5G POLICY PRIMER: FUTURE WIRELESS NETWORKS WILL HAVE UNPRECEDENTED SECURITY

Our economic and social lives rely on connectivity, so policymakers rightly wonder whether the wireless networks of the future are being designed and built with security in mind. This Policy Primer explains how the intersection of several innovations in network design and wireless technology will create a secure and resilient future as the nation moves to 5G. As we transition from centralized core and radio access networks to distributed, virtual networks, we will have more agile and layered security. Significant strides were made to address security in LTE networks, and now industry is building in additional capabilities, like stronger encryption and embedded protections from Distributed Denial of Service (DDoS) attacks, across the network.

EVOLVING GLOBAL CYBERSECURITY THREATS WILL BE MET WITH DESIGN ENHANCEMENTS

Wireless network operators face an array of security threats and challenges that exploit our interconnectedness, from DDoS attacks[1] to malware targeting customers. Cyber threats continue to grow, both in number and sophistication. The threats are serious, often launched by highly resourced intelligence services abroad, organized criminal networks, and entities seeking to disrupt domestic and global communications networks. Because connectivity is so essential to economic and national security, the U.S. communications sector has been using cybersecurity tools and best practices for years, developing innovative methods to defeat those who try to do harm. Carriers use filtering, re-routing, scrubbing, firewalls, and other cutting-edge techniques to protect networks and consumers. The industry also collaborates[2] because attacks change and adapt to defensive measures, so collective defense benefits everyone.

U.S. network operators have successfully managed vulnerabilities and attacks. As operators evolve their network design and wireless technologies, they are aggressively building in security and are structuring networks in a distributed manner that virtualizes functions so that critical functions can be processed at the network's edge in near real-time. This move to distribution and virtualization, coupled with security attributes built into new wireless telecommunications protocols, offers the promise of flexible, secure networks.

THE DIFFERENCE BETWEEN 5G AND PREVIOUS WIRELESS TECHNOLOGY

There are some significant key characteristic and architectural differences between 5G and 4G LTE, impacting the Radio Access Network (RAN), Core, and Edge. The 5G RAN supports a new larger antenna array known as Massive Multiple Input Multiple Output, and the 5G RAN components are decoupled and distributed. The 5G core network features new design configurations, such as network slicing, to support the unique 5G services. And 5G introduces a new network segment, the Mobile Edge, to enable next generation ultra-low latency and high bandwidth applications. The Mobile Edge includes elements traditionally part of the RAN and Mobile Core. These architectural improvements, including the Mobile Edge, will provide enhanced security capabilities in 5G such as:

MYTH: SOME BELIEVE THE MOVE OF 5G TO THE EDGE WILL MAKE NETWORKS LESS SECURE.

REALITY: To the contrary, network virtualization, edge computing power, device management, and automated threat detection and response will create **more flexible and secure networks.**

√ Stronger 3GPP encryption for over-the-air interface to enhance the security between the 5G mobile devices and the 5G network.

√ Roaming or network-to-network protection using 5G's new Security Edge Protection Proxy (SEPP) element at the operators roaming border, which will help mitigate against signaling attacks (e.g., SS7, Diameter) when subscribers are roaming between different carriers' networks.

√ 5G Subscriber Identity Privacy using a Subscription Concealed Identifier (SUCI) to conceal and protect the 5G Subscription Permanent Identifier (SUPI), which should help mitigate vulnerabilities to IMSI catchers.

√ Increased Home Network Control for Authentication for the 5G home network to verify that the mobile device is present and requesting service from the serving network.

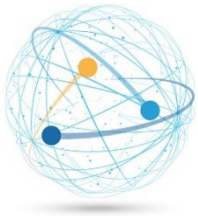
√ 5G Unified Authentication Framework to facilitate use of the same authentication methods for both 3GPP (cellular) and non-3GPP (Wi-Fi) access networks.

√ 5G Security Anchor Function (SEAF) to facilitate re-authentication of the mobile device when it moves between different access networks or serving networks without having to run the full authentication.

OUR WIRELESS FUTURE WILL USE 5G TECHNOLOGY, SOFTWARE DEFINED NETWORKS, AND OPEN NETWORKING AUTOMATION PLATFORMS (ONAP) TO SECURELY CONNECT BILLIONS

The next phase of wireless connectivity represents the convergence of multiple advancements that will enable massive connectivity and innovative security.

Security Policy Orchestration & Data Acquisition	Open Network Automation Platform	Software Defined Networks & Network Function Virtualization	New 5th Generation wireless communication technology



These innovations are maturing at the same time, presenting an opportunity to dramatically enhance security. Carriers are structuring their networks to approach security differently. The core elements of security best practices remain, but carriers will be able to do them differently and more effectively in future networks.

Security Architecture	Identity & Access Management	DDoS Mitigation and Prevention	Logging /Threat Monitoring	Encryption	Edge/ Threat Analytics	Vulnerability Management

In future, virtualized wireless networks, we can secure distinct elements and data sets and automate security functions that previously were manual. With the new technology being built into our future networks, carriers will be able to detect and mitigate DDoS attacks in near real-time and automatically. A major enhancement to previous technologies is the introduction of DDoS detection and mitigation at the edge of the network. This capability will be embedded in network elements and will no longer require a separate security solution, enhancing the ability to respond to attacks.

The convergence of all these developments will be a game-changer and enable carriers to adapt security nimbly and target work to evolving needs and threats.

5G WILL HELP PROTECT SUBSCRIBERS WHEN THEY ROAM BETWEEN NETWORKS

A major enhancement in 5G is the introduction of the Security Edge Protection Proxy, which will be embedded in the Mobile Core and will help mitigate against signaling attacks when subscribers are roaming between different carriers' networks. This embedded capability will help protect against known roaming vulnerabilities in previous wireless technology (e.g., SS7 and Diameter).

THE ENTIRE ECOSYSTEM IS ENGAGED IN WIRELESS NETWORK SECURITY

5G security is being addressed in 3GPP and other standards bodies. 3GPP has a dedicated working group for 5G security, SA3, which makes its work public and is tackling key improvements and lessons learned from 4G. For example, inter-operator security presented challenges in earlier generations of mobile communications, but "5G Phase 1 provides inter-operator security from the very beginning."[3] Primary and secondary authentication are improved as well. Going forward, "the authentication mechanism has in-built home control" which helps with roaming and authentication. Secondary authentication services which were possible in 4G are "now … integrated in the 5G architecture." In addition, "[t]he 5G hierarchy reflects the changes in the overall architecture and the trust model using the security principle of key separation." These are just a few examples of the work underway to embed security into 5G wireless standards.

WHAT IS 3GPP?

3GPP IS A STANDARDS BODY THAT DRAWS ON SEVEN **ORGANIZATIONAL PARTNERS** FROM ASIA, EUROPE, AND NORTH AMERICA—WHICH ARE REGIONAL STANDARDS DEVELOPMENT ORGANIZATIONS (SDOS) THAT HAVE AS THEIR MEMBERS WIRELESS CARRIERS, EQUIPMENT MANUFACTURERS AND OTHER STAKEHOLDERS. THERE ARE ALMOST 600 INDIVIDUAL MEMBERS CONTRIBUTING TO 3GPP SPECIFICATIONS THAT WILL BE REVIEWED BY **THE INTERNATIONAL TELECOMMUNICATIONS UNION** (ITU) AS THE BASIS FOR THE NEXT GENERATION OF WIRELESS TECHNOLOGY.

- **Internet Engineering Task Force (IETF)** is developing security requirements for network protocols for end-to-end device security and the IoT.12. These efforts build on several successful security protocols and standards IETF has developed, such as IP Security, Transport Layer Security, and Simple Authentication and Security Layer.

- **European Telecommunications Standards Institute (ETSI)** is responsible for the standardization of cybersecurity standards internationally and for providing a center of relevant expertise for information and communications technologies, including mobile. The standards include global encryption technologies and algorithms to support integrity, authentication, and privacy.

U.S. carriers are leading the industry and driving the 3GPP standard organization toward stronger encryption algorithms to enhance the over-the-air interface.

Software defined networking and virtualization promise substantial security enhancements. In the past, networks used perimeter defenses and tried to secure everything inside a system, focusing on the core network and the Radio Access Network (RAN). As network design and security thinking have matured, we are looking to virtualize our networks, storing functions and elements in the cloud.

Wireless providers are increasingly deploying network components that are virtual instead of relying on the hardware of the past. And as network functions are virtualized, through Network Functions Virtualization (NFV) and Software Defined Networking (SDN), 5G's virtual and cloud-based network systems will allow for more adaptable security since they can be quickly adjusted, removed, or replaced using software, reducing the likelihood that an entire network would be impacted by a cyberattack.

Cloud-based security systems will support:

- Secure interconnection and transport from the core to the cloud and Internet
- Mutual authentication techniques to constantly authenticate a device and the network connection
- Features that restrict and monitor the entry points into a mobile network
- Highly secure communication between network links

- Localized security tied to virtualized network functions
- Distributed functions, making the systems more difficult to attack
- Data-driven elements that can detect and clean malware and replace compromised functions virtually.

There are significant **security benefits of distributed and virtual networks**. 5G Edge cloud will be built on a virtualized platform taking advantage of NFV and SDN along with an **Open Network Automation Platform ("ONAP")**. Therefore, the security advantages associated with virtualization, and ONAP will apply to 5G. Closed-loop automation based on ONAP and virtualization's inherent elasticity feature will be a significant 5G security advantage. For example, a network can be quickly scaled to mitigate DDoS attacks. And, with edge computing, critical functions can be processed at the network's edge in near real-time, while protecting data. This will support innovative services like IoT and autonomous transportation, which will require massive amounts of near real-time computation. Overall, there will be more ways to store, manage, and secure network components and data, because of the compartmentalization and flexibility that virtualization will enable. Previously, operators had to set up a perimeter and vigorously defend everything in it. In the networks of the future, the bad guys will not have a centralized target. Instead of having physical servers and routers at a building, infrastructure can be virtualized in the cloud.[4] With software-defined networking, it will be possible to develop a multi-layered approach to security that takes the communication layer, hardware layer, and cloud security into consideration simultaneously.[5]

Platform design is being crowdsourced by global stakeholders, improving security. The **Linux Foundation** launched an open source project to create an **ONAP**. It is a comprehensive platform for real-time, policy-driven coordination and automation of physical and virtual network functions, to enable software, network, IT and cloud providers and developers to rapidly automate new services and support complete lifecycle management. This approach is the future of platform management and will support better security.

ONAP'S IMPORTANCE

"BY UNIFYING MEMBER RESOURCES, ONAP IS ACCELERATING THE DEVELOPMENT OF A VIBRANT ECOSYSTEM AROUND A GLOBALLY SHARED ARCHITECTURE AND IMPLEMENTATION FOR NETWORK AUTOMATION–WITH AN OPEN STANDARDS FOCUS–FASTER THAN ANY ONE PRODUCT COULD ON ITS OWN."

The Linux Foundation and a growing community of operators and vendors support open source solutions for operator networks. The foundation's ONAP now brings together over 50 of the largest network and cloud operators and technology providers from around the globe, representing more than 60% of the world's mobile subscribers. The Linux Foundation work includes major global operators, including Vodafone and China Mobile. But U.S. carriers are leading.[6] AT&T, for example, has the software code contributions that will deliver "functioning software, tools, applications and platforms" that will be used "around the world."[7]

Global players are actively involved in developing this next generation of network platform technology. A review of contributions (called "commits") reveals a diverse set of global participants.[8] According to Jim Zemlin, the Executive Director of the Linux Foundation, "AT&T is largely responsible for the success of open source in the telecom space" and its "leadership in SDN/NVF and open source is unquestionable and one that has truly transformed the industry."[9] U.S. leadership in building the foundation of network design bodes well for the security of future wireless networks.

WHAT ABOUT DEVICES?

The wireless industry has not only been focused on its core and radio networks. Operators and manufacturers have spent considerable time securing devices and building the systems that will support more secure devices and connections. Carriers and manufacturers are including new and embedded security functionalities to ensure a highly secure mobile network. For example:

- **Encryption**: 5G networks will offer enhanced protections like the encryption of each device's IMSI, or unique user identifier. Industry is implementing this update to further secure device-specific and consumer-specific information as it moves on a 5G wireless network.
- **Enhanced and Seamless Authentication**: Industry is implementing enhanced and seamless authentication capabilities including seamless authentication of users between cellular and Wi-Fi technologies, home network authentication for device roaming on other networks, etc.
- **Updating**: Industry is constantly refining the process for updating and patching mobile operating systems and applications. This is a complex task due to the thousands of contributors to the mobile ecosystem, which benefits consumers with diverse hardware and software. Wireless providers have developed systems that will allow consumers to receive new and advanced security technology updates meant for their device type—referred to as providing native support for plug-in security. Previous generations of wireless networks were only able to support a one-size-fits-all approach.

INDUSTRY IS LEADING THE WAY IN DEVELOPING SECURITY BEST PRACTICES FOR IOT DEVICES

Managing device security will become more complicated as we enter the Internet of Things era. New opportunities for possible exploits are afforded to hackers and cybercriminals with the development of sensors, cameras, meters, monitors, and other devices that can be targeted if core network and mobile device protections are insufficient. In recognition of this, the U.S. wireless sector developed a **certification program for IoT cybersecurity**.

CTIA's Cybersecurity Certification Program for cellular-connected Internet of Things (IoT) devices is the first of its kind. It was developed in collaboration with the nationwide wireless providers. Leading wireless operators, technology companies, security experts and test labs collaborated to develop the program's test requirements and plans. The program builds upon IoT security recommendations from the National Telecommunications and Information Administration (NTIA) and the National Institute of Standards and Technology (NIST).

- https://www.ctia.org/news/wireless-industry-announces-internet-of-things-cybersecurity-certification-program

The IoT certification program and other efforts will make good on the declared need for baseline common sense security practices that are consistent with the risk associated with a device. This effort illustrates the role that voluntary device certification and independent testing can play to improve security.

NOTES

[1] Distributed Denial of Service (DDoS) attacks are among one of the most disruptive and vicious activities passing over the Internet. DDoS attacks can overwhelm web servers and saturate a company's connections to the Internet resulting in the inability to maintain efficient communications. DDoS attacks have been the subject of extensive government inquiry recently, with an Executive Order and work by The President's National Security Telecommunications Advisory Committee, which in a report observed, "[d]istributed attacks are a complex challenge. No single segment of the Internet ecosystem can solve this issue alone." https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20ICR%20FINAL%20DRAFT%20-%20508%20compliant.pdf

[2] The Communications Security, Reliability and Interoperability Council IV, Working Group 4, *Cybersecurity Risk Management And Best Practices Working Group 4: Final Report* March 2015 http://www.atis.org/01_legal/docs/CSRICIV/CSRIC_IV_WG4_Final_Report_031815.pdf

[3] http://www.3gpp.org/news-events/3gpp-news/1975-sec_5g

[4] https://www.business.att.com/learn/secure-networking/security-and-the-edge-combat-threats-shift-thinking.html

[5] https://www.business.att.com/learn/secure-networking/why-are-we-talking-about-the-edge.html

[6] L. Hardesty, *AT&T Wields Disproportionate Influence in ONAP, But Everyone's OK With It* (Nov. 8, 2017) https://www.sdxcentral.com/articles/news/att-wields-disproportionate-influence-onap-everyones-ok/2017/11/

[7] http://about.att.com/innovationblog/att_framework

[8] https://onap.biterg.io/app/kibana#/dashboard/Overview?_g=h@44136fa&_a=h@e1e6474

[9] http://about.att.com/innovationblog/att_framework