NIST SPECIAL PUBLICATION 1800-33A

5G Cybersecurity

Volume A:
Executive Summary

Mike Bartock
Jeff Cichonski
Murugiah Souppaya
National Institute of Standards and Technology
Information Technology Laboratory

Karen Scarfone
Scarfone Cybersecurity
Clifton, Virginia

February 2021

PRELIMINARY DRAFT

This publication is available free of charge from
https://www.nccoe.nist.gov/projects/building-blocks/5g-cybersecurity

Executive Summary

Fifth generation technology for broadband cellular networks – or 5G will significantly improve how humans and machines communicate, operate, and interact in the physical and virtual world. 5G brings with it increased bandwidth and capacity, and low latency, which will benefit organizations in all sectors as well as home consumers. As 5G rolls out, cybersecurity professionals are focused on safeguarding this new technology while 5G development, deployment, and usage are still evolving.

This project, which is currently in an early stage of designing and building a solution, will demonstrate how operators and users of 5G networks can mitigate 5G cybersecurity risks. This is accomplished by strengthening the system's architectural components, providing a secure cloud-based supporting infrastructure, and enabling the security features introduced in the 5G standards. These measures support common use cases and meet industry sectors' recommended cybersecurity practices and compliance requirements. As the project progresses, this preliminary draft will be updated, and additional volumes will also be released for comment.

CHALLENGE

5G is at a transition point where the technologies are simultaneously being specified in standards bodies, implemented by equipment vendors, deployed by network operators, and adopted by consumers. Although standards for some 5G cybersecurity features have been published by standards bodies, organizations planning to deploy, operate, and use 5G networks are challenged to determine what security capabilities 5G can provide and how they can deploy these features to safeguard data and communications.

Current 5G cybersecurity standards development primarily focuses on the security of the standards-based, interoperable interfaces between 5G components. The 5G standards do not specify cybersecurity protections to deploy on the underlying information technology (IT) components that support and operate the 5G system. This lack of information increases the complexity for organizations planning to leverage 5G. With the 5G architecture based on cloud technology, 5G systems could potentially leverage the robust security features available in cloud computing architectures to protect 5G data and communications.

This practice guide can help your organization:

- Understand the cybersecurity opportunities, challenges, and risks associated with 5G network deployment, operation and usage
- Design, acquire, integrate, implement, and operate 5G networks from the hardware to software stack to provide the necessary cybersecurity capabilities to support various use cases

SOLUTION

After discussions with the community of interest and the industry collaborators participating in the effort, and given the evolution of the standards, the availability of commercial products, and the alignment with commercial networks, the project will focus on 5G standalone (SA) networks. Telecom carriers have started or are planning to migrate to 5G SA, since the newest 3rd Generation Partnership

Project (3GPP) standards-based 5G security enhancements are available only for a 5G core in a 5G SA network (not a 5G non-standalone [NSA] network). To fully demonstrate and showcase these 5G security capabilities, the NCCoE project will demonstrate a typical implementation of a secure 5G SA deployment.

This project will begin with a 5G SA deployment that operates on and leverages a trusted and secure cloud-native hosting infrastructure. The example implementation will demonstrate how cloud technologies can provide foundational security features outside the scope of 3GPP's 5G security architecture. Next, the project will showcase how 5G security features can be utilized to address known security challenges found in previous generations of cellular networks such as LTE. It will also demonstrate how both commercial and open source products can leverage cybersecurity standards and recommended practices for each of the 5G use case scenarios. If gaps in 5G cybersecurity standards are identified during the project, the appropriate standards development organizations (SDOs) will be notified, and some of the project's collaborators may contribute to SDO efforts to address the gaps.

The solution will be designed around two focus areas:

- The **Infrastructure Security Focus Area** will concentrate on the trusted and secure cloud resources required to operate a modern mobile network, specifically the supporting infrastructure's cybersecurity protections. The objective is to provide a trusted infrastructure to support the 5G Core Network functions, radio access network (RAN) components, and associated workloads. Since security for the underlying infrastructure is not within the scope of 3GPP specifications, this focus area is included in the project to provide a holistic security reference architecture for a complete 5G network.
- The **5G Standalone Security Focus Area** will deploy a 5G SA Network to enable the foundational configuration of the 5G Core's security features in a manner that demonstrates the cybersecurity capabilities available in a 5G SA deployment. The deployment will include 5G New Radio base stations and a 5G Next Generation Core. The deployment will demonstrate how security capabilities can be used for continuous monitoring of 5G traffic on both signaling and data layers to detect and prevent cybersecurity attacks and threats. The NCCoE anticipates that the initial deployment will include classical RAN components, potentially leveraging virtualized RAN components in the future depending on the availability of commercial technology and collaborator contributions.

The following is a list of the project's collaborators.

While the NCCoE is using a suite of commercial products to address this challenge, this guide does not endorse these particular products, nor does it guarantee compliance with any regulatory initiatives. Your organization's information security experts should identify the products that will best fit your organization. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a solution.

HOW TO USE THIS GUIDE

Depending on your role in your organization, you might use this guide in different ways:

Business decision makers, including chief information security and technology officers, can use this part of the guide, *NIST SP 1800-33A: Executive Summary*, to understand the drivers for the guide, the cybersecurity challenge we address, our approach to solving this challenge, and how the solution could benefit your organization.

Technology, security, and privacy program managers who are concerned with how to identify, understand, assess, and mitigate risk can use *NIST SP 1800-33B: Approach, Architecture, and Security Characteristics* once it is made available. It will describe what we built and why, including the risk analysis performed and the security/privacy control mappings.

IT professionals who want to implement an approach like this can make use of *NIST SP 1800-33C: How-To Guides* once it is available. It will provide specific product installation, configuration, and integration instructions for building the example implementation, allowing you to replicate all or parts of this project.

SHARE YOUR FEEDBACK

You can view or download the preliminary draft guide at https://www.nccoe.nist.gov/projects/building-blocks/5g-cybersecurity. Help the NCCoE make this guide better by sharing your thoughts with us. There will be at least one additional comment period for this volume, and the other volumes of this guide will be released for review and comment on individual schedules so that each volume is available as soon as possible.

Once the example implementation is developed, you can adopt this solution for your own organization. If you do, please share your experience and advice with us. We recognize that technical solutions alone will not fully enable the benefits of our solution, so we encourage organizations to share lessons learned and best practices for transforming the processes associated with implementing this guide.

To provide comments, join the community of interest, or to learn more about the project and example implementation, contact the NCCoE at 5g-security@nist.gov.

COLLABORATORS

Collaborators participating in this project submitted their capabilities in response to an open call in the Federal Register for all sources of relevant security capabilities from academia and industry (vendors and integrators). Those respondents with relevant capabilities or product components signed a Cooperative Research and Development Agreement (CRADA) to collaborate with NIST in a consortium to build this example solution.

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in order to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.