# 5G technologies create the most secure wireless networks

**By Chris Pearson, President, 5G Americas**

July 31, 2019

Security has always been at the forefront of mobile communications networks. It is the immune system which keeps a cellular network and ecosystem running. Yet, with each new generation of networking technologies, sophisticated hackers drive the need to build a bigger and better mousetrap. Staying one step ahead of some of the most creative “bad actors” in the world requires constant vigilance, dedication and continuous improvement in skills, hardware and technology.

I’ve been around the block a few times, seeing each new generation of wireless technology improve security capabilities from the previous generation. This current 5G generation is a bit different because, compared to those before, 5G networks are not just about being faster, bigger and better. They’re also about managing a colossal ecosystem of different services, applications and uses.

5G Americas’ latest white paper, [The Evolution of Security in 5G](http://www.5gamericas.org/files/4715/6450/2267/5G_Security_White_Paper_07-26-19_FINAL.pdf), takes a deep dive into the incredible world of 5G security. In it, we explore how networks will be dealing with services and uses that will have different stringent security requirements. For instance, the real-time security requirements for a vehicle-to-vehicle/infrastructure/environment (V2X) will be much different than that of a network slice managing predominantly video conferencing in an office.

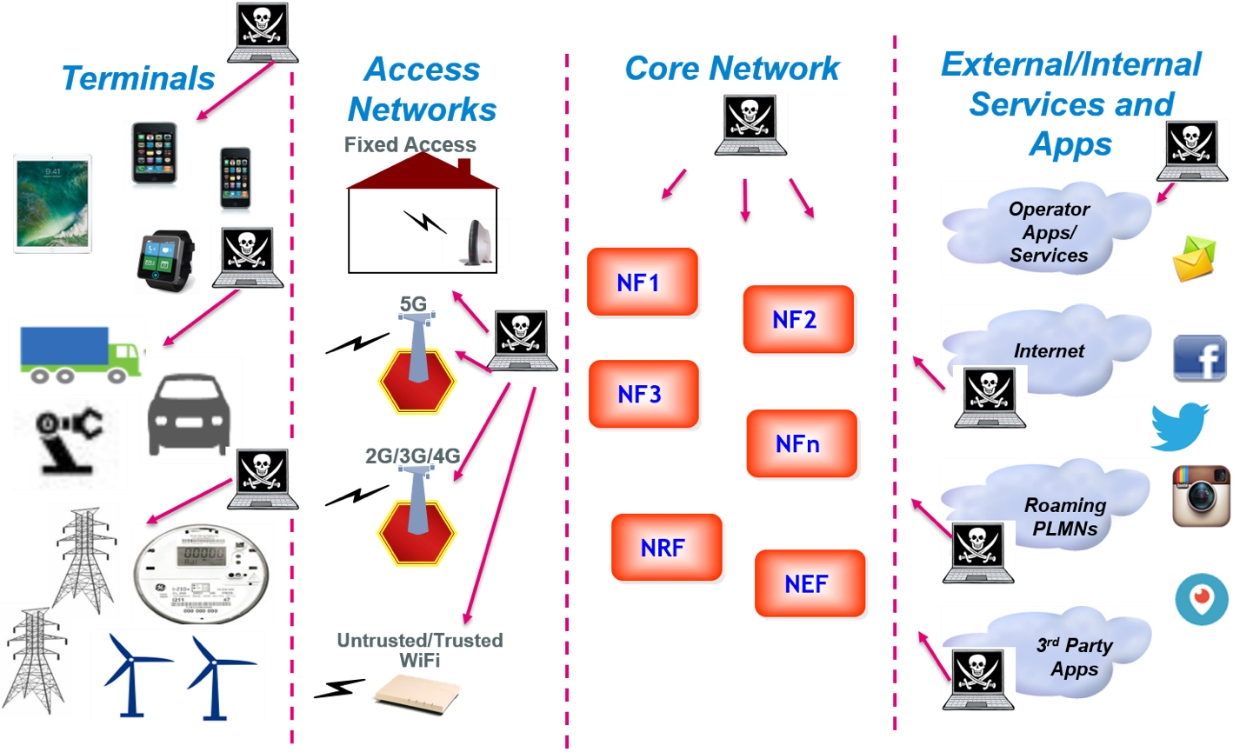
As of July 19, 2016 there are 23 5G commercial network deployments around the world. In most every use case, 3GPP-developed 5G standards provide far and away the strongest, most robust sets of protections compared to other network architectures. Indeed, 5G doesn’t just provide incremental improvements to security, it provides new ***transformational security safeguards*** to protect networks, devices, services and customers.

3GPP has created new 5G security standards that include enhancements for encryption, mutual authentication, integrity protection, privacy and availability. These enhancements make improvements throughout the network, targeting the user plane, control plane and management traffic with a variety of improvements, such as:

* **Unified authentication framework** that enables seamless mobility across different access technologies and support of concurrent connections
* **User privacy protection** for vulnerable information often used to identify and track subscribers (for example, SUPI, IMSI, and IMEI)
* **Secure Service-Based Architecture and slice isolation** optimizing security that prevents threats from spreading to other network slices
* **Improving SS7 and Diameter** protocols for roaming.
* **Adding native support for secure steering of roaming** (SoR), allowing operators to steer customers to preferred partner networks – improving the customer experience, reducing roaming charges, and preventing roaming fraud.
* Improved rogue base station **detection and mitigation** techniques
* And even **more proprietary operator and vendor analytics** solutions that offer additional layers of security.

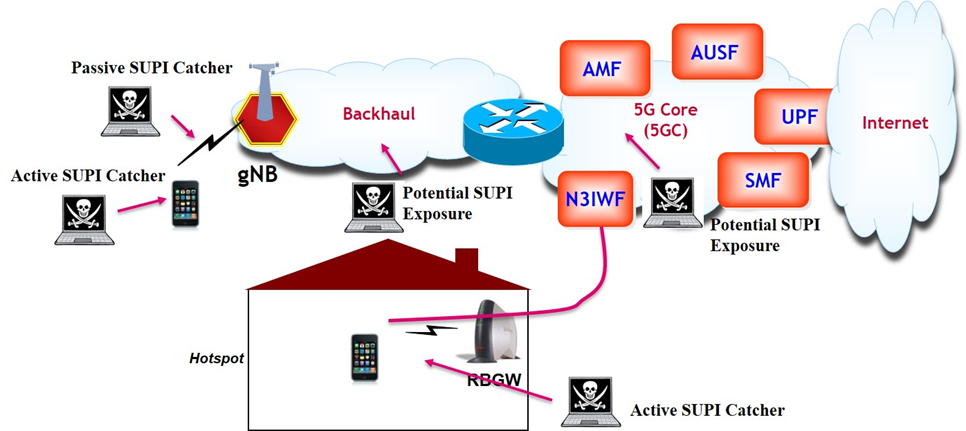
But why all the additional scrutiny? According to [Cisco](https://www.cisco.com/c/en/us/products/security/security-reports.html#~stickynav=2), thirty-one percent of organizations have experienced cyber-attacks on operational technology infrastructure. [Symantec](http://images.mktgassets.symantec.com/Web/Symantec/%7B3a70beb8-c55d-4516-98ed-1d0818a42661%7D_ISTR23_Main-FINAL-APR10.pdf?aid=elq_) believes there are around 24,000 mobile apps blocked every day. Modern networks experience threats from a wide variety of different sources and attack routes – and the quantity and quality of these attacks typically increase each year.

Sophisticated attackers understand there are vulnerability points in any network, which can include user devices or equipment, radio access networks, mobility or “edge” threats, network core, secure gateway internet LAN firewall, roaming, or air interfaces.



*5G Threat Landscape: Numerous vulnerability points in wireless networks*

At each vulnerability point, there are potentially several different types of threats, which can include attacks on authentication, integrity, network availability or privacy that range from message blocking, denial of service, or man-in-the-middle techniques or more. For instance, for an attack involving a wireless subscriber’s privacy alone, there are numerous points in which a customer’s Subscription Permanent Identifier (SUPI) number on his or her device could be exposed or captured.



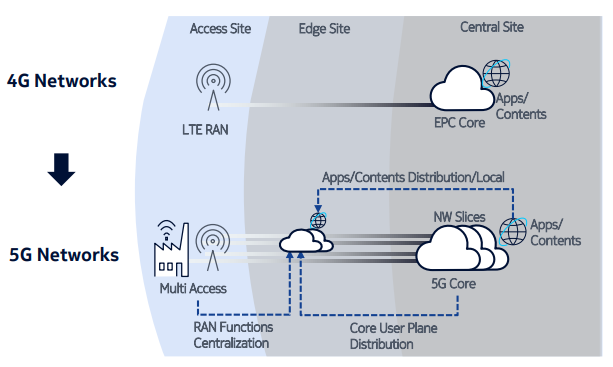
*Exposure points compromising subscriber privacy.*

When it comes to the Internet of Things, the threat surface becomes very broad indeed. Targets of vulnerability within a network involving IoT devices can attack several different layers, including service, application, node/platform, network/transport, or the IoT device itself. Massive IoT requires even more vigilance with the proliferation of the massive quantity of devices and sensors.

With all these points of exposure and vulnerability threats, security can put significant strain on network operator resources. Fortunately, mobile wireless operators do not need to re-invent the wheel.

5G security [builds on](https://www.ericsson.com/en/blog/2019/7/3gpp-5g-security-overview), and is compatible with, key functions and frameworks developed in 4G and other standards. Indeed, innovations in 4G LTE are at the very the foundation of security improvements in 5G. In Release 8, the Third Generation Partnership Project (3GPP) added a variety of advanced security/authentication mechanisms via nodes such as the services capability server. Release 11 provided even more capabilities to enable secure access to the core network.

Additionally, 5G Radio (NR) can be “plugged” into a 4G core and coexist with 4G radios as part of an existing network, even as edge computing creates additional nodes at network edge sites. In addition, 5G allows for a proliferation of access technologies of all types with data speeds from Gbps to Kbps, licensed and unlicensed, that are based on wide swaths of spectrum bands and include technologies specified by standards bodies other than 3GPP.



*Evolution of 4G to 5G builds out edge computing distribution*

Finally, 5G offers amazing new security capabilities for networks that use network slicing via software defined networking (SDN). In network slicing, virtual networks are created, allocating compute, spectrum, and other data management capabilities to provide just the right amount of resources necessary. 5G provides two types of isolation: resource isolation that lets a slice remain available when others may become overloaded, and security isolation which ensures a slice is quarantined – much like bulkheads in a submarine are used for compartmentalization to prevent it from sinking.

These are heady times for the mobile wireless industry with tremendous opportunities in the front of us. You can’t turn a corner without seeing a 5G article. I’ve never been more confident that the industry is doing everything in its power to protect citizens and wireless customers throughout the Americas and beyond.

Chris Pearson

President, 5G Americas

*###*