White paper

First Principles for Securing 5G

The Design, Deployment, Operation and Innovation of Secure 5G Networks

December 2019

verizon

Contents

I. Introduction and Executive summary

A. The 5G Security Imperative

The advent of 5G wireless communications constitutes a new era of network connection that will revolutionize many aspects of commerce and our personal lives. As with previous advancements in wireless communications, the transition from 3G and 4G to 5G will provide dramatic increases in both bandwidth and upload/download speeds, along with extraordinary decreases in latency. Together, these improvements will not only expand technical capabilities but also drive exponential increases in the number of connected devices in every sector of the economy, ranging from autonomous and connected vehicles to remote surgery.

The 5G revolution will also expand the "attack surface" for cyber threats, including sabotage and espionage by sophisticated actors, both through the convergence of the cyber and physical worlds and through the massive increase in all types of commercial and personal data. Technology advancements as far back as the control of fire and the invention of the wheel have created opportunities for both good and bad, and there is no doubt that criminals, spies and saboteurs will seek to leverage 5G to their malicious ends.

Verizon is designing and deploying its 5G network with full awareness of these threats, and we will operate and innovate the security functions of this network in a manner that accounts for them. Verizon and the communications sector have a long history of protecting against threats to customers' security and ensuring the reliability and resilience of communications services against all manner of hazards, including cyber threats. We are building on decades of experience and technological leadership to do this, and we are leveraging the unique benefits of 5G technology to develop and operate a more secure network.

Verizon embraces "security by design" principles by architecting and deploying its 5G network with security baked in from the beginning. Though new threats will try to exploit 5G's expansion of the attack surface, the distinctly new architecture and capabilities of 5G networks give operators opportunities to detect and address cyber threats faster and more efficiently than ever before. In contrast to previous advancements in wireless technologies, 5G is an altogether different network technology that will introduce a virtualized, cloud-based architecture, enabling highly specialized functions – and security – for different network applications.

In short, Verizon will leverage the technological capabilities of 5G to design, deploy, operate and innovate the functions of its 5G network to provide best-of-breed security. Our 5G network will provide a brand-new customer experience, but it is also an evolution of our state-of-the-art 4G LTE foundation. 5G leverages security measures that exist today in the 4G environment, and it ushers in new innovations such as sophisticated encryption and authentication features, as well as a new Security Edge Protection Proxy (SEPP) that prevents threats from less-secure interconnected networks from harming 5G networks. This paper will introduce these new security technologies and features for 5G in the context of the existing security features of Verizon's network, and will set forth generally applicable principles that can guide all stakeholders as they do their parts to secure 5G communications.

B. Key Principles for Addressing 5G Security Risks

Experts at Verizon and other private sector and government entities have identified several cybersecurity risks that will continue, or arise anew, in the 5G network environment. Verizon is approaching these concerns in two phases, guided by first principles in security that have undergirded our previous networks and that we can use with greater efficiency and effect in 5G.

Design and Deployment.
Verizon is designing and deploying its 5G network with security as a central element of the network. As discussed below in Section II, Verizon relies exclusively on trusted vendors that have undergone our rigorous supply-chain vetting processes. We routinely assess the software and hardware that goes into our network, and we employ rigorous, documented policies and procedures for secure configuration and operation of equipment and devices we deploy throughout the network. Components of our 5G infrastructure, even within the network itself, are required to authenticate to one another prior to performing their functions. Further, we leverage the new 5G architecture and technical standards, which we ourselves have helped develop, to provide new security features that did not exist in previous generations of wireless technology.

Operation and Innovation.
We continually advance security in operating and innovating the functions of all our networks, including 5G. As discussed below in Section III, we begin with the basic fundamentals of securing the physical aspects of and access to various network components. With the physical network secure, we employ the innovations of 5G network virtualization – also known as "network slicing," or cloud-enabled specialization of software-defined network functions – which in previous generations were conducted through hardware infrastructure. This virtualization capability sets 5G apart from previous generations, providing powerful new efficiencies and effectiveness in communications security.

Moreover, outside the core network, we secure the Radio Access Network (RAN) – the antennas and base stations of cell towers have long been the most visible elements of wireless networks – through advances in Open RAN (O-RAN) technology, which is bringing the security benefits of network virtualization and related software innovation to the RAN. (In turn, this software innovation favors a diverse and competitive market among RAN vendors. This is one way to address the recent troubling concentration of the RAN market among suspect vendors.) Finally, Verizon has helped spearhead global advances in the security of the Internet of Things (IoT) and the other devices that connect to the 5G network, and we are continuing to advance promising new security innovations that will be deployed in the future.

Overall, Verizon has traditionally implemented a holistic view of security risk management and will continue to do so in the 5G environment. Security risks will persist, but we are accounting for these risks in everything that we do to build and operate the network, using 5G-enabled security innovations to advance the security practices that we have employed and refined for decades. Verizon's 5G network presently consists of a new RAN known as New Radio (NR), which is connected to the current 4G LTE core. This deployment, referred to as Non-Stand Alone (NSA) 5G, already includes several security improvements over 4G LTE which are discussed in this paper. As Verizon's trusted vendors begin to support the forthcoming new technical standards for the 5G core standards – due to be completed in the coming months – our core network will migrate to a new 5G core which uses software-based architecture and network virtualization. When Verizon deploys a Stand Alone (SA) 5G service – 5G RAN using a virtualized 5G core – we will implement the cutting-edge technology solutions for assessing and mitigating risk that are currently being advanced and standardized with Verizon's active leadership in research and development, real-world deployments, and standards bodies.

C. Partnering with Government and Other Stakeholders

Since the threats of the Cold War era, communications providers have prioritized partnership with the U.S. government to ensure the security, reliability and resiliency of our nation's communications networks.

The National Coordinating Center for Communications (NCC) – now also known as the Communications Information Sharing and Analysis Center (Comm ISAC) – is the communications sector's security operations center. Physically located in the Department of Homeland Security (DHS), the NCC/Comm ISAC is where Verizon and other private sector communications companies convene with U.S. government partners to promote the security and reliability of our nation's communications infrastructure and services. Established largely for the purpose of ensuring that the government's emergency communications capabilities could continue in the event of a nuclear war, the NCC/Comm ISAC was the first of the critical-infrastructure ISACs, setting the model that other critical-infrastructure sectors such as energy, finance and transportation later adapted to their own distinct needs.

Verizon's approach to 5G security is premised on this ethos of participation and leadership in public-private collaborative efforts that are indispensable to communications security. For example, we are leaders in the industry-government Supply Chain Risk Management (SCRM) Task Force hosted by DHS, involved as the co-chair of one of the working groups. We also co-chair the initiative that the Alliance for Telecommunications Industry Solutions (ATIS) heads to advance supply chain security standards, and we are a leader in Department of Defense efforts to develop methods to operate securely in a "zero trust" network environment.

We have also helped lead multiple landmark industry-government efforts through the Communications Security, Reliability and Interoperability Council (CSRIC), the Federal Communications Commission's communications security advisory committee – including its comprehensive September 2018 Report on Best Practices and Recommendations to Mitigate Security Risks to Emerging 5G Wireless Networks. Additionally, with our private sector partners, we were among the founding members of two organizations that will play significant roles in the future of 5G security: The Council to Secure the Digital Economy, which among other initiatives is leading the global effort to advance the security of the IoT, and the O-RAN Alliance, which promotes open, interoperable, standards-based, virtualized RAN.

In short, Verizon operates from the presumption that neither the government nor any individual private sector entity can adequately secure our nation's communications networks by itself. That is why we will continue to invest heavily in these partnerships with the government and other important stakeholders in the communications and IT sectors.

In Section II below, we describe Verizon's security principles in the design and development of our 5G network, first through security in the supply chain and network equipment, and next through developing and implementing 5G's new security features. In Section III, we describe Verizon's approach to security in the operation of our 5G network, both in the present and through future innovations to come.

II. Embedded Security: Network Design and Deployment

Verizon ensures that security is an integral part of designing and deploying the 5G network. We rely exclusively on trusted network components, managing supply chain security risks through our rigorous supplier vetting processes. We then work with suppliers and engineers to secure these components in the equipment and devices we deploy throughout the network. Further, we leverage the new 5G architecture and technical standards, which we ourselves have helped develop, to provide new security features that did not exist in previous generations.

A. Security in the Supply Chain and Network Equipment

1. Trusted Supply Chain

Verizon's trusted supply chain is the foundation of our secure 5G network. Leveraging a diverse, competitive marketplace of trusted vendors of network hardware and software is a security imperative for Verizon and other 5G service providers. This is the fundamental principle of our supply chain security policy; it guides everything we do in vetting our trusted suppliers and in testing and configuring the equipment and devices we acquire from them.

For both hardware and software, Verizon purchases all our 5G inputs from a small group of sophisticated vendors with whom we have close, trusted relationships developed through thorough vetting and scrutiny, including pre-deployment testing of equipment. Verizon has long been aware of concerns about Chinese technology. We did not use Huawei or ZTE when building our 3G or 4G networks, and of course will not use them for our 5G infrastructure.

Verizon has a complex and rigorous risk management framework for identifying and eliminating risks across our global supply chain for numerous products and services, including public cloud services. Verizon's contractual supplier security requirements, which are designed to address risk management goals, are based on Verizon's own corporate information security policies as well as open industry standards and control objectives found in National Institute of Standards and Technology (NIST) guidance and additional security standards regimes such as ISO2700x, SSAE16, PCI-DSS, HIPAA and others.

Verizon has developed its supplier risk assessment and management discipline over many years. The Supplier Risk Office (SRO) Program manages the risk assessments of suppliers and their individual engagements in a methodical and centralized process. Through the SRO Program, Verizon identifies, assesses, monitors and manages any risks associated with our suppliers throughout the supplier lifecycle, employing highly trained risk management experts to review and approve each contract request. The SRO Program has established a detailed corporate policy that identifies specific roles and responsibilities, as outlined briefly below.

Senior Executive Responsibility.
The Verizon Leadership Committee (VLC), which consists of the Chief Executive Officer and direct reports, assumes the ultimate accountability to define strategic direction and objectives for the SRO Program. On a day-to-day basis, the Supplier Risk Management Executive Committee[1] performs oversight and governance of the SRO Program based on the VLC's strategic direction and objectives.

Contract Review and Risk Assessment.
The organizational sponsor of a proposed contract, with the assistance of the Category Sourcing Expert and the SRO, must complete a risk questionnaire for each contract and statement of work under which products or services are provided by a supplier. The contract's risk level, determined through an assessment under the SRO's formal Supplier Risk Management System, drives due diligence by the appropriate Risk Expert team.

Pre-Contract Due Diligence and Ongoing Testing and Scrutiny.
The SRO has established formal processes for conducting due diligence and addressing all assessed risks prior to use of a supplier and prior to contract execution for a particular product or service. This scrutiny covers suppliers of all types.

Beyond the more focused scrutiny discussed below on suppliers whose products are pertinent to cybersecurity and national security review, our Supplier Risk Management Program scrutinizes our suppliers' general reliability, sound corporate governance, trustworthiness and legal compliance culture, including their regimes for complying with the Foreign Corrupt Practices Act and counter-fraud programs, as well as their financial viability. Verizon reviews information on suppliers' policies and procedures in these areas, along with supporting evidence for each applicable area of risk.

More specifically, we conduct ongoing due diligence with our most in-depth and frequent activities focusing on areas of high risk, such as suppliers of critical equipment that make up our networks. (As discussed in the next section regarding equipment testing and device configuration, we also conduct internal and third-party penetration testing on such equipment, devices and applications prior to launch.) The following risk considerations directly pertinent to cybersecurity and national

1 The Executive Steering Committee for Supplier Risk consists of the following senior executives: Chief Information Security Officer, Chief Security Officer and Chief Privacy Officer; business unit Chief Financial Officers, Controller and Chief Compliance Officer; and the Senior Vice Presidents for Supply Chain & Real Estate, Operations and Human Resources.

security are specifically addressed through our Supplier Risk Management Program:

- Business Continuity & Resiliency
- Cross Border Data Legal Compliance
- Export Compliance
- Geopolitical Risk
- HIPAA Compliance
- Information Security and Data Privacy
- Physical Security
- Sanctions and Screening

The processes outlined above help ensure that our networks are built with trusted components derived from a secure supply chain.

Verizon recognizes that supply chain risk management benefits from effective collaboration and information sharing, both among private sector entities and between the public and private sectors. We therefore have taken formal leadership roles in DHS's SCRM Task Force and in the ATIS initiative to advance supply chain security standards. We also have participated in nascent efforts to advance software supply chain security assurance, such as the multi-stakeholder process convened by the National Telecommunications and Information Administration (NTIA) to develop best practices for vendors to communicate to enterprise buyers the components of the "software bill of materials" – that is, the software supply chain. As discussed in Section III below, further improvements in software supply chain security and software security assurance will be an increasingly important element of Verizon's holistic approach to 5G security as it migrates its network to a virtualized 5G core and operates and innovates this sliced network through software and cloud-based functionalities.

2. Equipment Testing and Device Configuration

After the supplier vetting and scrutiny described above, our next steps in building a secure network foundation include rigorous inspection and security testing as well as standardized configuration of the components that make up our network. Secure configuration of network equipment and devices is a structural necessity in building a secure 5G network.

For this reason, our technical security experts conduct a pre-launch security risk assessment for internal and external branded applications and devices, subjecting critical 5G components to testing to uncover potential security vulnerabilities. Our Network Security Team employs a dedicated group of specialized security testing experts to vet critical software (including updates) after installation. That team, complemented by outside experts, also tests 5G user equipment such as phones, MiFi pucks and 5G home routers.

First, through a process called threat modeling, we evaluate specific potential risks that may pertain to deploying the application or device. Based on specifically identified threats, we conduct internal and third-party security testing on device and application layers to identify vulnerabilities that could be exploited on two fronts: (1) the "insider threat" from a nefarious actor inside the company, and (2) the external threat from an outside hacker. The insights provided by this security risk assessment determine whether or not changes are required before Verizon moves forward with the product or service in question. We then work with the product or platform vendor to ensure that we have resolved security concerns prior to launch and that we have properly and securely configured the equipment and devices in question.

Additionally, Verizon requires that its retail 5G user equipment – for instance, smartphone handsets – conform to industry security standards and to Verizon device security requirements and processes. For instance, Verizon mandates the use of a Universal Mobile Telecommunications System (UMTS) Subscriber Identity Module (SIM) card equipped with a Tamper Resistant Element (TRE), so as to prevent the exposure of Verizon's network authentication and subscriber privacy credentials, which are stored on the Universal SIM (USIM). The TRE may also function as a secure element, which can be extended to protect services by storing and performing cryptographic operations. Further, the user equipment leverages defense-in-depth security principles in its architecture. All network operations relevant to establishing 5G network connectivity are done in a dedicated processor (referred to as the baseband or modem processor), independent from the application processor, providing a layer of protection against escalated privilege attacks, which are common on the main operating system of the device.

To promote secure configuration, in addition to industry standards, Verizon also defines and publishes Verizon-specific technical requirements to which user equipment vendors must conform. These requirements provide the best experience of Verizon services to users, ensure seamless integration of user equipment and 5G network functions, and address out-of-scope items in industry-standard specifications, such as the following:

- Secure boot and update using roots of trust
- Discrete hardware or trusted execution environment-based storage for user application credentials
- Atomic procedure for firmware update failures
- Certificate management
- Signing process of container-based microservice applications

Verizon performs security testing in-house and via third parties for retail devices. Verizon has a list of approved security labs and sends user equipment to these labs for security testing. The devices are assessed for technical compliance with Verizon Device Security Retail requirements as well as industry standards. To promote improvement in user equipment configuration, any problems found during testing are shared with our vendors, who are required to provide fixes within a predefined period, depending on severity, as defined by Verizon's security processes.

3GPP standards ecosystem

Partners
Organizational Partners and
Market Representation Partners

Other standards bodies

broadband forum · IEEE · IETF · tmforum · oma · ITU · one M2M

5G projects

5G Forum · 5GMF · 5GAA · 5G americas · IMT-2020 · ngmn · 5G IA · 5GMF

Certification bodies

PTCRB · GCF

Formal external liaisons

450 MHz Alliance
AISG
Bluetooth Broadband Forum (BBF)
CableLabs
International Special Committee on Radio Interference (CISPR)
CTIA
Digital Video Broadcasting (DVB) Project
Ecma International
Expert Group for Emergency Access (EGEA)
Eurescom
COST 273
European Radiocommunications Committee (ERC)
Fixed Mobile Convergence Alliance (FMCA)
Global Certification Forum (GCF)
Global TD-LTE Initiative (GTI)
GPS Industry Council
GSM Association
HomeRF Forum
IDB Forum
IEEE
Internet Engineering Task Force (IETF)
IrDA
International Multimedia Telecomunications Consortium (IMTC)
Internet Streaming Media Alliance
ISO-ITU expert group
ISO MPEG/JPEG
ITU-T SG2
Java APIs for Integrated Networks (JAIN)
Java Community Process (JCP)
Liberty Alliance Project
LTE/SAE Trial Initiative (LSTI)
Metro Ethernet Forum (MEF)
National Emergency Number Association Next Generation Mobile Networks (NENA NGMN)
oneM2M
Open Mobile Alliance (OMA)
Open Networking Foundation (ONF)
Open IPTV Forum
Object Management Group (OMG)
PCS Type Certification Review Board (PTCRB)
Portable Computer and Communications Association (PCCA)
Presence and Availability Management (PAM) Forum
RSA Labs
SDR Forum
Sun Microsystems, Inc.
Steerco
SyncML Initiative
Trusted Computing Group (TCG)
TeleManagement Forum (TMF)
TCCA
TIA /TR-45
TIA/TR-47
TV-Anytime Forum
Voice eXtensible Mark-up Language(VoiceXML) Forum
Wi-Fi Alliance
Wireless Broadband Alliance (WBA)
WLAN Smart Card Consortium
Wireless World Research Forum (WWRF)
World Wide Web Consortium (W3C)

Figure 1: 3GPP interactions with other organizations

B. Security by Design: Developing and Implementing 5G's New Security Features

Verizon has been operating and improving its state-of-the-art 4G network for years. We will remain at the cutting edge of technological advances and standards development regarding the transitions from 3G and 4G to 5G. New 5G security features in Verizon's 5G network are enabled by rigorous technical security standards development processes – in which, as outlined below, Verizon participates as an industry leader.

1. Overview of 5G Standards for Security

Technical standards provide a common understanding of technical systems among operators, developers and users, which in turn leads to greater stability, ease of use and interoperability. This also leads to greater security because the standards process is open and transparent. Nothing is or can be hidden in the standards process, and this transparency allows all parties to perform security analyses of proposed standards and to input corrections for any vulnerabilities identified.

a. The 3GPP Standards Development Process

Verizon is participating in and influencing the 5G standards setting process through the 3rd Generation Partner Project (3GPP), which has previously provided LTE, LTE-Advanced and LTE Advanced Pro for commercial cellular/mobile systems. There are seven organizational partners in 3GPP which work on the standards and also several peripheral organizations that reference or provide input to 3GPP standards (Figure 1).

3GPP Technical Specification (TS) 33.501 specifies a security architecture for the 5G network.[2] It includes security features, mechanisms, and procedures for the 5G New Radio and core. This TS leverages security protocols or recommendations from organizations such as the Internet Engineering Task Force (IETF) and NIST. Other organizations providing requirements or recommendations to 3GPP include Next Generation Mobile Networks Alliance and the International Telecommunication Union. Additionally, the European Telecommunication Standards Institute (ETSI) has provided security specifications for network function virtualization and Multi-access Edge Compute (MEC).

verizon

2 3GPP, June 13, 2019, "Security architecture and procedures for 5G System" retrieved from http://www.3gpp.org/ftp//Specs/archive/33_series/33.501/33501-f50.zip.

The standards development process, including work on security features, benefits from input from companies with real-world experience deploying new technology. It is common for companies like Verizon who are "first movers" to deploy service using new technology while the standards are still in development. There is nothing inherently insecure about non-standard, proprietary communications equipment, and indeed substantial portions of the communications ecosystem (such as most early Wi-Fi routers and all smartphone operating systems) have involved proprietary, non-standards-based technology during early stages of deployment. That is the path Verizon took when securely deploying its fixed-wireless 5G network to accelerate the 5G ecosystem; now that the standards (with our input into them based on our learning with real-world deployments) have been issued, we will upgrade the pre-standard equipment with standards-compliant equipment to support operational compatibility.

Some policymakers have expressed concerns that China may be influencing the 5G standards to potentially introduce cybersecurity deficiencies into them.[3] We do not see evidence of this; even though Chinese-based companies have a large coordinated presence, no single entity can dictate the consensus-driven technical standards. The standards processes are public, open and transparent. Although highly competitive, there is nothing in these processes that has inhibited Verizon with respect to becoming the first carrier in the world to launch a 5G service; to the contrary, these processes are a venue in which we provide influential global leadership.

b. Verizon's Role in Advancing and Implementing 5G Security Standards

Last year, Verizon was the first provider in the world to launch a commercial 5G service, and in doing so, we embraced "security by design" principles that included working with our vendors on cutting-edge security features. For example, our deployment uses the same encryption techniques for the link between the consumer device and the edge of our network that were later articulated in 3GPP TS 33.501, Security Architecture and Procedures for 5G System (Release 15). By being out in front of the rest of the industry, we can lead the standards process so that eventually all providers will deploy equipment with appropriate security features.

Verizon continuously monitors and participates in the standards development process to identify and prioritize new security features to be implemented in its network. Prioritization of feature implementation is based upon a risk assessment process that evaluates the likelihood and impact of the threats a given security feature could mitigate. Verizon is already evaluating security enhancements for the 5G core as we begin planning for future deployment (Figure 2).

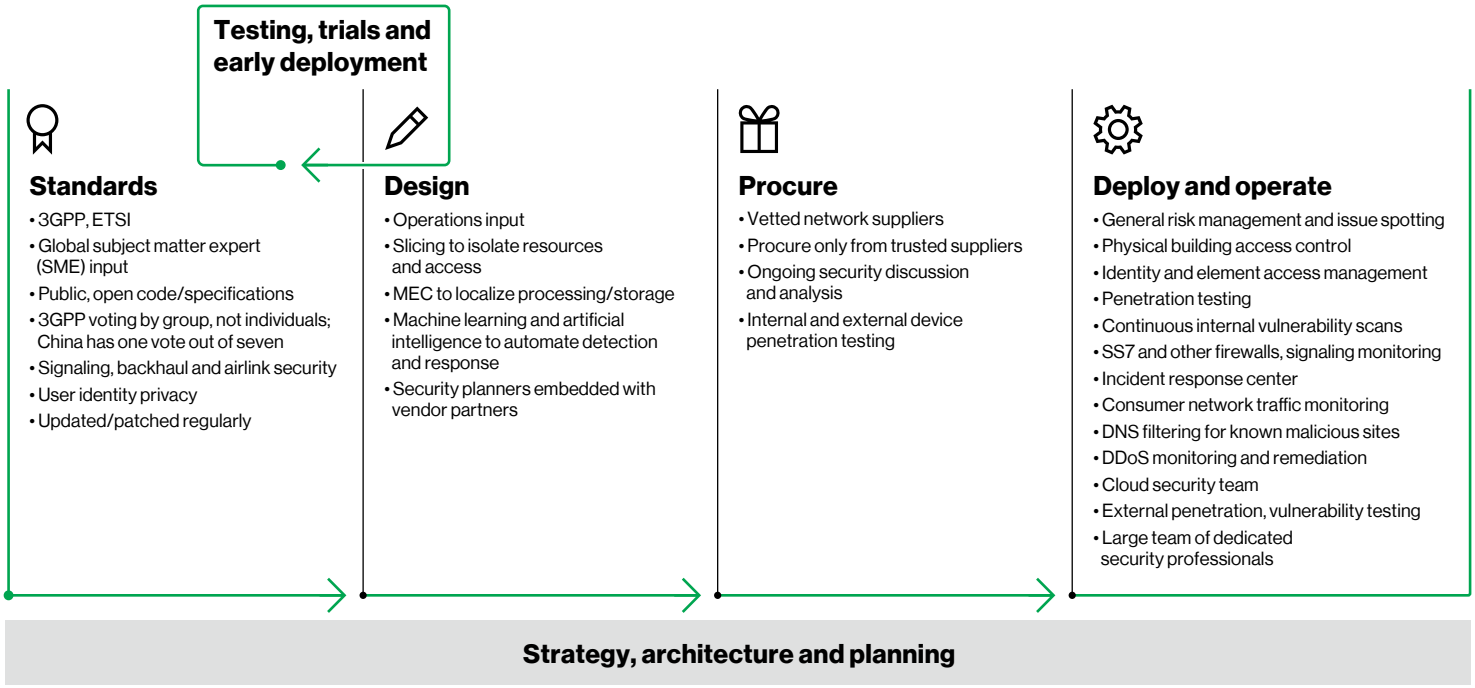


Figure 2: 4G/5G Security Development Process

verizon

3 See, e.g., John Eggerton, March 1, 2019, "Sens. Seek Report on China's Impact on 5G Standards" retrieved from https://www.broadcastingcable.com/news/sens-seek-report-on-chinas-impact-on-5g-standards.

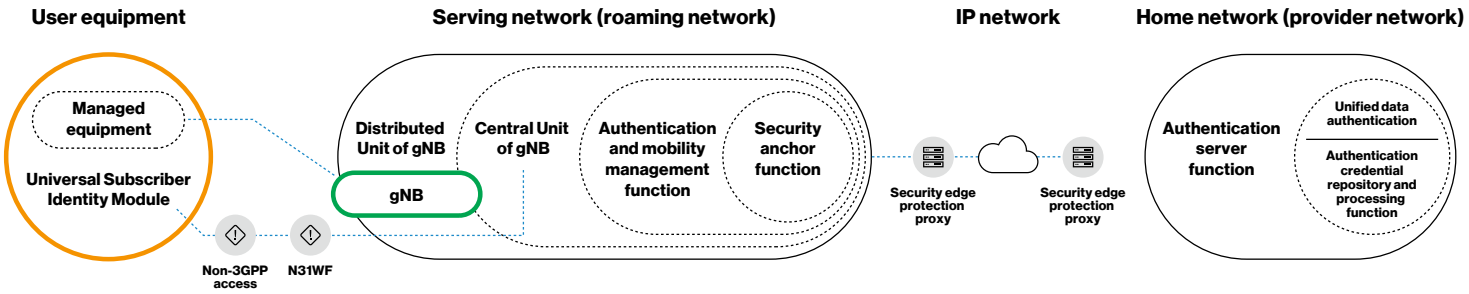


Figure 3: 5G Security Architecture Model

2. Deploying 5G's New Security Features

5G builds upon the security mechanisms of 4G by introducing multiple enhancements, which are discussed in 3GPP TS 33.501, Security Architecture and Procedures for 5G System (Release 15). The focus of many of the new features involves mutually authenticating the User Equipment (UE) and the base station (gNB) to prevent fraud, service theft and disclosure of credentials to eavesdroppers. Other improvements update the encryption methods and prevent the user's identity from being transmitted over the air in the clear.

The diagram above (Figure 3) serves as a reference for the discussion that follows of the major 5G security features. The security architecture is depicted as an "onion" of ever-increasing trust, with central ovals showing the most trusted portion of the trust model. In the case of the UE, on the left, the Universal Subscriber Identity Module (USIM) is the portion of the UE that is trustworthy. It comprises the USIM and the ME (Mobile Equipment, or the phone itself), the two major components of the UE. The USIM is a tamper-proof trust anchor that securely stores the user's authentication credentials, computes cryptographic keys, and stores the home network's public key and other network data. The UE may connect to either a wireless gNB base station – the "eNB" of 5G[4]– or a non-3GPP network such as Wi-Fi or a cable network. In the case of the diagram and for the sake of generality, the UE is roaming outside its home network's access footprint and has attached to the serving network. The home network is shown on the right of the diagram. The serving network and home network are connected to each other via an IP network via security gateways (SEPPs, or Security Edge Protection Proxies). As discussed below, the serving network and home network cooperate to authenticate the UE, thereby ensuring the security of the 5G service. In any case, whether the subscriber is roaming or not, the home network has the final authority regarding authentication of the UE.

Some important new security enhancements in 5G are discussed in the following sections. These new features prevent spoofing attempts to fraudulently obtain service or UE credentials, thwart rogue base station impersonations used to track users and steal their credentials (often referred to as "IMSI catchers"), and strengthen subscriber privacy and identity. New protocols and functions improve authentication and key exchange, prevent downgrading of encryption protocols, and provide protection at the boundaries to other networks. These and other security improvements introduced in 5G have built upon the security from 4G LTE networks.

a. Wireless Subscriber Authentication

The goal of subscriber authentication by the home (or provider) network is to ensure that the network that "owns" the mobile subscriber (or customer) – as distinct from a serving network to which the subscriber may connect through while roaming – is the network that actually verifies that the customer is legitimate. That is, Verizon should verify Verizon customers. Home network control is a unique feature of 5G, and it means that the visited network, or the network the customer is roaming to, must pass the customer's credentials to the home network for final verification. (The roaming network can, however, refuse a connection from a customer if the presented credentials are falsified or otherwise out of order.) The serving/roaming network authorizes the UE using the subscription profile vouched for by the home network, which has the final authorization decision authority. The home network relies upon the serving network to deliver all relevant parameters and to verify that the device is actually on its network. This enhanced procedure prevents spoofing of visited networks in attempts to fraudulently obtain service or UE credentials (keys). The section below on SEPP provides more details of the security used at the serving network/home network boundary.

b. Authenticating the Network

Regardless of whether the UE is roaming or not, the device will authenticate the network using implicit keys derived from the Key Agreement procedure discussed later. Also, the UE will verify the network regardless of network technology – that is, whether connecting to 3GPP (5G) or non-3GPP (Wi-Fi). This helps eliminate rogue base station or false base station attacks. The false base station is also known as an "IMSI catcher" or "Stingray." A false base station can lead to a wide variety of privacy and security problems, such as stolen user credentials or a user's location being tracked nefariously. Base station impersonation by criminals and others is a dynamic problem and is typical of the "arms race" often seen between technology innovations and those who would exploit it for nefarious reasons.

verizon

4 LTE access networks use base stations that are called eNBs, which utilize 3GPP standards Release 8 up to Release 15. gNB, or "next-generation" NB, supports next-generation interfaces as described in 3GPP standards Release 15 and onward.

c. Registering a New Phone: Binding the Security Relationship with the Provider
The Subscriber Permanent Identifier (SUPI), akin to IMSI in 4G, is part of the user's credentials used to authenticate to the network. The SUPI is contained in the USIM and is typically 15 digits, composed of the Mobile Country Code (MCC); the Mobile Network Code (MNC), which identifies the network operator; and finally the Mobile Subscriber Identification Number (MSIN), which is unique to the particular user. When the phone is commissioned or registered, the network provider or home network places the SUPI, telephone number, the provider's public key, and sequence number (SQN) in its network database and in the USIM. This forges the cryptographic relationship used between the UE and the network provider and forms the basis of all subsequent security activity.

d. Protecting the User Equipment's Identity
When the UE seeks to attach to the network, it sends either the Subscription Concealed Identifier (SUCI, an encrypted form of the SUPI) or the Globally Unique Temporary Identifier (5G-GUTI). The UE does not send the SUPI in unencrypted form across the network – instead, the SUCI contains the SUPI, which is "concealed" or rather encrypted using standardized encryption mechanisms. The home network provider's public cryptographic key is used in the encryption, which conceals the subscriber's identity from the roaming network. The SUPI is extracted from the SUCI by the network using the Subscription Identifier De-Concealing Function (SIDF).

If it is not the first time the UE has authenticated, the USIM may have been given a 5G-GUTI by the network, which serves as a proxy or substitute for the SUPI. Because the network assigned the GUTI, it can index or cross-reference a corresponding, previously stored SUPI to positively identify the user. 5G-GUTIs are short-lived, changed frequently and, like the SUCI, can serve to hide the identity of the UE. In either case, the SUPI is not sent in clear text across the radio network, which protects the phone against being tracked or having the user's privacy breached for the purpose of profiling or identity theft. This is among the most significant security improvements in 5G over 4G.

The Access and Mobility Management Function (AMF) of the serving network confirms the SUPI/5G-GUTI based on information provided by the home network. The home network receives either the user's SUPI, which is cross-referenced and extracted from the serving network's database of assigned 5G-GUTIs, or the SUCI, which the home network "de-conceals" to extract the SUPI.

e. The Key Agreement Procedure
Now that the phone is authenticated, the network performs one of two flavors of key agreement: 5G-Authenticated Key Agreement (5G-AKA), or Extensible Authentication Protocol AKA' (EAP-AKA'). The protocols are similar. (There is also a third protocol, EAP-TLS, but it is used only for certain private network or IoT applications.)

Authentication and Key Agreement have two main goals: (1) mutual authentication between UE and its home network (even though the AKA process may pass through an intervening serving or roaming network), and (2) establishing session keys between the UE and the serving network. Components of the process include a permanent UE identifier (a SUPI), the provider's public key and a sequence number, each of which were placed into the 5G device when it was first commissioned by the network provider. The UE sends its SUPI, encrypted by the home network's public key so that it is now a SUCI, to the home network. The sequence number helps protect against replay attacks

The end result is the anchor key (K_{SEAF}), which is provided by the Authentication Server Function (AUSF) of the HN to the Security Anchor Function (SEAF) of the SN. The anchor key is bound to the SN, which prevents other networks from pretending to be a legitimate network. K_{SEAF} is a symmetric key shared among 5G entities.

When the network has the anchor key as a result of the UE and the network mutually authenticating each other, the components of the network are able to build the cryptographic material required to perform the various functions needed to keep the network's integrity, confidentiality and authentication intact. K_{SEAF} is used to derive signaling and RAN uplink and downlink user plane keys for encrypting traffic. Practically every key used in the radio portion of 5G is derived from K_{SEAF}. For example, the keys needed to perform the following functions are directly or indirectly derived from K_{SEAF}:

- Keys for Non-Access Stratum (Non-Access Stratum)
- Keys for NG-RAN (used by gNB, the 5G base station)
- Keys for User Plane traffic (Access Stratum)
- Keys for Radio Resource Control (RRC, Access Stratum)
- Keys for non-3GPP access (Wi-Fi, cable, etc.)

With key agreement and derivation complete, all signaling, radio resource control traffic, payload traffic and other communications are encrypted for the sake of confidentiality. That is, unauthorized entities cannot decode and read these data flows. Furthermore, traffic has integrity, which means it is protected by Message Authentication Code (MAC) using derived keys so that recipients know that it has not been altered or tampered with. Finally, the identity of the UE (the user and phone) and the identity of the network(s) cannot be impersonated or stolen. Man-in-the-Middle attacks are thus thwarted, but efforts in the 5G community continue to develop security measures to address Distributed Denial of Service (DDoS) attacks that can take place with messages sent in the attachment process prior to authentication (so-called pre-authentication messages). Radio Resource Control (RRC) messages are examples of pre-authentication messages that could be used, perhaps in volume, by a bad actor to create a DDoS attack.

The 5G security architecture provides for combined Wi-Fi and 3GPP authentication (access independent). That is, when connecting to the 5G network via an intervening Wi-Fi network (non-3GPP), the data will pass through a Non-3GPP Interworking Function (N3IWF). To secure this portion of the network, the UE will establish an IP Security (IPSec) tunnel to the N3IWF over which 5G security procedures will take place.

f. Security Edge Protection Proxy and Other 5G Security Architecture Features

As shown in Figure 3, the Security Edge Protection Proxy (SEPP) provides gateway protection when connecting to another operator's network. Different providers connect across an N32 interface. Specifically, the serving network uses the N32 to connect to the home network. The SEPP receives and processes communications between network functions, which include the AUSF, AMF, UDM, etc., per 3GPP TS 23.501, System Architecture for 5G System. The SEPP protects application layer control plane traffic between different network functions, negotiates cipher suites, handles key management, and performs topology hiding to external networks. It also discards malformed and untrustworthy N32 messages, among other duties.

Other notable 5G security architecture features include:

The Security Anchor Function (SEAF) plays the role of a pass-through authenticator. It also provides the serving network's name. SEAF can initiate authentication with the UE, and it transparently forwards authentication traffic between the AUSF and the UE. The AUSF (the back-end authentication server) handles authentication requests and informs the UDM of the results. The UDM provides secure storage for keys and must be protected against physical attacks.

- The Security Anchor Function (SEAF) plays the role of a pass-through authenticator. It also provides the serving network's name. SEAF can initiate authentication with the UE, and it transparently forwards authentication traffic between the AUSF and the UE. The AUSF (the back-end authentication server) handles authentication requests and informs the Unified Data Management (UDM) of the results. The UDM provides secure storage for keys and must be protected against physical attacks.
- 5G ensures that available security features are in fact used between the UE and the network and that the features are not mistakenly or misleadingly viewed as unavailable, a protection known as "bidding down attack immunity." Bidding-down attacks attempt to trick systems into believing that they must avoid using essential security features for the sake of backward compatibility, so that the attacker can gain advantage. Algorithm negotiation is designed to prevent the use of an ineffective security suite; for instance, an attachment request from a UE could be rejected if it tried to "downshift" to an outdated cipher algorithm. An Anti-Bidding down Between Architectures (ABBA) parameter may be developed in later 3GPP releases.
- The gNB, or base station of 5G, is composed of a Central Unit (CU) and one or more Distributed Units (DUs). Thus, the gNB is split between the CU and DU, which are connected via the F1 interface. To promote security on the control plane and user plane, the F1 interface employs IPsec. In the control plane, Datagram Transport Layer Security (DTLS) is also used.

The security specifications discussed above are part of 5G Security Phase 1 from 3GPP Release 15.[6] This release has generally focused on the RAN, whereas 5G Security Phase 2, which will be part of 3GPP's Release 16 due in the coming months, will focus more on the 5G core and NFV. As such, Release 16 will address, among other things, solutions for IoT security, which is often considered to be a primary 5G cybersecurity risk due to the large number of new devices that will be accessing the network.

III. Continuous Security: Network Operation and Innovation

Verizon further advances security in operating and innovating the functions of its 5G network. We will employ the innovations of 5G network virtualization and artificial intelligence (AI) to provide powerful new efficiencies and effectiveness in communications security. Verizon's 5G network creates opportunities for risk assessments and risk management responses that benefit from greater visibility and more detailed insights into the network than in previous generations.

A. Operational Security

Following the release of 3GPP standards pertaining to the 5G core in the coming months, this Non-Stand Alone 5G deployment, which already includes several improvements over 4G LTE, will transition to Stand Alone 5G service.

When Verizon deploys a Stand Alone 5G service – 5G RAN using a virtualized 5G core – we will implement the cutting-edge technology solutions for assessing and mitigating risk that are currently being advanced and standardized with Verizon's active leadership. These advanced virtualization capabilities will increase the effectiveness of the state-of-the-art and holistic security risk management practices described below – namely, the corporate governance policies, security monitoring and response capabilities, and software vulnerability management processes that Verizon has employed in previous generations and will be further improved upon through 5G capabilities.

1. Corporate Policy and Governance

A wide range of risk management activities occur continually across Verizon's network footprint, both on customer-facing products and services that might contain sensitive information and on internal platforms and networks.

5 The N32 interface serves as a new application layer between SEPPs to filter sensitive data attributes during the interconnection.

6 Anand R. Prasad, Alf Zugenmaier, Adrian Escott and Mirko Cano Soveri, August 6, 2018, "3GPP 5G Security" retrieved from https://www.3gpp.org/news-events/1975-sec_5g

Verizon's Corporate Information Security Group internally publishes a suite of security practices and procedures that align with the NIST Cybersecurity Framework. These formal, internal, corporate-wide policies map to each of the Framework's five Core Functions – Identify, Protect, Detect, Respond and Recover – and each sets forth the individual behaviors and business processes that are required for security, as well as the standards for our infrastructure and its supporting systems and applications. Verizon also internally publishes dozens of detailed Corporate Information Security Standards, which provide detailed descriptions of the underlying security controls that must be implemented to support each security instruction.

Verizon reviews and updates these policies and standards annually and on an as-needed basis along with evolving regulatory compliance obligations, technology capabilities, improvements to industry best practices, field experience and implementation. The Corporate Information Security Group gathers recommendations from multiple sources, including individual contributors' ideas, results of internal audits and business unit audits for compliance. Updates are incorporated into the policy after a rigorous review and approval process, and they are communicated to internal stakeholders on roughly a monthly basis via Security Governance Briefs.

2. Security Operations
Verizon invests heavily in securing all of its networks, including 5G, against known and potential threats. We continuously monitor our networks to identify and respond to threats. Our networks are monitored 24/7 by a Security Operations Center to identify potential malicious activity. All of the relevant connections – including between subscribers and 5G antennas, and among different parts of the 5G networks – are encrypted to prevent eavesdropping and are appropriately segmented (e.g., with firewalls and intrusion prevention systems) to prevent an "infection" associated with one piece of equipment from affecting the rest of the network.

In addition to those technical controls, Verizon deploys other preventive controls and strategies, including:

Segregation of Duties:
The practice of dividing steps in a function among different individuals, keeping a single individual from being able to subvert the overall process.

Dual Control:
The process of using two or more separate entities (usually persons) operating in concert to protect sensitive functions or information. No single person is permitted to access or use the materials (for example, the cryptographic key).

Role-based Access Control:
Mechanisms that limit availability of information or processing resources only to authorized user roles or applications that require it.

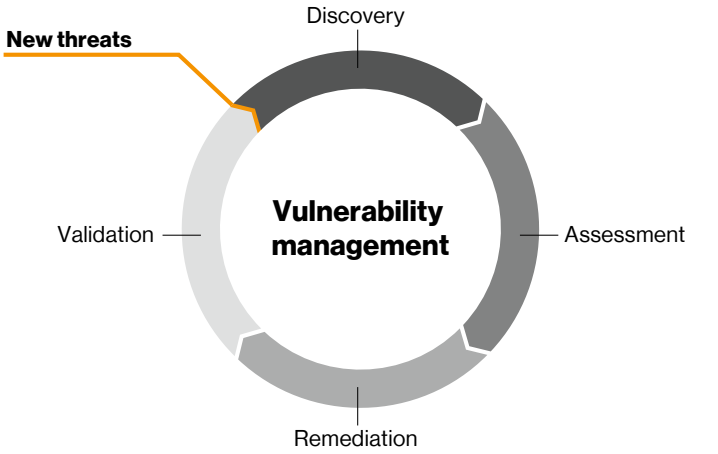
Principle of Least Privilege:
The practice in which a user is granted the minimum level of access to perform actions necessary for the job function.

Multi-factor Authentication:
Two or more authentications required for remote login.

To identify issues not prevented by other controls, Verizon also uses detective mechanisms like intrusion detection and network Data Loss Prevention (DLP) to analyze network traffic for malware and unauthorized information transmissions.

Looking forward, the use of AI promises a more efficient approach to security, allowing continuous monitoring for potential threats. The 5G network creates the opportunities for use of AI in the network through incorporation into the software-based architecture. Large amounts of data could be quickly analyzed for rapid detection of threats and immediately mitigated through the combination of AI capabilities with security automation. Verizon's 5G network will increasingly create opportunities for better and faster visibility into network activity, as well as the capability to isolate threats and anomalous network activity, all of which naturally will greatly benefit security monitoring and response.

3. Software and Hardware Vulnerability Management
Addressing vulnerabilities plays a central role in 5G security risk management. In addition to procuring software and hardware from trusted vendors, Verizon has established a robust vulnerability management process, outlined in Figure 4 below. These processes will continue to evolve and will play an increasingly central role through the transition to Stand Alone 5G, with its virtualized, software-defined 5G core.



Discovery	Automated tools that remotely and continuously check for known vulnerabilities in operating systems, services and devices that could be used to target the company's private network.
Assessment	Vulnerabilities detected during the discovery stage are rated and prioritized and documented.
Remediation	Vulnerabilities are addressed based on the priority identified in the previous assessment step.
Validation	After the vulnerabilities are addressed, subsequent scans are used to validate the successful resolution of all identified vulnerabilities.

Figure 4: Stages of Vulnerability Management

In addition to the four stages outlined above, we regularly monitor various sources to identify trends for potential new vulnerabilities. Tracking vulnerabilities is one measure of how well we are performing when it comes to security assessment, evaluation and resolution.

Verizon's corporate policy requires that patches, fixes and service packs be applied to Information Resources in a repeatable, prioritized and standardized manner in order to keep Verizon Information Resources secure.

Software vulnerability management will also become more effective the further we progress into the Stand Alone 5G transition, because patches and software upgrades are more efficiently deployed at scale in a software-oriented network than in a largely hardware-based network.

B. The Cyber-Physical Convergence: Real-World Safety and Security

In the coming years, potentially millions of new RAN antennas and base stations will connect billions of new devices to each other – and to the physical world in which we and our family and friends live. The smart devices enabled by 5G will lock and unlock our doors, heat and cool our homes, steer and stop our cars, track our kids and our vital signs, monitor our babies sleeping, and allow doctors to treat or even conduct surgery on us remotely, along with thousands of other important functions in our lives. Their security will be, to put it lightly, quite important in our lives. The reliable functioning of these devices – protected against sabotage, manipulation, espionage and AI-powered nefarious uses – will become an increasingly critical element of communications capabilities the further we advance into the 5G era.

Securing the cyber-physical convergence is another imperative for Verizon's 5G network, because that convergence is where our network matters most in our customers' lives.

1. Physical Security

The technical literature addressing 5G security does not prominently address physically securing access to the network, but all network security – 5G and otherwise – relies on the security of the infrastructure that enables the network. With this in mind, Verizon will continue its rigorous physical security measures outlined below.

a. Partitioned Access Control Systems
Verizon enforces its established standards that require that an individual's access to the network, be it physical or logical access, is based on the access that the individual needs in order to do his or her job – no more, no less. The Mobile Switching Centers (MSCs), Network Equipment Centers (NECs), Network Operations Centers (NOCs) and other sites housing critical equipment are designed and equipped with access control systems with multiple, layered security access zones such as core equipment spaces, building services spaces, office spaces, public spaces, shipping/receiving spaces, etc. Critical spaces are surrounded and shielded by less critical spaces. Electronic keys control access to the buildings and interior spaces; mechanical keys are issued to only a few critical personnel as backups. Access to any of those spaces is controlled by the access control system for each individual, according to the legitimate need for his or her access.

Since not all employees need access to all spaces all the time, the access control systems can be programmed to allow an individual's access by time of day, day of the week, per room or space, as required. The access control systems maintain log files of all access attempts, authorized or unauthorized.

b. Systems Surveillance 24/7/365
MSCs, NECs, NOCs and macro cell sites are designed and equipped with intrusion detection and alarm systems that are tied into their access control systems. The intrusion detection system (IDS) includes, but is not limited to, door contacts, motion detectors, infrared sensors, cameras with motion

detection, glass break sensors, timers, etc., that will generate alarm signals locally and to remote locations such as the NOCs or central station security monitoring points.

Alarm conditions of all types, including those from the Access Control System (ACS) and IDS, are monitored and logged in the system itself, the local control point, and the NOCs fault management system. In addition, a facility's IDS may also be monitored by a third-party central station depending on the facility and local assessment of the security environment. Local personnel are on-call 24/7 to respond if necessary.

c. Network Access Control and Cell Site Security
The primary concern regarding cell site security is that the distributed nature of 5G, including small cells, might increase the risk that bad actors could physically tap into Verizon equipment to eavesdrop or to disable it. Verizon's 5G network, and the 4G networks that it currently rides on, are monitored 24/7 to identify and address potential tampering. As discussed above, all of the relevant data flows – including between subscribers and 5G antennas, and among different parts of the 5G networks – are encrypted and subject to various controls (e.g., firewalls) to prevent an "infection" associated with one piece of equipment from affecting the rest of the network.

If physical security were to be breached at the cell sites, specific controls are in place to limit the access of an attacker to the network. Unused network ports at the cell sites are disabled to prevent their use by attackers. Equipment at the sites is configured to be automatically provisioned so that attackers cannot overwrite the configuration locally. Finally, only network elements authenticated to the Verizon network are allowed to connect. Rogue systems will be denied access and will raise an alarm.

Therefore, while bad actors may in some cases have the ability to disable or destroy distributed equipment such as small cells that sit at the edge of the network, this risk is more akin to that of a physical event (such as a storm) than a cyberattack – that is, a temporary localized absence of service that prompts our network resiliency response, rather than a cybersecurity risk that impacts the rest of the network.

2. Securing the IoT and Devices that Connect to the Network
The rapid deployment of billions of new IoT devices carries significant risks, to the extent that many of these devices have not been developed with certain baseline technical security requirements. Largely to help lead a promising effort to address these very security challenges – made manifest by the IoT-driven Mirai botnet DDoS attack in October 2016 – Verizon became a founding and active member of the Council to Secure the Digital Economy (CSDE). Among several other significant activities that have been recognized by top leaders in the U.S. government,[7] perhaps the CSDE's most notable accomplishment to date is its development of the world's leading industry consensus on IoT security technical baseline requirements through the "Convene the Conveners" (C2) consensus process.

Through the C2 process, Verizon and other CSDE members[8]– supported by the Consumer Technology Association, USTelecom and more than a dozen other major cybersecurity and technology organizations, industry associations, consortia and standards bodies – identified baseline IoT security requirements for the rapidly growing IoT marketplace. There were multiple purposes of this landmark initiative:

1. Promoting global harmonization of security specifications
2. Bolstering global market forces that favor secure devices
3. Developing a common language on these issues that speaks to different policy and technical audiences
4. Aligning policy development internationally and in the United States

The resulting C2 Consensus on IoT Device Baseline Security Capabilities, or "C2 Consensus Baseline," was released on September 17, 2019. We believe that this global market approach, which is supported by U.S. government agencies and materially aligns with the draft IoT recommendations that NIST has developed, will be an effective industry-driven approach to security for the IoT.

More specific to Verizon's participation in the IoT ecosystem, we have established rigorous development processes for Verizon retail IoT devices and network certification security requirements for IoT devices, and we will continue to do so as we further deploy our 5G network. While networks that are less trustworthy than 5G networks may be appropriate for some limited IoT use cases where devices do not present significant security risks, critical and sensitive IoT applications will benefit from the enhanced security of 5G networks. This is due to the 5G network's new capabilities to be configured as needed to implement traffic segregation via private network Access Point Names (APNs), end-to-end data encryption and enhanced authentication requirements, among other security features.

IoT devices that are subject to managed security can benefit from the enhanced authentication capabilities that 5G offers – both in terms of the IoT device authenticating the 5G node it is connecting to, as well as the network requiring enhanced authentication for connectivity. In addition, with network slicing, IoT devices can be put on an isolated slice so that, for instance, a DDoS attack from the IoT devices cannot impact other slices on the network.

verizon✓

7 For example, the Director of DHS's Cybersecurity and Infrastructure Security Agency (CISA), Christopher Krebs, has recently praised the CSDE and its accomplishments in his keynote speeches at the DHS CISA 2nd Annual National Cybersecurity Summit, September 26, 2019; and Mobile World Congress Los Angeles 2019, October 22, 2019; and in his testimony at the U.S. Senate Committee on Homeland Security and Government Reform hearing on "Supply Chain Security, Global Competitiveness, and 5G," October 31, 2019.

8 Other than Verizon, CSDE's member companies are Akamai, AT&T, CenturyLink, Cisco, Ericsson, IBM, Intel, NTT, Oracle, Samsung, SAP and Telefónica.

9 See Draft NISTIR 8259 ("Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufacturers), published July 2019.

C. Looking Ahead

Verizon's state-of-the-art operations regarding network management, monitoring and response will continue in 5G. Moreover, virtualization and other innovations that 5G enables, including as described below in the RAN, will bring new efficiencies and effectiveness to our existing security operations.

1. Open RAN and Virtualization Standards

Beyond the RAN-oriented security features discussed in Section II regarding User Equipment authentication and related capabilities – all of which are directly relevant to securing the edge network – Verizon has been an active leader in other efforts to secure the edge of the network. Specifically, as an early and very active member of the O-RAN Alliance and through our own real-world learning, we have advanced the potential for standards-based open interfaces to promote virtualization of the RAN. This effort produces technical specification and reference architecture, which conforms to and influences technical standards, and promotes two security benefits.

First, virtualization of the RAN will allow for specific security advances at the edge of the network. For instance, as noted above, the flexibility presented by the 5G design to reconfigure and create segregated network slices can help mitigate broader damage caused by insecure IoT implementations. Network operators now have the ability to segregate certain IoT devices from the general population of devices, and this capability will be improved through further virtualization at the edge.

Second, standards-based open interfaces within RAN can facilitate a new competitive and diverse market of RAN vendors. Open RAN is thus a tool to promote RAN vendor diversity and to level the playing field in a previously hardware-oriented RAN market that has been increasingly consolidated in recent years. Carriers need to have a robust set of competitive options to choose from in the trusted vendor market, and standards-based open RAN can help ensure that reality. More broadly, open RAN is fundamentally about software and innovation – where the future of 5G lies, and where the United States and its allies lead.

2. Security Opportunities through Network Slicing and Multi-access Edge Compute

Network slicing is the concept of isolating different services into isolated slices in terms of network resources and traffic. Network slicing can be thought of as a Virtual Private Network (VPN) with the addition of network resource allocation and isolation. Slicing plays an important role in separating and protecting mission-critical systems from non-managed devices and systems. As noted above, if there is a DDoS attack on or emanating from non-managed IoT devices, slicing can ensure that only the IoT slice is impacted, and that others that manage mission-critical network functions are not affected. Importantly, slices can be customized based on mission needs with different security mechanisms and policies, such as firewall configurations, access policies, packet inspection and authentication schemes. This could provide separate slices with specialized or tailored security for critical systems such as smart energy meters at distribution stations and generation plants, road sensors providing traffic controls at busy intersections, safety messages from autonomous vehicles, or connected medical devices and equipment in a hospital.

Another component in Verizon's 5G deployment is the Multi-access Edge Compute (MEC) capability. The MEC brings compute capability geographically closer to the customer, thus enabling extremely low-latency services such as interactive training. Verizon is considering both public and private MECs. Public MECs would be shared resources across multiple different services, while a private MEC can be dedicated to individual customers such as a factory floor for robotics control. In addition to localizing data, a private MEC also allows a customer to physically secure the MEC in their own location, thus adding another layer of security customized to the customer's particular needs.

3. Future 5G Security Opportunities

Verizon will continue to lead the development of innovative security service concepts and capabilities for 5G. One of the most important opportunities for future security innovation is the utilization of Software Defined Perimeter (SDP) to create a "zero trust" security layer over a 5G network. Zero trust is the concept of verifying user and device identity and providing access to the appropriate network slice based on service category or application. Additionally, SDP can also be combined with a quantum Random Number Generator (qRNG) as an effective countermeasure to future quantum computing encryption attacks.

We will also continue to develop and improve upon new tools such as AI, security automation, virtualization and other proactive security measures that create promising opportunities for rapidly identifying and mitigating threats in a 5G world.

IV. Conclusion

5G communications will bring dramatic new benefits and capabilities to commerce and personal life. 5G's new capabilities will also expand the attack surface for bad actors at the convergence of the cyber and physical worlds. Verizon is designing and deploying its 5G network, and will operate and innovate it, in a manner that accounts for these threats. We are building on decades of experience, at Verizon and in the communications sector more broadly, in protecting against these threats. Our customers' secure communications, and the reliability and resilience of our communications services, are our top priorities.

The new architecture and capabilities of the 5G network will allow operators to detect and address cyber threats faster and more efficiently than ever before. Our 5G network will provide a virtualized, cloud-based architecture that enables highly specialized security measures for different network applications.

Our first principles in addressing 5G security risks guide us in the two phases that are crucial to any network.

1. In our design and deployment of this network, we rely exclusively on trusted network components, with supply chain security assured through our rigorous supplier vetting processes. We have strong policies governing the configuration of these components in all the equipment and devices we deploy throughout the network. Components of this network are required to authenticate to one another prior to performing their functions. We leverage the new 5G architecture and technical standards, which we ourselves have helped develop, to provide new security features that did not exist in previous generations.
2. In our operation and innovation of this network, we continually advance security in the network. We secure the physical network, and we employ the groundbreaking innovations of 5G network virtualization to provide powerful new efficiencies and effectiveness in communications security. Outside the core network, we secure the RAN through advances in open RAN standards and technology, which in turn promotes a diverse and competitive market among RAN vendors. Verizon also has helped spearhead global advances in the security of the IoT and the other devices that connect to the 5G network, and we will continue to advance promising new security innovations that will be deployed in the future.

Finally, because neither the government nor any individual private sector entity can secure our nation's communications networks alone, we will continue to invest heavily in partnerships with the government and other important stakeholders in the private sector to secure 5G.

Appendix: Glossary

3GPP: 3rd Generation Partnership Project

5G: 5th Generation of cellular network technology

ABBA: Anti-Bidding down Between Architectures

ACS: Access Control Systems

AI: Artificial Intelligence

AKA: Authenticated Key Agreement

AMF: Access and Mobility Management Function

APN: Access Point Name

ARPF: Authentication Credential Repository and Processing Function

ATIS: Alliance for Telecommunications Industry Solutions

AUSF: Authentication Server Function

CSDE: Council to Secure the Digital Economy

CSRIC: Communications Security, Reliability and Interoperability Council

CU: Central Unit of gNB

DDoS: Distributed Denial of Service

DHS: Department of Homeland Security

DLP: Data Loss Prevention

DTLS: Datagram Transport Layer Security

DU: Distributed Unit of gNB

EAP-AKA: Extensible Authentication Protocol-Authenticated Key Agreement

EAP-TLS: Extensible Authentication Protocol-Transport Layer Security

ETSI: European Telecommunication Standards Institute

FCC: Federal Communications Commission

gNB: New Radio (5G) Node B (base station)

GUTI: Globally Unique Temporary Identifier

HIPAA: Health Insurance Portability and Accountability Act

IDS: Intrusion Detection System

IETF: Internet Engineering Task Force

IMSI: International Mobile Subscriber Identity

IoT: Internet of Things

IPSec: IP security

ISAC: Information Sharing and Analysis Center

ISO: International Organization for Standardization

IT: Information Technology

K_{SEAF}: Security Anchor Function Key

LTE: Long-Term Evolution

MAC: Message Authentication Code

MCC: Mobile Country Code

MEC: Multi-access Edge Compute

MNC: Mobile Network Code

MSC: Mobile Switching Centers

MSIN: Mobile Subscriber Identification Number

N3IWF: Non-3GPP Interworking Function

NCC: National Coordinating Center for Communications

NEC: Network Equipment Center

NG-RAN: Next Generation Radio Access Network

NIST: National Institute of Standards and Technology

NOC: Network Operations Center

NR: New Radio

NSA: Non-Stand Alone

NTIA: National Telecommunications and Information Administration

O-RAN: Open Radio Access Network

PCI-DSS: Payment Card Industry Data Security Standard

qRNG: quantum Random Number Generator

RAN: Radio Access Network

RBS: Rogue Base Station

RRC: Radio Resource Control

SCRM: Supply Chain Risk Management

SDP: Software Defined Perimeter

SEAF: Security Anchor Function

SEPP: Security Edge Protection Proxy

SIDF: Subscription Identifier De-Concealing Function

SIM: Subscriber Identity Module

SQN: Sequence Number

SRO: Supplier Risk Office

SSAE: Statement on Standards for Attestation Engagements

SUCI: Subscription Concealed Identifier

SUPI: Subscriber Permanent Identifier

TRE: Tamper Resistance Element

TS: Technical Specification

UE: User Equipment

UDM: Unified Data Management

USIM: Universal Subscriber Identity Module

UMTS: Universal Mobile Telecommunications System

VLC: Verizon Leadership Council

VPN: Virtual Private Network