June 10, 2020

COMMUNICATIONS SECURITY, RELIABILITY, AND INTEROPERABILITY COUNCIL VII

REPORT ON RISKS TO 5G FROM LEGACY VULNERABILITIES AND BEST PRACTICES FOR MITIGATION

Working Group 2: Managing Security Risk in the Transition to 5G

Table of Contents

1 Results in Brief

1.1 Executive Summary

The 5th Generation (5G) in telecommunications technology is a revolutionary shift in core network architecture to a services-based approach that supports multiple access types, massive and unprecedented connectivity at much higher speeds and reduced latency. Connected vehicles, connected (smart) cities, wearables, healthcare and the Internet of Things (IoT) represent the initial set of use cases that 5G requirements has been designed to support. However, the introduction of 5G is a transition from 4G to 5G, based on the 5G Non-Standalone (NSA) Architecture. The NSA endeavors to bring 5G technology to market quickly, help service providers preserve 4G investment while introducing new services enabled by 5G and the evolution to the 5G Standalone (SA) Architecture. The transition is based on 3rd Generation Partnership Project (3GPP) standards that continue to evolve. The scope of Communications Security, Reliability and Interoperability Council (CSRIC) VII Working Group 2 (WG2) is to address the NSA and is the focus of this Report. CSRIC VII Working Group 3 (WG3) is chartered to address the SA and both groups leverage extensive collaboration; which is highlighted throughout this Report. While focused on the NSA, this report is the first in a series of reports from CSRIC VII regarding 5G.

Since the NSA architecture leverages existing 4G deployments and core network, many of the risks associated with 4G networks carry over to 5G NSA deployments. The security risks associated with 4G have been extensively studied by previous CSRIC Reports. These reports are a comprehensive compendium of threat analysis and risk mitigation. The corresponding recommendations are relevant to and greatly benefit risk management for the introduction of the 5G NSA. This Report uniquely builds upon previous CSRIC findings and recommendations by reviewing the threat landscape as 5G is introduced, leverages the National Institute of Standards and Technology (NIST) risk assessment methodology and creates a foundation for the efforts in WG3 and future CSRIC efforts. The recommendations herein focus on security enhancements brought about by 5G NSA, device threat mitigation and changes in workforce skills and training. In addition, recommendations for future CSRIC study are identified.

2 Introduction

As 5G telecommunications technologies are deployed by wireless service providers in the United States and around the world, its evolutionary design will incorporate a number of existing standards from previous generations. In this report, WG2 explores managing security risk in the transition to 5G and examines the risk to 5G from legacy vulnerabilities. WG2 then recommends best practices for mitigation.

5G wireless technology is poised to be the network of the future, delivering on the promise to reshape business, healthcare and to enable the applications that enrich people's lives and enhance their productivity. 5G will impact many aspects of people's lives. The way people live and work will become increasingly dependent on the availability and security of wireless communications. To meet this need, it is critical that 5G networks are highly reliable and

secure, ensuring the confidentiality and integrity of their intended use.

Like each preceding generation, 5G represents major advancements in speed. However, it is important to recognize that 5G is about more than speed alone. 5G is the first architecture that has been designed to support multiple network access types, including wireless, broadband and Wi-Fi. Connected vehicles, connected (smart) cities, wearables, healthcare and the IoT represent just a few of the use cases that 5G requirements have been designed to support. Much like 4G-enabled applications such as streaming video, the explosion of social media and the existence of services like Uber, 5G will enable the creation of new businesses and applications. Law enforcement, education, and commerce are likely sectors to be impacted in ways that enhance productivity and protect the environment through more efficient use of resources.

Architecturally, the transition from 4G to 5G is unlike preceding advancements in wireless technology. Where 4G represented a complete replacement of 3G radio networks and cores, 5G offers a network operator with a path that allows the focused introduction of services based on 5G radio while utilizing elements of 4G infrastructure. This will allow operators to begin introducing 5G radio while ensuring interoperability and backward compatibility with existing network infrastructure. Indeed, many operators will continue investing in their 4G networks for several years after beginning the introduction of 5G radio access.

To accomplish this feat of rolling out 5G radio access while preserving and expanding its 4G investment, an operator may elect to deploy 5G using an NSA architecture. In fact, some operators are already introducing services based on 5G radio access using NSA architecture, in which signaling and limited user plane traffic traverses the 4G network while the significant user plane traffic is carried on the 5G radio nodes. In this way the NSA architecture offers the operator a migration path to a full 5G SA network architecture.

WG2 has focused its efforts on this NSA architecture and the security issues related to it. Because this NSA architecture relies heavily on the 4G infrastructure in the core and radio access networks, many of the vulnerabilities of 4G networks will exist in an NSA deployment. In this report, WG2 will discuss those vulnerabilities from the perspective of those carried forward from 4G technology as well as new vulnerabilities that might be introduced in 5G radio. Finally, WG2 will provide its analysis of those vulnerabilities and put forward recommendations to the Federal Communications Commission (FCC) and industry regarding best practices and additional study.

2.1 CSRIC VII Structure

CSRIC VII was established at the direction of the Chairman of the FCC in accordance with the provisions of the Federal Advisory Committee Act, 5 U.S.C. App. 2. The purpose of CSRIC VII is to provide recommendations to the FCC regarding ways the FCC can strive for security, reliability, and interoperability of communications systems. CSRIC VII's recommendations will focus on a range of public safety and homeland security-related communications matters. The FCC created informal subcommittees under CSRIC VII, known as Working Groups, to address specific tasks. These Working Groups must report their activities and recommendations to the

Council as a whole, and the Council may only report these recommendations, as modified or ratified, as a whole, to the Chairman of the FCC.

Communications Security, Reliability, and Interoperability Council (CSRIC) VII					
CSRIC VII Working Groups					
Working Group 1: Alert Originator Standard Operating Procedures	Working Group 2: Managing Security Risk in the Transition to 5G	Working Group 3: Managing Security Risk in Emerging 5G Implementations	Working Group 4: 911 Security Vulnerabilities during the IP Transition	Working Group 5: Improving Broadcast Resiliency	Working Group 6: SIP Security Vulnerabilities
Chair: Craig Fugate, America's Public Television Stations	Chair: Lee Thibaudeau, Nsight	Chair: Farrokh Khatibi, Qualcomm	Chair: Mary Boyd, West Safety Services	Chair: Pat Roberts, Florida Association of Broadcasters	Chair: Danny McPherson, Verisign
FCC Liaison: James Wiley	FCC Liaison: Kurian Jacob	FCC Liaison: Steven Carpenter	FCC Liaison: Rasoul Safavian	FCC Liaison: Robert "Beau" Finley	FCC Liaison: Ahmed Lahjouji

Table 1 - Working Group Structure

2.2 Working Group 2 Team Members

WG2 consists of the members listed below.

Name	Company
Lee Thibaudeau* - Chair	Nsight
Jitendra Patel	AT&T
Susan M. Miller*	ATIS
Paul Diamond	CenturyLink
Charlotte Field*	Charter Communications
David Villyard	CISA DHS
Michael Geller	Cisco
Fei Yang	Comtech
John A. Marinho	CTIA
Jason Boswell	Ericsson
Brandon Abley*	NENA
Mohammad Khaled	Nokia
Travis Russell*	Oracle Communications
Sandeep Shrivastava	Orchestra Technology
Farrokh Khatibi*	Qualcomm
Greg Schumacher	T-Mobile
Drew Morin	T-Mobile
Brian Trosper*	Verizon

Table 2 - List of Working Group Members

* CSRIC Member

WG2 members had an option to nominate an alternate to participate in the discussions when the member was not available. Although the alternate is not a member of the WG2 and may not vote, they provide valuable input toward the completion of this report and should be acknowledged for their contributions. WG2 alternate members are listed in Table 3.

Name	Company
Steve Barclay	ATIS
Jeff Matisohn	Charter
Yousif Targali	Verizon
Kathy Whitbeck	Nsight
Jeff Wirtzfeld	CenturyLink
Scott Poretsky	Ericsson

Table 3 - List of Working Group Alternate Members

WG2 members had several subject matter experts present material relevant to the group's scope and charter. The subject matter experts are listed in Table 4.

Name	Company	Topic
Alper Kerman	NIST	Zero Trust Architecture
Peter Schneider	Nokia Bell Labs	Network Slicing Security
Peter Thermos John Kimmins	Palindrome Technologies	5G Mobile Security Technology & Services – Cybersecurity Perspective
Syed Rafiul Hussain	Purdue University	LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE

Table 4 - List of Subject Matter Experts

2.3 Working Group 2 Charter

Description*:* CSRIC VII WG2 is tasked to review risks to 5G wireless technologies that may carry over from existing vulnerabilities in earlier wireless technologies that can lead to the loss of confidentiality, integrity, and availability of wireless network devices. WG2 will recommend best practices to mitigate the risks for each vulnerability it identifies and address recently proposed solutions by security researchers.[1] Additionally, WG2 will recommend any updates, if appropriate, to the 3GPP SA3 (security working group) standards, including digital certificates and pre-provisioned Certificate Authorities, to mitigate these risks and then place the vulnerabilities on a scale that accounts for both risk level and remediation expense. Finally, WG2 will identify optional features in 3GPP standards that can diminish the effectiveness of 5G security and provide recommendations to address these gaps.

Milestones*:*

1. Report on Risks to 5G From Legacy Vulnerabilities and Best Practices for Mitigation – June 2020 (report contained herein)
2. Report on Recommended Updates to 3GPP Standards and Comparison of Risk and Remediation Expenses for 5G Vulnerabilities (this report will include identifying optional features in 3GPP standards that can diminish the effectiveness of 5G security and recommendations to address these gaps). – December 2020

[1] *See, e.g.,* Syed Rafiul Hussain et al., *Insecure Connection Bootstrapping in Cellular Networks: The Root of All Evil*, ACM WiSec 2019 (2019), https://wisec19.fiu.edu/accepted-papers.

3 Objective, Scope, and Methodology

3.1 Objective

The FCC directed CSRIC VII to review risks to 5G wireless technologies that may carry over from existing vulnerabilities in earlier wireless technologies and can lead to the loss of confidentiality, integrity, and availability of wireless network devices. CSRIC VII will recommend best practices to mitigate the risks for each vulnerability it identifies and address those recently proposed by security researchers.

Additionally, the FCC directed CSRIC VII to recommend any updates, if appropriate, to the 3GPP SA3 (security working group) standards, including digital certificates and pre-provisioned Certificate Authorities, to mitigate these risks and then place the vulnerabilities on a scale that accounts for both risk level and remediation expense.

Finally, the FCC directs CSRIC VII to identify optional features in 3GPP standards that can impact the effectiveness of 5G security, and recommendations to address these gaps.

The objective of WG2 is to provide the following deliverables with the focus on the transition from 4G to 5G:

- ❑ Review lessons learned from the previous generation of wireless technology (4G)
- ❑ Gather input from researchers, technologists and thought leaders
- ❑ Perform an assessment of implementation best practices
- ❑ Identify updates needed to the existing body of knowledge
- ❑ Identify barriers to implementation
- ❑ Advise and recommend accordingly

3.2 Scope

The scope of this report is to address a risk assessment as it relates to the transition from 4G to 5G wireless technology as defined in 3GPP standards. Additionally, the report provides recommendations to mitigate the identified transition risks, corresponding best practices as well as possible areas for future consideration. The analysis and assessment are based upon industry best practices and standards including NIST and International Organization for Standardization (ISO) Standards.

3.3 Methodology

CSRIC VII WG2 was directed to examine the security risks associated with the transition from 4G to 5G that result from both infrastructure and device changes that may introduce incremental security risk. The 3GPP, as well as several other standards organizations, continues work on 5G standards. A full 5G core (5GC) will not be likely until after 2020, and even then, on a limited basis. Wide-scale deployment of the 5GC will take time, as we have seen with other technologies (including 4G). As a result, the body of work on threats, risks and best practices to mitigate risk to 5G networks is still maturing. To address this limitation, WG2 relied upon several sources to compile the data to identify and evaluate the emerging security risks anticipated in the transition to 5G, including:

- Industry SME presentations
- Standards bodies and industry associations (GSMA, CTIA, ETSI, 3GPP, NIST, ISO)
- Individual contributor research gathered by WG2 members
- Academic papers

Some of the specific topics under consideration by WG2 arise because of the migration away from traditional, engineered systems designed to support specific network functions to a more distributed, software-based architecture. This new architecture exposes telecom networks to new attack vectors stemming from the adoption of information technology (IT) technologies. As a result, the research into the co-existence 4G and 5G, IoT, network function virtualization (NFV), software-defined networking (SDN) etc. are influenced by body of work addressing risk mitigation in the IT domain where these capabilities have existed for a number of years. The methodology and analysis within WG2 is focused on the NSA architecture and also considers interoperability with the 5G SA architecture relative to threats that may be introduced by 5G technology.

4 Background 5G

5G is commonly associated with the next generation of wireless network technology, but it is not limited to wireless access. 5G is more than an evolution from 3G or 4G networks. 5G represents a significant change for the telecommunications industry. 5G has been developed to support all access types, including Wi-Fi and wireline access, making 5G the network of networks.

Work on 5G began in 2012 with the ITU–R defining the vision and requirements for the next generation of wireless, IMT-2020. The 3GPP is writing the specifications for 5G to meet the IMT-2020 vision and requirements. 3GPP has submitted its specifications to the ITU as a candidate technology meeting the IMT-2020 requirements. The 3GPP, as well as several other standards organizations, such as the IETF, ATIS and others, continue to work on 5G standards.

The first release for 5G specifications in 3GPP is Release 15, with the early release complete in Dec of 2018 and two additional Release 15 “drops” in 2019. Currently, 3GPP is working on phase 2 of the 5G specifications in Release 16 (targeted for 2020) and has just defined the content and timelines for Release 17 (targeted for 2021), which further extends 5G for verticals.

Key advantages and benefits of 5G technology overall may be summarized as follows:

1. provides very high-speed access, even in densely populated areas,
2. connects everything, thereby supporting massive IoT and M2M communications**,**
3. provides real-time latency, thereby minimizing delays in network response time and enabling entirely new services and applications for vertical industries,
4. delivers significant improvements to security and privacy,
5. provides a Service-Based Architecture (SBA) that delivers increased flexibility and service diversity.

These key benefits are summarized in many industry papers including white papers from CTIA.[2,3]

There are three major use cases for 5G as specified by the ITU:

- Enhanced Mobile Broadband (eMBB) to provide high-data speed rates across a wide coverage area,
- Massive Machine-Type Communications (mMTC) for IoT to support connectivity for IoT, and
- Ultra-Reliable Low-Latency Communication, (URLLC) to support mission critical communications.

3GPP Release 15 concentrated on implementation of 5G New Radio (NR) to support the eMBB use case, while Release 16 adds the mMTC and URLLC use cases.

eMBB
This represents mobile broadband data services delivered to consumers via smart devices.

There are several features of 5G that support eMBB:

- High density – Radio Access Network (RAN) densification
- Gigabit data rates – multi gigabits per second
- Session awareness – discovery and optimization of sessions

mMTC
There are many predictions as to how many devices will be connected to the network beginning in 2020, with most falling in the range of 20 billion or more. This is one of the drivers of the requirements for 5G, and it has had the largest impact on the architecture of the 5G network.

- Ultra-low energy consumption – supporting 10+ years of battery life in some cases
- Ultra-low complexity – requiring 10s of bits per second to communicate with applications
- Ultra-high density – 1 million devices per Km

URLLC
Mission critical communications require URLLC. This is accomplished by supporting:

- Ultra-low latency – less than 1 millisecond
- Ultra-high reliability – less than 1 packet lost in every 100 million packets
- Strong security – to be trusted by governments, health, and financial institutions

4.1 What is 5G?

The telecommunications industry is in the process of deploying the next generation of technology, known as 5G.

[2] https://api.ctia.org/docs/default-source/default-document-library/5g_white-paper_web2.pdf
[3] https://www.ctia.org/news/protecting-americas-next-generation-networks

For the past several years, the telecommunications industry has been moving away from traditional engineered systems designed to support specific network functions in a point-to-point network architecture to adopt a virtualized, software-defined cloud-native IT architecture. 5G represents perhaps the largest change we have seen in communications networks since cellular service was introduced. Operators around the world are gearing up for cloud deployments of their critical infrastructure. As telecom networks move into the data center and cloud, the future architecture will draw increasingly from IT technologies that have supported the internet for many years.

While many operators have been focusing on the implementation of 5G networks in 2019 and 2020, the reality is that 5G NR will be deployed on a 4G Long-Term Evolution (LTE) network core and will leverage the LTE radio network for early implementations in NSA mode. The LTE network will be used for control and data, while the NR network will be limited to user plane data traffic. The 5GC will not be likely to begin seeing deployments until after 2020, and even then, on a limited basis. Wide-scale deployment of 5G next-generation core (NGC) will take time to implement, as we have seen with previous generations of network technologies (including 4G).

One of the goals of 5G is to be more resilient, and 3GPP has introduced new security procedures in the specifications. These 5G security specifications address several vulnerabilities that have impacted previous network evolutions. As with any new technology, 5G has the potential to introduce new attack vectors and requires a solid security framework to be implemented throughout the network. To address this, security considerations are an integral design consideration in the development of the 5G architecture specifications and standards that will result in a more resilient and secure framework for 5G network implementation.

The CSRIC VI, WG3 Report[4] focused on four main areas of 5G technology: IoT, NFV, SDN, and Open Source Software. This report builds upon the previous report and focuses on the evolution from 4G to 5G using the NSA architecture as the transitional phase prior to deployment of a full 5G NGC.

[4] 5G Final Report – Report on Best Practices and Recommendations to Mitigate Security Risks to Emerging 5G Wireless Networks - https://www.fcc.gov/files/csric6wg3sept18report5gdocx-0

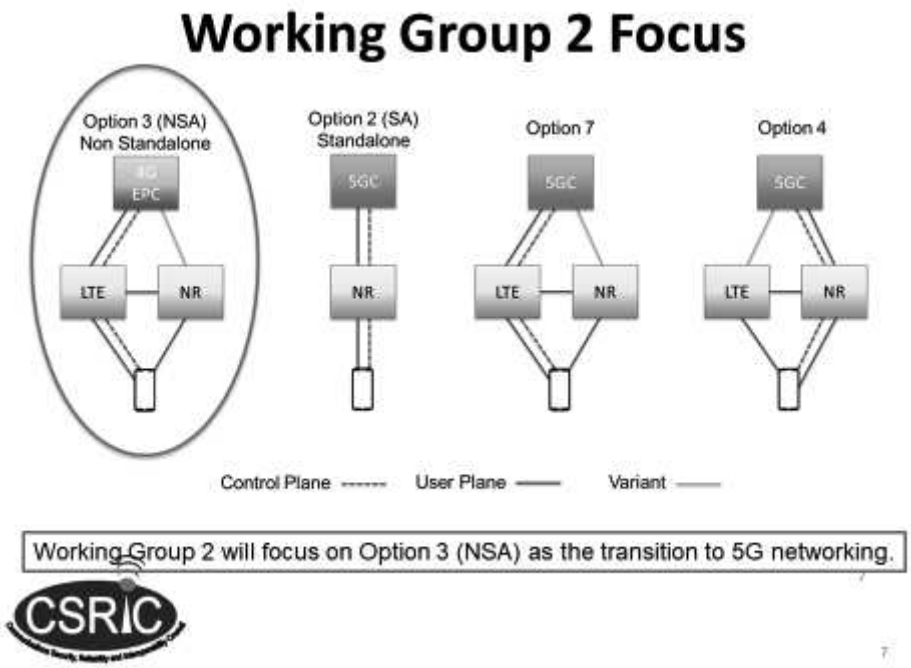


Figure 1, Working Group 2 NSA Focus

5G represents a complete change in the architecture and the business model for deploying networks. 5G changes the architecture of the core of the network to take advantage of IT technologies typically found in cloud implementations.

The 5G NGC is designed as a SBA, with the network functions in 5G acting more like web applications, providing services to the other nodes in the network and to the devices accessing the network. This represents the largest change in architecture the industry has seen in decades.

4.1.1 Speed and Latency Requirements in 5G

Performance speeds and latency requirements for 5G systems based on vertical industry service requirements are specified in 3GPP TS 22.261, titled Service Requirements for the 5G System.[5]

Unlike previous 3GPP systems that attempted to provide a one-size-fits all system, the 5G system provides optimized support for a variety of different services, different traffic loads, and different end user communities. Industry papers and specifications describe a multi-faceted 5G system capable of simultaneously supporting multiple combinations of reliability, latency, throughput, positioning, and availability. This is achievable with the introduction of new technologies, both in access and the core, such as flexible, scalable assignment of network resources. In addition to increased flexibility and optimization, a 5G system needs to support stringent key performance indicators (KPIs) for latency, reliability, throughput, etc. Enhancements in the air interface contribute to meeting these KPIs as do enhancements in the core network, such as network slicing, in-network caching and hosting services closer to the end

[5] https://www.3gpp.org/ftp/Specs/archive/22_series/22.261/

points which is referred to as Mobile Edge Computing (MEC) as outlined in the Figure below.

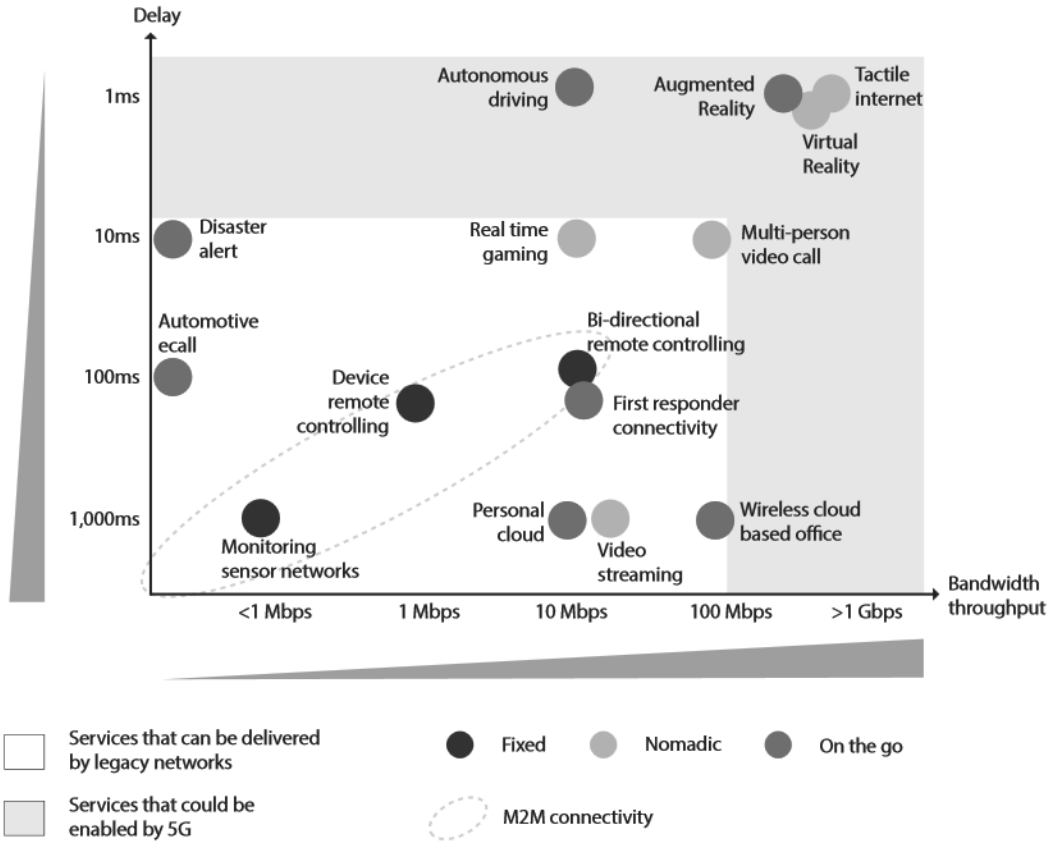


Figure 2 – Speed and Latency (Source: GSMA)

4.1.2 Evolution to 5G (3G-4G-5G)

In previous generations of wireless networks, services were delivered through engineered hardware appliances that provided specific network functions. There were not many functions in the previous networks. For example, the 3G network consisted of the following core network functions:

- Base Station Subsystem (BSS)
- Mobile Switching Center (MSC)
- Visitor Location Register (VLR)
- Home Location Register (HLR)
- Serving GPRS Support Node (SGSN)
- Gateway GPRS Support Node (GGSN)
- Equipment Identity Register (EIR)

3G was the first introduction of internet protocol (IP) in the network core, supporting data through technologies such as General Packet Radio Services (GPRS) and Universal Mobile Telecommunications System (UMTS). These represented data overlays in the 3G network

designed to support user data sessions without using the MSC.

In 4G LTE networks, the IP protocol was extended into the network core. The network functions remained somewhat similar, based on network appliances:

- eNode B
- Mobile Management Entity (MME)
- Visitor Location Register (VLR)
- Home Subscriber Server (HSS)
- Serving Gateway (SGW)
- Packet Gateway (PGW)
- Equipment Identity Register (EIR)
- Policy and Charging Rules Function (PCRF)

There are many functions provided by each of these network elements, making it difficult for operators to scale their networks up and down without having to upgrade an entire appliance.
In 5G networks, these functions have been decoupled from the hardware. Network functions are virtualized and run on common hardware platforms. There are a number of choices in implementing virtualization including NFV and cloud native.
There are many more network functions in the 5G network as many functions have been decoupled from previous elements:

- gNode B
- Access and Mobility Function (AMF)
- Radio Access Network (RAN)
- User Plane Function (UPF)
- Authentication Server Function (AUSF)
- Session Management Function (SMF)
- Service Communication Proxy (SCP)
- Network Slice Selection Function (NSSF)
- Network Exposure Function (NEF)
- Network Resource Function (NRF)
- Policy Control Function (PCF)
- Unified Data Management (UDM)
- Application Function (AF)

It is not the intent of this report to provide an overview of all 5G components. Rather, it is the intent of this report to raise awareness of what is different in 5G compared to previous network technologies and how this may impact security.

4.1.3 Evolution from NSA to SBA

Many operators will view an NSA 5G architecture implementation as a stepping stone to a full standalone implementation. The NSA option allows the operator to begin providing 5G services such as eMBB while preserving and leveraging investment in 4G technology.
In an NSA deployment the user equipment (UE) will signal to the 4G eNodeB that it is capable of simultaneously connecting to both the 4G and 5G networks. Once authorized by the core, the

4G eNodeB is notified that the UE is authorized to connect to the 5G network. The 4G eNodeB communicates with the 5G gNodeB to establish a bearer channel on the 5G network.

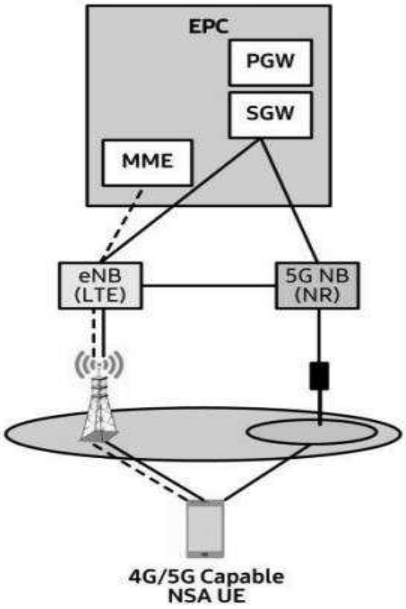


Figure 3, NSA Configuration, Source: Samsung[6]

CSRIC VI reviewed the security of the 4G network. The security characteristics and vulnerabilities of the 4G network will carry forward and be present in a 5G NSA implementation as well. Additionally, in an NSA implementation the interconnection of the 5G gNodeB with the 4g eNodeB and the evolved packet core (EPC) present new security challenges to the operator.

In previous generations, network appliances connect to one another using point-to-point interfaces. In voice services, there are specific network functions that are used for every voice call. Likewise, in data sessions there are specific network appliances that support every data session. This proves problematic for IoT, where support of billions of devices trying to send simple data sets to an application do not need all of the functionality provided in traditional networks. This is one of the drivers to moving to a SBA. It is important to note that the SBA will be deployed in the 5G SA core and is not part of 5G NSA which relies on the existing 4G LTE core. It is included here only for completeness. CSRIC VII WG3 is focused on the 5G SA and will comprehensively address the topic in their report.

A SBA is not new. Cloud applications use SBA to deliver services through a web application programming interface (API). This concept has been adopted by the 3GPP and used in 5G where network functions are delivered as services, as needed.

To accomplish this, traditional signaling such as SS7 or Diameter is eliminated. There is no need

[6] https://images.samsung.com/is/content/samsung/p5/global/business/networks/insights/white-paper/4g-5g-interworking/global-networks-insight-4g-5g-interworking-0.pdf

for complex signaling protocols with specific message sets defined for each function. In place, each network function is able to advertise the services it can provide to the network and when a specific function is needed to support a session, the device is able to connect to the function through a common RESTful API using HTTP commands.

4.1.4 User Plane-Control Plane

Separation of the control plane from the user plane was defined in 3GPP Release 14, for 4G LTE. The intent was to improve the scalability of the packet core components, and to provide more flexibility for operators when implementing the packet core.

As operators began moving their packet core to the cloud, additional latency became an issue because user data had to be sent to the centralized cloud for processing. This was because the control and user plane were combined, and all processing had to take place in the core.
To address critical, time-sensitive traffic that required low latency, the control plane was separated from the user plane, allowing higher priority traffic with low latency requirements to be sent to the internet at the edge of the network, while keeping the control traffic in the core. This also allows for more scalability. If there is a lot of video streaming for example, additional bandwidth may be necessary at the user plane, but the control plane does not need the additional capacity. Likewise, if there is a lot of messaging traffic, the control plane may need additional bandwidth to process all of the signaling traffic, but the user plane does not need additional capacity.

4.1.5 Network Slicing

There is no accepted industry-wide definition for network slicing. In basic terms, network slicing provides operators the ability to provide Network Functions (NF) for specific services such as eMBB. The radio access and the network core functions needed to support that service are dedicated in the network slice (a virtual network dedicated to the use case). This allows operators to provide dedicated resources to support services, while sharing the network functions across all of the services. NF can be shared across network slices, or they can be dedicated to a specific slice. Network slicing segments traffic for traffic isolation and service differentiation, as shown in the Figure below; the purpose of the network slice is to meet SLAs for QoS and security that are specific to the service and use case.

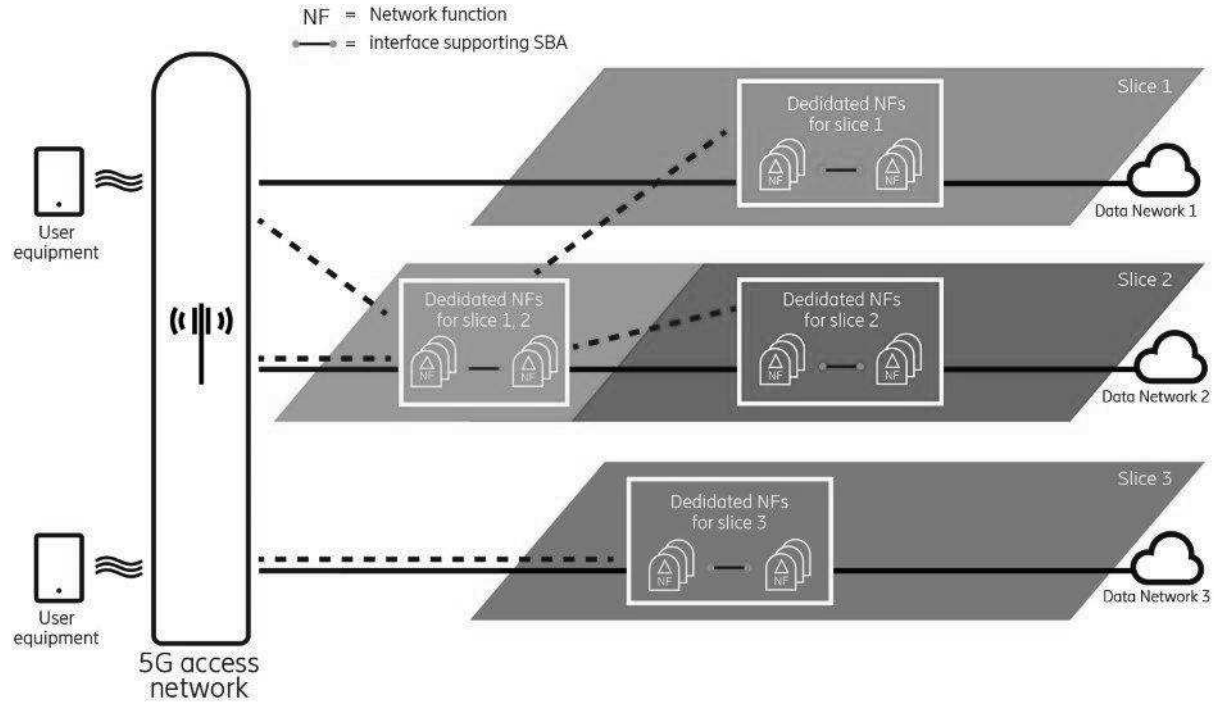


Figure 4, 5G Network Slicing, Source: Ericsson[7]

The Single Network Slice Selection Assistance Information (S-NSSAI) identifies network slices. The Network Slice Selection Assistance Information (NSSAI) consists of the Slice/Service Type (SST) and the Slice Differentiator (SD). The SD identifies individual slices when there are multiple slices of the same type.

Access to a network slice can be secured by authenticating the users for specific network slice access. This could be accomplished along with network access authentication by the operator, and additionally enterprises who uses the network slice can also authenticate for additional control. Slicing also provides for two distinct types of protection – resource isolation and data/security isolation. Resource isolation ensures that necessary resources assigned to a slice (compute, memory, storage, networking, etc) cannot be consumed by another slice. Data isolation ensures that information in one slice cannot be accessed or modified by other slices sharing the same underlying infrastructure.

These additional security protections and considerations should be considered, even when/if the operator's core is not terminating the slice, as slicing specific requests can be extended to other cores or through roaming connections via the Security Edge Protection Proxy (SEPP). The Security Edge Protection Proxy is similar to the DEA (diameter edge agent) in 4G – it provides centralized roaming partner management, topology hiding and traffic management, while additionally supporting security protocols, certificate exchanges and application layer security.

[7] https://www.ericsson.com/en/digital-services/trending/network-slicing

4.1.6 NG-RAN New Radio

The 5G NR refers to a radio architecture that builds upon and expands certain capabilities originally introduced in LTE. 5G NR was designed to provide enhancements in flexibility, scalability and efficiency, both in terms of power and spectrum utilization. In 5G NSA deployment the LTE network is utilized for control functions while the 5G NR is used exclusively for user plane traffic.

5G NR was designed to accommodate a wide range of frequency bands in a single or grouped radio interface. The OpenRAN Project Group under the Telecom Infra Project (TIP) organizes these bands into two basic ranges: (1) frequency range 1 refers to frequency bands below 6GHz, and; (2) frequency range 2 refers to frequency bands in the millimeter wavelength range, basically above 24GHz. By accommodating this wide range of frequency bands, 5G NR can provide radio access for the wide variety of applications anticipated for 5G networks and the performance demands of each.

Additionally, 5G NR has been designed to handle much wider channels than LTE, up to as much as 400MHz. As well, a variety of channel spacing options are specified to optimize the noise and interference characteristics of the frequency in use.

In the next generation radio access network (NG-RAN), the gNB consists of two major functions; the distributed units (DU) and the central unit (CU). The CU is divided into the CU-control plane and the CU-user plane. The same is true of the DU. The CU-CP is responsible for connecting to the 5GC network control plane (N2) towards AMF, while the CP-UP is responsible for connecting to the DUs in the RAN and user plane (N3) towards UPF. The relationship between the CUs and DUs is generally a one-to-many, where one CU may control multiple DUs. CU functionality does not require colocation with DUs to facilitate virtualization.

4.1.6.1 Sub 6 GHz

Sub-6GHz includes the spectrum range below 6GHz. Generally, this spectrum range can provide broad network coverage with lower probability of interruption than the spectrum range above 6GHz. Spectrum below 6GHz, due to its longer wavelength and capability to penetrate obstacles, requires lower capital and fewer base stations, therefore offering more rapid deployment than networks utilizing millimeter wave (mmWave) spectrum. Sub-6GHz will provide a broader solution for more wide area 5G coverage in the near term.

4.1.6.2 6 GHz and Above

Spectrum above 6GHz is generally referred to as mmWave, typically above 24 GHz for 5G deployments. This spectrum range offers several advantages for 5G deployments. The spectrum's shorter wavelengths create narrower beams and with the wider channel bandwidths available at the mmWave frequencies, it allows for large amounts of data at increased speeds with lower latencies.

However, mmWave spectrum is not without its share of challenges. The very qualities that make

mmWave attractive, higher speeds and lower latency, also limit the distances it can propagate as well as its ability to penetrate objects. These characteristics create high infrastructure costs, as a mmWave network would require a very dense base-station deployment.

5G networks utilizing mmWave spectrum will undoubtedly be deployed in environments where demand requires it and the propagation and cost considerations are not prohibitive.

4.2 Improvements of 5G NR over 4G LTE

Interference mitigation is listed as one of the key issues in 3GPP TR33.809 (Study on 5G NR Security Enhancement Against False Base Stations). A few 5G NR techniques are mentioned as potential mitigation techniques including beamforming and RAN slicing. The vulnerabilities of 4G LTE to interference are well documented.[8] The 4G LTE vulnerabilities on physical channels and signals include:

- Synchronization signals (primary and secondary) are at the fixed locations of the 2-dimensional orthogonal frequency division multiplexing (OFDM) resource grid.
- Master information block (MIB) inside physical broadcast channel (PBCH) is at a fixed location.
- Cell-specific reference signal (CRS) is at fixed locations although the specific locations are a function of the Physical Cell ID (PCI).
- The downlink physical control format indicator channel (PCFICH) is at a fixed location.

In general, 4G LTE design in the frame structure is rigid and transmissions of broadcast messages and signals are repetitive. However, 5G NR design is highly flexible and transmissions of broadcast messages and signals are mostly on-demand such that various services (e.g. eMBB, URLLC and massive IoT) can be supported.

The following presents some improvements of 5G NR over 4G LTE. These improvements can be leveraged to provide interference mitigation. For each improvement, the operation in 4G LTE is described to establish the baseline.

In 4G LTE, the primary synchronization signal (PSS), secondary synchronization signal (SSS) and PBCH are always located in the center of the downlink channel bandwidth. PSS and SSS are used to assist the UE to acquire time and frequency synchronization with a cell and detect its physical cell identity (PCI). After the UE detects the PCI, the UE completes the cell search. The PBCH is adjacent to the PSS and MIB is carried inside the PBCH. In each 10 ms frame, there are two occurrences of PSS/SSS where PBCH is associated with just one PSS/SSS. The pattern for transmissions of PSS/SSS and PBCH (i.e., the locations of the signals and channels within a frame) is always fixed. After UE acquires MIB, it decodes system information blocks (SIBs) on the downlink to understand the cell configurations and prepare for establishing radio resource control (RRC) connections.

For 5G NR, its MIB is part of synchronization signal block (SSB) which consists of all three: PSS/SSS/PBCH. The numerology (μ) and cell-operating frequency determine the transmission pattern of SSB. SSB is not always in the center of the channel bandwidth. 5G NR has a new

[8] M. Lichtman, R. P. Jover, M. Labib, R. Rao, V. Marojevic, and J. H. Reed, "LTE/LTE-A jamming, spoofing, and sniffing: threat assessment and mitigation," IEEE Communications Magazine, vol. 54, no. 4, 2016.

concept called the synchronization raster that indicates the candidate frequency locations of SSBs when explicit signaling of the SSB position is not present. Numerology (μ) defines the OFDM configurations: 0 – 4 where 0 is the same as LTE. When μ becomes larger, wider subcarrier spacing, shorter symbol duration, and more slots per frame are the result.

The 4G LTE CRSs are sent continuously on the downlink. They are transmitted on equally spaced subcarriers at the first and third from last symbol of each slot. RSs are sent on every sixth subcarrier. The starting position of RSs on the frequency domain is a function of PCI. In 5G NR, the CS-RSs are eliminated. 5G NR introduces new types of RSs and RSs are sent on-demand.

In 4G LTE, the PCFICH (downlink channel) indicates the amount of resource in the time domain for control channels to use (i.e., it indicates the size of control region). PCFICH is always at the beginning of a downlink subframe. In 5G NR, this channel is eliminated.

In 4G LTE, the PHICH (downlink channel) transmits Hybrid ARQ (HARQ) acknowledgements responding to uplink shared channel transmissions. Its symbol location is always at the beginning of a downlink subframe. In 5G NR, the HARQ is asynchronous so there is no need for a dedicated channel to handle acknowledgements. As a result, the PHICH is removed.

In 5G NR, a bandwidth part (BWP) is a set of contiguous physical resource blocks (PRBSs) within a given frequency carrier using a given numerology for a UE to receive and send user applications, where the BWP is ≤ operating carrier bandwidth. Instead of using the whole channel bandwidth of the operating carrier for UE to communicate with the 5G NR base station (gNB), a UE uses a BWP. Flexibility in BWP allows vendors to build different categories of UE (e.g., supporting different sizes of BWP) and that UE will still work in any 5G NR cell whose channel bandwidth may be much larger than the BWP. In addition, BWPs allow for asymmetric allocation of channel sizes for UL/DL of a 5G NR connection which is not possible in LTE.

5G NR also supports antenna beamforming capability whose beam directivity can be used to mitigate interference.

A comparison of the differences in channels and signals between 4G LTE and 5G NR is summarized in the following table.

	5G NR	4G LTE
PCFICH, PHICH and cell-specific reference signal (CRS)	Eliminated	At fixed location of two-dimensional resource grid
Synchronization Signals and Master information block (MIB)	The location is a function of numerology or configured by higher layer	Fixed in center of channel bandwidth
Channel Bandwidth	Variable via the use Bandwidth Part (BWP) Asymmetric for uplink / downlink	Fixed Symmetric for uplink / downlink
Beam	Multiple Beams	Does not exist

Table 4 – Comparison 5G NR and 4G LTE[9]

[9] See: 3GPP TS 33.809, https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3539

4.3 New Security Enhancements in 5G

There are a number of enhancements made in 5G specifications to provide increased security as compared to 3G and 4G. These include, unified authentication framework and access-agnostic authentication, primary authentication by the network operator and additional secondary authentication to an external data network, Increased home operator control, enhanced subscriber privacy, user plane integrity protection in RAN, SBA and interconnect security in the 5GC etc.

However, these enhancements are only available in 5G SA networks, and do not apply in NSA configurations where 4G core networks are used. As a result, 5G networks that are using the Option 3 NSA implementation model face the same core network security vulnerabilities as 4G LTE networks.

The CSRIC VI, WG3 published a report[10] on 4G security (See Section 5.1.2) that identifies the vulnerabilities with using the 4G network.

4.4 Use Cases

5G is well suited for the transformation of the vertical industries outlined in the preceding section, supporting a wide variety of applications and use cases with high variability in key performance attributes such as mobility, data rate, scale, latency and reliability. For example, mobility could range from an application like fixed wireless service to connected vehicles that may be moving at speeds of 80 miles per hour. Data rates could vary across a similar range from bits per second for some IoT devices to gigabits per second for virtual reality. The ultra-low latency needed to enable real-time applications like industrial automation is different from smart home applications that may be more delay tolerant. The rapidly increasing number of devices will necessitate the ability to rapidly scale services. Reliability is critical for remote surgery and healthcare monitoring but maybe less so for some remote sensors and meters in smart cities.

In the previous section, a few use cases for different verticals were described and it is notable that even use cases within the same vertical can have distinct KPIs. As an example, an automated product line use case in the industrial automation vertical requires low latency and highly reliable communication. These are different KPIs when compared to the use case on inventory and supply chain optimization in the same vertical, which requires many sensors and the latency requirements are much less strict. As a result, use cases can be categorized based on their performance attributes.

1) *eMBB:* These use cases generally have requirements for higher data rates and better coverage.
2) *mMTC:* These use cases generally have requirements to support a very large number of devices in a small area, therefore, they support a large device density.

[10] 5G Final Report – Report on Best Practices and Recommendations to Mitigate Security Risks to Emerging 5G Wireless Networks - https://www.fcc.gov/files/csric6wg3sept18report5gdocx-0

3) *Critical Communications:* These use case have strict requirements on latency and reliability. They are also referred to as URLLC.

With such a large variation in performance attributes, it is also useful to consider these different use cases in terms of their types of interaction: between people, between machines, or between people and machines.

Combining these types of interaction and grouping the use cases by the primary categories that 5G will impact extreme mobile broadband, massive scale communication and ultra-reliable low-latency service creates a powerful alternative visualization. It enables a vision of the way certain use cases will span across multiple types of interaction and various performance requirements. Figure 5 shows this new taxonomy for some 5G use cases.

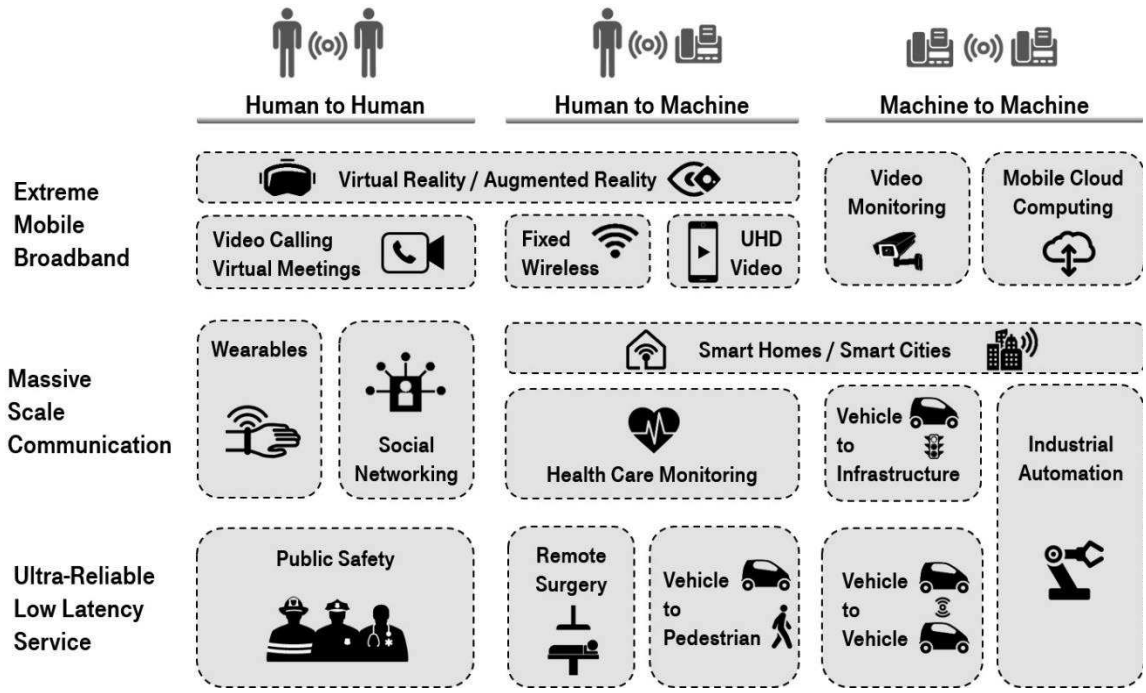


Figure 5: 5G use cases grouped by the type of interaction and the range of performance requirements. SOURCE: page 19 of 5G Americas Services & Use Cases.

The use cases associated with the mMTC depicted as massive scale communication in the Figure above will typically leverage the emerging low power wide area (LPWA) needs for low cost devices, extended coverage, and long battery life. The use cases are expected to make up a large part of the new types of services that 5G systems will address by connecting the massive number of devices such as sensors, actuators, cameras, and wearables.

This family of use cases is expected to be pervasive in smart cities, as buildings and industries will evolve that leverage these devices providing metering, lighting management in buildings and cities, environmental monitoring (pollution, temperature, noise, etcetera) and traffic control, among many other applications.

These services are expected to require the ability to support a high density of devices with different characteristics in a common communication framework. The mMTC service category includes applications used in a wide spectrum of industries across society, including both human-to-machine interaction and machine-to-machine interaction, as shown in the following figure:

Figure 6: Several use cases in mMTC category enabled by 5G technologies. SOURCE: 5G Americas Services & Use Cases

4.5 Implementation Models – Architecture

There are three parts in wireless networks: the RAN, the packet core, and the network core. In 5G, this has narrowed to the radio access network and the network core (but no functions have been eliminated – the packet core and network core have been combined).

The RAN is independent of the network core but cannot deliver services by itself. It relies on the network core to provide authentication of devices, authorization for devices to access services, and charging. Services cannot be delivered by the radio access network alone; it requires the network core.

The RAN is usually the most discussed part of the network because this is where the requirements for speeds get defined. However, the radio access network cannot deliver the speeds of 5G alone; it requires the new architecture of the 5GC to deliver the full 5G benefits, including speeds.

There are four implementation models proposed by 3GPP:

- Option 2 – SA

- Option 3 – NSA
- Option 4 – 5GC with both 4G and 5G radio
- Option 7 – 5GC with both 4G and 5G radio

Option 2 is a stand-alone network. That is, there is no dependency on previous technology to support the network. In Option 2, there is no dependence on 4G network core, nor is there an option to support 4G radio. This is most likely the model to be used years down the road.

Option 3 is the most popular and what is being used today to deliver 5G services to subscribers. Option 3 is also referred to as NSA because of its reliance on the existing 4G core network. WG2 is focused on the vulnerabilities with option 3.

Option 4 requires a 5G network core and 5G NG-RAN. This option allows the operator to use their 5G network and 5G radio, taking advantage of all of the 5G features, while also continuing to support 4G radio access. The 4G radio node (eNB) acts as a secondary node, connecting to the 5G radio node (gNB), which then provides connectivity and signaling to the 5GC network.

Option 5 is similar, but the 4G network remains as the main anchor in the network, connecting to the 5GC network directly. This requires an upgrade to the 4G eNB to be able to support direct 5GC connectivity.

Option 7 supports another 5G capability known as dual connectivity. It requires a 5GC network and an upgraded eNB able to connect directly with the 5GC. This is very similar to option 4 and 5, with the eNB (4G radio node) connecting to the 5GC directly. The 5G gNB can send packet data through the 4G eNB or connect directly with the 5GC as well (hence the dual connectivity).

4.5.1 Standalone Architecture

A 5G SA architecture refers to a fully independent 5G network. The 5G air interface, new radio, and 5G core (5GC) are in place and provide an end-to-end 5G customer experience. A 5G standalone network is capable of providing a full range of 5G use cases, including eMBB, URLLC and mMTC. While a 5G standalone SA network can operate independently, interoperability with LTE networks may be required to provide coverage in areas not yet covered by 5G as well as to provide connectivity between 5G and non-5G users.

4.5.2 Non-standalone Architecture

In an NSA 5G implementation, 5G NR cells are in place using the 4G EPC as the core. While the 5G NR cell site radios serve the user plane, the network depends entirely on the LTE network for all control functions, such as mobility management. Typically, a 5G NSA implementation allows the operator to launch seamless 5G services faster, and potentially requiring lower initial investment, by leveraging existing infrastructure than might be the case with a 5G standalone implementation. However, while a 5G NSA implementation will support eMBB, it will not support advanced use cases such as URLLC. Further, a 5G NSA network may provide one step on a carrier's migration path to a 5G SA network.

4.5.3 Transition Options (Options 2 and 3, and others)

As indicated in previous sections of the Report, the NSA option (option 3) relies upon the 4G EPC, while the SA options rely upon the 5GC. The SA architecture operates within the Zero Trust security model,[11] while the NSA option operates within the existing 4G security paradigm. It is envisioned that both security models may coexist with the same carrier network or across differing carrier networks (i.e. roaming).

Table 5[12] is an excerpt from the referenced paper and compares 4G and 5G authentication methods, highlighting differences between the two. For example, 5G authentication has different entities from 4G because 5G adopts service-based architecture. Other major differences include the trust models in methods based on EAP-TLS or AKA protocols.

This report will endeavor to study the security model differences and provide a risk assessment for mixed NSA and SA environments.

		4G Authentication	5G Authentication		
		EPS-AKA	5G-AKA	EAP-AKA'	EAP-TLS
ENTITIES (LOCATED IN)	USER EQUIPMENT (UE)	USIM	USIM		USIM/Non-USIM
	SERVING NETWORK (SN)	MME	SEAF		
	HOME NETWORK (HN)	HSS	AUSF UDM/ARPF/SIDF		
MESSAGE FORMAT	UE <-> SN	NAS	NAS	NAS|EAP	NAS|EAP
	SN <-> HN	Diameter	HTTP-based web APIs		
TRUST MODEL		Shared symmetric key	Shared symmetric key		Public key certificate
UE IDENTITY	UE -> SN	IMSI/GUTI	SUCI/5G-GUTI		
	SN -> HN	IMSI	SUCI/SUPI		
SN IDENTITY		SN id (MCC+MNC)	SN name (5G:MCC+MNC)		
AUTHENTICATION VECTOR GENERATED BY		HSS	UDM/ARPF	UDM/ARPF	N/A
AUTHENTICATION OF UE DECIDED BY		MME	SEAF & AUSF	AUSF	AUSF
HN INFORMED OF UE AUTHENTICATION?		No	Yes	Yes	Yes
ANCHOR KEY HIERARCHY		K_i -> CK+IK -> K_{ASME}	K_i -> CK+IK -> K_{ASME} -> K_{SEAF}	K_i -> CK+IK -> CK'+IK' -> EMSK -> K_{SEAF}	EMSK -> K_{AUSF} -> K_{SEAF}

Table 5 – Comparison 4G and 5G Authentication, Source: CableLabs

4.5.4 Open and Interoperable Network Architecture

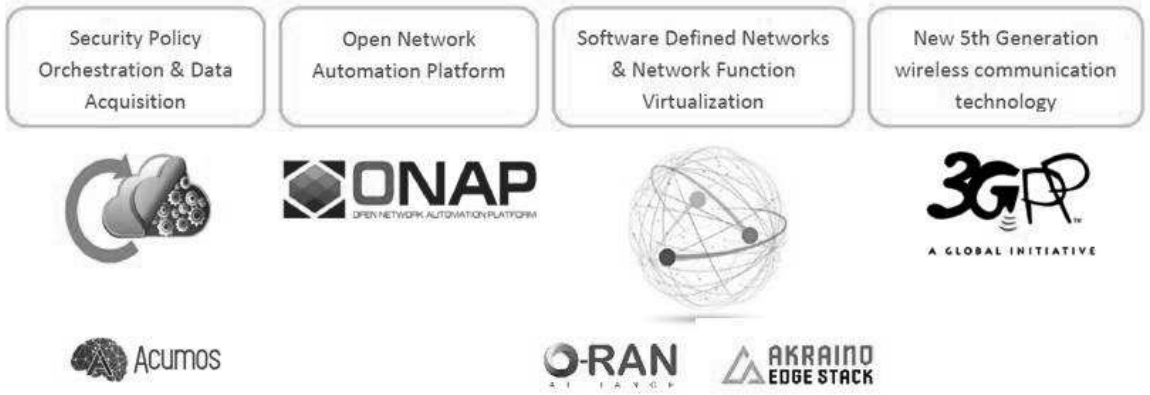
There are two major industry initiatives looking at evolving and opening up the radio access networks. The first is the O-RAN Alliance,[13] and the second is the OpenRAN project group

[11] https://csrc.nist.gov/publications/detail/sp/800-207/draft
[12] https://www.cablelabs.com/insights/a-comparative-introduction-to-4g-and-5g-authentication
[13] https://www.o-ran.org/

under the Telecom Infra Project (TIP).[14] ORAN is expected to be addressed in the Report from CSRIC VII WG3, and is mentioned here for completeness.

As the core network leverages more instances of the traditional IT platforms to enable all services, the use of open and interoperable software by mobile network operators (MNO) will inevitably increase. While this will not drive specific changes in best practices related to the use of open source software, the community as a whole will benefit from the expanded use that will result from the addition of companies in the 5G ecosystem. As a result, it is likely that the increased visibility into open-source software will result in improvements in vulnerability detection, reporting, and patching. Open source can also introduce new security risks due to publicly reported vulnerabilities, re-use of code, and trust exploits enabling backdoor attacks. A security program built on best practices and proper due diligence will determine the level of risk in open source deployments.

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



4.6 Standards

The 3GPP unites seven telecommunications standard development organizations (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC), known as "Organizational Partners", and provides their members with a stable environment to produce the reports and specifications that define 3GPP technologies[15]. 3GPP standards work comes in releases. Release 15 defines the first set of 5G requirements, including continued work on the enhancements of the current 4G network core that many network operators will use to launch 5GNR, until the full work of the 5GC is complete in Release 16 (see Figure below). There are a number of standards bodies that will work to enable 5G. No single standards body can be said to control the definition of 5G. Of course, 3GPP, which has been instrumental in the development of mobile wireless standards to date, will continue to play a leading role, especially as it evolves to include non-terrestrial technologies such as satellite and high-altitude platforms. In addition, other standards bodies,

[14] https://telecominfraproject.com/openran/
[15] http://www.3gpp.org/about-3gpp

such as ATIS and GSMA, will play an important role.

The ITU 5G Infrastructure Public Private Partnership (5GPPP) has been working with 3GPP and others to define spectrum requirements, as well as other areas not addressed by 3GPP. Likewise, the Internet Engineering Task Force (IETF), the Next Generation Mobile Networks (NGMN) Alliance, IEEE, the GSM Association (GSMA), and Small Cell Forum have been contributing requirements.[16]

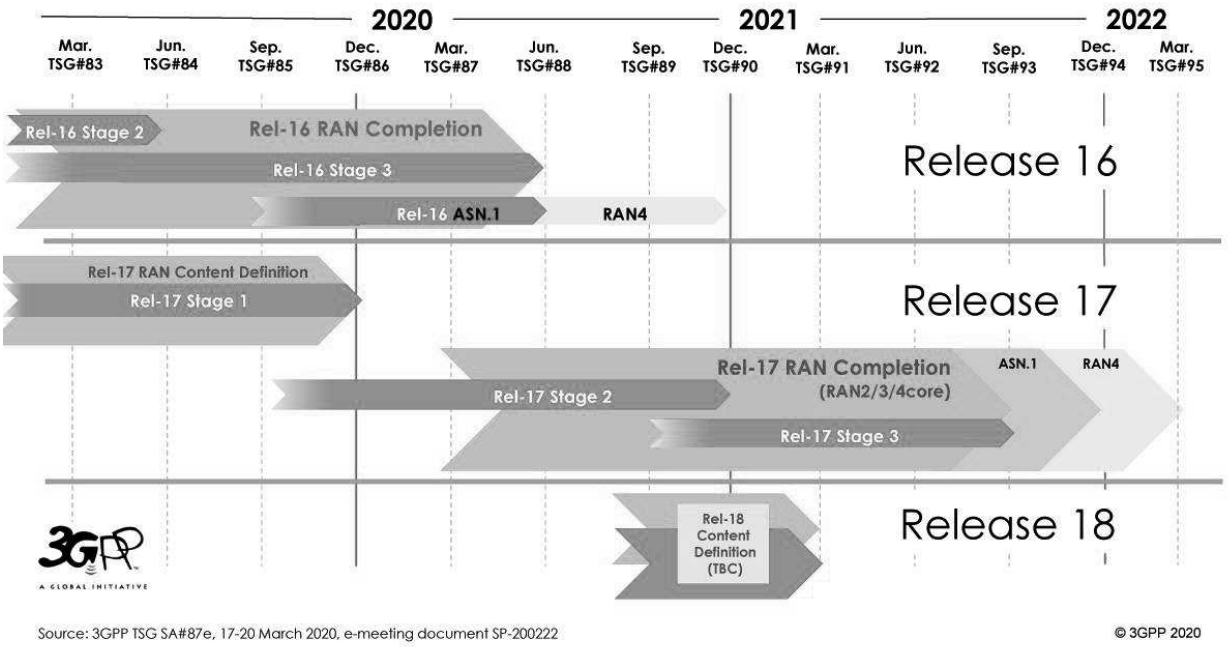


Figure 7 – 3GPP 5G Standards [17]

[16] Fierce Wireless; "How ITU, 5GPPP, NGMN and others will create the standard for 5G"

[17] See: https://www.3gpp.org/images/articleimages/Releases/graphic_version3_SP-200222.jpg

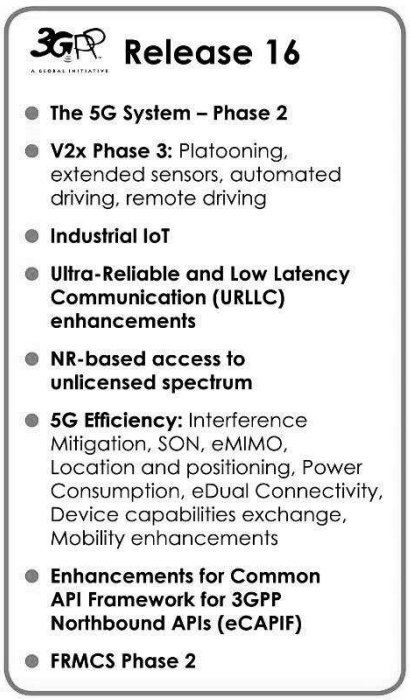


Figure 8 – 3GPP Release 16 Standards[18]

4.7 Previous Work Efforts

There has been a substantial focus on identifying threats, mitigating actions and best practices to address the cyber security of the IoT. Numerous reports have been generated as a result of the work of these public/private partnerships. Since much of this content will be directly applicable in the 5G environment, some of these reports are referenced below.

4.7.1 CSRIC – Previous Working Groups

4.7.1.1 CSRIC IV, WG3 Network Reliability and Security Risk Reduction

CSRIC IV, WG3 was tasked to evaluate mechanisms to best design and deploy 5G networks to mitigate risks to network reliability and security posed by the proliferation of IoT devices and open-source platforms used in 5G networks.[19] Specifically, WG3 was tasked to evaluate security risks within:

- IoT
- Open-source 5G software (e.g. OpenStack)
- NFV and SDN

As part of this assessment, WG3 developed risk impacts for each of the key areas and provided recommendations to mitigate the identified risks and best practices within design, deployment

[18] 3GPP Release 16, https://www.3gpp.org/release-16
[19] CSRIC VI Final Report – Report on Best Practices and Recommendations to Mitigate Security Risks to Emerging 5G Wireless Networks v14.0

and operation of risk-tolerant 5G. WG3 submitted an addendum for the supply chain section separately to allow more time to consider work in progress in industry.

4.7.1.2 CSRIC IV, WG5 Remediation of Server-Based Distributed Denial of Service (DDoS) Attacks

CSRIC IV Working Group 5 (WG5) provided recommendations that communications providers can take to mitigate the incidence and impact of DDoS attacks from data centers and hosting providers, particularly those targeting the information systems of critical infrastructure sectors. The recommendations are mainly in the form of server-based DDoS mitigation best practices. In addition, several actionable recommendations were included to further the work to prevent, detect, and mitigate server-based DDoS attacks.

4.7.1.3 CSRIC III, WG7 Botnet Remediation and the Anti-Botnet Code of Conduct

The CSRIC III tasked Working Group 7 (WG7), Botnet Remediation, with proposing a set of agreed upon voluntary practices that would constitute the framework for an opt-in implementation model for Internet Service Providers (ISPs) to follow to mitigate the botnet threat. In response, the U.S. Anti-Bot Code of Conduct for ISPs was developed to address the threat of bots and botnets in residential broadband networks through voluntary participation. It was determined in developing the code that constituents of the entire internet ecosystem have important roles to play in addressing the botnet threat and that ISPs depend on support from the other parts in the ecosystem.

4.7.1.4 CSRIC II, WG8 ISP Network Protection Practices

CSRIC II, Working Group 8 (WG8) addressed the area of ISP Network Protection, with a focus on addressing bots and botnets. Botnets are formed by maliciously infecting end-user computers and other devices with malware through a variety of means, and surreptitiously controlling the devices remotely to transmit onto the internet spam and other attacks (targeting both end users and the network itself). WG8 examined potentially relevant existing Best Practices (BPs), and in consultation with industry and other experts in the field, identified additional best practices to address protection for end users as well as the network. The best practices identified were primarily for use by ISPs that provide service to consumer end users on residential broadband networks but may apply to other end users and networks as well.

4.7.2 Communications Sector Coordinating Council White Paper

The Communications Sector Coordinating Council (CSCC) published a technical white paper specifically to inform the process undertaken by the Government in response to the Executive Order 13800 by describing the shared responsibilities of key participants in the internet ecosystem for mitigating the threats posed by botnets.

The internet ecosystem has been working collaboratively to neutralize the threats from bots and botnets for years. In this paper, the CSCC identified a number of challenges of mitigating

botnets, and opportunities for increased collaboration and cooperation among members of the internet ecosystem to address the problem.

4.7.3 Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats

In recognition of the growing global threat represented by malicious botnets, President Trump signed Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,*[20] tasking the Department of Commerce (DoC) and the Department of Homeland Security (DHS) to lead an open and transparent process to identify ways to improve the resilience of the internet and communications ecosystem and reduce the threats perpetuated by bots and botnets. The final report was transmitted by the Secretary of Commerce and the Secretary of Homeland Security on May 22, 2018. This final report was the result of a joint effort involving three approaches – hosting workshops, publishing requests for comment, and initiating an inquiry to the President's National Security Telecommunications Advisory Committee.[21] The resulting report included recommendations and identified challenges to reduce the threat from automated, distributed attacks.

4.8 Other related industry, Government, Regulatory Efforts

Extensive risk analysis regarding the transition to 5G has been undertaken by industry in collaboration with government entities. See Figure below. Both NIST and DHS have been and remain very active in their efforts to address 5G security, as well as the Department of Defense (DoD). The list below highlights some of these efforts:

1. DHS 5G Risk Assessment, https://www.cisa.gov/5g
2. NIST, https://www.nccoe.nist.gov/events/workshop-5g-cybersecurity-preparing-secure-evolution-5g
3. ATIS / DoD 5G Supply Chain Risk Management Working Group, https://www.atis.org/01_strat_init/5g-supply-chain/
4. DHS ICT Supply Chain Risk Management Task Force (SCRM), https://www.dhs.gov/news/2018/11/15/dhs-announces-ict-supply-chain-risk-management-task-force-members
5. FCC CSRIC, https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-councilcouncil
6. NTIA, https://www.ntia.doc.gov/[22]
7. Dept. of Defense CMMC, https://www.acq.osd.mil/cmmc/contact-us.html
8. Dept. of Commerce, https://www.commerce.gov/bureaus-and-

[20] The White House Office of the Press Secretary, *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (May 11, 2017), available at https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal.

[21] *NSTAC Report to the President on Internet and Communications Resilience* (2017)

[22] https://www.ntia.gov/press-release/2019/ntia-releases-first-annual-report-spectrum-repurposing

offices/bishttps://www.commerce.gov/bureaus-and-offices/bis[23]

9. Cyberspace Solarium Commission Report[24]

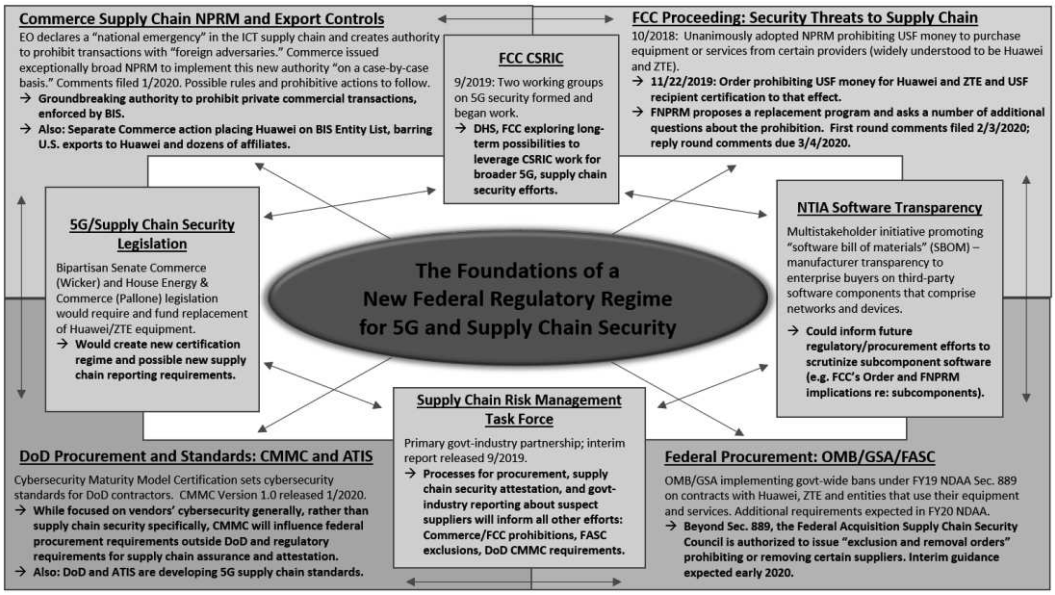


Figure 9 – Government Activities 5G

4.8.1 DHS Information and Communications Technology Supply Chain Risk Management Task Force

The Task Force's combination of industry and governmental expertise has yielded strong results in its first year. These results were captured in an interim report published in September of 2019[25] highlighting impacts of the Task Force's overall mission on supply chain risk management. This report details the Task Force's methodologies, areas of discussion and, where appropriate, key findings, recommendations, and potential areas for further study identified by each of the Task Force's four constituent Working Groups (WG). Each WG addressed an area of significant policy concern in addressing Supply Chain Risk Management (SCRM) challenges, including:

- The timely sharing of actionable information about supply chain risks across the community (WG1);
- The understanding and evaluation of supply chain threats (WG2);

[23] https://www.commerce.gov/news/blog/2018/10/presidents-national-spectrum-strategy-will-give-america-boost-5g
[24] https://www.solarium.gov/report
[25] INFORMATION AND COMMUNICATIONS TECHNOLOGY SUPPLY CHAIN RISK MANAGEMENT TASK FORCE: INTERIM REPORT, Status Update on Activities and Objectives of the Task Force, September 2019

- The identification of criteria, processes and structures for establishing Qualified Bidder Lists (QBL) and Qualified Manufacturer Lists (QML) (WG3); and
- Policy recommendations for incentivizing the purchase of Information and Communications Technology (ICT) from original equipment manufacturers and authorized resellers only (WG4).

The findings and recommendations of the WG from this past year (2019) will be foundational to the Task Force's second year of activity. In its next phase, the Task Force and the WG will continue to support efforts by the federal government and industry to manage ICT supply chain risk.

4.8.2 Federal Acquisition Security Council

The Federal Acquisition Security Council (FASC) looks to collect data on supply chain threats and help agencies counter such threats through guidance. The FASC will prioritize the development of guidance in 2020 to help agencies address threats to the supply chain. The Federal Acquisition Supply Chain Security Council is authorized to issue "Exclusion and Removal Orders" prohibiting or removing certain suppliers. Title II of the SECURE Technology Act, the Federal Acquisition Supply Chain Security Act of 2018, creates the FASC. The FASC is led by the Office of Management and Budget (OMB) and interim guidance is expected in 2020.

4.8.3 Department of Commerce

The Bureau of Industry and Security (BIS) establishes the Entities List, where BIS evaluates license applications to any listed entity, regulates the export of sensitive goods and enforces export controls, including anti-boycott and public safety laws. This program has the authority to prohibit commercial transactions, trade, and has critical effects to the global supply chain. The Department of Commerce (DoC) issued a Notice of Proposed Rulemaking (NPRM) to implement a new authority on a case-by-case basis. Public comments were filed in January 2020. Possible rules and prohibitive actions will follow. BIS added Huawei and 68 non-USA Huawei affiliates to the BIS Entity List, effective May 2019. BIS issued a Temporary General License through February 2020, and again for another 45 days through April 1, 2020, partially restoring the previous licensing requirements and polices for export, re-export, and transfer of items subject to the Export Administration Regulation (EAR) to Huawei and the 68 affiliates.

4.8.4 NIST Supply Chain Risk Management

NIST developed SP 800-161, SCRM Practices for Federal Information Systems and Organizations. This publication provides guidance to federal agencies on identifying, assessing, and mitigating ICT supply chain risks at all levels of their organizations. This publication integrates ICT SCRM into federal agency risk management activities by applying a multi-tiered, SCRM-specific approach, including guidance on supply chain risk assessment and mitigation

activities.

4.8.5 Executive Order 13873 Securing the Information and Communications Technology and Services Supply Chain

Executive Order (EO) 13873, in May 2019, declared a national emergency on exploitation and vulnerabilities in ICT technology via foreign adversaries. The EO prohibits any "...acquisition, importation, transfer, installation, dealing in, or use of any ICT technology or service (transaction) subject to jurisdiction within the USA". The EO prohibits transactions with "foreign adversaries".

4.8.6 Federal Communications Commission

The FCC issued a supply chain NPRM where it proposed prohibiting use of Universal Service Fund (USF) support on equipment and/or services from companies that pose "national security threats". The FNPRM proposes a replacement program and asks a number of additional questions about the prohibition. In October 2018 the FCC unanimously adopted NPRM prohibiting USF money to purchase equipment or services from certain providers (widely understood to be Huawei and ZTE). In November 2019 the FCC adopted an Order prohibiting USF money specifically naming Huawei and ZTE and USF and required USF recipient certification to that effect.

4.8.7 Department of Defense

Department of Defense (DoD) Cybersecurity Maturity Model Cybersecurity (CMMC) sets cybersecurity standards for DoD contractors. While focused on vendors' cybersecurity generally, rather than supply chain security specifically, CMMC will influence federal procurement requirements outside DoD and regulatory requirements for supply chain assurance and attestation. The CMMC Version 1.0 was released January 2020 and the CMMC Accreditation body has been established.

5 Analysis

5.1 Analysis Overview

The analysis contained in this report reflects the managing of security risk or a risk assessment in the transition from 4G to 5G wireless technology. The analysis leverages:

1. review of lessons learned from previous technological advances,
2. input from researchers, technologists and standards bodies,
3. an assessment of implementation best practices,
4. updates to the existing body of knowledge, and
5. barriers to implementation.

As 5G continues to mature and operators execute deployments of 5G networks, security is top-of-mind. The risks identified in prior technologies are still applicable to 5G. 5G will also introduce new attack vectors and a completely new network architecture that is software-based and embraces virtualization, IoT, SDNs, edge computing and open-source software. This expanded threat environment is being addressed by industry up front through security improvements early in the development of the architecture and specifications for 5G.

The previous 5G CSRIC Report Recommendations[26] in Section 10 and 11 of the report provided an initial but comprehensive set of security recommendations for 5G deployments. The recommendations are inclusive of protections for the existing 4G core, IoT, NFV/SDN, API security, etc. The analysis contained herein builds upon the previous recommendations based on the latest standards developments, industry best practices, and changing threat landscape. It leverages NIST SP 800-39[27] to frame 5G security risks, where risk context must be framed, the corresponding risks must be assessed, risk response recommendations must be identified, and ongoing monitoring must be performed.

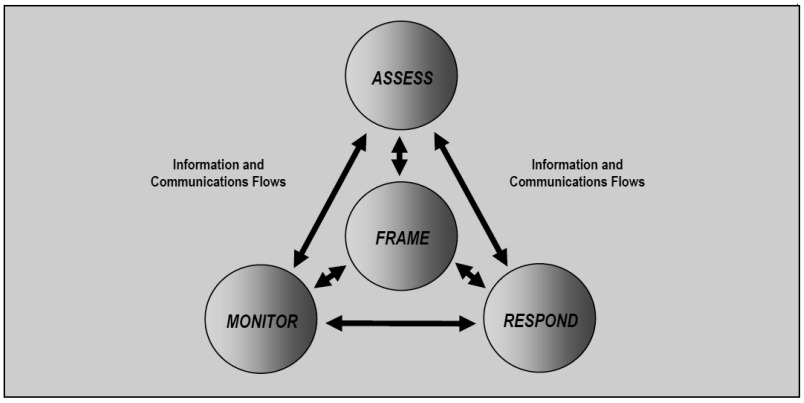


Figure 10, NIST SP 800-39 Managing Information Security Risk

5.1.1 Academic Papers and Analysis

5.1.1.1 Protecting the 4G and 5G Cellular Paging Protocols

The focus of the academic paper[28] is on analyzing the security and privacy of the cellular paging protocol with respect to the quality-of-service and battery consumption of a device. The paper

[26] 5G Final Report – Report on Best Practices and Recommendations to Mitigate Security Risks to Emerging 5G Wireless Networks - https://www.fcc.gov/files/csric6wg3sept18report5gdocx-0
[27] https://csrc.nist.gov/publications/detail/sp/800-39/final
[28]Singla, Ankush & Hussain, Syed & Chowdhury, Omar & Bertino, Elisa & Li, Ninghui. (2020). Protecting the 4G and 5G Cellular Paging Protocols against Security and Privacy Attacks. Proceedings on Privacy Enhancing Technologies. 2020. 126-142. 10.2478/popets-2020-0008. https://www.researchgate.net/publication/338475577_Protecting_the_4G_and_5G_Cellular_Paging_Protocols_against_Security_and_Privacy_Attacks/fulltext/5e169cf24585159aa4bffd8c/Protecting-the-4G-and-5G-Cellular-Paging-Protocols-against-Security-and-Privacy-Attacks.pdf

claims that attacks against this protocol can have severe repercussions, for instance allowing an attacker to infer a victim's location, leak a victim's IMSI, and inject fabricated emergency alerts. It analyses the underlying design threats and propose approaches to address them.
The paper analyses the Attach procedure as shown in Figure 11. When a UE is switched on with a valid SIM card, it first scans the network and selects the base station that satisfies its selection criteria. To establish a connection with the core network, the UE then sends an attach_request message to the MME, containing its International Mobile Subscriber Identity (IMSI)/ Temporary Mobile Subscriber Identity (TMSI) and the supported cipher suites. The UE and the core network authenticate each other using a challenge-response protocol (using a pre-installed symmetric master key in the SIM card) and then negotiate the cipher suite to be used for encryption and message authentication based on their individual capabilities. Finally, the MME completes the attach procedure by sending an encrypted and integrity protected attach_accept message containing the UE's TMSI.

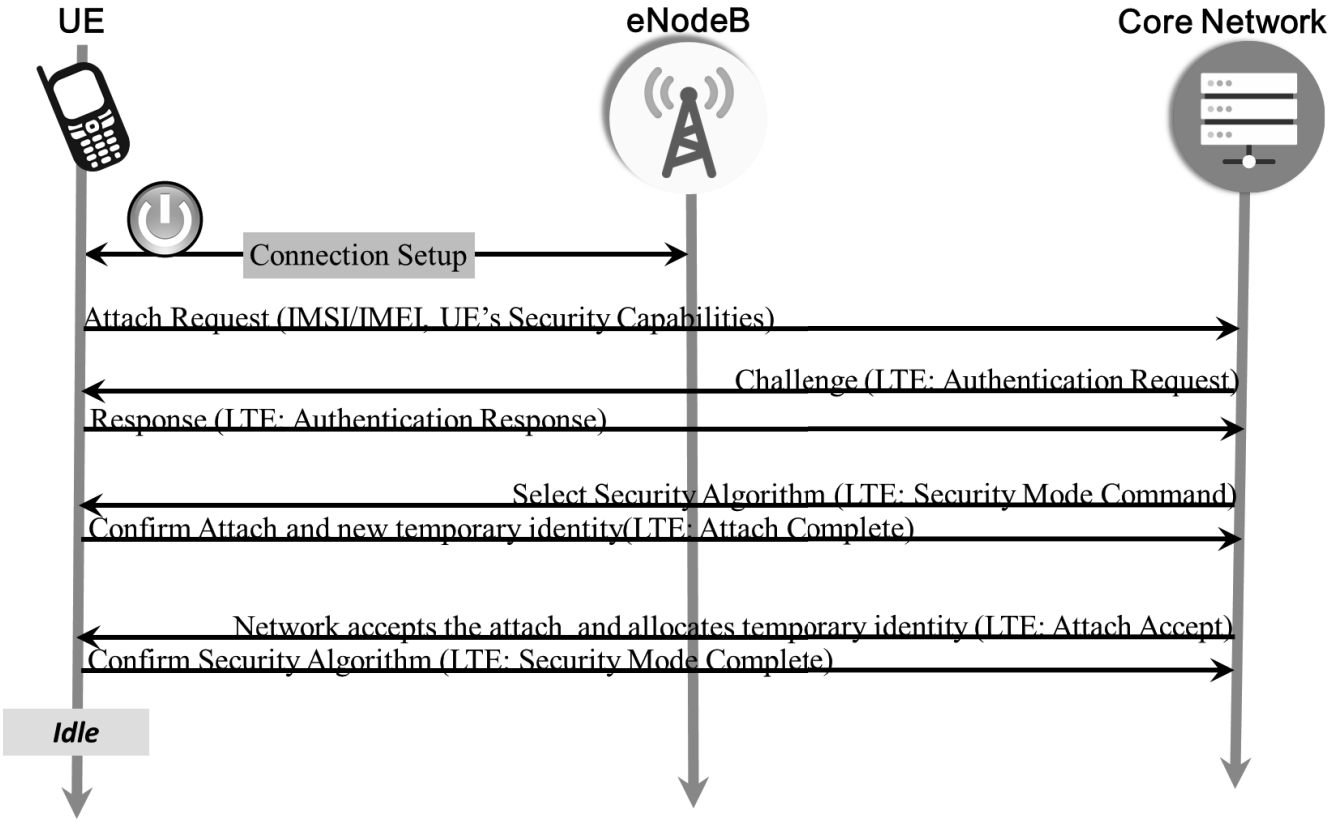


Figure 11 - Attach Procedure

The paper then analyses the paging and detach procedures, as shown in Figure 12, that allows a UE to enter a low power-consumption mode only when there are no uplink or downlink messages for a pre-defined amount of time. The paper also describes paging cycle as when in idle mode, the UE periodically wakes up to check if there is any notification for pending service(s). Finally, it describes paging frame as the radio frame at which the UE wakes up in every paging cycle to check for a paging message. The specific subframe of the paging frame at which the UE wakes up is also computed. The paging frame and the sub-frame together form a UE's paging occasion.

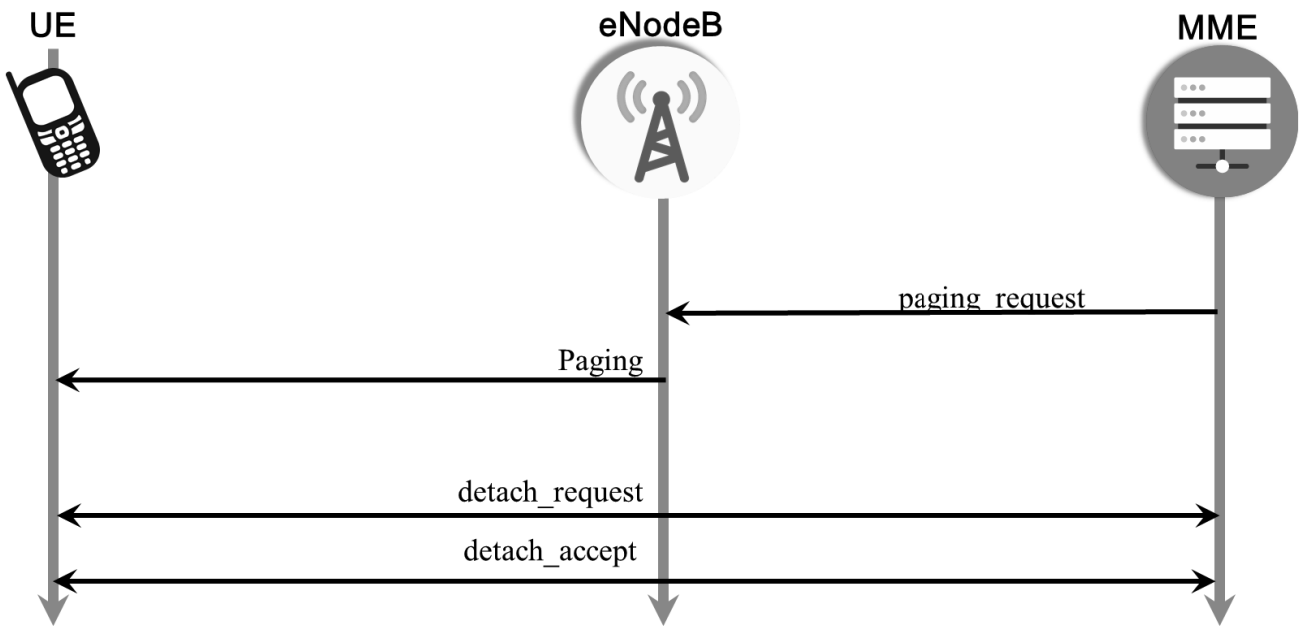


Figure 12 - Paging and Detach Procedures

The paper then concludes that fundamental weakness exist in the 4G paging protocol. For a particular device in a specific cell, the time intervals when the device wakes up from the low-power state to check for paging messages (i.e., the paging occasions) are fixed. This is because the paging occasion is computed from the device's persistent IMSI. This essentially exposes side-channel information which is shown to be exploitable by the ToRPEDO (TRacking via Paging mEssage DistributiOn) attack. So, the paper concludes that 4G is vulnerable because paging contains IMSI as device identifier. Also, the infrequent update of TMSI could expose the location of the UE.

While in 4G, it is optional to refresh the SAE Temporary Mobile Subscriber Identifier (S-TMSI). After paging, on 5G networks it becomes compulsory to refresh the 5G-S-TMSI. Furthermore, it is also compulsory to allocate new 5G-S-TMSI at initial registration and mobility registration update procedures. But the paper authors claim that since the configuration-update procedure requires additional interactions between the device and the core network, the upcoming 5G deployments may similarly try to get away without introducing such additional interactions and run into similar issues as 4G operational networks, thus becoming susceptible to location tracking attacks.

The authors have developed a tool called LTEInspector for "A Systematic Approach for Adversarial Testing of 4G LTE" as shown in Figure 13.

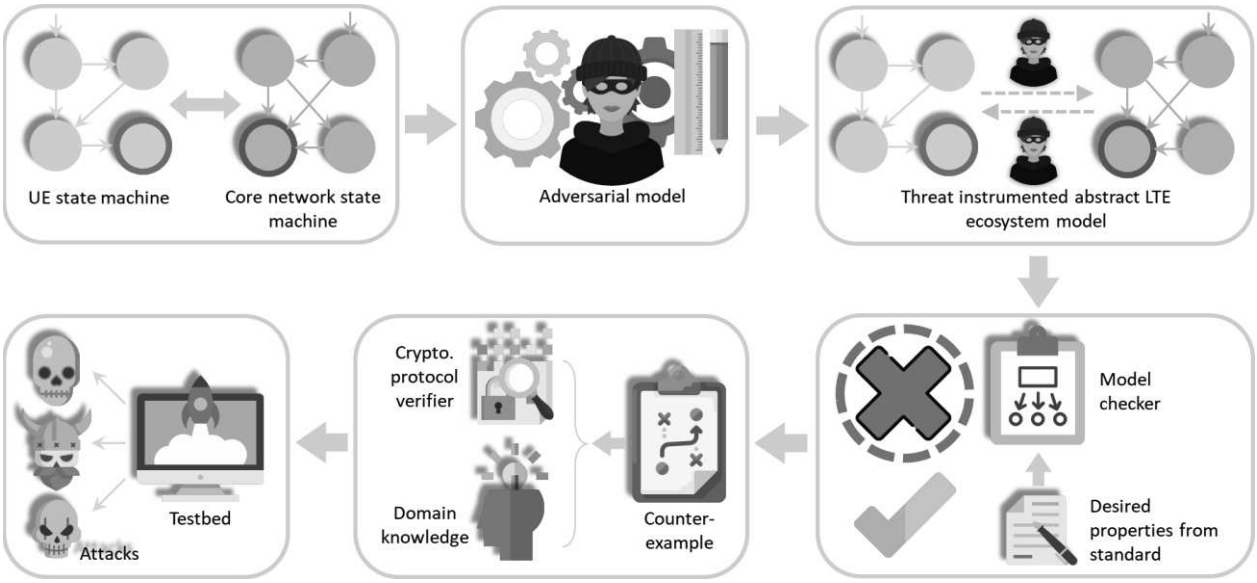


Figure 13 - LTEInspector: "A Systematic Approach for Adversarial Testing of 4G LTE"

Based on the analysis of WG2, the paper does not introduce new attacks. The previously identified vulnerabilities continue under industry review and assessment.

5.1.1.2 Insecure Connection Bootstrapping in Cellular Networks[29]

This academic paper focused on the potential 5G threat that man-in-the-middle relay/replay attacks could present. The research team analyzed the ability to lure a device to a rogue base station based on the 3GPP TS 33.501 version of Release 15.1.0 (2018-07). The study examined a number of approaches and presents findings and suggestions to strengthen authentication between the device and the base station.

The authors suggest that adding cryptography-based authentication mechanisms can be accomplished through the use of Public-Key Infrastructure (PKI) -based authentication on top of the asymmetric cryptography used in 5G. They further leverage precomputation-based digital signature generation algorithms and employ optimizations in three dimensions: PKI scheme-level, protocol-level, and cryptographic scheme-level to address processing and latency requirements. The research team acknowledges that these authentication methods could require major protocol/infrastructure overhaul and/or break backward compatibility.

Based on testing in a 4G lab environment, the team found that they could inject this solution without breaking backward compatibility in the specific, narrowly defined, test architecture. Impacts to overhead included injecting additional overhead (~220 bytes) with an increase in time delay (~28ms delay) to the connection process.

The research team suggests the proposed scheme could be modified for resource-constrained cellular IoT devices and 5G URLLC protocols but additional research is needed.

[29] https://par.nsf.gov/servlets/purl/10094853

5.1.1.3 Assessment of - "Imp4GT: ImPersonation Attacks in 4G NeTworks"[30]

5.1.1.3.1 Overall description

This attack allows impersonation of the UE, including hijacking of Transmission Control Protocol (TCP) connections by which the UE communicates with servers. In what the paper calls "Uplink Impersonation", the UE may be impersonated towards services provided by the MNO itself, like a customer portal where the subscriber may manage a subscription, and where authentication and security relies on the mobile network security only. (In contrast, a UE cannot be impersonated towards a server that uses its own security protocol, such as Transport Layer Security (TLS), and authenticates the UE based on username/password or a client certificate.)

In "Downlink Impersonation", the attacker is able to address the UE directly, circumventing any firewall that may be in place between the mobile network and the internet. For this communication, the attacker can spoof an arbitrary IP source address.

The attack requires the usage of a false base station (fBTS) acting as relay between the UE and the network and therefore suffers from the limitations of fBTS attacks. In particular it has only local impact, against single UE, and only as long as they remain in the proximity of the fBTS.

This is not a theoretical attack but has been implemented and tested successfully in a commercial network, with an only slightly modified commercial UE.

This attack is highly significant, as it breaks confidentiality and integrity of the LTE user plane, i.e. one of the most important security features provided by the 3GPP security architecture. The attack affects standard compliant equipment of any vendor. It cannot be prevented by proprietary changes of vendor equipment as this would kill interoperability between UE and networks.

5.1.1.3.2 Details on How the Attack Works

The attack exploits the fact that LTE encryption is done using stream ciphers (in contrast to block ciphers) and that no integrity protection is applied in the user plane. In addition, it exploits a feature of the IP stack specified by the IETF: In case the IP stack receives an IP packet with unknown "protocol type" ("protocol" refers here to the next layer protocol transported in the IP packet, such as TCP or User Datagram Protocol [UDP]), the stack replies with an Internet Control Message Protocol (ICMP) error message that contains the received packet. This procedure is called "reflection" in the paper.

The attack builds on the "aLTEr" attack previously published by the same author(s), where DNS requests of a UE can be manipulated in a way that the UE uses a malicious DNS server instead of the legal one. However, the present attack goes far beyond "aLTEr".

In a first phase, the attacker performs an aLTEr attack with a fBTS to hijack a TCP connection that the UE initiates. For example, Android smartphones typically connect to a known server to check internet connectivity after connecting to the mobile network. The attacker is then able to send TCP packets to the UE from the attacker's malicious TCP proxy in the internet. The attacker sees the encrypted downlink packet at the fBTS and changes the protocol type "TCP" to an undefined value. Consequently, the protocol stack of the UE reflects the packet. As this reflected uplink packet may not be able to traverse the firewall of the mobile network towards the internet,

[30] See: https://imp4gt-attacks.net

the fBTS changes the protocol type to an allowed value and receives the packet, decrypted by the network, at the attacker's server in the internet. By this, the attacker learns the complete cleartext of the downlink packet, as it is contained in the uplink packet due to the reflection mechanism. By this, the attacker learns how the IP header of a packet from the internet to the UE is changed by Network Address Translation (NAT) and by routers decrementing the time-to-live (TTL) field in the IP header.

When the attacker sends another packet to the UE in the hijacked TCP connection, and again changes via the fBTS the protocol type in the downlink packet, the fBTS can calculate the complete cleartext of the reflected uplink packet and can therefore extract the complete keystream. This allows the fBTS to craft an arbitrary packet (as long as it is not longer than the captured keystream), encrypt it and send it to the internet. At this point, the fBTS crafts a UDP packet to a server of the attacker, and by this a UDP session is established which allows the attacker to send a UDP packet to the UE at any time (which would otherwise not be possible due to the firewall of the mobile network towards the internet). This concludes the preparation phase.

In in uplink impersonation, when the attacker wants to send an uplink packet, the attacker sends a UDP packet from the internet to the UE, changes the protocol type with the fBTS, captures the reflected packet at the fBTS, extracts the keystream, encrypts its own faked packet with the keystream and passes it to the network. For successful uplink impersonation, the attacker must be able to understand the respective downlink traffic, i.e. decrypt it. For this, again the attacker lets the UE reflect the downlink packet and modifies the uplink packet in a way it will be routed to the attacker's server in the internet, decrypted by the network.

In downlink impersonation, when the attacker wants to send a downlink packet, the attacker sends a UDP packet from the internet to the UE and when the packet passes the fBTS, the fBTS changes the packet as needed, e.g. sets the IP source address to that of the impersonated communication peer and the protocol identity to the desired value. For successful downlink impersonation, the attacker must be able to receive the respective uplink traffic. For this, the fBTS modifies the uplink packet in a way that it will be routed to the attacker's server in the internet, and decrypted by the network.

5.1.1.3.3 Limitations

- Limited to local attacks against UE in the range of a fBTS.
- Meaningful impersonation only for sessions that do not use security mechanisms such as TLS, which is very common e.g. for smartphone applications. (The attack gives the attacker the same possibilities as someone controlling a router in the path between the UE and its communication peer, and most internet communication today uses protection against such potential attacks.)
- No decryption of arbitrary traffic. For uplink/downlink traffic of the UE, the attacker needs to know the destination/source IP address, respectively, to be able to redirect the packet to the attacker's server and get the decrypted packet.
- Not applicable for certain UE operating systems that do not implement the reflection in all cases (in deviation of IETF specs).
- The packet rate for impersonation attacks is limited by the rate at which the IP stacks generates (reflected) ICMP packets. This rate may be set per default to a relatively low value, as high rate ICMP traffic is not required in normal operation and could be a sign of some abuse (as it is the case in this attack).

- Reflected packets are limited in size, so the original downlink packet may get truncated. Thus, downlink packets cannot be decrypted in arbitrary size, and keystreams cannot be generated in arbitrary size.
- The attack works if no user plane integrity protection is used on the radio interface. This is always the case in LTE and in 5G NSA operation. In 5G SA, user plane integrity protection is mandatory to support up to a bandwidth of only 64 kbit/s. If it is used, the attack does not work. However, it may not be used in many cases as the support is not guaranteed for higher bandwidths.

5.1.1.3.4 Countermeasures

- Use of security mechanisms on the IP layer or above, such as TLS (does not affect the mobile network, is up to the applications); in particular, for access of a UE to an application of the MNO (e.g. a portal for subscribers to book services or manage their subscriptions otherwise), the MNO-application must not authenticate a UE simply by its IP source address, but must use proper authentication and integrity protection e.g. by TLS. This requires either the use of GBA, or the UE must have additional credentials (such as user name and password) to authenticate to the application server.
- More restrictions on the use of ICMP (may be enforced by the firewall of the mobile network)
- Use of user plane integrity protection (not specified for LTE, only in 5G SA)
- Specifying other forms of user plane encryption on the radio interface: Block ciphers instead of stream ciphers. This would be a rather significant change and is therefore rather unlikely.

5.1.2 Open-Source 5G Software Platforms

Open-source software (OSS) is a type of computer software in which source code is released under a license in which the copyright holder grants users the rights to study, change, and distribute the software to anyone and for any purpose[31]. Open-source products typically evolve through community cooperation among individual programmers as well as large companies. An open-source license permits anybody in the community to study, change and distribute the software for free and for any purpose.[32] Open-source collaborations drive innovation, making it easier to deploy technology in the marketplace.

In a U.S. DoD CIO memorandum "Clarifying Guidance Regarding Open Source Software (OSS)"[33], open-source software is defined as "software for which the human-readable source code is available for use, study, re-use, modification, enhancement, and re-distribution by the users of that software". OSS is typically developed through a collaborative process. Most OSS projects have a "trusted repository" (web) location where people can get the "official" version of the program, as well as related information (documentation, bug report system, mailing lists,

[31] https://en.wikipedia.org/wiki/Open-source_software
[32] Oracle White Paper, September 2013, The Department of Defense (DoD) and Open Source Software
[33] https://dodcio.defense.gov/Portals/0/Documents/OSSFAQ/2009OSS.pdf

etc.). Trusted developers can modify the software in the trusted repository

One of the fundamental differences between OSS and proprietary software is that the source code of OSS must be made available with the software. This does not mean that the source code must be physically delivered with the software, just that it must be available at a freely accessible location.

Commercially available software, or proprietary software, does not provide access to its source code because the software is the intellectual property of the developer. As a result, users often pay for licensing the intellectual property or software. In comparison, OSS is shared intellectual property among all contributors that have helped develop or alter it.

Potential advantages of OSS:

- Reduces the cost and effort to produce common functionality.
- Larger numbers of developers producing and maintaining more popular functionality.
- Platform design is being crowdsourced by global stakeholders.
- Provides for faster distribution of bug fixes.

Potential disadvantages of OSS:

- Usually not subjected to any formal review, validation or verification processes.
- May provide a higher opportunity for malicious code injection.
- OSS code equally available for study by developers and potential attackers.
- Widespread use of OSS creates a larger base of exploit targets (as opposed to potentially smaller bases of vendor proprietary software).

5.1.2.1 Risks of Open Source in 5G

OSS is incorporated into applications in many ways, and often an operator will not know where open source is used. When open source is used as the foundation for a vendors' product, any vulnerabilities could threaten the integrity of the vendors' solution. OSS provides attackers with a target-rich environment because of its widespread use. This means vendors must ensure they have mechanisms in place to monitor Common Vulnerabilities and Exposures (CVEs) against any OSS components and libraries that they may use in their own products. Vendors must test and perform security assurance assessments on all OSS and bug fixes. Vulnerabilities such as Heartbleed were exploits that targeted OSS vulnerabilities, threatening systems using the open source code.

According to the BlackDuck report[34], 67 percent of vulnerabilities discovered in open source code were known for more than four years. 52.6 percent of vulnerabilities were considered as high-severity by NIST. Open source vulnerabilities are published on sites such as the National Vulnerability Database (NVD) and are public documents. Network operators should be monitoring this as well and should understand where their vendors are using open source.

Use of open source will continue to increase as operators and vendors rely on OSS to speed

[34] See report at: https://www.blackducksoftware.com/

delivery of new solutions and reduce total cost of ownership (TCO). OSS can be viewed as being analogous to corporations outsourcing functions not related to their core competencies. This introduces a new set of security challenges in terms of keeping a consistent and coherent assurance of security-by-design, and prevention of resulting security flaws. To compound this issue, asking vendors to disclose the open source components used in their products may disclose more vulnerabilities and add to the risk. Note that many times while there may be a vulnerability in a specific software component, that vulnerability may only exist as a SA component, and may be nullified when incorporated into the vendors' solution (through middleware where the open source component is isolated, for example). Care must be given in how open source components are disclosed to prevent exposure.

5.1.2.2 Threat Assessment for Open Source in 5G

While the use of open source offers benefits to enterprises and development teams in terms of time to market, cost and reliability, it also can be the source of vulnerabilities that pose significant risk to application security. Many development teams rely on OSS to accelerate delivery of digital innovation. Both traditional and agile development processes frequently incorporate the use of prebuilt, reusable OSS components. As a result, some organizations may not have accurate inventories of OSS dependencies used by their different applications, or a process to receive and manage notifications concerning discovered vulnerabilities or available patches from the community supporting the open source.

Open source allows for platform design that is crowdsourced by global stakeholders. Merely hiding source code does not counter attacks; "people who break software don't actually need to look at the source code". Even when the original source is necessary for in-depth analysis, making source code available to the public significantly aids defenders and not just attackers. Continuous and broad peer-review, enabled by publicly available source code, improves software reliability and security through the identification and elimination of defects that might otherwise go unrecognized by the core development team. Use of any commercially available software, be it proprietary or OSS, creates the risk of executing malicious code embedded in the software. OSS projects have a "trusted repository" that only certain developers (the "trusted developers") can directly modify. Since the source code is publicly released, anyone can review it, including for the possibility of malicious code.

5.1.2.3 Threat Mitigation for Open Source in 5G

For larger enterprises with multiple and vast repositories of code, identification of all of the applications where open source vulnerabilities may exist can be difficult. Addressing the identification and mitigation challenge requires an intentional effort that includes activities such as code inspection, dynamic security scanning and vulnerability testing. These are the same techniques that should be applied to all software code repositories, whether open source or not. There are also enterprise specific products that offer a complete end-to-end solution for third party components and supply chain management with features such as licensing, security, inventory, and policy enforcement. These products are offered by vendors such as Black Duck Software, Sonatype Nexus, and Protecode, to name a few.

Most organizations search the Common Vulnerabilities and Exposures (CVE)[35] and NIST[36] Vulnerability Database for vulnerability information, but these sources provide little information on open-source vulnerabilities. Information on open-source vulnerabilities is distributed among so many different sources that it is hard to track it. To address the risk of open-source vulnerabilities in the software supply chain, groups such as PCI and Open Web Application Security Project (OWASP) have specific controls and policy in place to govern the use of open-source components. Other security repositories exist including the Node Security Project for JavaScript/Node.js-specific vulnerabilities and Rubysec for Ruby-specific vulnerabilities. However, there are still many open-source projects and ecosystems that are not well covered.

As a result, an entire market of open source and commercial tools has emerged over the years to tackle this problem. These tools vary in approach and capabilities, and some are open source themselves. Most of these tools use the NIST NVD as a starting point for sourcing OSS vulnerabilities. Each tool is then enhanced with usability features and/or additional data sourcing for improved functionality. A sample of these tools was included in the CSRIC VI report[37].

In general, an open-source security analysis should:

- **Check for public vulnerabilities**—Ensure the open-source components do not contain publicly known vulnerabilities, reported with vulnerabilities described in other public resources.
- **Use commercial security intelligence**—Use additional vulnerability data sources (such as from data vendors) to augment the public vulnerability data.
- **Perform static analysis**—Use static analysis tools to validate that the open-source components do not contain unreported security vulnerabilities.
- **Perform comprehensive security reviews**—Perform a comprehensive security review of the open-source component.
- **Perform security testing** – Perform testing like fuzz testing to detect applications vulnerabilities and programming errors.

5.1.2.4 NTIA Software Bill of Materials

In 2018, NTIA Software Transparency Working Group on Standards and Formats engaged stakeholders across a diverse set of industry verticals to address the challenge of transparency in the composition and functionality of software products:

> "Explore how manufacturers and vendors can communicate useful and actionable information about the third-party and embedded software components that comprise modern software and IoT devices, and how this data can be used by enterprises to foster better security decisions and practices…The goal of this process is to foster a market

[35] See: https://www.us-cert.gov/related-resources
[36] See: https://nvd.nist.gov/
[37] 5G Final Report – Report on Best Practices and Recommendations to Mitigate Security Risks to Emerging 5G Wireless Networks - https://www.fcc.gov/files/csric6wg3sept18report5gdocx-0

> offering greater transparency to organizations, who can then integrate this data into their risk management approach."[38]

The work of this group continues in 2020 with NTIA kicking off the next phase in February of 2020 with the workgroup following the publication of the first round of software bill of material (SBOM) deliverables. While there are differing opinions as to the overall value and impact of SBOM on 5G risk management, there is no denying that understanding the components embedded in vendor products can prove valuable in assessing vulnerabilities.

5.1.3 Orchestration and Virtualization

The capability to virtualize network functions and define networks within software brings significant advantages to network operators. 5G networks will be built on a virtualized platform taking advantage of NFV, SDN and containerization along with Open Network Automation Platform (ONAP). Therefore, the security advantages associated with virtualization and ONAP will apply to 5G. For example, closed-loop automation based on ONAP along with virtualization's inherent elasticity feature will be leveraged as a significant 5G security advantage. Those advantages, however, carry with them risks previously unseen in traditional hardware-defined networks.

Because NFV and SDN are still comparatively new architectures, many network operators may still be unfamiliar with the risks inherent in networks more defined by software than hardware. This unfamiliarity introduces new risk. To take full advantage of the benefits of NFV and SDN, as well as to provide the greatest security for these networks, operators will need new tools to ensure they have full visibility and control of network topology. While these principles have been in place in data centers for some time, they are often new to telecom engineers and planners. The ability to deploy NFV and SDN on COTS hardware, thereby avoiding the cost of purpose-built appliances such as routers and firewalls, represents one of the major attractions of network deployments using NFV and SDN.

Unlike traditional networks in which security models are relatively static, in the future, orchestration of NFV / SDN network topology could introduce continually changing workloads. Reacting to such a dynamic environment requires that NFV and SDN rely on centralized orchestration to manage workloads, creating new virtual machines as network demand dictates. The hypervisor, whose role it is to ensure isolation of virtualized functions, introduces attack vectors in a virtualized network, which could be mitigated by NFV/SDN dynamic security controls. Compromising the hypervisor exposes the network to orchestration exploits, SDN controller exploits, data exfiltration or destruction, and malicious configuration attempts.

Elastic network boundaries are a totally new concept introduced by NFV and SDN. Traditional network models are fixed, and network boundaries are easily identified by the existence of hardware at the network edge. NFV and SDN network boundaries, on the other hand, can change based on the dynamic nature of workloads. This means that network topologies might change, and the automatic configuration capability of network orchestrators has introduced new vulnerabilities to an NFV/SDN network. Compromising the network orchestrator might allow

[38] https://www.ntia.doc.gov/files/ntia/publications/ntia_framing_wg_deliverable_0.1_06.25.pdf

parties to implement malicious network configurations, altering network parameters and moving a VNF to an unauthorized location. This could lead to a regulatory compliance failure in some cases. Additionally, this elasticity introduces the opportunity for amplification attacks when new instances of network functions can be orchestrated based on network dynamics or attacks on orchestrators or controllers. If an orchestrator were compromised, new virtual machines (VMs) could be instantiated, with the potential for a resultant flooding of network resources. This is another area where the dynamic security controls introduced by NFV/SDN will improve on security.

In addition to these new attack vectors, NFV/SDN introduces the increased use of OSS. OSS is often not subjected to the rigorous patching and update disciplines to which traditional network element software – that software with which many network operators are most familiar – is subject. This places a heavier burden for security on the operator and moves away from regularly scheduled updates from vendors to a model where software updates are continuous, based on need. While a security advantage, this can also be a risk. OSS benefits and risks are described in the Open Source section of this report.

SDN represents a departure from networks with known topologies that were designed over time and implemented in a methodical process. SDN networks are dynamic and ever-changing based on the real-time needs of the network. This means network operations will need new tools to ensure they have complete visibility and control of the ever-changing network topology. While these principles have been in place in data centers for some time, they are new to telecom engineers and planners. Traditional models based on purpose-built hardware and software maintained with rigorous patching and management disciplines will be replaced by highly flexible SDNs that are agile enough to meet the demands of future networks and subject to continuous update. Taking full advantage of these capabilities will place a greater burden on both the operator and the vendor to manage the risks associated with that greater agility. The figure below shows the various methods that are needed for securing the SDN.

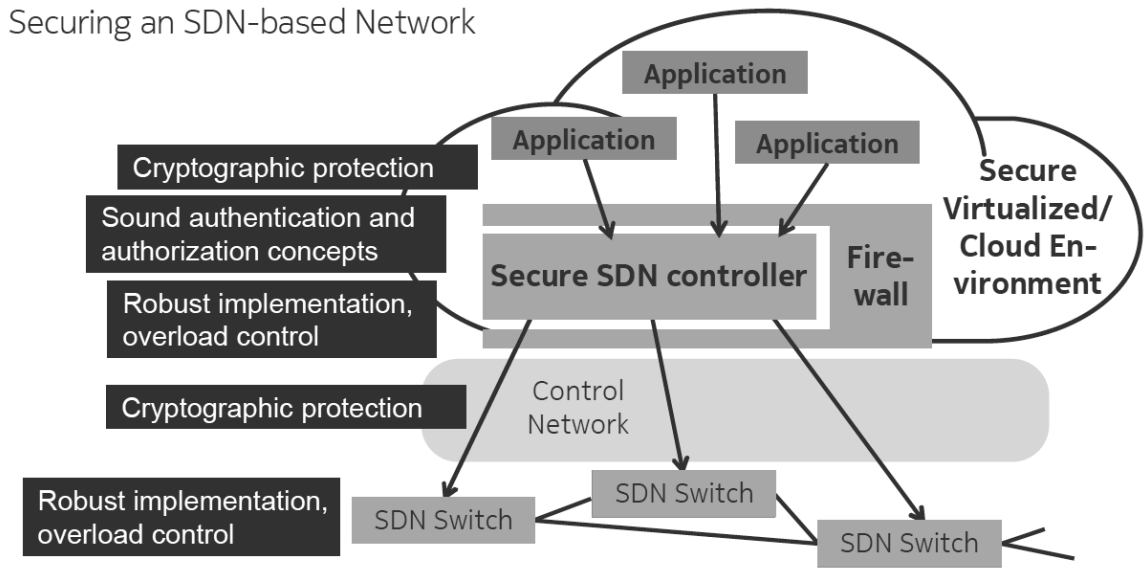


Figure 14: Securing the SDN. SOURCE: Peter Schneider, Nokia.

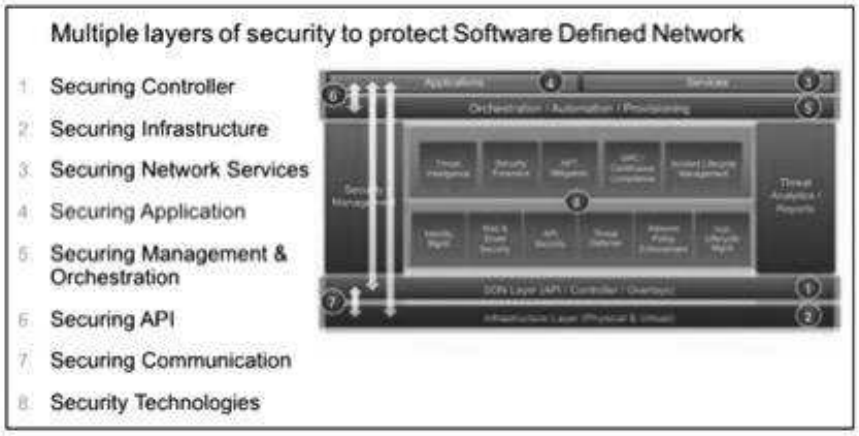


Figure 15: Layers of security in SDN. SOURCE: Mike Geller, Cisco.

NFV and SDN present new attack vectors that will be unfamiliar to operators who have not implemented this technology before. These vectors, however, are not new to 5G but are a result of the virtualization of network functions and the deployment of automated controls for services orchestration that are necessary in these emerging architectures. The benefit is that operators currently deploying this architecture in the 4G LTE environment are already developing experience that will benefit their deployment and operation of the 5G network.

An attack on a hypervisor could have a major impact on the network, depending on the deployment of the hypervisor. For example, if the hypervisor is supporting multiple critical network functions on the same hardware, a compromised hypervisor could result in a Denial-of-Service (DoS) attack on all of the network functions supported by the hypervisor. This is where isolation plays an important role, but physical isolation is not always the best choice because it eliminates the advantages of NFV/SDN. Physical and logical isolation of network functions must be carefully weighed to ensure maximum security of the network function while still realizing the benefits of NFV/SDN.

A lack of skillsets in virtualized networks represents perhaps the largest threat in NFV/SDN networks. This is new technology for telecommunication networks, and even though NFV/SDN has been around the IT world for some time, the standards for telecommunications NFV/SDN are new.

This means even a seasoned IT professional with experience in NFV/SDN will have to learn the new standards for NFV/SDN and its use in a telecommunications network. There are many important differences between the two types of networks and understanding these differences will be critical to securely maintaining NFV/SDN networks. Most operators will have legacy monitoring systems in their 3G/4G networks. These monitoring systems are designed to collect network data from various standardized interfaces in the network using probes located in strategic points, such as at major routers. With NFV/SDN, these probes will no longer be effective. They will not collect data between virtual machines and given the orchestration of new instantiations of network functions, they will not have visibility to newly instantiated network functions. Consideration needs to be given to how visibility will be enabled in a virtual network and between VNFs. This can be accomplished through the virtual switch itself or software agents that are instantiated with the VNF.

Since there lacks any industry standard definition for how virtual monitoring in telecom networks should be implemented, operators will be dependent on their vendors to define how virtual monitoring systems will work in their specific NFV/SDN networks. The lack of standards will result in proprietary systems that will lack interoperability. Operators will need to work with their vendors to ensure an approach that can later be aligned with industry standards for monitoring in a virtual network.

Security requirements in SDN / NFV network architecture differ significantly from the manner in which conventional networks have been secured. While conventional networks were generally considered to be secure when the edge elements were secure, the architecture of networks that are software defined and centrally controlled, and which are comprised of off-the-shelf hardware from a variety of vendors exposes those networks to new attacks vectors.

General classifications of potential attacks on software-defined networks include the following (although dependent on individual network configuration, all risk vectors may not exist in every software defined or virtualized network, the risks are not unique to NSA and are addressed in previous CSRIC reports, see Section 4.7.1):

- **Network Manipulation.** This attack occurs on the control plane when an attacker can compromise the SDN controller. Due to its basic architecture, the SDN controller is effectively the "brain" of the network, containing the capability to program traffic flows within the network. Therefore, attacks on the controller are the most severe threats to the SDN architecture. Once gaining access to the SDN controller, the attacker can produce false network data and initiate attacks on other network elements or the entire network. A compromised controller can give "root-like" access, enabling an attacker to configure virtualized network elements under its control, leading to data loss or further loss of network security.
- **Traffic Diversion.** This is an attack on the network element at the data plane. It allows the attacker to redirect traffic flows and allows eavesdropping.
- **Side Channel Attack.** This attack on the network elements, generally occurring in the data plane, results from the collection of externally observable network behavior by an attacker during normal network operations. Not requiring a connection to the network, the attacker might use information such as network timing to determine the length of time it takes the network to establish a connection. With that information, the attacker could determine whether or not a flow rule exists.
- **Application Manipulation.** Because SDN architecture is by nature defined in software, the network can no longer be defended solely by physical topology, and network firewalls generally are not designed to stop attacks on applications. Further, software applications are becoming increasingly complex, and security is not always properly built into applications. For these reasons, a successful attack on an application could provide the attacker with the ability to impact other portions of the network.
- **Denial of Service.** Perhaps the most common of attacks, this could impact all parts of an SDN. An attacker could flood the network with malicious messages and potentially cause a reduction or complete disruption of service to the network.
- **Access Resolution Protocol (ARP) Spoofing ("Man-in-the Middle Attack").** ARP spoofing is a type of attack in which a malicious actor sends falsified ARP messages

over a network, resulting in the linking of an attacker's MAC address with the IP address of a legitimate computer on the network. Once the attacker's MAC address is connected to an authentic IP address, the attacker will begin receiving any data that is intended for that IP address. ARP spoofing can enable malicious parties to intercept, modify or even stop data in-transit. ARP spoofing attacks can only occur on local area networks that utilize the address resolution protocol and are not specific to NFV and SDN networks.

- **API Exploitation.** Initially attacking the northbound interface, this attack could permit destruction or modification of data flows and could enable the unauthorized disclosure of data. It is important to recognize that API's may contain vulnerabilities that would allow an attacker access to other network elements.
- **Traffic Sniffing.** An SDN hacker can take advantage of any unencrypted communication interface to intercept or interfere with traffic to and from a central controller or network element.

In summary, NFV security should provide sound, robust implementations of the virtualization layer and the overall cloud platform.

- Sound robust security aware implementation of the VNFs
- Integrity assurance for both platform and VNFs

In virtual networks, isolation needs to be considered for critical network functions. Isolation can be implemented using logical or physical isolation. Even traffic isolation can be important for certain types of network traffic.

Also, virtual firewalls can provide perimeter security and network traffic filtering in addition to logically or physically separated security zones. Consistent with best practices, encryption should be used when moving traffic from one system to long-term storage.

For securing an SDN-based network a secure virtualized environment should include the protections for the SDN controller like cryptography, sound authentication and authorization, and robust implementation and overload protection. The control network should use cryptographic protection and the SDN switch should be protected using robust implementation and overload control that implies high-availability implementations with redundancy and fail-over capabilities.

5.1.3.1 SDN Transport

5G wireless technology introduces, among multiple technology advances, service delivery with ultra-low latency features which will bring about new industry services that were not feasibly plausible before. To maintain end-to-end low latency, some complementary functions will be moved closer to the edge, however, this is unlikely to be feasible for all functions. Early use cases include, but are not limited, to ultra-low latency IoT services, gaming and virtual reality stadium/concert experiences.

There are a number of enabling technologies that make this possible, some in the backhaul, some in the front haul, some at the MEC edge and some securely connecting consumers to the "edge." Key enabling technologies making 5G agile as required by ultra-low latency service delivery (and other 5G use cases) includes, but isn't limited to, segment routing connected to

network slicing to provide segmentation and performance classes in the backhaul network and extended out to the MEC edge and Software -Defined Wide Area Network (SD-WAN). Thus, the MEC edge becomes slice, service-class and performance-class aware.

SD-WAN technology may be used to connect data centers (DC) from the access point to edge and even core locations. SD-WAN introduces capabilities for traffic to be placed on network paths which meet the required Service- Level-Agreements (SLA) for specific services. SD-WAN monitors network paths to ensure the KPIs, e.g., latency, jitter and packet loss, are continuously being maintained and adjust traffic as necessary with varying network conditions. This implies that SD-WAN complements the low latency requirements for services introduced because of 5G.

SD-WAN can protect its overlay data streams through the use of encryption technologies. Also, SD-WAN may replicate flows over diverse paths to improve reliability in the event of packet loss or path loss, and performance by processing the first received packet of the replica.

In summary, SD-WAN provides intelligent and dynamic routing improving performance, reliability, and security to complement the new services capitalizing on 5G technology.

5.1.4 IoT in context of 5G

The security of the IoT is manifested in a broad ecosystem that is comprised of many participants including network operators, manufacturers, software developers, and service providers. In the 5G environment, this ecosystem will continue to expand to include vehicles, industrial control systems, and sensors driving intelligent municipalities (smart cities) to name but a few. CSRIC VI, IoT Service Enablement in 5G, focuses on the essential interconnectivity between the "things" and the "internet" that will be enabled as a result of the realization of a 5G network. The risks associated with IoT are many. The propagation of malware between devices continues to be a major issue for IoT, and the distribution of botnets will only continue as 5G networks are deployed, including the NSA. IoT risks to 5G are comprehensively covered in the CSRIC VI Report from WG3 and are described in the Appendixes[39].

5.1.5 Roaming

5.1.5.1 Signaling System 7

SS7 is a component of the United States telecommunications infrastructure supporting both wireline and mobile services as well as subscribers. These technologies have become targets of both domestic and international attackers with different motivations and creating different risks for both service companies and subscribers. The attacks have exploited the legacy trust ecosystem. The increased interconnection among different types of service companies and changing business and geo-political factors have also played a role in increasing the frequency and volume of targeted attacks. The result is that with more coverage, more networks, and more participants, the probability that bad actors will exploit this community of trust has increased.

[39] https://www.fcc.gov/files/csric6wg3sept18report5gdocx-0

SS7 threats remain relevant to roaming scenarios as do the mitigation recommendations contained in the CSRIC V Report on Legacy Systems Risk Reduction. [40]

5.1.5.2 Roaming in LTE Networks

The LTE networks use Diameter as the signaling protocol for their roaming networks, and GPRS Tunneling Protocol (GTP) as the tunneling protocol for the roaming users' traffic between the visited and the home networks as shown below.

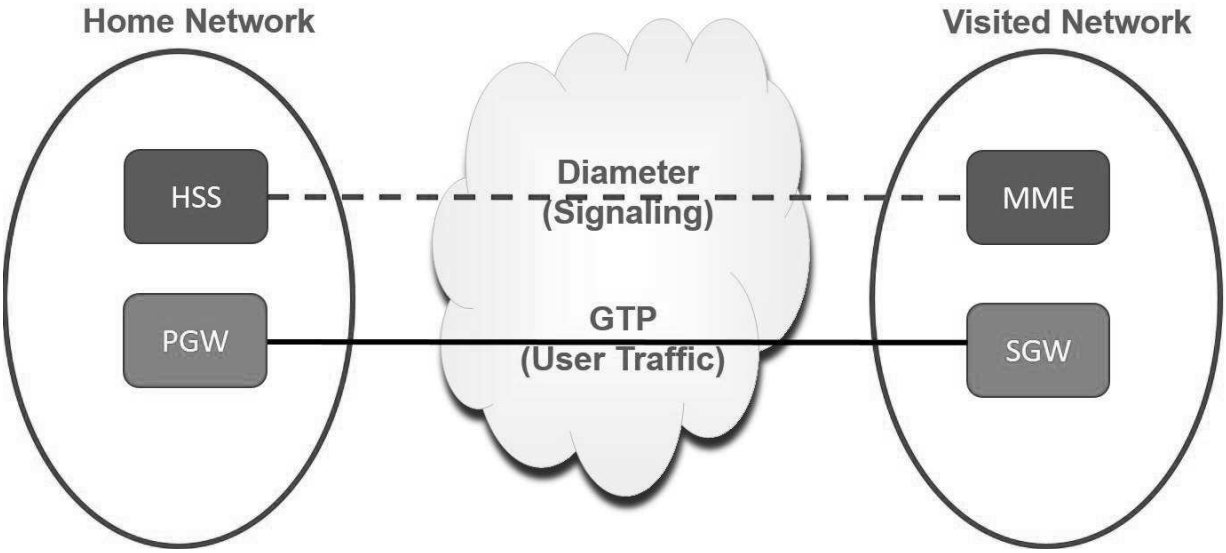


Figure16, Roaming in LTE Networks

Previous CSRIC efforts found that the use cases found in SS7 may exist in Diameter Protocol[41] as well, namely: location tracking, voice/SMS-interception, subscriber DoS, and account fraud/modification. In addition to these use cases, the Diameter protocol may be used for the interception of user data sessions. Previous research exposed the GTP to be vulnerable in 3G networks, but the functions provided by GTP have been replaced by the Diameter protocol in 4G. The Diameter protocol introduces the potential to spoof the identity of networks due to the way Diameter routes commands from hop-to-hop, which is unique to Diameter. Similar to SS7, nation state attacks are believed to be the largest threat, and such attackers can be highly sophisticated and well-funded.

In 2018 the report found that Diameter vulnerabilities were at the same stage that SS7 was at just a few years ago. The threats remain relevant to 4G and 5G systems and are further delineated in the recommendations in the CSRIC VI WG3 Report, including: blocking certain message types, as recommended by GSMA, employing monitoring platforms, and implementing advanced

[40] Legacy Systems Risk Reductions, Final Report https://www.fcc.gov/files/csric5-wg10-finalreport031517pdf
[41] Recommendations to Mitigate Security Risks for Diameter Networks Version 1.1, https://www.fcc.gov/file/13925/download

firewalls.

5.1.6 Threat Attack Surface

5.1.6.1 Nature and Type of Threats

This section of the Report provides analysis as to the new threat attack surface, the corresponding risks, overall assessment and previews the subsequent discussion regarding improvements provided by 5G and recommendations.

In the NSA architecture, the 4G risk and threat analysis from previous CSRIC Reports are still relevant given the re-use of the 4G EPC. In addition, new threats are introduced by the addition of the 5G NR.

5.1.6.1.1 4G Threats in NSA (5G 3X model)

Risk assessments and analysis from previous CSRIC Reports regarding 4G remain relevant with the introduction of the 5G NSA architecture that relies on the 4G EPC. These threats relate to the following:

1. DDoS[42]

   Previous CSRIC case studies looked at a number of DDoS attacks where an attack can involve multiple ISPs and multiple data and hosting centers. An attacker gains control of data center and hosting servers and leverages the sizable computational and network resources to launch a DDoS attack on an enterprise victim or network. The attack overwhelms access to the target, denying access from legitimate users as well as causing collateral damage by affecting other parties along the DDoS traffic path. This attack type is relevant to 4G and 5G systems in particular, given consideration of massive IoT, V-to-X and eMBB aspects. Mitigation of this type of attack requires action by all parties involved, including ISPs, hosting providers, data centers, resellers, target infrastructure such a mobile carrier, and ISP infrastructure of the originating attacker. Recommended best practices to mitigate DDoS threats are included in Appendix E of the report from CSRIC IV, WG5.

2. Botnets[43]

   Bots and botnets are a network of private computers or devices infected with malicious software and controlled as a group without the owners' knowledge, e.g., to send spam messages, and remain relevant attack types for both 4G and 5G. CSRIC III established WG7 to address botnet remediation in broadband networks. CSRIC III WG7 developed the Anti-

[42] Remediation of Server-Based DDoS Attacks. Final Report, https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG5_Remediation_of_Server-Based_DDoS_Attacks_Report_Final_(pdf)_V11.pdf
[43] U.S. Anti-Bot Code of Conduct (ABCs) for Internet Service Providers (ISPs) https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG7_Report_March_%202013.pdf

Bot Code of Conduct, a set of agreed-upon voluntary practices that constitute a framework for a voluntary implementation model for ISPs to follow to mitigate the botnet threat. In March 2012, CSRIC III delivered the U.S. Anti-Bot code of Conduct for ISPs to address the threat of bots and botnets in broadband networks. Furthermore, CSRIC III was charged with identifying potential ISP implementation barriers to the Code and identifying steps the FCC could take to help overcome these barriers. CSRIC III was also charged with identifying performance metrics to evaluate the effectiveness of the Code at curbing the spread of bot infections. The CSRIC III, March 2013 Final Report includes the Code from the March 2012 report as well as addresses the barriers to ISP implementation of the Code and Code effectiveness metrics.

3. Border Gateway Protocol[44]

The BGP is the glue that holds the disparate parts of the internet together by allowing independently-administered networks (called autonomous systems or ASes) to announce reachability to IP address blocks (called prefixes) to neighboring networks. Like many of the protocols underlying the internet, BGP is vulnerable to accidental misconfigurations, malicious attacks, and software bugs, which can cause the spread of "bogus" routing information throughout the internet. When ASes inadvertently select bogus routes, they may direct data traffic into "blackholes" that drop the traffic or detour the traffic over circuitous paths that traverse unexpected ASes that may snoop on the data. BGP threats remain relevant to 4G and 5G systems, as do the mitigation recommendations contained in the CSRIC III Working 6 Report.

5.1.6.1.2 Additional threats: NR in the NSA architecture, EPC, SS7 and Diameter

5G NR was engineered to complement existing resources. This is evidenced by a thrust of NSA flexible configurations in early deployments where the 5G radios attach to the 4G packet core network and use 4G LTE for coverage and 5G for capacity infill. Radio base stations are physically exposed and therefore particularly endangered. It is specific for 5G that the gNBs may be split into a CU and several DUs. This expands the threat surface for the radio base station. For example, mostly the DUs will be physically exposed to attackers, but also the new network interconnecting CU and DUs (F1 Interface). The confidentiality, integrity and availability of the F1 interface must be protected. 3GPP has defined the security mechanism to secure the F1 interface where IPsec is mandatory to implement on the gNB-DU and on the gNB-CU. In addition to IPSEC, The F1-C interface shall support data transport layer security (DTLS) for confidentiality and integrity of the control plane.

Protection and security of the 5GC will present new challenges to the operator when compared to the 4G EPC and will vary dependent on the operator's choice to deploy the 5GC in a SA or NSA architecture. The 4G EPC architecture is comprised of physical elements such as the MME, serving and packet gateways (S/PGW) and HSS, with the MME handling the control plane functions such as paging and tracking of UE's and directing other EPC elements how to

[44] Secure BGP Deployment Final Report, https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG6_Report_March_%202013.pdf

handle subscriber traffic.

The 5GC and its service-based architecture is made up of software functions. Each function advertises within the core the services and capabilities it is able to provide. These functions not only can be independently scalable but can also be located in geographically diverse locations.

The 5G NSA architecture allows the operator to leverage a certain level of network virtualization along with separation of the control and user planes (CUPS) to offer 5G services while preserving their 4G investment. After a subscriber is authenticated through the HSS in the EPC, the MME will direct the RAN to route the user plane traffic via the 5G NSA core. Therefore, the security of the 5G NSA core will be dependent on the security deployed across the LTE EPC while at the same time being able to take advantage of the security elements contained in the 5G user plane.

6 Findings

6.1 5G More than Wireless

5G is about more than wireless alone. 5G is designed to be access agnostic and capable of delivering 5G services to multiple access technologies. In addition to wireless, these access technologies might include wireline, satellite and Wi-Fi. However, in this Report, CSRIC VII has directed WG2 to focus on wireless access to 5G NSA network implementations. The NSA is focused on cellular access technologies, compared to the broader access technologies envisioned for the SA architecture.

6.2 NSA Stepping Stone to SA

While 5G NSA, the focus of the Report, might reasonably be viewed as a stepping stone to a full SA architecture, the NSA architecture does provide an operator with the opportunity to begin providing 5G services such as eMBB while preserving the operator's investment in 4G infrastructure and extending its useful life. The remaining key 5G use cases, mMTC and mission critical communications (URLLC), are not a part of 3GPP Release 15 and will not be available in NSA implementations.

6.3 4G Dependency

While 5G specifications include security enhancements that address existing 4G concerns, these enhancements will not be available to operators until they transition to a SA 5GC. Operators and service providers will need to be mindful that the NSA architecture will continue to rely on the 4G architecture for signaling. The corresponding risks are documented in earlier CSRIC reports as enumerated in Section 4.1.1.

6.4 Devices and IoT

6.4.1 Device-Network Interoperability Required

In the transition to 5G, devices will need to function on existing and emerging network elements. There are known threats in 4G networks such as denial of service (DDoS) attacks and the possibility of incorrect protocol implementation by device manufacturers that may risk control plane threats. Because of 4G's role during the transition from NSA to SA, these threats will remain. For improved protection of 5G networks, standards for structured testing of security should be developed.

6.4.2 IOT Developments in Device Management

The sheer number and potential variety of end user devices that will access a 5G network will impose new security challenges. The challenge of when to trust an end user device will require new monitoring disciplines, many of which do not currently exist. As well, the knowledge and expertise required to develop and manage these monitoring tools will require operator staffs with greater IT knowledge than in previous wireless technologies.

The broad diversity of IoT use-cases, and the vastly different service demands of those use-cases creates new risks and attacks that could be exploited on a 5G network.

With the anticipated diversity, scale, and complexities of IoT devices, previous CSRIC VI WG3 recommendations are essential for IoT – see Section 5.1.4.5. For example, a simple device may have a long life, never receive a software update, and may be capable of generating high volumes of short session traffic.

6.5 5G Departure from Purpose-Built Hardware

5G architectures, beginning with NSA, represent a marked departure from purpose-built hardware and single vendor implementations. Future 5GC implementations will be comprised of commercial off-the-shelf (COTS) hardware and open-source software. Operators will need to pay close attention to their hardware and software supply chains and OAM&P.

Supply chain issues are being addressed in greater detail in multiple other forums and have only been addressed by reference in this report. Operators should be prepared to address new challenges in securing and monitoring new and existing network elements and functions. In the case of open source, some bugs such as security flaws may take a trained eye to detect. Two pieces of code might be secure by themselves but be unsecure when combined. These types of bugs aren’t the types of bugs a casual open-source developer is likely to notice.

When introducing off-the-shelf hardware and open-source software, operators should carefully examine their interoperability and regression test plans, including their reliance on third-party and supplier testing. The amount of functional and non-functional testing of features, workflows, and use cases is expected to increase.

6.6 5G Standards

5G is the point where the telecommunications and IT worlds intersect, merging the telecommunications legacy of reliability and privacy with the IT legacy of scalability, see Section 4.6. As such, the establishment of standards for 5G may no longer be solely the domain of the traditional telecommunications standards bodies.

Implementations utilizing COTS hardware and open source software are taking the telecommunications sector into additional standards forums. As telecommunications standards become influenced by ICT, additional considerations of the standards will emerge, and there will be more variations in the implementation of those standards.

6.7 Wireline and 5G

Fiber optic networks will play a prominent role in enabling the 5G infrastructure because the many benefits that will be realized through the deployment of 5G are critically dependent upon fiber optic networks. 5G architecture utilizes small cell technology employing high-frequency transmissions. Such high frequencies allow extremely high-speed transmission of data from smartphones to small cells. Higher frequencies, however, are not well suited to penetrate urban structures of concrete, metal, or wood. In this environment, fiber is best used to transmit data between small cells and cell towers and, in turn, backhauled to switching offices at maximum speeds.

Additionally, once fiber is in place, it can easily scale to accommodate higher speeds and the expected growth of transmissions. Fiber will necessarily be deployed broadly throughout the emerging 5G networks to act as an essential partner in implementing 5G capabilities and capacities.

Finally, fiber transmission is highly secure, since fiber's signal can only be intercepted through a physical device that taps into the cable. Fiber will enable the secure transmission and both the fronthaul and backhaul of enormous quantities of transmissions as consumers, business including IoT, and manufacturing become more fully connected.

In the end, the power of fiber enhances the reach and security of 5G, and this partnership allows 5G in turn to become more exciting, more widespread, and more powerful.

6.8 Virtualization and Orchestration

Virtualization and orchestration are not new technologies for 5G. Operators are introducing the capabilities in LTE networks. Attacks against the hypervisor is one example of possible risks. Since this technology is applicable to LTE networks, mitigation scenarios are also relevant to 5G NSA implementations.

6.9 Workforce Considerations, NSA

While RAN densification and increasing data rates may be par for the course for today's operators, new 5G features such as eMBB and the associated need to discover and optimize to meet a wide range of service levels on the existing NSA core will present additional layers of complexity for the workforce to manage. CSRIC V WG7 was tasked to examine and develop recommendations to improve the security of the nation's critical communications infrastructure through actions to enhance the transparency, skill validation, and best practices related to recruitment, training, retention, and job mobility of personnel within the cybersecurity field. The final report demonstrated the applicability of the National Cybersecurity Workforce Framework to the Communication Sector specific cybersecurity skills requirements. The applications, templates, and other tools documented by CSRIC V WG7, will benefit the communications sector as operators incorporate 5G-based technologies.

6.10 Control Channel Threats

In general, for 4G LTE the digital radio frame structure is rigid, and transmissions of broadcast messages and signals are repetitive. However, for 5G NR the digital design is highly flexible, and transmissions of broadcast messages and signals are mostly on-demand such that various use cases (e.g. eMBB, URLLC and massive IOT) can be supported. Section 4.2 presents improvements of 5G NR over 4G LTE. These improvements can be leveraged to provide interference mitigation and resilience. 5G NR also supports antenna beamforming capabilities and its beam directivity can also be used to mitigate interference.

7 Recommendations

7.1 Recommendations for the FCC

7.1.1 Previous CSRIC Recommendations

WG2 commends the FCC's efforts to support CSRIC recommendations as shown by previous Public Notices (PNs).[45, 46] WG2 recommends that the FCC encourage industry for continued implementation of CSRIC's prior recommendations[47, 48, 49] and continue to promote awareness.

7.1.2 Supply Chain Recommendations

CSRIC VI WG3 published an addendum to their final report[50] regarding supply chain recommendations. WG2 reiterates the recommendation that the FCC continue to actively participate in the ICT SCRM Task Force, engage with NIST on the review of SP 800-161 rev 1

[45] See: https://www.fcc.gov/document/fcc-seeks-comment-implementation-diameter-best-practices
[46] See: https://transition.fcc.gov/Daily_Releases/Daily_Business/2017/db0824/DA-17-799A1.pdf
[47] CSRIC VI Final Report – Report on Best Practices and Recommendations to Mitigate Security Risks to Emerging 5G Wireless Networks v14.0
[48] See: Legacy Systems Risk Reductions, Final Report https://www.fcc.gov/files/csric5-wg10-finalreport031517pdf
[49] See: Recommendations to Mitigate Security Risks for Diameter Networks Version 1.1, https://www.fcc.gov/file/13925/download
[50] ADDENDUM to Final Report – Report on Best Practices and Recommendations to Mitigate Security Risks to Emerging 5G Wireless Networks, September 2018

and continue as an active member of the ATIS 5G Supply Chain Working Group. These SCRM programs represent strong public and private partnerships that are working to develop the framework for trusted 5G networks.

7.1.3 4G Security Best Practices and User-Plane

WG2 recommends that the FCC consider future CSRIC efforts to review upcoming improvements in 4G security best practices and 3GPP standards enhancements to address user-plane security.

7.2 Recommendations for Industry

7.2.1 Previous CSRIC Recommendations

WG2 recommends that industry rely upon previous CSRIC recommendations to mitigate threats to the 5G NSA system, specifically CSRIC VI, V and IV Reports.

7.2.2 Device Security

WG2 recommends consideration of a device-security management system for 5G networks. The following areas should be considered for standards development:

1. A policy-based security management system,
2. Leverage Artificial Intelligence (AI) to detect malicious or anomalous device behavior, and
3. Leverage device management capabilities to act as a policy feedback loop.

7.2.3 Workforce, NSA

Based on the CSRIC V WG7 Report, WG2 recommends that industry establish best practices for employee training to address the transition to 5G SA highlighting the key activities that maintain carrier grade reliability and security. This may include workforce training on cloud architecture, network virtualization and software defined networking, all of which are important foundational aspects of 5G SA architecture.

7.2.4 Control Channel Threats

For 5G NR, the WG2 recommends that the industry leverage the flexible transmissions capabilities of broadcast messages and signals as outlined in Section 4.2. These improvements should be leveraged to provide interference mitigation and resilience.

7.2.5 Threat Response Analysis, Academic Papers

Based on the analysis of WG2, the papers in Section 5.1.1 do not introduce new attack vectors. Previously identified threats continue under industry review and assessment. WG2 recommends higher layer security protections to mitigate user plane threats.

8 Appendix 1 – IoT and 5G

8.1 IoT Service Enablement in 5G

As discussed in CSRIC VI, *IoT Service Enablement in 5G* focuses on the essential interconnectivity between the "things" and the "internet" that will be enabled as a result of the realization of a 5G network. Examples of IoT applications include connected things that are industrial, medical, and consumer products. All have one thing in common: they represent another attack vector that can be used against critical infrastructure if not managed and secured. Industrial processes, localized or geographically distributed, are increasingly automated to ensure quality, consistency, and cost-effective production of goods or services. Connectivity is required for these sensors and actuators both indoors and outdoors with high availability and reliability to ensure seamless production and the ability to adapt processes in real time for maximum flexibility.

Autonomous cars use a combination of technologies to detect their surroundings including wireless communication technologies, laser and radar sensing, GPS, odometers, computer vision, and advanced control systems. 5G technologies are anticipated to enable these cooperative automatic driving use cases in an enhanced fashion where sensor information will be exchanged in real time between thousands of cars connected in the same area. Smart grids will enable enhanced monitoring, better management, and greater control of energy generation and distribution networks leading to increased availability and resilience. Lastly, the media and entertainment industry seek to improve the user experience and enable access to an expanding universe of content anytime and anywhere. This vertical opportunity focuses on different types of multi-media services that include regular live/linear media, on-demand content, user-generated content and gaming. Reference CSRIC6 for additional detail and information.

8.2 GSMA IoT-SAFE Model

IoT SAFE (IoT Sim Applet For Secure End-to-End Communication) enables IoT device manufacturers and IoT service providers to leverage the SIM as a robust, scalable and standardized root of trust to protect IoT data communications. Leveraging a hardware secure element, or root of trust, to establish end-to-end, chip-to-cloud security for IoT products and services is a key recommendation of the GSMA IoT Security Guidelines. This requires both the provisioning and use of security credentials that are inside a secure place within the device. The SIM is best suited to function as the hardware root of trust in an IoT device as it has advanced security and cryptographic features and is a fully standardized secure element, enabling interoperability across different vendors and consistent use by IoT device makers. The latest version of the GSMA IoT security documents include references to the IoT SAFEinitiative,

leveraging the SIM for IoT security.

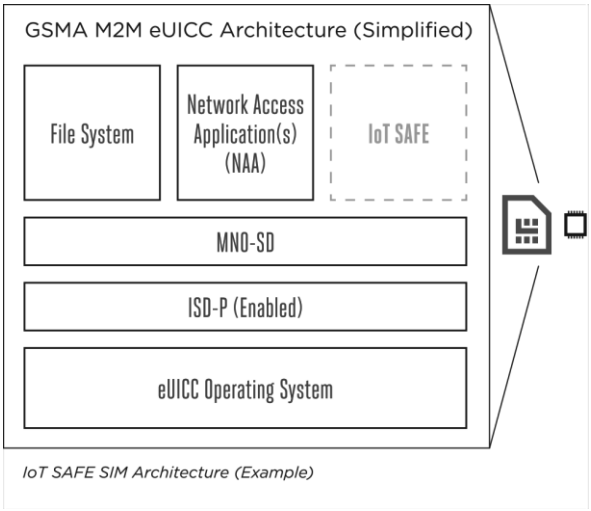


Figure A1 – 1, IoT SAFE SIM Architecture. Source: GSMA

As shown in the Figure above, the SIM is used as a mini 'crypto-safe' inside the device to securely establish a DTLS session with a corresponding application cloud/server. This is compatible with all SIM form factor: SIM, eSIM, iSIM, etc. This provides a common API for the highly secure SIM to be used as a hardware root of trust by IoT devices. The IoT SAFE SIM architecture helps solve the challenge of provisioning millions of IoT devices.

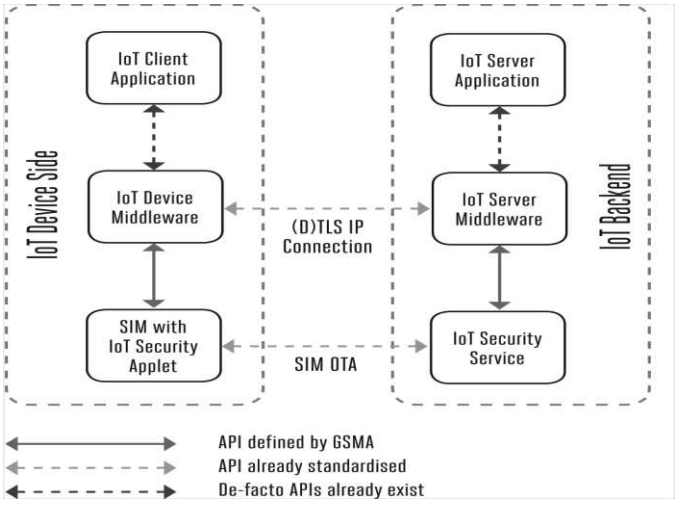


Figure A1 – 2, Security Services. Source: GSMA

IoT SAFE provides security services that enable IoT devices to securely perform mutual DTLS authentication to a server using either asymmetric or symmetric security schemes. Additionally, IoT devices will compute shared secrets and keep long-term keys secret.

8.3 Industry Certification Initiatives

IoT devices often lack device cybersecurity capabilities. Manufacturers can help customers by improving how to better secure the IoT devices they make are, meaning the devices provide functionality that customers need to secure them within their systems and environments. Within the IoT industry are numerous certifications published, all working on an equal basis to find common ground on IoT device security for new designs. While individual industry segments work on security, broad efforts are taken to address the challenge in harmonizing the industry. These efforts are occurring in all parts of the globe, such as the European Union, Japan, U.K, and United States.

CTIA Cybersecurity Certification Working Group: CTIA manages a cybersecurity certification program for IoT devices, establishing an industry baseline for device security on wireless networks. The CTIA IoT Cybersecurity Certification Test Plan supports a variety of use cases and levels of device sophistication.

- CTIA's Certification Test Plan defines the cybersecurity tests that will be conducted in CTIA Authorized Test Labs (CATLs) on devices submitted for CTIA Cybersecurity Certification. CTIA's Cybersecurity Certification is defined in three levels: the first level identifies core IoT device security features; the second and third levels identify security elements of increasing device complexity, sophistication and manageability.

CSDE's C2 "The Consensus Baseline IoT Device Security Capabilities": This is a common set of device security capabilities that can be applied to all new IoT devices that connect to the internet. The baseline is a set of best practice capabilities that are broadly applicable—vertically and horizontally—across markets. The baseline is a starting point for IoT device security that will need to evolve over time based on both changes in technology and changes to the threat landscape. This document informs further work on capabilities for IoT device cybersecurity that is more targeted to specific verticals, device types, use cases, etc.

UL IoT Security Rating: The UL IoT Security Rating Framework aligns with prominent industry standards, including the European Telecommunications Standards Institute (ETSI), and can serve to demonstrate conformance to those standards. This effort is based on UL's IoT Security Top 20 Design Principles, which aims to serve two purposes-

1. Help manufacturers and developers improve the security posture of their solutions by leveraging proven security best practices
2. Rate the security posture of IoT solutions in order to make security more transparent and accessible to consumers

BITAG IoT Security and Privacy Recommendations: Broadband Internet Technical Advisory Group (BITAG) believes that following the guidelines in this report can dramatically improve the security and privacy of IoT devices and minimize the costs associated with the collateral damage that would otherwise affect both end users and ISPs. This document was issued in November 2016.

ETSI: This work effort helps in ensuring that IoT devices are compliant with the General Data Protection Regulation (GDPR). This present document can also help organizations implement a future EU common cybersecurity certification framework as proposed in the Cybersecurity Act [i.13] and the proposed IoT Cybersecurity Improvement Act in the United States.

ioXt Alliance: The purpose of this certification program is to define a common method for the assessment and rating of a products (and organizations) fulfillment of the ioXt security pledge. With the engagement and support of their members companies, the certification program foundation has been created and Alliance staff is working with key members to review and fine tune the assessment process.

9 Appendix 2 – NIST Standards and IoT

9.1 NIST Standards

The NIST 8259 publication describes voluntary, recommended activities related to cybersecurity that manufacturers should consider performing before their IoT devices are sold to customers. This standard describes six voluntary but recommended activities related to cybersecurity that manufacturers should consider performing before their IoT devise are sold to customers.

- Four out of six activities primarily impact decisions and actions performed by the manufacturer before a device is sent out for sale. The remaining two activities impact decisions and actions performed by the manufacturer after device sale.
- Pre-market activities identify expected customers and define expected use cases, research customer cyber goals, determine how to address customer goals, and plan for adequate support of customer goals.
- Post-market activities identify expected customers, decide what to communicate and how to communicate it.

The 2nd draft has made changes to Table 1 in 8259 but is still very similar to the first draft. Notable changes include:

- NIST has removed the “Rationale” column from the table, which previously explained why the device cybersecurity capability was included in the core baseline.
- NIST has updated its “Reference Examples” to include references to IoT device cybersecurity guidance documents from the Council to Secure the Digital Economy (CSDE), the Cloud Security Alliance (CSA), the International Electrotechnical Commission (IEC), the Internet Society/Online Trust Alliance (OTA), and the Platform Security Architecture Joint Stakeholder Agreement (PSA).
- The updated version of the table has moved the defined terms; they are included on the page where the defined term is used first, rather than at the end of the table

The NIST 8228 publication identifies three high-level considerations that may affect the management of cybersecurity and privacy risks for IoT devices as compared to conventional IT

devices.

- Many IoT devices interact with the physical world in ways conventional IT devices usually do not.
- Many IoT devices cannot be accessed, managed, or monitored in the same ways conventional IT devices can.
- The availability, efficiency, and effectiveness of cybersecurity and privacy capabilities are often different for IoT devices than conventional IT devices.

Cybersecurity and privacy risks for IoT devices can be in terms of three high-level risk mitigation goals such as:

1. Protect device security. In other words, prevent a device from being used to conduct attacks, including participating in DDoS attacks against other organizations, and eavesdropping on network traffic or compromising other devices on the same network segment. This goal applies to all IoT devices.
2. Protect data security. Protect the confidentiality, integrity, and/or availability of data (including personally identifiable information [PII]) collected by, stored on, processed by, or transmitted to or from the IoT device. This goal applies to each IoT device except those without any data that needs protection.
3. Protect individuals' privacy. Protect individuals' privacy impacted by PII processing beyond risks managed through device and data security protection. This goal applies to all IoT devices that process PII or that directly or indirectly impact individuals.

10 Appendix 3 - Devices

10.1 Device Ecosystem Evolution

5G will deliver fiber speeds with low latency and network slicing to enable real-time and mission critical use cases, while improving consumer quality of experience. Enterprises will no longer be tied down to a wired infrastructure and a less secure Wi-Fi network.

4G allowed us to experience the joy of mobile streaming but 5G will support the continued growth of networked systems, including IoT-enabled devices and constantly moving targets like self-driving cars. Issues with bandwidth, latency, and speed will all be exacerbated.

With the 5G evolution the device ecosystem has potential to add millions of connected devices.

Today consumers are depending on their devices more than ever and this dependency is increasing at an exponential rate. With the technology evolution and integration of technology in our day-to-day life, dependency on connectivity will go to whole another level. For example, today smart devices along with IoT are actively used to measure and monitor heart rate. One of the leading device OEM has constantly evolved their product towards recognizing patterns in the heart rate using smart device sensors and flagging anomalies almost real time.

This increasing connectivity needs also results in a growing loss of privacy, as these smart devices collect and share data with the manufacturer and others. It's a goldmine of data about how they're being used and, increasingly, who is using them. And that tradeoff is not always apparent or clearly understood by the consumers using the device.

There is an opportunity for consumers to know standards of testing being put in place to understand the security risks associated with technology and applications.
Today it is incumbent upon consumers to recognize risks associated with various sensors they are bringing into their homes, whether it's microphones, video cameras or just devices that are capturing all sorts of data.

There is an opportunity to define standards for smart devices in terms of gathering certain types of data to work properly and improve their performance. In the absence of these standards, device OEMs and carriers are collecting every possible information and exposing consumers to unknown risks.

10.2 Device Software vs. Hardware

Today's smart device complexity is not just attributed to technology (4g vs. 5g) but also from the evolving software applications. As an example, the most popular connected applications fall in six categories: smart home, entertainment, toys and games, wearables, health and exercise, and pet products.

It is recommended that industry define and publish basic standards for software applications that are preloaded on consumer devices including, but not limited to:

- Is there a privacy policy and how accessible is it?
- Does the product require strong passwords?
- Does it collect biometric data?
- Are there automatic security updates?

11 Glossary of Terms

3GPP	3rd Generation Partnership Project
5G	Fifth generation
5GC	5G core
AF	Application function
AMF	Access and mobility function
API	Application programming interface
AUSF	Authentication server function
BGP	Border gateway protocol
BIS	Bureau of Industry and Security
BITAG	Broadband Internet Technical Advisory Group
BSS	Base station subsystem
BWP	Bandwidth part
CATLs	CTIA Authorized Test Labs
CMMC	Cybersecurity Maturity Model Cybersecurity
CRS	Cell-specific reference signal
CSA	Cloud Security Alliance
CSCC	Communications Sector Coordinating Council
CSDE	Council to Secure the Digital Economy
CSRIC	Communications Security, Reliability and Interoperability Council
CU	Central unit
DDoS	Distributed denial of service
DHS	Department of Homeland Security
DoC	Department of Commerce
DoD	Department of Defense
DU	Distributed units
EAR	Export Administration Regulation
EIR	Equipment Identity Register
eMBB	Enhanced mobile broadband
EPC	Evolved packet core
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
GDPR	General Data Protection Regulation
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Services
GSMA	Global System for Mobile Communications
HARQ	Hybrid ARQ
HLR	Home Location Register
HSS	Home subscribers
ICT	Information and Communications Technology
IEC	International Electrotechnical Commission
IMT-2020	International Mobile Telecommunications
IoT	Internet of Things
IP	Internet protocol
ISO	International Organization for Standardization
ISP	Internet service providers

IT	Information technology
ITU	International Telecommunication Union
ITU-R	ITU Radiocommunication Sector
KPI	Key performance indicator
LPWA	Low power wide area
LTE	Long-term evolution
MEC	Mobile edge computing
MIB	Master information block
MME	Mobile management entity
mMTC	Massive machine-type communications
mmWave	millimeter wave
MSC	Mobile switching center
NEF	Network exposure function
NF	Network functions
NFV	Network function virtualization
NGC	Next generation core
NG-RAN	Next generation radio access network
NIST	National Institute of Standards and Technology
NPRM	Notice of Proposed Rulemaking
NR	New radio
NRF	Network resource function
NSA	Non-standalone
NSSAI	Network Slice Selection Assistance Information (NSSAI)
NSSF	Network slice selection function
OTA	Online Trust Alliance
PBCH	Physical broadcast channel
PCF	Policy control function
PCFICH	Physical control format indicator channel
PCI	Physical cell identity
PCRF	Policy and charging rules function
PGW	Packet gateway
PRBS	Physical resource blocks
PSA	Platform Security Architecture Joint Stakeholder Agreement
PSS	Primary synchronization signal
QBL	Qualified bidder lists
QML	Qualified manufacturer lists
RAN	Radio access network
RRC	Radio resource control
SA	Standalone
SA3	Security working group
SBA	Service-based architecture
SCP	Service communication proxy
SCRM	Supply chain risk management
SD	Slice differentiator
SDN	Software-defined networking
SGSN	Serving GPRS support node
SGW	Serving gateway

SIB	System information blocks
SMF	Session management function
S-NSSAI	Single Network Slice Selection Assistance Information
SS7	Signaling system 7
SSB	Synchronization signal block
SSS	Secondary synchronization signal
SST	Slice/Service type
UDM	Unified data management
UE	User equipment
UMTS	Universal Mobile Telecommunications System
UPF	User plane function
URLLC	Ultra-reliable low-latency communication
VLR	Visitor location register
VLR	Visitor location register
WG	Working Group