This file is a free sample of this chapter.

The full chapter is available exclusively to signed-in participants of the IEEE Future Networks Community.

Click here to join the Future Networks initiative (free for any IEEE Society member, and low-cost for non-members), then return to the INGR page to download full chapters.

Would you like to join an INGR Working Group?

Click here for contact information for each group.

Interested in booking a private session with INGR experts for your company? Contact an IEEE Account Manager to discuss an INGR Roadmap Virtual Private Event.

+1 800 701 4333 (USA/Canada)
+1 732 981 0060 (worldwide)

onlinesupport@ieee.org
Security and Privacy
# Table of Contents

1. *Introduction* .......................................................................................................................... 1  
   1.1. 2022 Edition Update .............................................................................................................. 3  

2.  *Working Group Vision* ............................................................................................................ 3  
   2.1. The Big Picture for Security ................................................................................................. 3  
   2.2. Vision for a Successful Future Network Industry ............................................................... 4  
   2.3. 3-, 5-, and 10-Year’s Goals ................................................................................................. 4  
   2.4. Security’s Projected Impact ................................................................................................. 5  
   2.5. Scope of Working Group Effort ........................................................................................... 5  
   2.6. Linkages and Stakeholders ................................................................................................. 7  
   2.7. Working Group Summary of Activities ............................................................................... 9  

3.  *Today’s Landscape* ................................................................................................................... 10  
   3.1. Current State of Technology and Research ....................................................................... 10  

4.  *Future State (2032)* ................................................................................................................ 11  
   4.1. Reference Architecture ........................................................................................................ 11  

5.  *Foundational Concepts* .......................................................................................................... 13  
   5.1. System Setup and Threat Model ......................................................................................... 13  
   5.2. Cybersecurity Frameworks ................................................................................................. 14  
   5.3. Cyber Risk Management Framework and Methodology .................................................... 15  

6.  *Security and Privacy Domains* ............................................................................................... 16  
   6.1. Management and Orchestration Security ........................................................................... 17  
      6.1.1. Virtualization / Softwarization Security ...................................................................... 17  
      6.1.2. SDN Security ................................................................................................................. 20  
      6.1.3. Network Slicing Security ............................................................................................. 21  
   6.2. Edge Security ...................................................................................................................... 23  
   6.3. Third Party Security ........................................................................................................... 24  
      6.3.1. Supply Chain Security ................................................................................................. 24  
      6.3.2. Open Source / Application Programmable Interface (API) Security ............................ 25  
      6.3.3. Device / Hardware Security ......................................................................................... 26  
   6.4. Data Privacy and Security .................................................................................................... 26  
      6.4.1. Satellite Security ........................................................................................................... 26  
   6.6. Massive MIMO Security ..................................................................................................... 29  
   6.7. mmWave Security .............................................................................................................. 29  
   6.8. Spectrum Security .............................................................................................................. 29  
   6.9. Physical Layer Security ....................................................................................................... 30  
      6.9.1.1. Resilience and Robustness Against Active Attacks ................................................. 30
6.9.1.2. Authentication Using RF Fingerprinting and Hardware Features  
6.9.1.3. Secret Key Generation (SKG) From Wireless Fading Coefficients  
6.9.1.4. Keyless Transmission of Confidential Messages  
6.9.1.5. Anomaly Detection at PHY  
6.9.1.6. Longer-Term Directions (2030+)  

6.10. Security Monitoring and Analytics  
6.11. Predictive / Proactive Security  
6.12. Digital Forensic Solutions for 5G  

7. Security Use-Cases for Various Verticals  
7.1. Application Security Requirements  
7.2. Critical Infrastructure Systems Security  
7.2.1. 5G and Critical Infrastructure Amalgamation  
7.2.2. Smart Grid Use Case  
7.2.2.1. U.S. 5G Strategy for National Network and Critical Infrastructure  
7.2.2.2. Threat on Critical Infrastructures  
7.2.3. Emergency and First-Responder Networks Security  
7.2.4. Autonomous Vehicles, V2X Security  
7.2.4.1. Cyber Risks and Few Risk Scenarios Exemplified Using Use-Cases Where Possible  
7.2.4.2. Trust Issues in 5G V2X Services: Issues and Attacks  
7.2.4.3. Security Attacks in 5G V2X: Issues and Attacks  
7.2.4.4. Privacy Issues in 5G V2X Services: Issues and Attacks  
7.3. AI/ML Security  
7.4. Interoperability  
7.5. Industrial Control Systems (ICS): Industrial IOT-Based SCADA  
7.5.1. Safety and Security  
7.5.2. Challenges and Opportunities  
7.5.3. Categories of Risk in the IIoT  
7.6. Quantum-Ready Security  

8. Standardization Opportunities  
9. Needs, Challenges, and Enablers and Potential Solutions  
10. Conclusions and Recommendations  
10.1. Summary of Conclusions  
10.2. Working Group Recommendations  
10.2.1. Future Work  
11. Contributor Bios  
12. References  
13. Acronyms/abbreviations
Tables
Table 1. Standards Organizations 8
Table 2. Selected 5G threat Scenarios 14
Table 3. Threats for Scada Systems 44
Table 4. Proactive Security for 5G-IoT—Needs, Challenges, Enablers, and Potential Solutions 48
Table 5. AI/ML Security – Needs, Challenges, Enablers and Potential Solutions 50
Table 6. Digital Forensics Solutions for 5G Environments—Needs, Challenges, and Enablers and Potential Solutions 51

Figures
Figure 1. Key dimensions of 5G Networks, courtesy of 5G Lab Germany [4]. 2
Figure 2. 5G & Beyond: Security Perspective, the progress of the 5G and beyond revolution may well be hindered if security issues are not tackled early on while the systems are being designed, standardized and deployed. 3
Figure 3. 3GPP security architecture 12
Figure 4. 5G Threat Model 13
Figure 5. NIST CSF Framework [12]. 15
Figure 6. Risk assessment process [13]. 16
Figure 7. Generic risk model with key factors [13]. 16
Figure 8. 5G Security Pillars 17
Figure 9. Potential security issues with virtualization 18
Figure 10. SDN Security - Select Cyber Risk Scenarios and Potential Mitigations 20
Figure 11. Network Slicing Security 22
Figure 12. Network Slicing Security – Select Risk Scenarios and Potential Mitigations 22
Figure 13. Mobile Edge Security Context 23
Figure 14. Mobile Edge Security - Select Cyber Risk Scenarios and Potential Mitigations 24
Figure 15. GEO (Geosynchronous Orbit), HEO (Highly Elliptical Orbit), MEO (Medium Earth Orbit), LEO (Low Earth Orbit), and HAP (High Altitude Platforms) [14]. 27
Figure 16. O-RAN Architecture 28
Figure 17. Cloud RAN Security - Select Cyber Risk Scenarios and Potential Mitigations 28
Figure 18. Proactive 5G security 32
Figure 19. Critical Infrastructure Inter-dependencies [1]. 35
Figure 20. First Responder Use Case on Orchestration 37
Figure 21. Architecture of the Machine Learning Function Orchestrator [17]. 40
Figure 22. IoT security Solution. 43
Figure 23. IIoT based Scada Risk by Threats 45
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

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