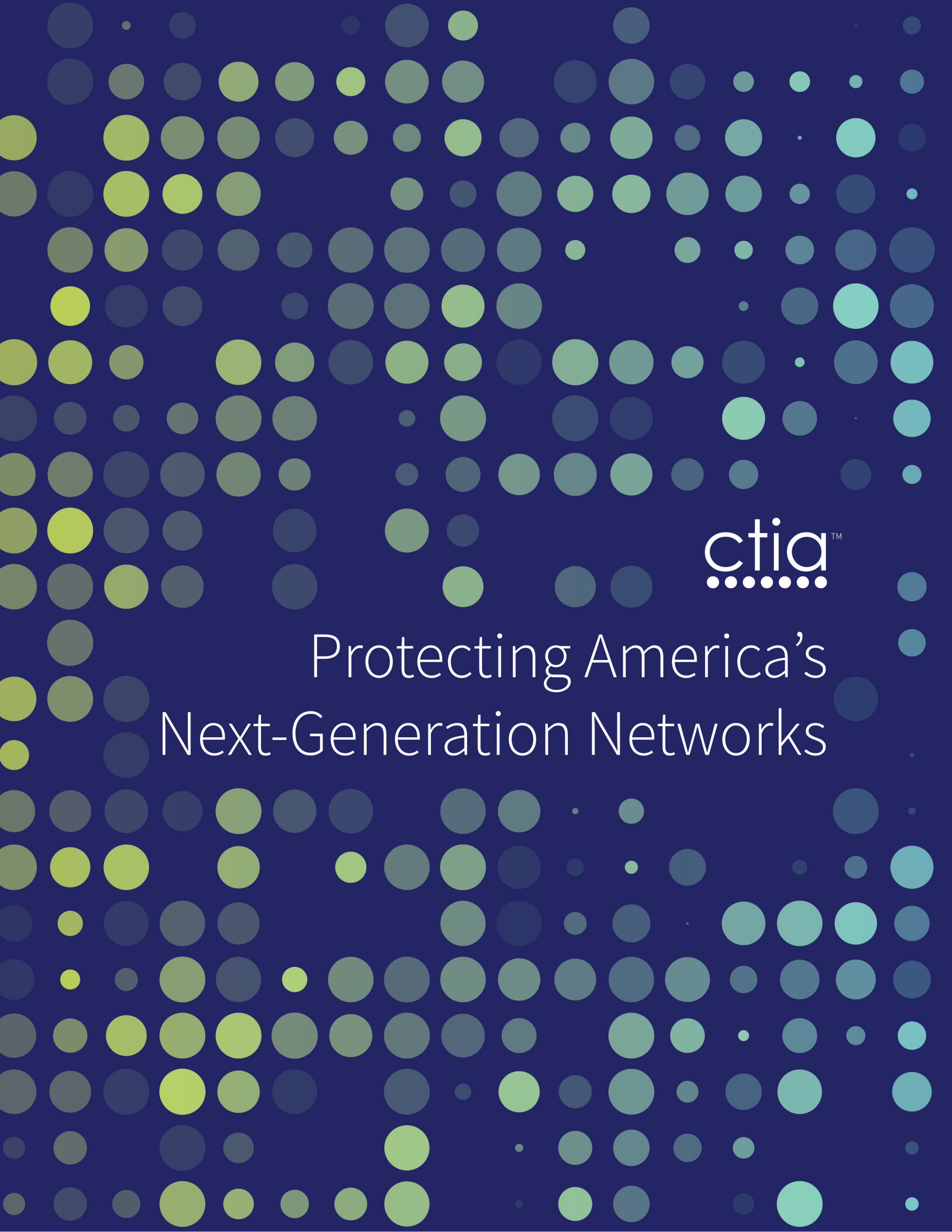


ctia™

Protecting America's Next-Generation Networks

Executive Summary

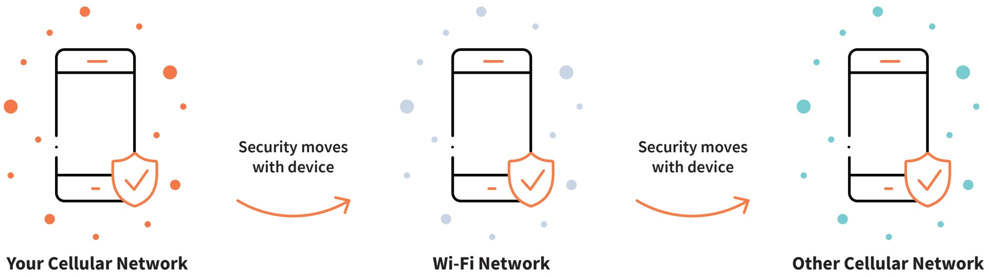
The wireless industry has baked security into our networks since the beginning, and works diligently to continually update and build on our security capabilities with every generation of wireless. Today's 4G LTE networks have the most advanced security features to date, and 5G will further improve upon them.

As 5G networks start to be deployed this year, wireless providers are leveraging new and advanced measures—after years of research, investment, and contributions to standards bodies—to secure 5G networks. This paper updates CTIA's 2017 Protecting America's Wireless Networks paper to feature 5G security highlights, including:

1

Enhanced privacy protections

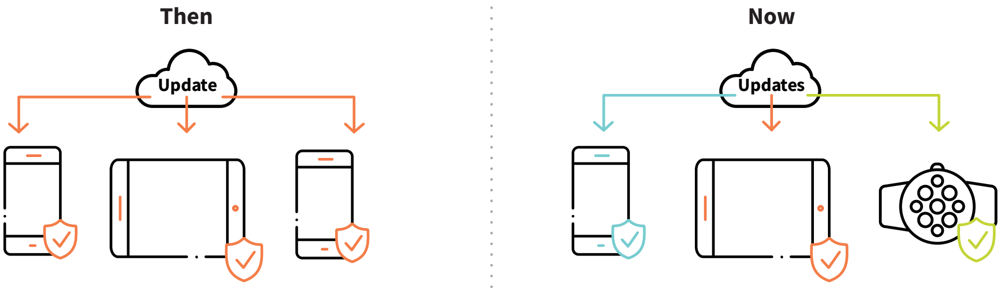
5G networks offer enhanced privacy protections like the encryption of each device's IMSI, or unique user identifier. Industry is implementing this update to further secure device-specific and consumer-specific information as it moves on a 5G wireless network.



2

The ability to leverage 5G "home" wireless network security when roaming or on Wi-Fi

Wireless providers are extending the security of 5G wireless networks to other networks—called home network control—when a user is roaming or using a non-wireless network like Wi-Fi. This use of home network security on all networks more thoroughly protects devices, consumer data, and even the network itself at all times.



3

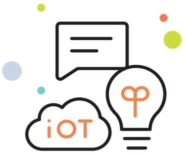
Device-specific security updates

Wireless providers 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.

Further enhancing security across the wireless ecosystem, wireless providers are increasingly deploying network components that are virtual instead of the hardware of years' past. 5G's virtual and cloud-based network systems 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.

Strong cybersecurity is key to the U.S.'s global wireless leadership. 5G is going to be up to 100 times faster, five times more responsive, and able to support 100 times more devices,[1] unlocking innovations we can't even imagine. For the U.S. to continue to attract investment in the app economy, as well as the virtual reality, artificial intelligence, and Internet of Things innovations of the future, our networks must be secure at every turn. And that's what our industry works tirelessly to provide every day.

Rising Threats



Internet of Things

New opportunities for possible exploits by hackers and cybercriminals have emerged with the development of sensors, cameras, meters, monitors, and other devices that can be targeted—and exploited—by hackers and other bad actors if core network and mobile device protections are insufficient.

Security is Critical to Everyone and Everything

Thanks to wireless, we're more connected than ever.

Across the United States, more than 400 million wireless connections join people and increasingly, every part of our world together.[2] These connections generate tremendous traffic over wireless networks—since 2010, mobile data traffic has grown over 40 times.[3]

We're only going to grow more connected.

Tomorrow's 5G networks will offer unparalleled speeds, support a massive increase of IoT devices, and power real-time connections with minimal delays in response, enabling entirely new services and applications.

The Internet of Things—bringing broadband connectivity to consumer and industrial devices, sensors, and objects—will usher in increased productivity and growth across every economic sector, from transportation and healthcare to public safety and energy. The number of connected devices worldwide is projected to total over 31 billion by 2023.[4]

Cyber threats are evolving.

Cyber threats continue to grow in number and sophistication, with new risks and exploits to address. These threats are serious, often launched by highly resourced intelligence services abroad, organized criminal networks, and motivated entities seeking to disrupt communications networks, here and around the world.

5G—Keeping America's Wireless Networks Secure

The entire wireless industry continues to innovate and advance security—across networks, devices, operating systems, and applications—as we move to 5G and implement virtualized and software-defined networks.

Given the cyber threat landscape and how it evolves, wireless network operators, device manufacturers, and operating system (OS) and application service providers continue leading-edge and risk-based management efforts that emphasize security as an integral component of every generation of technology. Today's protections will continue to evolve over the life of 5G and beyond.

Wireless Networks

5G will incorporate existing network protections as well as new ones and leverage lessons learned from the IT industry, such as the importance of mutual authentication techniques and multiple layers of security throughout a system. These enhancements will touch every cellular-capable device, given the growing connectivity of our world through the proliferation of Internet of Things (IoT) devices. 5G network defenses[5] include:

- Using standards-based encryption algorithms for on-air interfaces to prevent unauthorized access to information over the air, including the encryption of a device's unique user identifier, called the International Mobile Subscriber Identity (IMSI).
- Deploying authentication mechanisms that validate and authorize the user seeking to access the network in order to ensure that only legitimate people are accessing the network. These mechanisms include security anchor capabilities to authenticate and improve security across disparate networks.
- Ciphering or coding data sent over the network to ensure it is kept free from corruption and/or modification.
- Deploying a robust set of anti-spamming software on our networks to protect consumers from unsolicited SMS/MMS messages, illegal robocalls, and unwanted calls.
- Instituting strict access controls—physical and IT access—to limit and monitor network resources as protection against internal and external bad actors.
- Leveraging the flexibility of plug-in security schemes so that security updates directed toward certain devices can be sent to them and only them, avoiding the performance issues caused by non-compatible devices receiving these updates.

Network Threats

Cloud Infrastructure

For instance, a Distributed-Denial-of-Service (DDOS) attack could use commandeered IoT devices to overwhelm elements in the cloud to restrict or deny the availability of targeted online services.

Network Attacks

Attacks could be launched by leveraging existing network protocols to execute exploits.

Mobile Device Risks

Malware

Malware includes Trojan packages used to target financial information and ransomware[6] that locks a user out of their system until they pay for re-access.

Mobile Threats

These threats include attacks on mobile applications, phishing attacks to install malicious software, and attacks to trick users to divulge access credentials such as personal passwords or PINs.

Device Security is Key

Mobile Devices

Today, mobile devices are targets for cyberattacks. That's why mobile device manufacturers already build in a number of security mechanisms that protect devices from cyber threats, including:

SIM Cards
An integrated circuit for securely storing and authenticating critical subscriber identity information, a SIM (Subscriber Identification Module) card enables a secure and reliable voice and data connection and the ability to provision new applications and services remotely.[7]

Temporary Identities
To mitigate the risk of serial numbers being compromised, networks use temporary identities that vary regularly, helping prevent interception by unauthorized users.

Wireless Account Controls
To protect against unauthorized use, consumers can leverage PINs and passwords to protect wireless provider account information, multi-factor account controls to provide more complex user authentication, and text or email notifications regarding changes in account profiles or number porting requests.

Roots-of-Trust
Built into mobile devices, this hardware-based cryptographic information is used to detect malware and authenticate system software integrity.

Anti-Theft Tools
The mobile industry's voluntary anti-theft commitment provides consumers the tools to locate, lock and wipe their device in the event of theft or loss.[8]

Integrated Systems
Mobile devices will be able to leverage 5G's advanced authentication and encryption algorithms to work in near real-time with network security enhancements.

Consumer Security Trends

60%

of Americans report having the ability to remotely locate, lock, and erase their smartphones.[9]

77%

of consumers use PINs/passwords on their smartphones, an increase of 54% from five years ago.[10]

Mobile OS/Apps

Mobile operating system providers like Android and iOS work with application developers continuously to improve security while screening for bad applications at app stores in order to prevent the spread of viruses and malware. Operating system providers and app developers will continue to advance software that protects wireless devices and consumers, including:

Anti-Malware and Anti-Virus Software
This kind of software prevents, detects, and removes malware from a user’s device.

Device Security
If a device is stolen or lost, personal and sensitive information contained in the device can be rendered inaccessible to an unauthorized user. Tools are provided to consumers for such protection.

The wireless industry will use every tool to defend against cyber threats.

Setting Cybersecurity Standards

Standards

Wireless network security standards processes are comprehensive and constantly evolving and improving. Driven by industry participation, standards-setting and standards-developing organizations are expanding global standards to enable dynamic, resilient, and safe wireless networks that counter security threats in a connected world. Key guidance-setting organizations include the following:

3GPP, the main wireless standards-setting body, is developing 5G security and privacy standards for the next generation of wireless technologies, architectures and protocols.[11] 3GPP is also developing several cryptographic algorithms to enhance end-to-end security and providing for ongoing enhancements to mobile cybersecurity. The new 5G standards include items discussed throughout this paper, such as increased home network control, a unified authentication framework across cellular and non-cellular networks, native support for the plug-in of new authentication schemes, security anchor capabilities to re-authorize devices as they move across different networks, and IMSI encryption for enhanced privacy protections.

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.

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.

National Institute of Standards and Technology (NIST) is a U.S. standards body responsible for setting guidance for government agency conduct. CTIA and its members collaborate with NIST to share best practices and further refine an industry-driven methodology called the Cybersecurity Framework which helps companies assess and manage cybersecurity risks and outcomes.

CTIA's Cybersecurity Working Group brings together cybersecurity and policy experts from service provider, manufacturer, wireless data, internet, and application companies to develop best practices, common frameworks, and educational materials for consumers. The members work with the Department of Homeland Security (DHS), the Federal Communications Commission (FCC), the National Telecommunications and Information Administration (NTIA), and NIST, as well as with Congress to enhance technical and policy approaches to cybersecurity in the U.S.

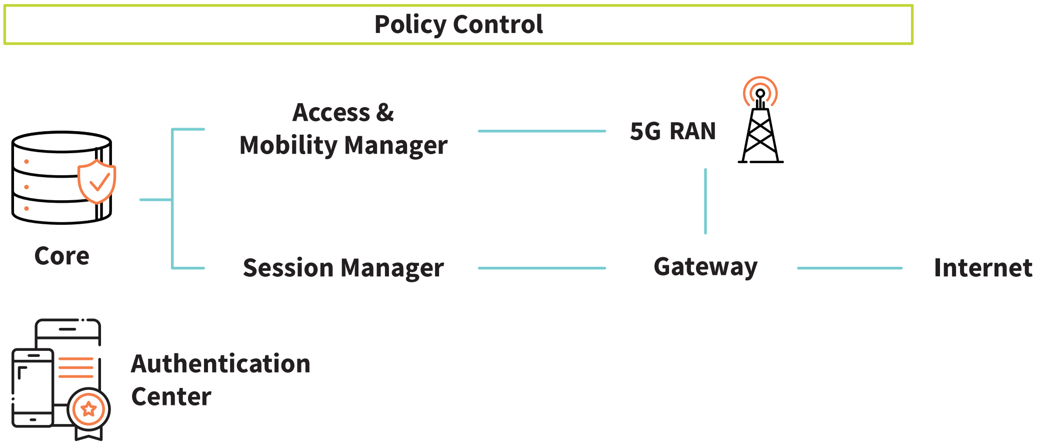
GSMA, a global trade association, leverages the contributions of its many members around the globe to share best practices for security management in mobile networks.

Network Security and Monitoring Tools are Key

Wireless Radio Access Network

The radio access network (RAN) provides the radio communications between the mobile and the core network. The base station provides the air-interface radio connection between the mobile device and core network, performs mobility and handover, and ensures good performance and allocation of shared radio resources.

5G Network Security



To prevent intruders from eavesdropping, wireless network operators equip their RAN with features that ensure the security of the radio communications functions and their connection to the core network. Specifically, RAN security features include:

Mutual Authentication Functions
To detect and prevent "spoofing," these functions use an Authentication and Key Agreement protocol between the mobile device and the RAN allowing the device to authenticate the network, and the network to authenticate the device.[13]

IPSec Encryption
This protocol allows the RAN to encrypt communications between the back-haul connections and the core network and also detect and mitigate unauthorized access, helping ensure proper radio access and prevent denial of service attacks.

Access Controls
These tools enable the detection of unauthorized access to RAN resources and the ability to deny access if appropriate.

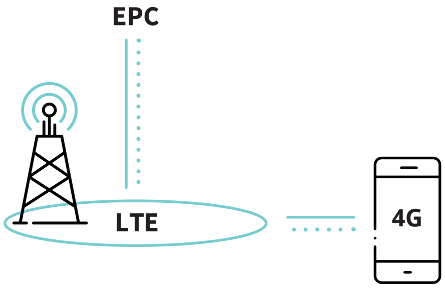
Wireless Core Network

The 4G LTE core network consists of data gateways or routers, mobility management platforms, policy and billing, and the home subscriber database.

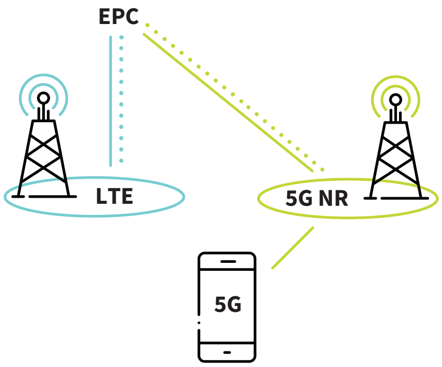
The data gateways and major routing platforms carry IP traffic from many connected devices through the core network and out to cloud services or the Internet. 5G networks will build on the core network used by 4G LTE networks, called an Enhanced Packet Core (EPC), to interpret and route data. Initial 5G networks will adapt EPC capabilities to the changing threat landscape.

Evolution

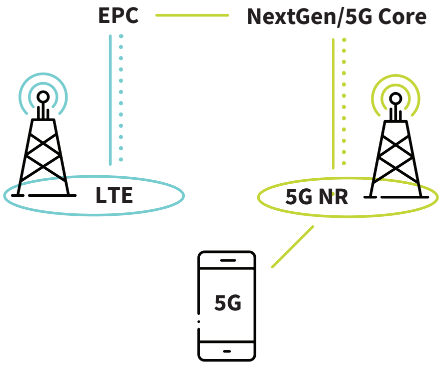
4G Operability



5G Interoperability



5G with NextGen Core



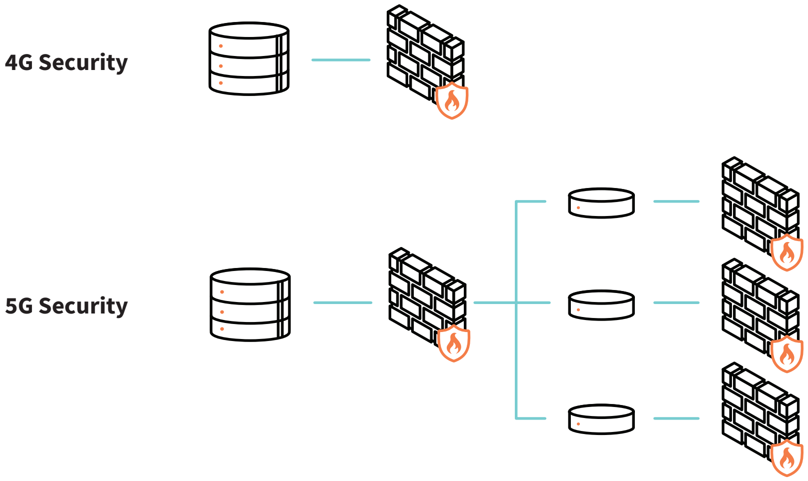
5G networks will be able to support interoperability between the Enhanced Packet Core and future advanced Core (NextGen) networks as they come online. This flexibility is key to rapid 5G deployment and allows providers to scale security quickly using a known, but adaptable core network system.

To monitor, guard, and protect the core platforms and subscriber databases against denial of service attacks or the threat of a stolen master key, wireless operators deploy a number of tools, including:

- Firewalls that block certain types of network traffic, forming a barrier between a trusted and untrusted network—analogous to a physical wall that blocks and isolates the spread of an attack.
- Intrusion detection and prevention systems that monitor network activities for malicious activity—helping identify the activity, record information about it, and block or stop it.
- Malware monitoring and detection to target hostile or intrusive software, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, and other malicious programs.
- Virtual Private Networks that enable traffic to be sent through a secure connection, isolating that traffic from other devices on intermediate networks. Capable of connecting individual users to a remote network, application or multiple networks, VPNs require authentication for remote access and use encryption techniques.
- Machine learning and artificial intelligence that detect anomalous behavior and automatically mitigate attacks.

Core network elements are highly secure functions in terms of physical security and access controls, requiring gated facilities, guards, secure card entry, sophisticated login/password controls, and other security measures. Not only are security functions a high priority, the core network is managed by trained and specialized personnel who are security and risk management experts.

Secure 5G Virtualization



Virtualizing 5G Networks

Whether running apps, storing data, or delivering services, the cloud—a network of servers—has proven popular and efficient for delivering provider grade text messaging, social networking, banking, ecommerce, and mobile health applications. These servers and the mobile applications and services they enable have become a target for new threats. This matters because the all-IP architecture and openness of the internet provides broad and diverse entry points for an attack on a mobile network.

As network functions become virtualized, often referred to as Network Functions Virtualization (NFV) and Software Defined Networking (SDN), cloud-based security is deployed by network providers to ensure the security of their networks against threats. Cloud-based security systems will support:

- Secure interconnection and transport from the core network out to the cloud and internet
- Mutual authentication techniques to continually authenticate a device and the network connection
- Features that limit and monitor the number of entry points into the mobile network

- Highly secure communication between links of a network
- Localized security tied to virtualized network functions
- Distributed functions, making cloud systems more difficult to attack
- Data-driven elements that can detect and clean malware or other threats that enter the system and replace compromised functions virtually—all in seconds.

Policies to Secure the Next Generation of Wireless

Wireless companies monitor, protect, diagnose, and fight potential cyberattacks in real time, and that's why policymakers should promote flexible, technology-neutral solutions and focus on cyber threat information sharing with appropriate liability protections for today's 4G LTE and tomorrow's 5G networks.

To ensure we can continue to innovate as fast as cyber threats do, we need voluntary, collaborative, industry-led efforts—avoiding mandates that quickly become outdated. While many federal agencies have roles to play, the Department of Homeland Security is critical in convening industry and government stakeholders to work together toward a common framework to address cybersecurity.

We urge policymakers to continue collaborating with the wireless industry on important and complex 5G security issues in order to encourage actions that can be taken in standards groups and other organizations. As 5G is deployed, flexibility is critical to meeting the challenge of protecting our networks and our consumers against the dynamic global threat landscape.

Acknowledgements

John Marinho, VP Technology and Cybersecurity
Thomas Sawanobori, SVP and Chief Technology Officer
Kevin Ryan, Assistant Vice President, Communications and Policy
Katherine Den Boer, Director, Communications and Policy

Endnotes

1. The Wireless Industry: An American Success Story, CTIA, https://www.ctia.org/the-wireless-industry/wireless-industry.
2. Id.
3. 5G networks will be 10 times faster than 4G networks, respond five times as quickly, and connect 100 times the number of devices. Thomas K. Sawanobori, CTIA, The Next Generation of Wireless: 5G Leadership in the U.S., at 5 (Feb. 9, 2016), at www.ctia.org/docs/default-source/default-document-library/5g-white-paper.pdf.
4. Ericsson Mobility Report 2018, at 16 (June 2018), at https://www.ericsson.com/assets/local/mobility-report/documents/2018/ericsson-mobility-report-june-2018.pdf.
5. The Sector Annual Report (SAR) is filed with DHS and highlights a more comprehensive description of the actions and capabilities that the mobile industry deploys to protect networks and consumers from threats and bad-actors, at https://www.dhs.gov/keywords/sector-annual-report.
6. Ransomware is malware that installs itself on a mobile device without the knowledge of the user and extorts payment once device information is locked, usually encrypted, and held hostage in exchange for a ransom payment.
7. Manufacturers limit access to SIM cards to minimize risks from the challenges of the application ecosystem.
8. Smartphone Anti-Theft Voluntary Commitment, CTIA (2016), at https://www.ctia.org/the-wireless-industry/industry-commitments/smartphonea-anti-theft-voluntary-commitment; Capabilities that the wireless industry deploys to protect networks and consumers from threats and bad actors.
9. CTIA commissioned Harris Poll to conduct these surveys. Four such surveys have been conducted since 2012. An online survey was conducted Feb. 19-31, 2017, using a sample from the Harris Poll Panel of 1,007 U.S. adults who own and use a smartphone and/or tablet. A supplemental survey of 1,690 smartphone owners was conducted the week of March 6, 2017. A full methodology is available upon request.
10. Id.
11. SA3 – Security, 3GPP, http://www.3gpp.org/specifications-groups/sa-plenary/sa3-security#term0_1 (last visited Jun. 11, 2018).
12. See e.g., Best Current Practices for Securing Internet of Things (IoT) Devices, IETF, https://datatracker.ietf.org/doc/draft-moore-iot-security-bcp/ (last visited Jun. 11, 2018).
13. Such authentication functions include SNOW 3G (designed by Lund University, Sweden), and the Clock cipher standard (NIST, USA), or Stream cipher.

ctia™

www.ctia.org