5G CYBERSECURITY: PREPARING A SECURE EVOLUTION TO 5G

The National Institute of Standards and Technology's (NIST's) National Cybersecurity Center of Excellence (NCCoE) is addressing the challenge of improving the secure adoption of 5G networks through collaborative efforts with industry and the IT community, including vendors of IT components and telecommunications components. This fact sheet provides an overview of the 5G Cybersecurity: Preparing a Secure Evolution to 5G project, including challenge, proposed solution, and potential benefits.

We are currently seeking feedback on a draft project description, *5G Cybersecurity: Preparing a Secure Evolution to 5G*. The public comment period is open through March 31, 2020. Please submit your feedback. If you have questions or suggestions, please contact us at 5G-security@nist.gov.

CHALLENGE

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. 5G networks support increased cybersecurity protections through the addition of standards-based features and the increased use of modern information technologies. With cellular networks transitioning from 4G to 5G, it is important for organizations to understand and address the challenges, opportunities, and risks associated with the use of 5G networks.

The 5G system introduces new cybersecurity protections as well as the concept of a service-based architecture (SBA) for the first time in cellular networks. It is envisioned with SBA that 5G network components will be deployed on a hyper-scalable containerized and virtualized infrastructure, similar to modern internet applications. This shift in network architecture brings with it the security challenges and opportunities associated with modern internet technologies. As 5G becomes a ubiquitous technology, it will provide new capabilities tailored to specific use case scenarios stemming from industry verticals such as autonomous vehicles, smart manufacturing, and smart cities. 5G technologies are continuously being specified in standardization bodies, implemented by equipment vendors, and deployed by network operators, so organizations using or planning to use 5G technology can be aware of the cybersecurity features currently supported by technology, the maturity of applicable standards, and the state of commercial deployments.

PROPOSED SOLUTION

The NCCoE and its collaborators are initiating an effort in collaboration with industry to demonstrate how the components of 5G architectures can be used securely to mitigate risks and meet industry sectors' compliance requirements for a number of 5G use case scenarios. 5G standards have been designed to support use case-specific capabilities by way of network deployment options. The proposed proof-of-concept solution will integrate commercial and open source products that leverage cybersecurity standards and recommended practices to showcase 5G's robust security features.

Phase 1 of the project will establish a foundational infrastructure that aligns with current available cybersecurity capabilities, including specific security configurations of the 5G Non-Standalone (NSA) architecture to support various industry standards and regulations. The phase 1 implementation aims to couple the 5G system with the NCCoE's trusted cloud implementation, 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, e.g., 2G. Subsequent phases are expected to focus on standalone deployment architectures and extend the initial work to cover additional 5G use case scenarios that are still evolving.

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 using commercially available technology.

LEARN MORE ABOUT NCCOE
Visit https://www.nccoe.nist.gov

CONTACT US
nccoe@nist.gov
301-975-0200

BENEFITS

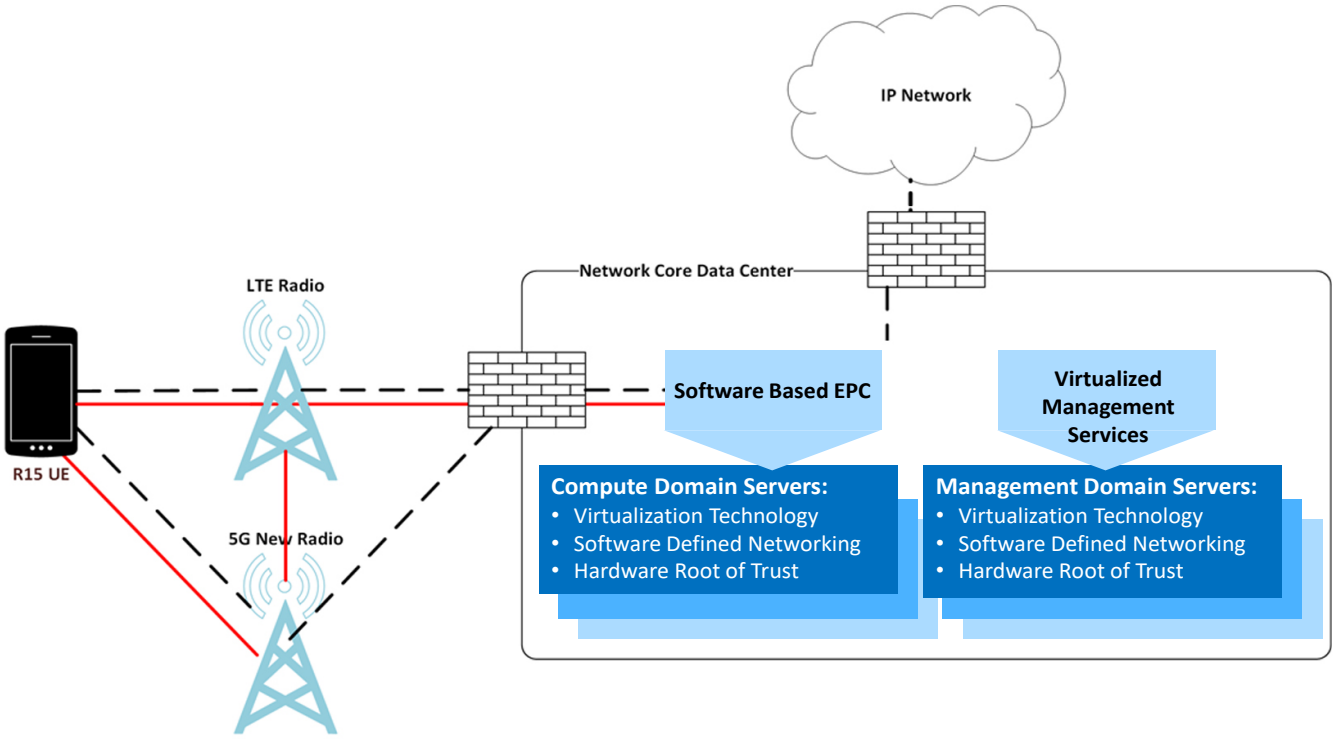
The NCCoE's practice guide to 5G Cybersecurity will help organizations:

- design, acquire, integrate, and operate 5G-based networks to be used for adopting and deploying 5G technology
- increase their understanding of 5G's standards-based security features
- prioritize 5G-related contributions to standards developing organizations

HIGH-LEVEL ARCHITECTURE

The proposed high-level architecture for Phase 1 is depicted in the diagram below. It is representative of a 5G NSA deployment, showing the user equipment's (UE's) dual connectivity to both a Long-Term Evolution (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 3rd Generation Partnership Project (3GPP) system. In 5G NSA deployments, all control plane traffic is routed via the LTE radio to the Evolved Packet Core (EPC), with the 5G New Radio providing extra capacity and throughput for user plane traffic.

This architecture 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.



DOWNLOAD PROJECT DESCRIPTION

This fact sheet provides a high-level overview of the work underway on 5G cybersecurity. For more details, download the project description or scan the QR code which takes you to the 5G Cybersecurity project page.

HOW TO PARTICIPATE

As a private-public partnership, we are always seeking insights from businesses, the public, and technology vendors. If you have questions about this project, or if you are interested in contributing technology or expertise, please email to 5G-security@nist.gov.