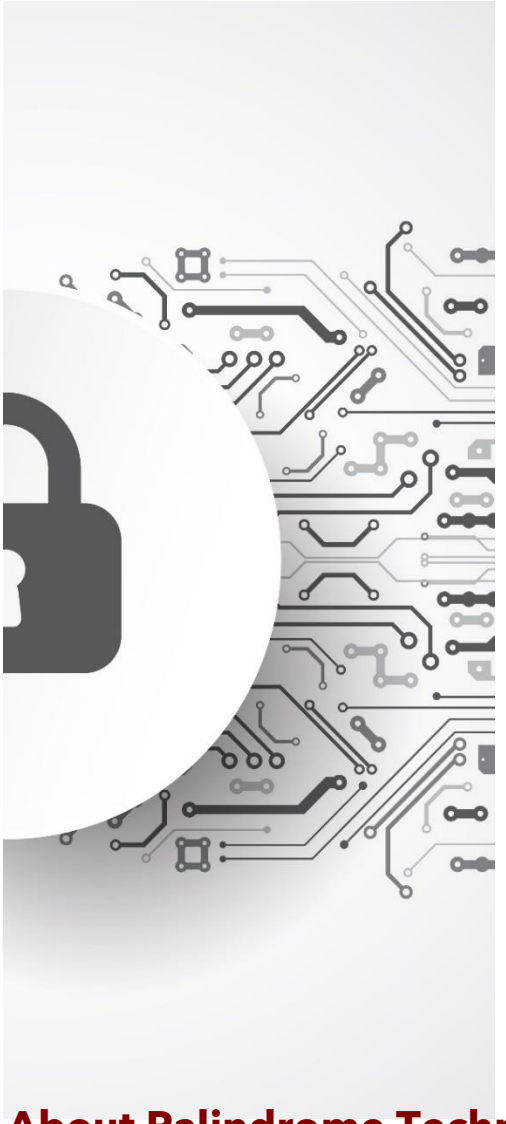


Figure 4 Holistic Security Framework

Path Forward: Eleven Critical Areas to Address

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

- **Transparency –** there needs to be visibility into the security of products, deployments, and user services so that risks can be determined and the appropriate security controls implemented
- **Maturing Threat Modeling–** Applying new frameworks such as MITRE ATT&CK™ framework to mobile networks 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 all of the time and the testing and analysis efforts needs to continue
- **Enhanced security testing & processes –** the evolution of the GSMA Network Element Security Assurance Scheme (NESAS), and other testing approaches being developed need to be encouraged and implemented.
- **Coexistence Policy Management –** the interworking across private/public and 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 communications technology domains needs further study to be able to build integrated security that meets 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) continue to evolve standards and specifications and gaps and mandatory/option requirements need to be adequately identified and addressed
- **Securing key areas such as Roaming, Interconnection, Slicing –** there are ongoing GSMA activities that are addressing the security elements of these areas and they need to reach closure
- **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 future 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. They bring a meticulous discipline to cybersecurity through applied research, scientific analysis, and rigorous testing. With an unwavering commitment to excellence, they enable clients to operate with confidence in an insecure world. Visit www.palindrometech.com.