IEEE

IEEE

INGR

International Network Generations Roadmap

2022 Edition

Security and Privacy

IEEE Future NETWORKS™

An IEEE 5G and Beyond Technology Roadmap

futurenetworks.ieee.org/roadmap

Table of Contents

Tables

Figures

ABSTRACT

The digital transformation brought on by 5G is redefining current models of end-to-end (E2E) connectivity and service reliability to include security-by-design principles necessary to enable 5G to achieve its promise. 5G trustworthiness highlights the importance of embedding security capabilities from the very beginning while the 5G architecture is being defined and standardized. Security requirements need to overlay and permeate through the different layers of 5G systems (physical, network, and application) as well as different parts of an E2E 5G architecture within a risk-management framework that takes into account the evolving security-threats landscape. 5G presents a typical use-case of wireless communication and computer networking convergence, where 5G fundamental building blocks include components such as Software Defined Networks (SDN), Network Functions Virtualization (NFV) and the edge cloud. This convergence extends many of the security challenges and opportunities applicable to SDN/NFV and cloud to 5G networks. Thus, 5G security needs to consider additional security requirements (compared to previous generations) such as SDN controller security, hypervisor security, orchestrator security, cloud security, edge security, etc. At the same time, 5G networks offer security improvement opportunities that should be considered. Here, 5G architectural flexibility, programmability and complexity can be harnessed to improve resilience and reliability.

The working group scope fundamentally addresses the following:

- 5G security considerations need to overlay and permeate through the different layers of the 5G systems (physical, network, and application) as well as different parts of an E2E 5G architecture including a risk management framework that takes into account the evolving security threats landscape.
- 5G exemplifies a use-case of heterogeneous access and computer networking convergence, which extends a unique set of security challenges and opportunities (e.g., related to SDN/NFV and edge cloud, etc.) to 5G networks. Similarly, 5G networks by design offer potential security benefits and opportunities through harnessing the architecture flexibility, programmability and complexity to improve its resilience and reliability.
- The IEEE FNI security WG's roadmap framework follows a taxonomic structure, differentiating the 5G functional pillars and corresponding cybersecurity risks. As part of cross collaboration, the security working group will also look into the security issues associated with other roadmap working groups within the IEEE Future Network Initiative.

Disclaimer: in this document we use 5G to refer to future networks including evolution such as B5G, 6G, etc.

Key words:

5G Cybersecurity, security, privacy, data protection, reliability, resilience, mMTC, URLLC, SDN/NFV, cyber risk assessment and management, threat scenarios, cyber-attacks, security controls, mitigation, defense.

CONTRIBUTORS

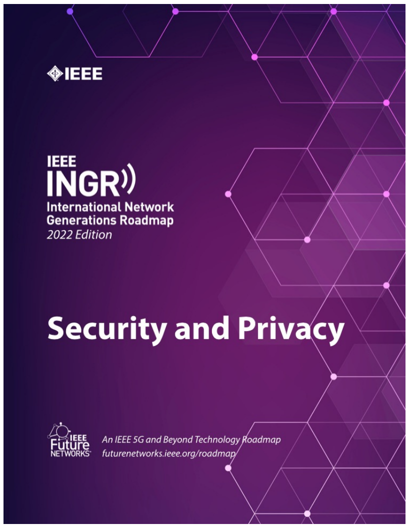
Ashutosh Dutta	John's Hopkins University / Applied Physics Lab, Security Working Group Co-Chair
Eman Hammad	Texas A&M University – RELLIS, Security Working Group Co-Chair
Michael Enright	Quantum Dimension, Inc.
Fawzi Behmann	IEEE ComSoc North America Regional Board, TelNet Management Consulting, Inc.
Arsenia Chorti	ENSEA, CNRS
Ahmad Cheema	Shared Services Canada
Kassi Kadio	Shared Services Canada
Julia Urbina-Pineda	IEEE HKN Member and CyberIIoT CEO
Khaled Alam	Rogers Communications (Formerly)
Ahmed Limam	Higher Institute of Engineering and Technology (ESPRIT)
Fred Chu	University of California, Los Angeles
John Lester	Our Lady of Fatima University Valenzuela, Philippines
Jong-Geun Park	Seoul National University of Science and Technology
Joseph Bio-Ukeme	Carleton University
Sanjay S Pawar	Usha Mittal University of Technology
Roslyn Layton	Aalborg University
Prakash Ramchandran	Intel
Kingsley Okonkwo	Chevron
Lyndon Ong	Ciena
Marc Emmelmann	Fraunhofer FOKUS
Omneya Issa	Department of National Defence, Canada
Rajakumar Arul	Amrita Vishwa Vidyapeetham
Sireen Malik	T-Mobile
Sivarama Krishnan	National Library of Medicine
Suresh Sugumar	Intel Corporation
Tk Lala	ZecureZ Consulting Company
Matthew Borst	IEEE Future Networks Initiative
Brad Kloza	IEEE Future Networks Initiative

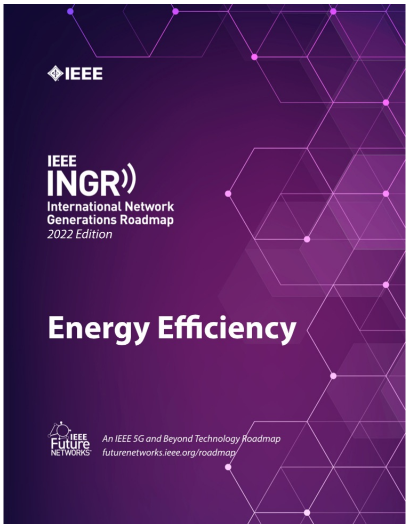
Want to read the full chapter?

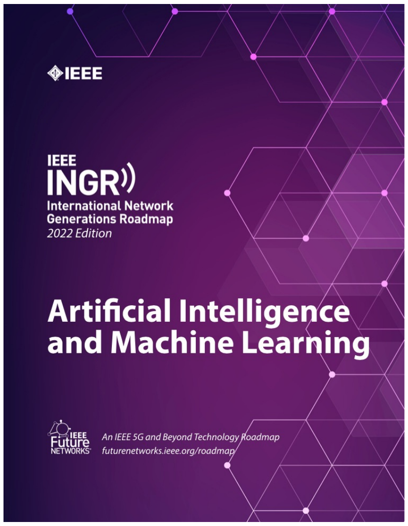
Accessing full INGR chapters is easy and affordable.

Step 1. Click here to join the Future Networks initiative (free for any IEEE Society member, and low-cost for non-members)

Step 2. Return to the INGR page to download full chapters.







14 chapters available!