



Applying 5G Cybersecurity and Privacy Capabilities

Introduction to the White Paper Series

NIST Cybersecurity White Paper

NIST CSWP 36 ipd

Michael Bartock, Jeffrey Cichonski,
Murugiah Souppaya
Information Technology Laboratory

Karen Scarfone
Scarfone Cybersecurity

Parisa Grayeli, Sanjeev Sharma
The MITRE Corporation

Thomas McCarthy, Muthukkumaran
Ramalingam, Presanna Raman,
Stefano Righi
AMI

Jitendra Patel, Bogdan Ungureanu
AT&T

Tao Wan
CableLabs

Matt Hyatt, Steve Vetter
Cisco

Dan Carroll
Dell Technologies

Steve Orrin
Intel

Corey Piggott
Keysight Technologies

Michael Yeh
MiTAC Computing Technology Corp.

Gary Atkinson, Rajasekhar Bodanki,
Don McBride
Nokia Bell Labs

Aarin Buskirk, Bryan Wenger
Palo Alto Networks

Todd Gibson
T-Mobile

August 2024

Initial Public Draft

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.CSWP.36.ipd>

Abstract

This document introduces the white paper series titled Applying 5G Cybersecurity and Privacy Capabilities. This series is being published by the National Cybersecurity Center of Excellence (NCCoE) [5G Cybersecurity project](#). Each paper in the series will include information, guidance, and research findings for an individual technical cybersecurity- or privacy-supporting capability available in 5G systems or their supporting infrastructures. Each of the capabilities has been implemented in a testbed as part of the NCCoE project, and each white paper reflects the results of that implementation and its testing.

Audience

This series is intended for technology, security, and privacy program managers who are concerned with how to identify, understand, assess, and mitigate risk for 5G networks. The information is targeting three types of organizations:

Commercial mobile network operators. This series will provide them a better understanding of cloud security capabilities that are already available in the systems their vendors provide. These hardware-enabled security capabilities are beyond what 5G standards currently specify and can provide complementary protection at this time. This is increasingly important as operations move to commodity platforms and software, and as mobile network technology merges with IT.

Potential private 5G network operators. Private 5G networks are expected to become a reality, such as at universities and large companies. Any organization considering deploying and operating its own 5G network will need to manage its security using a risk-based approach. This series will explain a range of security capabilities and the risks each capability helps mitigate, which will provide valuable information for organizations' risk management purposes.

Organizations using and managing 5G-enabled technology. Before organizations adopt 5G-enabled technologies, they should make cybersecurity risk management decisions regarding their use, management, and maintenance. The information in this series should help to inform those decisions.

This series may be helpful to participants in 5G-related standards efforts (e.g., from standards developing organizations) who want to identify gaps in standards to inform their future work. Cybersecurity researchers who want to build 5G cybersecurity research testbeds may also find this series useful as a reference.

All readers should already know the basic concepts of 5G; there are many resources available on 5G basics, including those from the GSM Association (GSMA)¹ and Nokia². Readers should also be familiar with fundamental cybersecurity concepts. No previous knowledge of 5G-specific security or hardware roots of trust is necessary.

¹ <https://www.gsma.com/security/securing-the-5g-era/>

² <https://www.nokia.com/networks/5g/mobile/5g-resources/>

Keywords

5G, cybersecurity, privacy

Acknowledgments

We are grateful to the following individuals for their generous contributions.

Sallie Edwards, Mary Raguso, Charles Teague
The MITRE Corporation

Cherilyn Pascoe, Adam Sedgewick, Kevin Stine
NIST

5G Cybersecurity and Privacy Challenges

5G technology for broadband cellular networks will significantly improve how humans and machines communicate, operate, and interact in the physical and virtual world. 5G provides increased bandwidth and capacity and low latency. However, professionals in the fields of technology, cybersecurity, and privacy are faced with safeguarding this technology while its development, deployment, and usage are still evolving. As 5G evolves, its capabilities are simultaneously being specified in standards bodies, implemented by equipment vendors, deployed by network operators, and adopted by consumers.

Current standards development primarily focuses on the security of the standards-based, interoperable interfaces between 5G components. The 5G standards do not specify cybersecurity or privacy protections to deploy on the underlying IT components that support and operate the 5G system. This lack of specifications increases the complexity for organizations planning to leverage 5G. They are challenged to determine what cybersecurity and privacy capabilities 5G can provide, how they can deploy these features, and what supplementary capabilities they may need to implement to safeguard data and communications.

Addressing the Challenges

To address these challenges, the NCCoE is collaborating with technology providers to develop example solution approaches for safeguarding 5G standalone (SA) networks through a combination of the following measures:

- strengthening the system's architectural components;
- providing a trusted and secure cloud-native hosting infrastructure to support the 5G Core Network functions, radio access network (RAN) components, and associated workloads; and
- enabling the cybersecurity and privacy features introduced in the 5G standards, including demonstrating how to continuously monitor 5G traffic on both signaling and data layers to detect and prevent cybersecurity attacks and threats.

White Paper Series

Each white paper in the series presents information, guidance, and research findings for an individual technical cybersecurity- or privacy-supporting capability available in 5G systems or their supporting infrastructures. The capabilities have been implemented in a testbed³ as part of the NCCoE project, and each white paper's contents, especially guidance and research findings, directly stem from these implementations and their testing. The white paper series provides detailed information on selected cybersecurity and privacy capabilities from the broad range of capabilities available for 5G systems and infrastructures.


Each paper has an **Overview** covering the following topics for its cybersecurity or privacy capability:

- The **cybersecurity or privacy problem** that the capability is being used to address. This forms the rationale for why the specific capability exists and provides the reader enough technical context, including pointers to additional resources with more technical details about the problem, to inform risk-based determinations around using a specific capability.
- **How the capability addresses the problem**, including contextual information around when the capability was introduced, where is it expected to be available, and what is necessary to enable it.
- **Which 5G architecture components are involved** in the functionality of this capability.
- **Tips on enabling, configuring, and using the capability**, as informed by our testbed research.

Each paper has a **Technical Details** section. It is intended for readers seeking more in-depth knowledge of the cybersecurity or privacy capability. Much technical effort was invested in the deployment, configuration, and validation of each capability in the NCCoE 5G Cybersecurity project testbed. This section of the white papers provides an opportunity to share some of the know-how that was garnered while working with these capabilities. Expect this section to provide insights like what particular 5G messages contain, how to measure platform integrity, or how to verify that the capability is working as expected.

The white paper series can be found on <https://www.nccoe.nist.gov/5g-cybersecurity>

³ More information about the NCCoE's 5G Cybersecurity testbed can be found on www.nccoe.nist.gov/5g-cybersecurity.



Certain commercial equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.

NIST Technical Series Policies

[Copyright, Use, and Licensing Statements](#)

[NIST Technical Series Publication Identifier Syntax](#)

Author ORCID iDs

Michael Bartock: 0000-0003-0875-4555

Jeffrey Cichonski: 0009-0006-1137-2549

Karen Scarfone: 0000-0001-6334-9486

Murugiah Souppaya: 0000-0002-8055-8527

How to Cite this NIST Technical Series Publication:

Bartock M. et al. (2024) Applying 5G Cybersecurity and Privacy Capabilities: Introduction to the White Paper Series (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 36 ipd. <https://doi.org/10.6028/NIST.CSWP.36.ipd>

Public Comment Period

August 15, 2024 - September 16, 2024

Submit Comments

5g-security@nist.gov

Or submit the web form at <https://www.nccoe.nist.gov/5g-cybersecurity>

National Institute of Standards and Technology

Attn: Applied Cybersecurity Division, Information Technology Laboratory

100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

Additional Information

Additional information about this publication is available at

<https://www.nccoe.nist.gov/5g-cybersecurity>,

including related content, potential updates, and document history.

All comments are subject to release under the Freedom of Information Act (FOIA).