PROJECT DESCRIPTION

5G CYBERSECURITY

Preparing a Secure Evolution to 5G

Mike Bartock
Jeff Cichonski
Murugiah Souppaya

National Institute of Standards and Technology

Draft

February 2020

5G-security@nist.gov

National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges. Through this collaboration, the NCCoE develops modular, easily adaptable example cybersecurity solutions demonstrating how to apply standards and best practices by using commercially available technology. To learn more about the NCCoE, visit http://www.nccoe.nist.gov. To learn more about NIST, visit http://www.nist.gov.

This document describes several security considerations as industry is preparing for a migration to 5G technology. NCCoE cybersecurity team will develop approaches and proposed solutions in collaboration with a Community of Interest, equipment vendors, and telecommunication providers.

ABSTRACT

Cellular networks will be transitioning from 4G to 5G, and 5G networks will provide increased cybersecurity protections. This project will identify several 5G use case scenarios and demonstrate for each one how to strengthen the 5G architecture components to mitigate identified risks and meet industry sectors' compliance requirements. The project will demonstrate how commercial and open source products can leverage cybersecurity standards and recommended practices for each of the 5G use case scenarios, as well as showcase how 5G security features can be utilized. A phased approach will be employed to align with the development pace of 5G technology and availability of commercial 5G technology.

This iterative approach will provide the flexibility to add to the project as the phases evolve to take advantage of newly introduced security capabilities. This project will result in a freely available NIST Cybersecurity Practice Guide.

KEYWORDS

3GPP; 4G; 5G; 5G Non-Standalone; 5G Standalone; cloud; cybersecurity; Long-Term Evolution (LTE)

DISCLAIMER

Certain commercial entities, equipment, products, or materials may be identified in this document to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST or NCCoE, nor is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

COMMENTS ON NCCOE DOCUMENTS

Organizations are encouraged to review all draft publications during public comment periods and provide feedback. All publications from NIST's National Cybersecurity Center of Excellence are available at http://www.nccoe.nist.gov.

Comments on this publication may be submitted to 5G-security@nist.gov

Public comment period: February 21, 2020 to March 31, 2020

Table of Contents

1 Executive Summary

Purpose

As 5G-based networks are deployed in our nation and across the world, there is great promise of positive changes in the way humans and machines communicate, operate, and interact in the physical and virtual world. With cellular networks transitioning from 4G to 5G, it is critical for organizations to understand and address the challenges, opportunities, and risks associated with the use of 5G networks.

The National Cybersecurity Center of Excellence (NCCoE) is initiating an effort in collaboration with industry to secure cellular networks and, in particular, 5G deployments. The NCCoE is positioned to promote the adoption of the increased cybersecurity protections 5G networks provide, such as the addition of standards-based features and the increased use of modern information technologies, including the cybersecurity best practices they provide. As 5G technologies are continuously being specified in standardization bodies, implemented by equipment vendors, and deployed by network operators, it is important to effectively scope and prioritize this effort to align with the availability of the technology and maturity of applicable standards.

This project will identify a number of 5G use case scenarios and demonstrate how the components of the 5G architecture can provide security capabilities to mitigate identified risks and meet industry sectors' compliance requirements. This project will result in a publicly available NIST Cybersecurity Practice Guide as a Special Publication 1800 series, a detailed implementation guide describing the practical steps needed to implement a cybersecurity reference implementation. The proposed proof-of-concept solution will integrate commercial and open source products that leverage cybersecurity standards and recommended practices to demonstrate the use case scenarios and showcase 5G's robust security features. The publication can assist organizations that are considering adopting and deploying 5G technology with the design, acquisition process (including Request for Information [RFI] and Request for Proposal [RFP] development and response), integration, and operation of 5G-based networks. The findings from this work can be used by NIST and the industry collaborators to prioritize their contributions in standards developing organizations.

Scope

The scope of this project is to leverage the 5G standardized security features which are defined in 3GPP standards to provide enhanced cybersecurity capabilities built into the network equipment and end-user devices. In addition, the project aims to identify security characteristics of the underlying technologies and components of the supporting infrastructure required to effectively operate a 5G network.

Security capabilities and administration of mobile devices are key components of adopting 5G. This project focuses on the security implications of device connections to cellular networks. It leverages other NIST and industry guidelines and projects, such as the NCCoE's Mobile Device Security project, for guidance for securing and administering mobile devices.

Assumptions & Challenges

Foundational trust in the infrastructure is a key objective of the project. As a result, the network core datacenter computing infrastructure will leverage a tamper-resistant hardware root of trust, capable of attesting the integrity of the platform and logical boundary of the compute nodes. These capabilities are exposed to the higher-level operating system and orchestration layers to support the placement of sensitive workloads or other defined policies on trusted hardware.

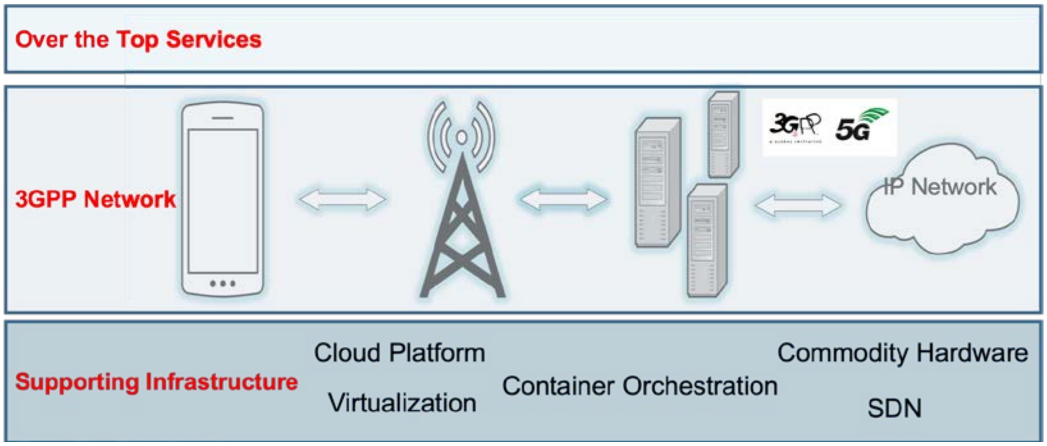
As 5G standards are continuously being developed to provide the features 5G technology promises, some of the components needed to meet the requirements discussed in the section below may not currently be commercially available. The project aims to use commercial off the shelf technology or open source solutions capable of providing the functionality and the security capabilities described in later sections of this project description. The project will adopt and demonstrate the features as the vendors and community introduce and enable them in commercial and open source products and technology.

As there are some strict operational requirements, such as licensing and broadcasting radio frequency (RF) signals, that apply to deploying the radio access network on premise at the NCCoE facility, NIST is considering connecting a subset of the components to collaborators' remote laboratories in order to compose a complete demonstrable solution described in the architecture to exercise the use case scenarios. In general, though, it is expected that the majority of the components will be located in a lab at the NCCoE facility in Rockville, Maryland. This will ease the integration of the components and allow an open and transparent environment for the participants to collaborate on building and testing the environment.

Background

Within the general topic of 5G cybersecurity, the standards-based features specified by 3GPP represent an important aspect of the system. The notional architecture depicted in Figure 1 provides context for how the NCCoE is approaching the topic of 5G cybersecurity. The approach aims to permit understanding the system from a vertical viewpoint that is inclusive of all supporting technologies, as well as provide a horizontal view of the specialized 5G workload that will realize the services and capabilities 5G promises. One of the major enablers of this differentiated technology stack is that the 5G system introduces the concept of a service-based architecture (SBA) for the first time in cellular networks [1]. It is envisioned that 5G network components will be deployed on a hyper-scalable containerized and virtualized infrastructure, similar to modern internet applications. This introduction of SBA and the adoption of cloud and internet technologies are expected to lead to the increased reliance on commodity infrastructure and common internet security protocols. The supporting infrastructure includes components like commodity server hardware, virtualization platforms, cloud operating systems, and container orchestration tools.

Figure 1: Notional 5G Network Architecture



In previous evolutions of mobile broadband technology, speed and throughput have been the key drivers, but 5G will become a ubiquitous technology, providing new capabilities tailored to specific use case scenarios stemming from industry verticals such as autonomous vehicles, smart manufacturing, and smart cities. 5G standards have been designed to support use case-specific capabilities by way of network deployment options. While 5G networks will use standards-based interfaces and protocols, the optionality built into the 5G system will mean each network's design and architecture may depend on the capabilities and services it is providing. The NCCoE project scopes a number of the use case scenarios that focus on the cybersecurity components, challenges, and opportunities.

The project defines a high-level roadmap that includes topics that resonate with NIST and its industry collaborators. The topics are prioritized based on industry's needs and the availability of supporting 5G technology. The cybersecurity capabilities and characteristics help scope the development, implementation, configuration, and demonstration of the project. A core objective of the effort is to showcase the practical 5G cybersecurity capabilities provided by the 5G system and complementing technology.

2 Phases & Scenarios

This NCCoE project will use a phased approach to align with the development pace of 5G standards, the availability of commercial 5G technology, and commercial 5G deployments. This iterative approach reflects the nascent state of 5G standards and the limited availability of appropriate technology. It will provide the flexibility to add more use cases and capabilities as the phases evolve, taking advantage of newly introduced security capabilities and reflecting the priorities of project collaborators. Each phase can be divided into multiple workstreams, where each workstream demonstrates a specific set of security capabilities. Each new phase is built upon the outcome of the previous phase. For example, phase 1 starts out by establishing a foundational infrastructure that aligns with current available cybersecurity capabilities, including specific security configurations of the non-standalone core to support various industry standards and regulations. Subsequent phases extend the initial work to cover additional 5G use case scenarios that are still evolving.

The demonstration platform is intended to be hosted, in whole or in part, at the NCCoE and may connect across the internet to industry collaborators' facilities based on operational need, functional requirements, and security capabilities required to support desired use case scenarios and demonstrate achievement of the desired security capabilities.

Phase 1 - Preparing a Secure 5G Infrastructure & Architecture

This initial phase focuses on two critical components. Component 1 is deploying the underlying infrastructure consisting of the hardware and software needed to achieve the scenarios described below. The implementation of phase 1 component 1 will highlight the security characteristics and capabilities of the supporting infrastructure and is envisioned to be deployed in combination with the mobile network services described in phase 1 component 2. Component 2 involves the implementation and configuration of security capabilities offered with 5G Non-Standalone deployments. These two components may be divided into multiple workstreams which can be executed in parallel, depending on dependencies identified during the design process of the project.

Component 1 - Infrastructure Security

This component focuses on the computing resources required to operate a modern mobile network, specifically focusing on the infrastructure's cybersecurity protections. LTE Evolved Packet Core (EPC) components are being increasingly packaged and deployed as Virtualized Network Functions (VNFs) that are dependent on commodity compute platforms. The Infrastructure security component of this phase will be focused on the security capabilities that can be achieved when deploying EPC VNFs on a cloud-like supporting infrastructure. The supporting infrastructure will utilize hardware roots of trust for platform measurement and attestation to ensure that certain workloads run on hardware in a good known state and within a well-defined logical boundary. For example, these cryptographic protections could support VNF isolation, ensuring security-critical functions are running on hardware independent from less critical functions [5].

Component 2 - 5G Non-Standalone (NSA) Security

This component of the project will focus on taking advantage of the robust cybersecurity protections and features provided by the 3GPP specifications and commercial solutions. While 3GPP has designed many new cybersecurity features built upon 4G LTE, they are only available with a 5G Core. The 5G specifications define multiple deployment models to support different configurations and architectures. One of these configurations is referred to as 5G Non-Standalone (NSA) options, which utilizes the 5G New Radio (NR) in conjunction with an LTE EPC to take advantage of the technological advancements of 5G NR without the need to deploy an entirely new core network [1].

The objective is to enable and configure the LTE EPC's security features in a manner that demonstrates the robust cybersecurity provided in a 5G NSA deployment. The implementation will incorporate solutions that address the threat of false base stations in mobile network deployments, protecting the core from potential internet-based threats, and will investigate existing protections that mitigate the risks posed by legacy radio access technologies (RATs), e.g., 2G.

Scenarios:

Scenario 1: Basic functionality of voice, text, and data on a 5G NSA deployment

This will be an initial demonstration of the infrastructure's functionality involved in setting up a call, sending SMS, and connecting to data services. The scenario will utilize the functionality of the initial 3GPP system's configuration and protections provided by native IP-based security protocols (e.g., Network Domain Security/Internet Protocol [NDS/IP] [3]) to form a baseline for future scenarios. This scenario can be demonstrated without a fully complete infrastructure security component.

Scenario 2: Basic functionality of voice, text, and data on a 5G NSA deployment that includes the infrastructure security component

This scenario will demonstrate the robust security protections provided by the infrastructure with the 5G NSA functionality demonstrated in scenario 1 operating unencumbered. The underlying infrastructure will be measured, attested, and policy tagged so that 5G NSA VNFs will only run on hardware that is trusted and meets specific security policies. In addition, SDN policies will be implemented to isolate the network data flows between specific VNFs.

Scenario 3: Cybersecurity features provided by the 3GPP system and configuration of those cybersecurity features

This scenario will demonstrate the standards-based security features available with a Release 15 EPC. Capabilities like mutual authentication, hardware-backed credential storage, and algorithm configurations relevant to the US market will be highlighted.

Scenario 4: False base station detection and protection

Due to the nature of RF-based communications, cellular networks are exposed to certain risks caused by impersonation of networks. This scenario will demonstrate the use of commercial solutions provided by vendor partners to detect and protect against risks posed by false base stations.

Scenario 5: Protection from risks posed by legacy radio access technologies

Legacy cellular networks using legacy radio access technologies are starting to be phased out and turned off in favor of newer, more robust technologies. However, devices that utilize cellular connectivity are designed to connect to any network available. The legacy networks do not have the same security protections and capabilities afforded by technologies like LTE and 5G, and inadvertently using them may pose unwanted risks to organizations. This scenario highlights the potential use of standards-based features or commercial solutions to disallow connections to legacy networks.

Phase 2: Secure 5G Infrastructure & Architecture

The second phase of this project will focus on the evolution of LTE EPC technology from the Phase 1 5G NSA deployment to a 5G Standalone (SA) deployment. This will allow implementation and demonstration of the new 5G security features made available with a 5G Core.

An objective of phase 2 is to enable and configure the 5G Core's security features in a manner that demonstrates the robust cybersecurity provided in a 5G SA deployment. The implementation will look to incorporate solutions that address known security challenges found in previous generations of cellular networks. Many of these solutions have been incorporated into the 3GPP specifications as interoperable standards-based features [2] while some may be customized solutions developed by vendors.

Component 1 - Enhanced Infrastructure Security Capabilities

The 5G Core introduces the SBA in cellular networks. This modern design is a fundamental shift in how new services are created and how the individual Network Functions (NFs) cooperate. Not only is the core network decomposed into smaller functional elements, but the communication between these elements is also expected to be more flexible, routed via a common service bus, and almost completely deployed using virtualization and containerization technologies. 5G Core components may be packaged and deployed as VNFs or Containerized Network Functions (CNFs) dependent on commodity compute platforms. In addition to the new technologies, there will be an increased use of common security protocols (e.g., Transport Layer Security [TLS], Internet Protocol Security [IPsec], JavaScript Object Signing and Encryption [JOSE]) that include their own sets of recommended practices. The configuration and management of these protocols are important aspects of network security that need to be demonstrated. This will build from phase 1 component 1, to include new infrastructure capabilities and security features. For example, this may include extending the hardware roots of trust into platforms that run CNFs to ensure that certain CNFs run on hardware in a good known state and within a well-defined logical boundary.

Component 2 - 5G Standalone Security

The 5G SA deployment model requires the 5G Core Network. 3GPP has designed and specified the 5G Core Network to include many new cybersecurity features and capabilities that improve upon 4G LTE. These new features are intended to strengthen the security posture of the network while addressing known risks associated with previous generations of mobile networks. This component of phase 2 is focused on enabling and demonstrating the new cybersecurity protections afforded by a 5G SA deployment. The component will enable and configure the cybersecurity features with industry recommended practices and standards.

Scenarios:

Scenario 1: Basic functionality voice, text, data on 5G SA deployment

This will be an initial demonstration of the infrastructure's functionality: setting up a call, sending SMS, and connecting to data services. The scenario will utilize the functionality of the initial 3GPP 5G Core configuration and form a baseline for future scenarios. This scenario will leverage the trusted infrastructure deployed in phase 1.

Scenario 2: Demonstration of the subscriber privacy features provided with the 5G Core

This scenario will enumerate the information sent in cleartext in an NSA deployment and compare it with cleartext transmissions from an SA deployment, demonstrating that the subscriber identity is no longer available to false base stations.

Scenario 3: Standalone standards-based 5G security features

This scenario will incorporate protections gained from all the standards-based security features provided by SA deployments. This will highlight capabilities like subscriber privacy, user plane integrity protection, CU/DU split, enhanced authentication, and protections provided by native IP-based security protocols (e.g., NDS/IP). These features are defined in more detail in Section 3 under Desired Security Characteristics and Properties.

Scenario 4: Core internet protocols

This scenario will explore industry-recommended practices for properly implementing the core internet security protocols needed to protect communications between all VNFs deployed inside a core network. This may include topics like configuration and management of TLS cipher suites, IPsec, and Domain Name System Security Extensions (DNSSEC).

Future Phases

A critical driver for the development of 5G has been the expected increase in cellular-connected Internet of Things (IoT) devices. As the standards solidify and technology becomes commercially available, this project aims to incorporate an IoT-specific phase and use case scenarios.

Another new feature of 5G is more advanced network slicing capabilities beyond LTE's basic support for aspects of slicing around dedicated Core Networks. Compared to its predecessor, 5G network slicing is envisioned to be a more powerful concept and includes the ability to create a slice that is an entire Public Land Mobile Network (PLMN). Within the scope of the 3GPP 5G system architecture, a network slice refers to the set of 3GPP-defined features and functionalities that together can form a separate PLMN or isolated network for providing services to subscribers. Network slicing allows for orchestrated deployment and configuration of network functions to provide services that are required for a specific usage scenario. A future phase of this 5G security project will aim to explore the use of network slicing to provide a higher level of assurance to customers who have unique security requirements. This work could focus on enabling standards-based security features as well as operational/deployment best practices within a specific slice.

The benefits of an ultra-reliable and ultra-low latency 5G network will contribute to the enablement of autonomous vehicle communications. Autonomous vehicles will be able to establish massive numbers of connections and communicate over them with very low latency, allowing for real-time data exchange. This will be necessary for autonomous vehicles operating safely in the real world. A future phase of this 5G security project aims to explore implementing 3GPP Vehicle-to-Everything (V2X) standards. This work could focus on implementing the standards-based security features while demonstrating the usability of the V2X communications.

Edge computing will play a critical role in 5G service offerings. To reduce the latency that comes with centralized cloud computing, network appliances, services, and applications are being deployed closer to the end user devices or network edge, providing capabilities commonly referred to as "edge computing." Edge computing decentralizes cloud infrastructure components, so the compute functions are pushed further to the network edge, closer to the data, in geographically separate areas. A future phase of the NCCoE 5G security project will enable trust and security for running network and industry sector-specific services on the edge.

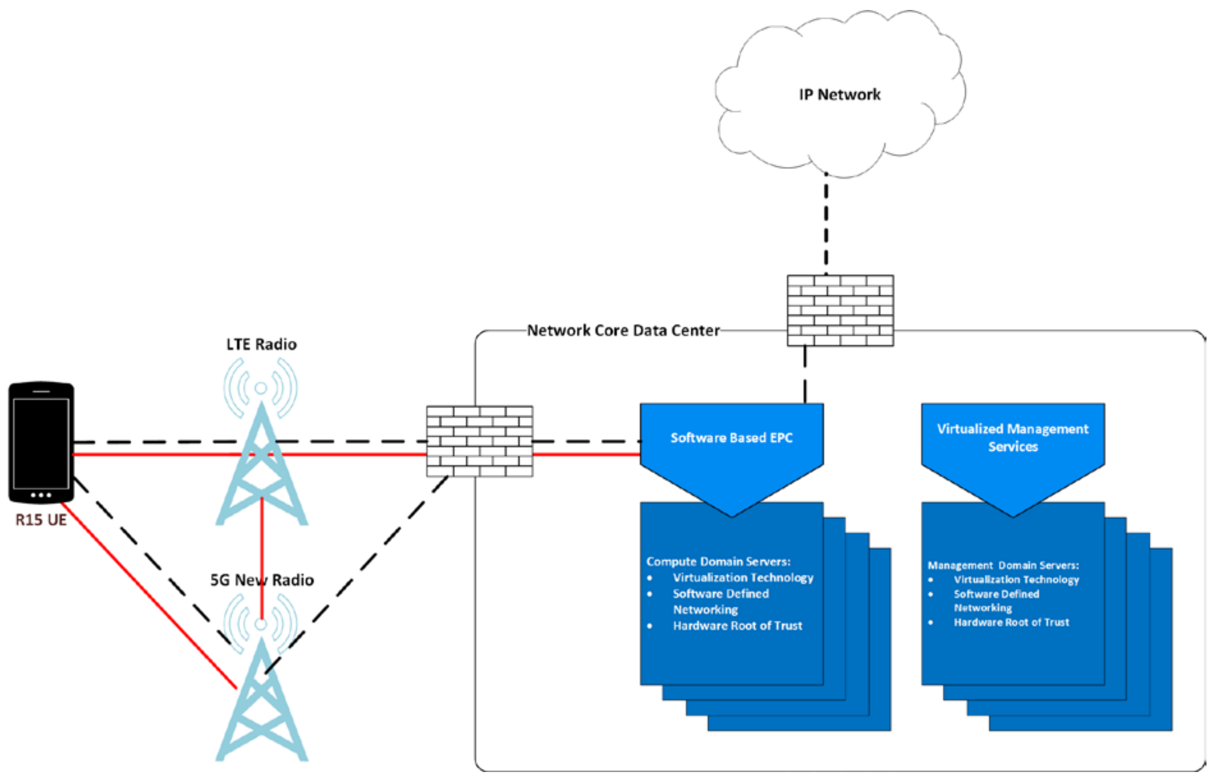
NCCoE will develop future phases and use case scenarios with the community of interest in the future.

3 High-Level Architecture

This section provides a high-level illustration of the Phase 1 architecture and list of the components that are part of the architecture considered

Figure 2 provides a logical depiction of the proposed Phase 1 implementation. This diagram is representative of a 5G NSA deployment, showing the user equipment's (UE's) dual connectivity to both an LTE Radio and a 5G New Radio. The data flow is represented using black dotted lines and red solid lines, with black representing control and red user plane communication flow through the 3GPP system. In 5G NSA deployments, all control plane traffic is routed via the LTE radio to the EPC, with the 5G New Radio providing extra capacity and throughput for user plane traffic. Figure 2 includes the concept of a network core data center, hosting the infrastructure and services required for the 3GPP system services to operate. In this implementation the data center includes the components required to achieve security characteristics associated with a trusted cloud deployment. These components consist of two trust domains: one for the operation and management of the secure infrastructure fabric, and one to provide the compute resources required by the 3GPP network functions.

Figure 2: Phase 1 Architecture



Component List

Phase 1: Preparing a Secure 5G Infrastructure & Architecture

- Commodity hardware with trust measurement capability
- Local and network storage
- Switches, routers
- Security gateways (SEGs), firewalls (e.g., roaming General Packet Radio Service [GPRS] Tunneling Protocol [GTP] control [GTP-C]/GTP user data tunneling [GTP-U] FW, SGi/N6 interface FW)
- Virtualization software
- Security and policy enforcement software, governance, risk, & compliance (GRC) / security information and event management (SIEM) / dashboard
- Virtualized LTE EPC components
- Home Subscriber Server (HSS)
- LTE eNodeB
- 5G NR gNodeB
- 5G NR UE / consumer IoT (CIoT) device
- Universal Integrated Circuit Card (UICC) components
- False base station detection capability
- Simulation equipment
- Network and telecommunication test tools

Phase 2: Secure 5G Infrastructure & Architecture

- Phase 1 components
- Container orchestration software
- Certificate management software
- Standalone 5G Core components
- gNodeB – centralized unit & distributed units
- Standalone-capable 5G UE
- Standalone-capable 5G CIoT device

Future Phases

- The components will be identified once the use case scenarios are developed in the near future.

Desired Security Characteristics and Properties

To address the scenarios discussed in Section 2, this project will utilize commercially available hardware and software technologies, which will include traditional IT components to support the underlying infrastructure as well as telecommunications components to support the 5G NSA and 5G SA functionality. The commercially available hardware and software will provide the following security capabilities.

Infrastructure Security Capabilities

This project will leverage the security features and capabilities described in the NCCoE Trusted Cloud project [6].

Trusted Hardware – The computing hardware will provide the capability to measure platform components and store the measurements in a hardware root of trust for later attestation. Custom values can be provisioned to the computing hardware root of trust, known as asset tags, which can also be used for future attestation. The platform measurements and asset tags can be used to define placement and migration policies for virtual workloads that run on top of the computing platform.

Isolation and Policy Enforcement – Once trust is established in the infrastructure, workloads can be restricted to run only on trusted hardware that meets specific asset policies. The platform trust measurement and asset tagging can also be used as part of the data protection policy of the workloads. Workloads can be encrypted at the virtual hard drive level, and only compute nodes that meet the defined trust and asset tag policies will have access to the decryption keys to run the workloads. Additionally, workloads can be logically isolated by utilizing SDN technologies. The SDN capability will allow network traffic policies to be defined for the workloads and ensure that authorized network communications between the different components are implemented and enforced.

Visibility and Compliance – Technical mechanisms will be continuously enforced and assessed to secure the environment over the lifecycle of the platform and workloads. These mechanisms enable the organization to manage risks and meet the compliance requirements by documenting and monitoring configuration changes. A governance risk compliance (GRC) tool can be leveraged to provide a detailed report or high-level dashboard view of the configuration of the environment, trust status of the infrastructure, network flows, or compliance posture of the system.

5G Non-Standalone Security Capabilities

EPC-Based Security Feature Enablement – The EPC in the NSA deployment will be configured in accordance with recommended practices, including enabling standards-based security features and configuring parameters in accordance with relevant guidelines.

False Base Station Protections – False base stations are unlicensed base stations that are not owned and operated by an authentic network operator. They broadcast cellular network information, masquerading as a legitimate network [4]. This threat exists due to the inherent properties of any RF system and are not specific to cellular networks. Phase 1 of this project is interested in utilizing commercial solutions to mitigate this threat and provide protections from false base stations that are not provided by the 3GPP standards.

Prevent Downgrade to Legacy Technology by Disabling UE's 2G Radio – As 5G technology is being deployed, it will coexist with previous cellular infrastructure already in place. As a result, there is a high probability that 5G networks will be deployed alongside LTE, 3G, and 2G networks. This multigenerational deployment of cellular networks provides interoperability for the customers, but it may impact the overall security posture of the network in these previous network generations.

Enhanced Infrastructure Security Capabilities

VM and Container Orchestration – The infrastructure components will rely on the foundational security characteristics of hardware roots of trust and asset tagging for placement of 5G Core workloads. The features and capabilities from the Infrastructure Security Capabilities will be augmented with any new features and functionality that come with Phase 2 of the project.

TLS Recommended Practice – TLS guidance will be utilized during this phase, specifically for handling secured communications within the infrastructure and between VNFs. Recommended practices regarding TLS version, cipher suites, certificate key size, and certificate management will be incorporated and documented.

5G Standalone Deployment Security Capabilities

Subscriber Privacy – The inclusion of subscriber identifier privacy-preserving features, like the ability to encipher the 5G subscriber identifier and restrict it from being sent over the air in the clear, mitigates threats present in previous generations of cellular networks. Phase 2 of this project may enable this standards-based feature available in commercial solutions and demonstrate the protections against threats like IMSI catching [4].

User Plane Integrity Protection Implementation – Control plane integrity protection has been available since UMTS, and with 5G's new key hierarchy, it is possible to apply integrity protection to user plane traffic. Phase 2 of this project will enable user plane integrity protection and configure it to use recommended cryptographic algorithms.

Security Protections Provided by the CU/DU Split – The split of the 5G base station, known as the CU/DU split, into a Distributed Unit (DU) and Centralized Unit (CU) enables security sensitive functions to be operated closer to the core network in a potentially more trusted environment. Phase 2 of this project will investigate how to most effectively take advantage of and implement this deployment option from a cybersecurity perspective.

Authentication Enhancements – A unified authentication framework will allow credential storage in embedded UICCs, allow network access via 3GPP and non-3GPP access technologies, and allow Native Extensible Authentication Protocol (EAP) support over 3GPP access networks. These enhancements enable operators to plug in different credentials and authentication methods without impacting intermediate network functions. Phase 2 may enable one or more features provided by this enhanced authentication framework.

Roaming Security – Security is required on inter-operator network connections (roaming) via a network function called the Security Edge Protection Proxy (SEPP). The SEPP implements application layer security for all the service layer information exchanged between the two networks. The SEPP also provides security functions for integrity, confidentiality, replay protection, mutual authentication, authorization, negotiation of cipher suites, and key management, as well as the notion of topology hiding and spoofing protection.

LTE to 5G interworking defined in 3GPP 23.501 [1] will be widely used as 5G SA deployments become more common. This interworking will require the use of secure procedures and security demarcations. Security will be especially critical when 5G to LTE interworking is occurring between two security domains or operators.

Phase 2 of the project will focus on these standards-based security features as well as commercial customized solutions in the reference implementation.

Network Exposure Function – This new element allows for secure exposure of network services such as voice, data connectivity, charging, and subscriber information to third-party applications over APIs. The element utilizes the topology hiding features provided with 5G's new SBA, allowing for a secure mechanism that internal and external third parties interact with to consume network services. The security protections offered by the network exposure function will be demonstrated with the implementation of 5G Core in phase 2 of the project.

The following table summarizes the required and optional capabilities for each phase. A complete and robust implementation will include capabilities defined in all the phases.

	Phase 1: Preparing a Secure 5G Infrastructure & Architecture	**Phase 2: Secure 5G Infrastructure & Architecture**	**Future Phases**
Trusted hardware	X	X	X
Isolation and policy enforcement	X	X	X
Visibility and compliance	X	X	X
VM and container orchestration		X	X
TLS recommended practice		X	X

	Phase 1: Preparing a Secure 5G Infrastructure & Architecture	Phase 2: Secure 5G Infrastructure & Architecture	Future Phases
EPC-based security feature enablement	X	X	X
False base station protections	X	X	X
Downgrade to legacy technology protections	X	X	X
Subscriber privacy		X	X
User plane integrity protection		X	X
CU/DU split		X	X
Authentication enhancements		X	X
Roaming security		X	X
Network exposure function		X	X

4 Relevant Standards and Guidance

Here is a list of relevant standards and guidance documents.

- 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".
- 3GPP TS 33.401: "3GPP System Architecture Evolution (SAE); Security architecture".
- 3GPP TS 23.501: "System Architecture for the 5G System".
- 3GPP TS 33.501: "Security architecture and procedures for 5G system (Release 15)".
- 3GPP TS 33.210: "3G security; Network Domain Security (NDS); IP network layer security".
- ETSI GS NFV 002: "Network Functions Virtualisation (NFV); Architectural Framework".
- ETSI GS NFV-SEC 009: "Network Functions Virtualisation (NFV); NFV Security; Report on use cases and technical approaches for multi-layer host administration".
- ETSI GR NFV-SEC 016: "Network Functions Virtualisation (NFV); Security; Report on location, timestamping of VNFs".
- NIST SP 800-53 Rev 4: "Security and Privacy Controls for Federal Information Systems and Organizations"
- NIST SP 800-187: "Guide to LTE Security"
- NIST SP 1800-19: "Trusted Cloud: VMware Hybrid Cloud IaaS Environments"
- NIST SP 1800-16: "Securing Web Transactions: Transport Layer Security (TLS) Server Certificate Management"
- NIST SP 800-77 Rev 1: "Guide to IPsec VPNs"
- NIST SP 800-52 Rev 2: "Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations"

- NIST SP 800-124: “Guidelines for Managing the Security of Mobile Devices in the Enterprise”
- Securing Web Transactions: TLS Server Certificate Management - https://www.nccoe.nist.gov/projects/building-blocks/tls-server-certificate-management
- NCCoE Mobile Device Security - https://www.nccoe.nist.gov/projects/building-blocks/mobile-device-security
- CSRIC VII, WG 2, Managing Security Risk in the Transition to 5G - https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-vii
- CSRIC VII, WG 2, Managing Security Risk in Emerging 5G Implementations
- CSRIC VI, WG 3, Network Reliability and Security Risk Reduction
- CSRIC V, WG 10, Legacy Systems and Services Risk Reduction
- ATIS Technical Report, “5G Security Requirements (ATIS 1000077)”

5 Security Control Map

This table maps the characteristics of the commercial products that the NCCoE will apply to this cybersecurity challenge to the applicable standards and best practices described in the Framework for Improving Critical Infrastructure Cybersecurity, and to other NIST activities. This exercise is meant to demonstrate the real-world applicability of standards and best practices but does not imply that products with these characteristics will meet an industry’s requirements for regulatory approval or accreditation.

Table 5-1 List of NIST SP 800-53 Revision 4 Controls Addressed by Solution

ID	Control Description
Access Control (AC)	
AC-3	Access Enforcement
AC-4	Information Flow Enforcement
AC-17	Remote Access
AC-20	Use of External Information Systems
Audit and Accountability (AU)	
AU-2	Audit Events
AU-3	Content of Audit Records
AU-4	Audit Storage Capacity
AU-5	Response to Audit Processing Failures
AU-6	Audit Review, Analysis, and Reporting
AU-7	Audit Reduction and Report Generation
AU-8	Time Stamps
AU-9	Protection of Audit Information
AU-10	Non-Repudiation

ID	Control Description
AU-11	Audit Record Retention
AU-12	Audit Generation
Security Assessment and Authorization (CA)	
CA-7	Continuous Monitoring
Configuration Management (CM)	
CM-3	Configuration Change Control
CM-4	Security Impact Analysis
CM-8	Information System Component Inventory
CM-9	Configuration Management Plan
CM-10	Software Usage Restrictions
Identification and Authentication (IA)	
IA-2	Identification and Authentication (Organizational Users)
IA-3	Device Identification and Authentication
IA-4	Identifier Management
IA-5	Authenticator Management
IA-7	Cryptographic Module Authentication
Maintenance (MA)	
MA-2	Controlled Maintenance
MA-3	Maintenance Tools
MA-4	Nonlocal Maintenance
MA-5	Maintenance Personnel
MA-6	Timely Maintenance
Risk Assessment (RA)	
RA-3	Risk Assessment
RA-5	Vulnerability Scanning
System and Services Acquisition (SA)	
SA-18	Tamper Resistance and Detection
System and Communications Protection (SC)	
SC-2	Application Partitioning
SC-3	Security Function Isolation
SC-7	Boundary Protection
SC-8	Transmission Confidentiality and Integrity
SC-12	Cryptographic Key Establishment and Management
SC-13	Cryptographic Protection
SC-15	Collaborative Computing Devices

ID	Control Description
SC-16	Transmission of Security Attributes
SC-28	Protection of Information at Rest
System and Information Integrity (SI)	
SI-2	Flaw Remediation
SI-4	Information System Monitoring
SI-7	Software, Firmware, and Information Integrity

544 **Table 5-2 List of NIST Cybersecurity Framework Subcategories Addressed by Solution**

Cyber-security Framework Subcategory Identifier	Cybersecurity Framework Subcategory Name
Identify (ID)	
ID.AM-2	Software platforms and applications within the organization are inventoried.
Protect (PR)	
PR.AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes.
PR.AC-3	Remote access is managed.
PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation).
PR.AC-6	Identities are proofed and bound to credentials and asserted in interactions.
PR.AC-7	Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the privacy risks and other organizational risks).
PR.DS-1	Data-at-rest is protected.
PR.DS-2	Data-in-transit is protected.
PR.DS-3	Assets are formally managed throughout removal, transfers, and disposition.
PR.DS-6	Integrity checking mechanisms are used to verify software, firmware, and information integrity.
PR.IP-3	Configuration change control processes are in place.
PR.IP-4	Backups of information are conducted, maintained, and tested.
PR.IP-9	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.
PR.IP-12	A vulnerability management plan is developed and implemented.
PR.MA-1	Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools.

Cyber-security Framework Subcategory Identifier	Cybersecurity Framework Subcategory Name
PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.
PR.PT-4	Communications and control networks are protected.
Detect (DE)	
DE.AE-1	A baseline of network operations and expected data flows for users and systems is established and managed.
DE.AE-2	Detected events are analyzed to understand attack targets and methods.
DE.AE-3	Event data are collected and correlated from multiple sources and sensors.
DE.AE-4	Impact of events is determined.
DE.AE-5	Incident alert thresholds are established.
DE.CM-1	The network is monitored to detect potential cybersecurity events.
DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed.

Appendix A: References

[1] 3rd Generation Partnership Project (3GPP), 3GPP TS 23.501 System architecture for the 5G System (5GS); Stage 2 (Release 16), December 2019 http://www.3gpp.org/ftp//Specs/archive/23_series/23.501/23501-g30.zip

[2] 3rd Generation Partnership Project (3GPP), 3GPP TS 33.501 Security architecture and procedures for 5G system (Release 16), December 2019 http://www.3gpp.org/ftp//Specs/archive/33_series/33.501/33501-g10.zip

[3] 3rd Generation Partnership Project (3GPP), 3GPP TS 33.210 Network Domain Security (NDS); IP network layer security (Release 16), June 2019 http://www.3gpp.org/ftp//Specs/archive/33_series/33.210/33210-g20.zip

[4] National Institute of Standards and Technology (NIST), NIST Special Publication (SP) 800-187, Guide to LTE Security, December 2017 https://doi.org/10.6028/NIST.SP.800-187

[5] National Institute of Standards and Technology (NIST), NIST Special Publication (SP) 1800-19, Trusted Cloud: VMware Hybrid Cloud IaaS Environments, November 2018 https://www.nccoe.nist.gov/sites/default/files/library/sp1800/tc-hybrid-nist-sp1800-19b-preliminary-draft.pdf

[6] National Cybersecurity Center of Excellence (NCCoE), Trusted Cloud Projects https://www.nccoe.nist.gov/projects/building-blocks/trusted-cloud

Appendix B: Acronyms

Selected acronyms and abbreviations used in this paper are defined below.

2G	**2nd Generation**
3G	**3rd Generation**
3GPP	**3rd Generation Partnership Program**
4G	**4th Generation**
5G	**5th Generation**
API	**Application Programming Interface**
CIoT	**Cellular Internet of Things**
CNF	**Containerized Network Function**
CSRIC	**Communications Security, Reliability and Interoperability Council**
CU	**Centralized Unit**
DNSSEC	**Domain Name System Security Extensions**
DU	**Distributed Unit**
EAP	**Extensible Authentication Protocol**
eNodeB	**Evolved Node B**
EPC	**Evolved Packet Core**
FCC	**Federal Communications Commission**
gNodeB	**Next Generation Node B**
GPRS	**General Packet Radio Service**
GRC	**Governance Risk & Compliance**
GTP	**GPRS Tunneling Protocol**
GTP-C	**GPRS Tunneling Protocol control**
GTP-U	**GPRS Tunneling Protocol user data tunneling**
HSS	**Home Subscriber Server**
IaaS	**Infrastructure as a Service**
IMSI	**International Mobile Subscriber Identity**
IoT	**Internet of Things**
IP	**Internet Protocol**
IPsec	**Internet Protocol Security**
JOSE	**JavaScript Object Signing and Encryption**

LTE	**Long-Term Evolution**
NCCoE	**National Cybersecurity Center of Excellence**
NDS/IP	**Network Domain Security/Internet Protocol**
NF	**Network Function**
NFV	**Network Functions Virtualisation**
NIST	**National Institute of Standards and Technology**
NR	**New Radio**
NSA	**5G Non Standalone**
PLMN	**Public Land Mobile Network**
RAN	**Radio Access Network**
RAT	**Radio Access Technology**
RF	**Radio Frequency**
RFI	**Request for Information**
RFP	**Request for Proposal**
SA	**5G Standalone**
SAE	**System Architecture Evolution**
SBA	**Service-Based Architecture**
SDN	**Software Defined Networking**
SEG	**Security Gateway**
SEPP	**Security Edge Protection Proxy**
SIEM	**Security Information and Event Management**
SMS	**Short Message Service**
TCP	**Transmission Control Protocol**
TLS	**Transport Layer Security**
TR	**Technical Report**
TS	**Technical Specification**
UE	**User Equipment**
UICC	**Universal Integrated Circuit Card**
UMTS	**Universal Mobile Telecommunications System**
USIM	**Universal Subscriber Identity Module**
V2X	**Vehicle-to-Everything (V2X)**
VNF	**Virtualized Network Function**