SAMSUNG

5G Security – Improving User and Data Protection

Today's vertical industries are growing fast, and applications like automated manufacturing and augmented and virtual reality demand fast, ubiquitous network connectivity to help them succeed. 5G is perfectly suited to support these new domains of business-critical services. However, 5G's higher capacity to connect billions of people and devices also increases threat opportunities that must be resolved. 5G requires additional levels of security and privacy to mitigate threats from new user domains such as IoT devices and edge computing applications, which were not possible with previous wireless technologies.

From a service perspective, users expect their smartphones to easily connect everywhere they go. Mobile roaming delivers this access by providing secure, seamless service exchange between network operators. With the high volume of 5G-powered IoT devices and increased penetration of 5G in enterprise networks, the number of attack points for network breaches in 5G networks is significantly higher than with prior wireless networks.

As in any business, risk management is paramount, and inherent security technology and protocols provide the foundation for mitigating threats such as data breaches and identify theft. Cisco recently updated its Cisco Annual Internet Report (2018-2023) White Paper, which indicates that 1,272 breaches exposed 163 million records, as of November 2019.[1] This statistic alone makes it clear that data network security is vital.

The good news is that security is a top priority in each wireless network generation. From the early challenges in 2G and 3G networks, where device cloning and voice interception were eliminated, the mobile wireless industry continues to offer better security than other, more vulnerable network architectures. Today, users expect 5G security and privacy to be even further improved. The ability to eliminate the challenges encountered in the past is table stakes for business customers.

5G offers foundational improvements over prior technologies, and with the service-oriented system that spans the core and radio access network (RAN), network operators can create and roll out new solutions quickly and in a controlled manner to prevent or respond to new privacy and security threats.

Data attacks and thefts resulted in 1,272 breaches that exposed 163,000,000 records.

- Cisco Annual Internet Report

1. https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

5G Incorporates Security from the Start

Base 5G technology provides several important security features that keep cyber criminals at bay, including international mobile subscriber identity (IMSI) encryption, device-specific enhancements, home network control, and increased security benefits from network virtualization.

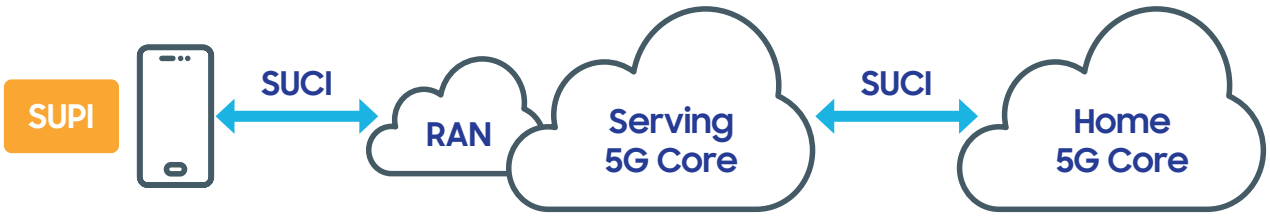
New Process to Better Authenticate the Device Before It Accesses the Network

Network operators certainly do not want invalid users consuming high-value spectrum and network capacity, and customers do not want their devices used without their knowledge. Wireless networks began eliminating these types of concerns back in 2G networks, but cyber crooks continued to find ways to unscrupulously join networks with pirated information. The process that 5G uses for granting access to the network has two significant upgrades that create critical roadblocks to user device identity theft: IMSI encryption and Home Network Authentication.

Encrypting Important User Information

Device security and privacy start with protecting the identity of the user's device, and this protection occurs on the device's subscriber identity module (SIM) card. The SIM stores the IMSI in 4G and the Subscription Permanent Identifier (SUPI) for 5G, which are different forms of the combination of the mobile phone number, a unique network operator identifier, and the mobile network code assigned for that device. These pieces of sensitive information are the targets of cyber crooks, who fake the identity of a device to access a network. It is therefore critical to prove the device is authentic prior to granting it access to the network. Every wireless network in the world uses these identifiers to authenticate the device before granting access for the device to their network, but 4G and 5G take different approaches. While 4G sends a plain-text version of the IMSI over the air to the device when it joins the network, 5G networks block the "IMSI catcher" approach because they do not transmit plain-text versions of the identifier over the radio interface. Instead, the 5G network sends an encrypted version of the SUPI – called the Subscription Concealed Identifier, or SUCI – over the RAN to conceal the identity of the SUPI.

128-bit encryption provides 340 billion, billion, billion, billion possible keys for use by the cypher algorithm – 5G uses 256-bit encryption.



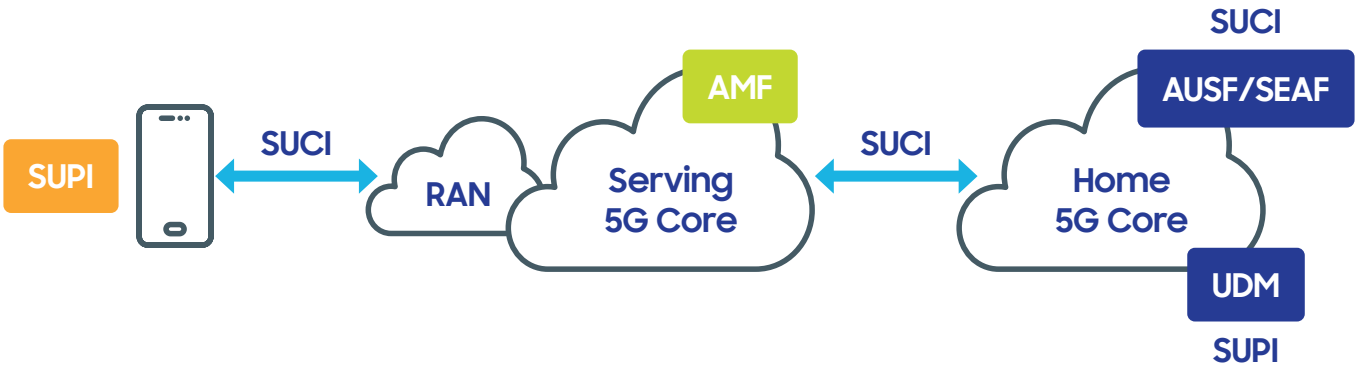
Another 5G improvement is the algorithm used for creating the encrypted SUCI. 5G's Authentication and Key Agreement (AKA) technique uses a randomized asymmetric process, which achieves better privacy than the 3G and 4G masking processes. The device uses the public key of the home network to encrypt the SUPI value before requesting service on the network. The authentication process in the home network uses a different private key to perform the authentication service. This private key is known only to the authentication service, and without the private key, the encryption algorithm is impenetrable, which makes stealing the identity of the device no longer possible.

The New 5G Owner of Authentication

With 5G, the authentication process for granting access to service networks has changed dramatically. In prior technologies, the serving system – the network where the user device was requesting service – conducted the authentication process, which required exchanging several messages between the serving system and the home system. Even though the system encrypted the sensitive information, the serving system stored the user identity data, thereby increasing the security risk for that user.

Before a device joins a network, the network authenticates the device, AND the device authenticates the network.

To reduce this risk to user information, 5G moves all authentication activity to the home system where two new network elements designed specifically for authentication and security reside. When a user requests service outside of their home network, that serving system RAN passes the encrypted SUCI value to the serving system's Access and Mobility Management Function (AMF) which then forwards it to the home 5G core network for authentication. In the home network, the Authentication and Security Function (AUSF) attempts to affirm that the device seeking access is authentic. The AUSF uses the Security Anchor Function (SEAF) to authenticate that the received SUCI for the device is currently in the network requesting service. This approach prevents fraudulent access such as spoofing the network into sending requests to the home network to request the IMSI and location of a device.



Through encryption and home authentication, the 5G network increases protection of the device and preserves the integrity of the network by only allowing access to authentic users. The 5G network now both enhances the authentication process and eliminates sending the user device's unprotected identity, preventing the theft of the ID by cyber criminals.

Better Security of User Data over the RAN

In addition to allowing only valid users on the network, 5G networks now provide more security to user data over the RAN. The 5G network can both validate traffic on each user data path – or bearer path – through the 5G network and establish on-demand, end-to-end secure connectivity using network slices for traffic that needs higher degrees of protection.

Data Path Integrity Protection

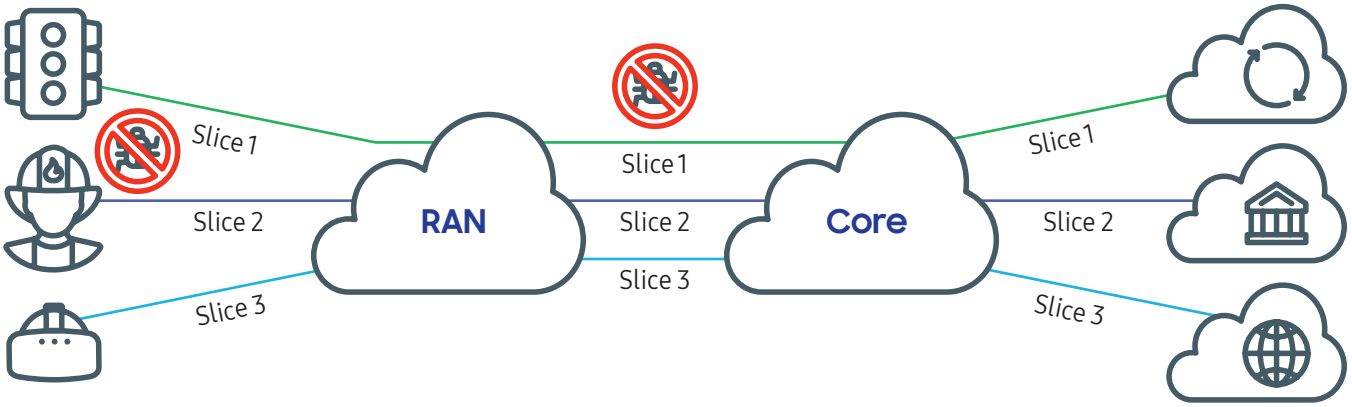
In LTE and 5G networks, the RAN encrypts the information sent between the user and the radio. While it is encrypted in LTE, the network does not include integrity checking for the masked data, so invalid data can consume spectral resources. 5G enhances the integrity of the RAN by providing integrity protection over the dedicated radio bearer (DRB). 5G's confirmation of integrity keeps traffic safe by discarding any traffic that fails the integrity protection check. Since the integrity validation is not needed on all bearer paths, Samsung makes this a configurable option on a per bearer path basis.

Slicing the Network to Segregate Private Traffic

Network slices provide service level agreements and incremental security using IPsec tunnels when needed for PDCP security configurations.

With its ability to virtualize and centralize control of the network and its resources, the 5G network provides more-secure management than distributed physical networks. With network slicing, the network automatically establishes multiple virtual networks over a single physical network. This creates virtually independent networks that can support a wide range of network services, ranging from business operations to creating new revenue streams, all on a common physical infrastructure. These individual slices of the network provide the user in that slice with the SLA they need, and additional security when needed, like IPsec tunnels for certain slices and different PDCP security configurations.

Virtualization in network slicing is key to its increased security. Like relying on isolation between virtualized components in virtualized and software-defined networks, network slicing requires isolation to prevent vulnerabilities from spreading to other components within the slice and between the slices in the case of malicious attacks.



In the virtualized RAN, backhaul and RAN architectures also require enhanced security to protect mobile devices, secure control and management of IoT devices, increase protection from distributed denial of service (DDoS) attacks, and solidify security between LTE eNB and 5G gNB and between gNBs. In addition, virtual firewall functions can block devices from reaching out to malicious servers, providing an additional layer of security to mitigate unknown air interface vulnerabilities.

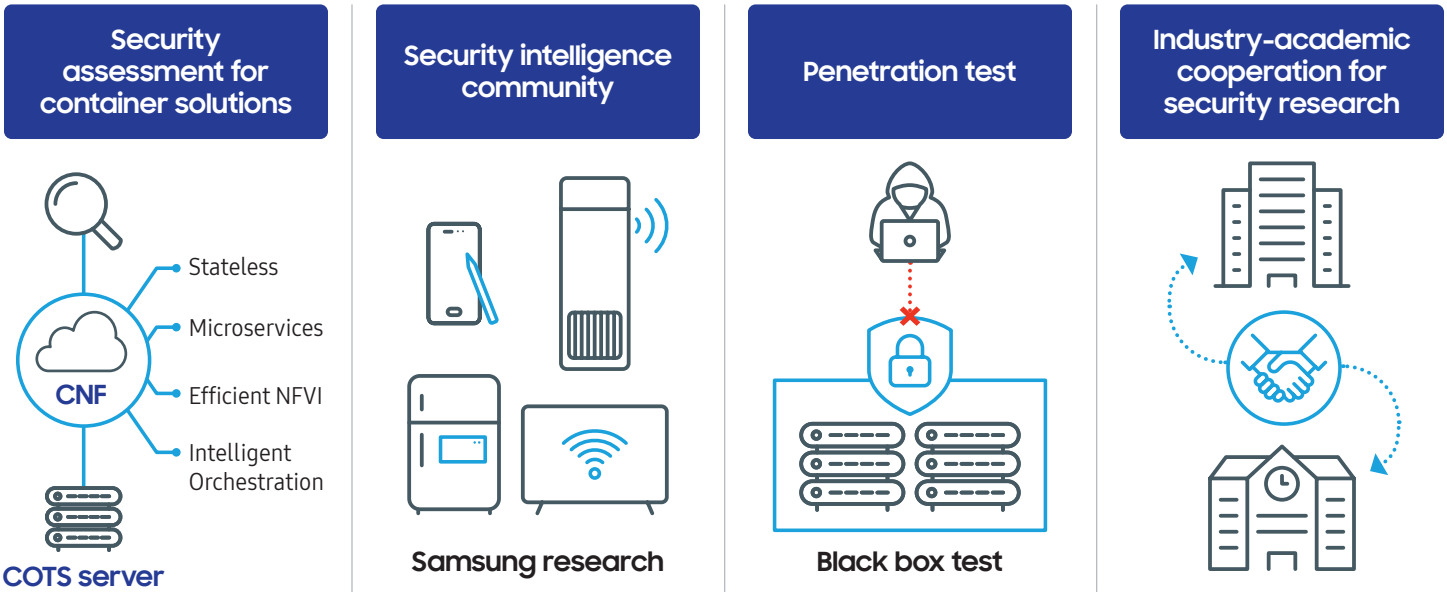
To protect mobile edge computing (MEC) servers and other datacenters, several techniques can help secure the traffic for the mobile network operator (MNO) and the enterprise. In addition to the user access control provided in 5G, network operators can also deploy DDoS protection in the locations housing the MEC server, the virtualized centralized unit (vCU,) and the virtualized distributed unit (vDU). A successful partnership between MNOs and enterprise and cloud providers can ensure a safe and secure datacenter that connects the vDU and vCU with other virtualized network functions to support MEC.

Samsung's 5G Security Protects It All

When it comes to keeping things safe and secure, Samsung knows operators are keenly focused on doing everything possible to secure their customers' data and communications. With Samsung's extensive industry-leading product breadth, from wireless networks and devices to connected home appliances and visual displays, Samsung constantly innovates security solutions that deliver in-depth defense and superior protection mechanisms. Samsung provides threat assessment and mitigation research, testing, and analysis for all facets of network products – including legacy physical network functions (PNFs), modern virtual network functions (VNFs), and cutting-edge containerized network functions (CNFs) that provide the foundation for Samsung's stateless, microservices-based cloud native 5G Core and vRAN.

To achieve these goals of enhanced security and privacy verification, Samsung Research focuses much of its efforts on developing core security technologies that provide full-stack security for product domains including device, network, service, and cloud. These security capabilities protect Samsung's products and all relevant data from theft and compromise. Samsung also works closely with academia to proactively research, study, design and test next-generation security technologies for future services.

In addition to research and design activities, Samsung proactively validates these architectures using white hat hackers to identify and resolve any vulnerabilities prior to solution deployment. Specifically, for wireless network solutions, Samsung subjects its LTE and 5G RAN and Core products to black box-based penetration attacks to ensure that the products can withstand even the strongest external attacks.



For 5G, security is vital, and Samsung participates with key standards groups to improve network performance in all areas of the network, including improved security designed into the 5G standards. Security is part of Samsung's DNA, and whether it is subscriber information, enterprise financial transactions, or mobile network management activities, Samsung provides the security central to ensuring that MNOs and their customers remain protected from cyber thieves. With defense-grade security designed from the chip up in Samsung's mobile device lineup and the highly scalable security functions incorporated into Samsung's vRAN and 5GC, Samsung delivers agile, end-to-end integrated security to protect MNOs and enterprises from the challenges of cyber threats.

SAMSUNG

6625 Excellence Dr
Plano, TX 75023

Sales: 1.877.556.9469
Service & Support: 1.800.737.7008

samsungnetworks.com