Mastering Mobile Network and Related Security

Protecting telecom networks in a connected world

Tiju Johnson

www.bpbonline.com

First Edition 2025

ISBN: 978-93-65897-746

LIMITS OF LIABILITY AND DISCLAIMER OF WARRANTY

The information contained in this book is true and correct to the best of author's and publisher's knowledge. The author has made every effort to ensure the accuracy of these publications, but the publisher cannot be held responsible for any loss or damage arising from any information in this book.

All trademarks referred to in the book are acknowledged as properties of their respective owners but BPB Publications cannot guarantee the accuracy of this information.

Dedicated to

To the two extraordinary women who raised me, thank you for believing in me when I didn't believe in myself. And to my wife and daughter, whose unwavering support and curiosity made this book possible.

About the Author

Tiju Johnson is a seasoned senior security architect with over twenty years of experience in the security field, with nearly a decade in securing telecommunications networks. He has specialized in designing and implementing robust security frameworks for both enterprise and service provider networks and has delivered solutions that address the most complex security challenges while ensuring alignment with industry standards and regulatory requirements. His strength lies in transforming high-level security strategies into actionable implementations that enhance organizational resilience against evolving cyber threats. This book represents the culmination of his hands-on experience and industry insights gained across a decade of securing telecom networks across the globe. He is currently working as a senior security solutions architect and has been part of white paper contributions with 5G Americas.

About the Reviewers

- **Balkrishna Patil** is a technology transformation manager with over 20 years of experience in IT infrastructure and cloud services. He assists clients in successfully executing digital transformation initiatives. With a proven ability to design and implement cloud migration strategies, manage complex IT projects, and provide expert technical guidance, he has dedicated himself to delivering cost-effective, innovative solutions that enhance business agility and resilience.

  Balkrishna has led multimillion-dollar projects across diverse industries, including life sciences, oil and gas, education, and federal, state, and local public services. His expertise spans enterprise IT infrastructure, specializing in analyzing, designing, deploying, and supporting cloud and on-premises solutions. Additionally, he has provided strategic technical and functional guidance to business and application teams, ensuring seamless alignment with organizational goals.

  Committed to continuous learning, Balkrishna holds several industry certifications, including AWS Certified Solutions Architect (professional and associate), Azure Cloud Practitioner, FinOps Practitioner, and VMware Certified Associate. His core competencies include AWS, Azure, hybrid cloud architecture, cybersecurity, and IT governance, enabling him to drive secure, scalable, and efficient cloud solutions for organizations navigating digital evolution.

- **Major Sumit Sharma** (*Retd.*) is a seasoned cybersecurity professional and Indian Army veteran, currently serving as Senior Manager - Cybersecurity at one of India's premier international airports. In this strategic role, he serves as deputy to the Chief Information Security Officer (CISO), where he leads governance, risk, and compliance (GRC) initiatives and drives both offensive and defensive cybersecurity strategies to protect critical infrastructure. His work ensures alignment of cyber risk with enterprise-wide frameworks, reinforcing stakeholder trust in the airport's digital resilience.

  Previously, Sumit was a Senior Consultant at Deloitte, specializing in AWS architecture and third-party risk management. His distinguished 12-year tenure in the Indian Army saw him spearhead cutting-edge projects in Al/ML-based drone surveillance, cloud security, and automation for mission-critical operations.

  Sumit holds an Executive Business Management certificate from IIM Indore, and is certified in ICS Cybersecurity, ISO 27001, AWS and Microsoft Azure certificates.

Acknowledgement

There are a few people I want to thank for the continued and ongoing support they have given me during the writing of this book. First and foremost, I would like to thank the two extraordinary women who raised me and supported me through thick and thin: my wife for keeping me away from easy streaming distractions, and my daughter for her patience during the many hours I spent writing instead of being with her.

I want to express my profound gratitude to the various telecom service provider projects I was fortunate to be part of during my tenure with Cisco Systems. These experiences not only shaped my understanding of the industry but also allowed me to contribute to nation-building efforts and positively impact millions of lives. I am equally indebted to Dr. Nadhem Al-Fardan, whose inspirational mentorship encouraged me to step beyond my comfort zone and make meaningful contributions to the security industry. Your guidance has been invaluable to both this work and my professional journey.

I would like to thank the team at BPB Publications for their support. I am grateful to all technical reviewers and editors for their helpful feedback and for accommodating the changes to chapter structures that differed from our original plan.

Preface

In an age where communication networks form the invisible infrastructure of our daily lives, the security of telecom service providers has never been more critical. From the earliest days of mobile technology to today's sophisticated 5G networks, telecommunications has undergone a remarkable evolution—one that has created unprecedented opportunities alongside complex security challenges.

This book was born from a simple observation: as telecom networks have evolved to be more powerful, they have also become more vulnerable, and there were very few resources covering the security considerations for this evolution. The systems that connect billions of people worldwide now present an expanded attack surface that spans physical hardware, virtualized infrastructure, cloud environments, and an increasingly software-defined ecosystem.

When the first generation of mobile networks emerged, security considerations were often secondary to functionality. The closed, proprietary nature of these early systems offered a form of security through obscurity. Today's networks, by contrast, are built on open standards, utilize commercial off-the-shelf hardware, and rely on software virtualization, creating a fundamentally different security paradigm that demands new approaches and methodologies.

Throughout these pages, we examine the full spectrum of telecom infrastructure, from the **radio access network** (**RAN**) to the transport networks to the **IP Multimedia Subsystem** (**IMS**), from **Mobile Edge Computing** (**MEC**) to the core virtualization technologies that underpin modern networks. Rather than treating these as discrete components, we approach telecom security holistically, recognizing that vulnerabilities in one area inevitably affect others.

For security professionals, this book offers practical guidance on implementing robust security architectures across diverse telecom environments. Engineers will find detailed technical analyses of vulnerabilities and countermeasures specific to telecom systems. Students and those new to the field will discover a comprehensive introduction to the unique security challenges of telecom environments.

It is my hope that this book serves as both a warning and a guide, illuminating the risks while providing the knowledge needed to mitigate them. The security of telecom service providers is not merely a technical concern but a societal imperative. The networks we

secure today will carry the communications, power the innovations, and connect the communities of tomorrow.

The journey through telecom security is complex and continuing. Let us embark on it together.

This book is divided into 17 chapters. They aim to cover the entire telecom components starting with the first generation of mobile networks and concluding with the fifth generation. The details are listed as follows.

Chapter 1: Global Security Standards and Evolution of Security in Mobility – The chapter explores how global security standards have shaped the evolution of mobility security from the earliest days of cellular networks to today's sophisticated 5G environments. The tracing of critical developments from the minimal security provisions in 1G systems to the comprehensive frameworks we now implement. Drawing from experiences working with major telecom providers, examining how standards bodies like 3GPP and GSMA have responded to emerging threats while balancing security with performance and interoperability.

Chapter 2: Generations of Mobile Networks and 1G – This chapter explores the evolution of mobile networks, focusing on the **first generation** (**1G**) that launched the cellular revolution in the 1980s. It examines how the early analog systems, while revolutionary for their time, were designed with minimal security considerations, lacking encryption and authentication mechanisms that we now consider fundamental. Through analyzing 1G's vulnerabilities, including susceptibility to eavesdropping and call interception, we establish a historical baseline that helps us understand how security requirements have evolved alongside network technologies.

Chapter 3: 2G and Enabled Services – This chapter explores the security landscape of 2G networks and their foundational services that continue to impact modern telecommunications. The chapter examines the vulnerabilities inherent in **Signaling System 7** (**SS7**), which, despite its age, remains a critical protocol underlying much of our global communications infrastructure. It also analyzes the security challenges of SMS services, revealing how these seemingly simple text messages created both revolutionary connectivity and persistent security gaps. Through many experiences implementing security measures across multiple carriers, the demonstration shows how these legacy systems continue to present significant risks even as we advance to newer technologies and provide practical approaches to mitigate these vulnerabilities without disrupting essential services.

Chapter 4: IP Multimedia Subsystem – This chapter explores the critical security considerations surrounding the **IP Multimedia Subsystem** (**IMS**), the architectural framework that has revolutionized how we deliver multimedia services across telecom networks. The chapter examines how IMS bridges traditional voice communications with IP-based services, creating both opportunities and vulnerabilities that security professionals must address. It also shares practical approaches to securing the various IMS components—from the session border controllers to the application servers—while maintaining the performance and flexibility that make IMS so valuable to modern telecom operations.

Chapter 5: Third Generation of Mobile Networks – This chapter examines the 3rd **generation of mobile networks** (**3G**), which marks a pivotal shift in telecom security architecture. It explores how the **universal mobile telecommunications system** (**UMTS**) implemented integrity protection for signaling messages, yet still contained security gaps that malicious actors could exploit. Through these experiences securing numerous 3G networks, the chapter also shares some practical approaches to mitigating these risks while maintaining the performance benefits that made 3G so transformative for mobile communications.

Chapter 6: 4G Mobile Networks – This chapter examines the security architecture of 4th Generation mobile networks, where the all-IP nature of LTE introduced both revolutionary capabilities and novel security challenges. It explores how the evolution from circuit-switched to packet-switched core networks fundamentally changed our approach to telecom security. In the implementation of 4G security frameworks across multiple operators, the chapter also analyzes the effectiveness of LTE's mutual authentication mechanisms, the vulnerabilities in inter-technology handovers, and the security implications of diameter signaling.

Chapter 7: 5G Mobile Networks – In this chapter, the readers will explore the revolutionary 5G ecosystem that has fundamentally transformed how we approach telecom security. It examines how 5G's software-defined architecture, network slicing capabilities, and distributed computing model create both unprecedented opportunities and complex security challenges. In the implementation of security frameworks for early 5G deployments, the chapter details the unique threat vectors targeting various 5G core components. It demonstrates why traditional perimeter-based security approaches fail in 5G networks and presents practical zero-trust implementations that have proven effective across multiple service provider environments.

Chapter 8: Private 5G – This chapter explores the rapidly evolving world of Private 5G networks and their unique security implications for enterprises and critical infrastructure. It examines how these dedicated cellular networks provide organizations with unprecedented control over their communications while introducing distinct security challenges compared to public networks. This chapter also presents frameworks for securing Private 5G deployments through specialized authentication protocols, physical security measures, and threat monitoring systems.

Chapter 9: Network Slicing and Related Security – This chapter explores the revolutionary concept of Network Slicing and its profound security implications for telecom providers. It discusses how this core 5G capability allows operators to create multiple virtual networks atop a shared physical infrastructure, each tailored to specific use cases with unique security requirements. It presents a comprehensive security framework addressing authentication, encryption, and monitoring specifically designed for multi-tenant slice environments. The security of network slicing is not merely a technical challenge; it is fundamental to delivering on 5G's promise of supporting critical services from autonomous vehicles to remote surgery.

Chapter 10: RAN and Transport Security – This chapter examines the critical domain of RAN and Transport Security, where the most vulnerable portions of our telecom infrastructure often reside. It will guide you through the evolution of security controls from physical site security to the complex cryptographic protocols protecting today's front haul and backhaul connections.

Chapter 11: Container Adoption in 5G Networks – In this chapter, the readers will know how container technology has revolutionized 5G network deployment, bringing unprecedented flexibility and scalability to telecom infrastructure. Through practical case studies, the chapter lists how secured containers can strengthen network isolation while enabling the agility demanded by modern telecom operations.

Chapter 12: Perimeter and Edge Security – The chapter examines the critical domain of perimeter and edge security—a fundamental yet increasingly complex aspect of telecom infrastructure protection. The traditional network perimeter has evolved dramatically with the advent of cloud computing, virtualization, and distributed architectures. It will also guide you through the essential strategies for securing these network boundaries, from next-generation firewalls to advanced traffic inspection techniques that protect the entry points to your telecom infrastructure.

Chapter 13: Identity and Access Management – This chapter explores the critical domain of Identity and Access Management within telecom environments—a cornerstone of the zero

trust security approach. It also examines how proper authentication, authorization, and accounting mechanisms create the foundation for securing complex telecom infrastructure spanning from legacy systems to modern 5G networks. Drawing from my field experience, it demonstrates practical implementations of privileged access management, identity federation, and multi-factor authentication tailored specifically for telecom operators.

Chapter 14: Security Monitoring – This chapter explores the critical domain of Security Monitoring within telecom environments. It demonstrates how continuous surveillance forms the backbone of effective security posture, particularly in complex telecom infrastructures spanning from legacy 2G to modern 5G networks. Drawing from my experience implementing monitoring solutions across various telecom providers, it also presents frameworks for establishing security operations centers tailored to telecom-specific threats.

Chapter 15: Network Security Testing – This chapter explores the critical discipline of Network Security Testing in telecom environments. It has detailed how rigorous testing methodologies can uncover vulnerabilities before malicious actors exploit them. The chapter aims to transform security testing from a periodic compliance exercise into an integrated, continuous process that strengthens your network's resilience against evolving threats.

Chapter 16: Beyond 5G – The chapter explores the emerging security landscape that lies beyond 5G technology. As we venture into the realm of 6G networks and quantum communications. The chapter also explores the security challenges that exist are not merely theoretical—they represent real considerations that security professionals must begin planning for today, even as these technologies remain on the horizon.

Chapter 17: Securing Future Networks – This chapter reflects on the critical security insights gained through decades of telecom evolution. The chapter also discusses how security considerations have transformed from afterthoughts to foundational elements of network design, and shares the hard-won lessons that only come from navigating real-world threats and vulnerabilities. Looking ahead, it also explores the emerging security paradigms that will shape our industry as 6G technologies, quantum communications, and AI-driven defenses converge to create both new opportunities and challenges.

Code Bundle and Coloured Images

Please follow the link to download the
Code Bundle and the ***Coloured Images*** of the book:

https://rebrand.ly/fedhynh

The code bundle for the book is also hosted on GitHub at
https://github.com/bpbpublications/Mastering-Mobile-Network-and-Related-Security.
In case there's an update to the code, it will be updated on the existing GitHub repository.

We have code bundles from our rich catalogue of books and videos available at **https://github.com/bpbpublications**. Check them out!

Errata

We take immense pride in our work at BPB Publications and follow best practices to ensure the accuracy of our content to provide with an indulging reading experience to our subscribers. Our readers are our mirrors, and we use their inputs to reflect and improve upon human errors, if any, that may have occurred during the publishing processes involved. To let us maintain the quality and help us reach out to any readers who might be having difficulties due to any unforeseen errors, please write to us at :

errata@bpbonline.com

Your support, suggestions and feedbacks are highly appreciated by the BPB Publications' Family.

Piracy

If you come across any illegal copies of our works in any form on the internet, we would be grateful if you would provide us with the location address or website name. Please contact us at **business@bpbonline.com** with a link to the material.

If you are interested in becoming an author

If there is a topic that you have expertise in, and you are interested in either writing or contributing to a book, please visit **www.bpbonline.com**. We have worked with thousands of developers and tech professionals, just like you, to help them share their insights with the global tech community. You can make a general application, apply for a specific hot topic that we are recruiting an author for, or submit your own idea.

Reviews

Please leave a review. Once you have read and used this book, why not leave a review on the site that you purchased it from? Potential readers can then see and use your unbiased opinion to make purchase decisions. We at BPB can understand what you think about our products, and our authors can see your feedback on their book. Thank you!

For more information about BPB, please visit **www.bpbonline.com**.

Join our book's Discord space

Join the book's Discord Workspace for Latest updates, Offers, Tech happenings around the world, New Release and Sessions with the Authors:

https://discord.bpbonline.com

Table of Contents

Chapter 1
Global Security Standards and Evolution of Security in Mobility

Introduction

This chapter delves into the intricate landscape of global security standards and the evolution of security practices in the mobile domain. We will explore the intricate interplay between technological advancements, regulatory frameworks, and the ongoing efforts to fortify our digital infrastructure against emerging cyber threats.

Firstly, we will examine the pivotal role of international organizations and regulatory bodies in developing and promoting security standards for mobile technologies. These standards serve as essential guidelines, ensuring a baseline level of security and interoperability across different platforms and regions.

Furthermore, we will trace the evolution of security measures in mobile devices, networks, and applications, shedding light on cutting-edge technologies and methodologies employed to safeguard mobile systems. From encryption and authentication protocols to secure communication channels and data protection mechanisms, this chapter will provide a comprehensive overview of the security landscape in mobility.

Structure

This chapter will cover the following topics:

- Global security standards

- 3rd Generation Partnership Project
- European Telecommunications Standards Institute
- International Telecommunication Union
- GSM Association
- National Institute of Standards and Technology
- Evolution of security in mobility
- Evolution of service provider network from 1G to 5G

Objectives

Through this comprehensive detailing of global security standards and the evolution of service provider networks, readers will gain a profound understanding of the challenges, solutions, and ongoing efforts to fortify our digital infrastructure, enabling secure and reliable mobile experiences for individuals, businesses, and societies worldwide.

Global security standards

Imagine a set of rules that everyone in a specific industry agrees on. These rules, called standards, guarantee that whatever products, systems, or services are made, they work well and follow the same guidelines. This ensures compatibility, meaning things fit together seamlessly, with safety, consistency, security, and high quality.

To create a new standard, different groups, such as companies that make things, phone carriers, regular people who use them, special interest groups, and even governments, all have to agree. This process guarantees that the final standard is based on the best practices, everyone involved approves, and experts have tested and verified it.

The standardization mechanisms ensure a baseline of best-practice solutions consensually agreed upon, tested, and verified by industry experts. Mobile network technology, from the early generation to the latest, has always evolved following these globally agreed-upon standards.

In the telecommunications industry, there are several global security standards forums and organizations that play critical roles in establishing and maintaining security standards.

3rd Generation Partnership Project

The **3rd Generation Partnership Project** (**3GPP**) is a global leader in mobile communications standardization. It is a collaborative effort driven by telecommunication associations (organizational partners) who work together to develop technical specifications for mobile technologies like 3G, 4G, and the ever-evolving 5G. These specifications ensure seamless connectivity and service interoperability between devices and networks from different vendors around the world.

At the heart of 3GPP are the **Technical Specification Groups** (**TSGs**). These working groups are responsible for creating, approving, and maintaining the technical specifications and reports that define the blueprint for mobile communication systems.

A few crucial TSGs of 3GPP are listed in the following section, with details on their scope of work.

Technical Specification Group SA2

The **Technical Specification Group SA2** (**TSG SA2**) is one of the most crucial groups within the 3GPP standardization organization. SA2 is responsible for the overall system architecture and high-level design of 3GPP-based mobile networks.

The primary focus of SA2 is to specify the core network architecture, defining the functional entities, interfaces, and protocols that enable the seamless operation and integration of the various components within the 3GPP ecosystem. This includes the specification of the **5G system** (**5GS**) architecture, which introduces a new, more flexible, and modular core network design compared to previous generations.

Some of the key areas that SA2 is responsible for include:

- **5G System architecture**: SA2 defines the core network architecture of the 5G system, including the functional entities such as the **Access and Mobility Management Function** (**AMF**), **Session Management Function** (**SMF**), and **User Plane Function** (**UPF**), as well as the interfaces between them.
- **Network slicing**: SA2 specifies the network slicing concept, which allows for the creation of customized logical networks tailored to specific use cases, such as enhanced mobile broadband, ultra-reliable low-latency communications, and massive machine-type communications.
- **Mobility management**: SA2 defines the mobility management protocols and procedures, enabling seamless **User Equipment** (**UE**) mobility across different access technologies, such as **5G New Radio** (**NR**), **Long Term Evolution** (**LTE**), and Wi-Fi.
- **Session management**: SA2 is responsible for specifying the session management functions, including the establishment, modification, and release of user sessions, as well as the associated **quality of service** (**QoS**) parameters.
- **Policy and charging control**: SA2 oversees the policy and charging control framework, which allows for the enforcement of operator-defined policies and the accurate charging of subscriber services.
- **Security and privacy**: SA2 collaborates with other 3GPP groups, such as SA3, to ensure the security and privacy aspects of the core network architecture, protecting the confidentiality and integrity of user data and signaling.

Technical Specification Group SA3

The **Technical Specification Group SA3** (**TSG SA3**) is responsible for defining the security and privacy-related aspects of 3GPP-based mobile networks. As one of the core technical groups within 3GPP, SA3 plays a vital role in ensuring the confidentiality, integrity, and availability of the cellular ecosystem. Their work ensures that mobile communications are protected from unauthorized access and that personal information remains confidential.

Some of the key areas that SA3 is responsible for include:

- **Security architecture and protocols**: SA3 specifies the overall security architecture of the 3GPP system, including the security protocols and mechanisms used for authentication, key agreement, and data protection. This includes the development of the **Authentication and Key Agreement** (**AKA**) protocols, which are essential for secure UE registration and connectivity.
- **Network access security**: SA3 defines the security measures for controlling access to the 3GPP network, such as the specification of the **Universal Subscriber Identity Module** (**SIM/USIM**)-based authentication procedures and the protection of the radio interface against eavesdropping and integrity attacks.
- **Application and service security**: SA3 is responsible for ensuring the security of the various applications and services running on top of the 3GPP network, including the specification of secure protocols for communication between the UE and application servers.
- **Privacy protection**: SA3 is tasked with defining the privacy-related aspects of the 3GPP system, ensuring the protection of user information and the minimization of personally identifiable data collected and processed by the network.
- **Security assurance**: SA3 oversees the development of security assurance specifications, which define the security requirements and testing procedures for 3GPP network elements and user equipment to ensure their compliance with the defined security standards.
- **Security management and monitoring**: SA3 specifies the security management and monitoring functions, enabling the detection and mitigation of security threats and attacks within the 3GPP network.

Radio Access Network

The TSG **radio access network** (**RAN**) is responsible for the development and specification of the radio access technologies that power cellular networks. This includes the 4G LTE and 5G NR standards, as well as the evolution of previous-generation radio access technologies.

The primary focus of the TSG RAN is to ensure the seamless and efficient operation of the radio interface, defining the protocols and mechanisms that enable UEs to connect and communicate with the cellular network.

Core Network and Terminals TSG

The **Core Network and Terminals** (**CT**) TSG is responsible for specifying the protocols and interfaces between the network elements and user equipment, ensuring the seamless integration of different components within the 3GPP architecture. The CT TSG's work includes the definition of signaling protocols for call and session management, as well as the specification of the protocols for user data transport, such as the **GPRS Tunneling Protocol** (**GTP**) and the **Session Initiation Protocol** (**SIP**). Additionally, the CT TSG oversees the standardization of terminal capabilities and features, ensuring that user devices can fully leverage the capabilities of the 3GPP network.

By working collaboratively, these TSGs, along with others within the 3GPP, play a pivotal role in shaping the future of mobile communications, guaranteeing a secure, reliable, and ever-evolving mobile experience for users worldwide. A couple of important 3GPP specifications for LTE and 5G include **TS 33.401** and **TS 33.501**.

ETSI

European Telecommunications Standards Institute (**ETSI**) is a non-profit organization that develops globally applicable standards for information and communication technologies, including telecommunications. It plays a crucial role in the service provider industry by establishing globally applicable **Information and Communication Technologies** (**ICT**) standards. ETSI brings together a diverse range of stakeholders, including service providers, network operators, manufacturers, and research institutions, to collaborate on developing and maintaining common standards. These standards encompass various aspects of telecommunications networks, services, and protocols, enabling interoperability, security, and quality assurance among different systems and technologies. Service providers heavily rely on ETSI standards to ensure seamless connectivity, roaming capabilities, and the delivery of reliable and secure services to their customers. ETSI's work extends across various domains, including mobile networks (2G, 3G, 4G, and 5G), fixed networks, broadcasting, internet protocols, cybersecurity, and emerging technologies like the **Internet of Things** (**IoT**) and **artificial intelligence** (**AI**). By adhering to ETSI's widely adopted standards, service providers can ensure compatibility, efficient resource utilization, and enhanced user experiences while maintaining regulatory compliance across different regions and countries.

It has several working groups dedicated to security-related standards and protocols for telecommunications, of which some are:

- **Security Algorithms Group** (**SAG**): SAG is a specialized group within ETSI that evaluates and recommends cryptographic algorithms for use in telecommunications security standards. They assess the strength and suitability of encryption algorithms for various applications, such as mobile networks, internet protocols, and cybersecurity.