



SECURING 5G

and
EVOLVING
ARCHITECTURES

PRAMOD NAIR



Securing 5G and Evolving Architectures

Pramod Nair

◆◆ Addison-Wesley

Boston • Columbus • New York • San Francisco • Amsterdam • Cape Town • Dubai •
London • Madrid • Milan • Munich • Paris • Montreal • Toronto • Delhi • Mexico City •
São Paulo • Sydney • Hong Kong • Seoul • Singapore • Taipei • Tokyo

Securing 5G and Evolving Architectures

Table of Contents

Cover

Title

Copyright Page

Dedication

Table of Contents

Foreword

Preface

Acknowledgments

About the Author

Part I: Evolution of Cellular Technologies to 5G, Security
Enhancements, and Challenges

Chapter 1: Evolution from 4G to 5G

Mobile Network Evolution from 4G to 5G

5G New Radio Features

Disaggregated Architecture

Flexible Architecture

Service-Based Architecture

Adoption of Cloud-Native Technology

Multi-access Edge Computing (MEC)

Network Slicing

Key 5G Features in 3GPP Releases

Key 5G Advanced Features

Summary

Acronym Key

Table of Contents

References

Chapter 2: Deployment Modes in 5G

5G NSA and SA Deployments

5G Non-Standalone (NSA) Deployments

5G Standalone (SA) Deployments

Network Slice as a Service (NSaaS)

5G Time-Sensitive Networks

5G Local Area NetworkType Service

Private 5G/Non-Public Networks

Standalone Non-Public Network (SNPN)

Public Network Integrated Non-Public Networks (PNI-NPN)

Summary

Acronym Key

References

Chapter 3: Securing 5G Infrastructure

3GPP 5G Security Enhancements

5G Trust Model: Non-Roaming

5G Trust Model: Roaming

Integration of Non-3GPP Network to the 5G Core Network

Other Key Security Enhancements in Release 16

Security Challenges in 5G

IoT and M2M

Perimeter-Less Deployments

Virtualized Deployments

Summary

Acronyms Key

References

Part II: Securing 5G Architectures, Deployment Modes, and Use Cases

Chapter 4: Securing RAN and Transport Deployments in 5G

Table of Contents

5G RAN and Transport Threats

- Vulnerabilities in Air Interface

- Vulnerabilities in the Transport Network

- Rogue/Fake Base Station Vulnerabilities

Securing 5G RAN and Transport

- Securing the Air Interface

- Using Trusted Transport Network Elements

- Secure Deployments and Updates Using Secure ZTP

- Using Security Gateway (SecGW/SEG) to Secure the RAN and Transport Layer

Real Scenario Case Study: Examples of Threat Surfaces and Their Mitigation

- A: The Attacker Takes Control of IoT Devices with Weak Security and Launches DDoS Attack

- B: The Attacker Uses the Vulnerability in S1 and Insecure Transport to Use Rogue eNBs and Uses MitM Attacks in the 5G NSA Deployment

- C: The Attacker Uses the Insecure Transport and Carries Out MitM Attacks in Back Haul

- Mitigation

Summary

Acronym Key

References

Chapter 5: Securing MEC Deployments in 5G

Service Provider Network-Based MEC

Enterprise Network-Based MEC

MEC Deployment Models

- Distributed UPF and MEC Application Deployment

- C-RAN/O-RAN/Open VRAN Deployment Enabled by MEC

- Enterprise MEC Deployment

- Hybrid MEC Deployment

Threat Surfaces in 5G MEC Deployments

- Physical Security

- Hardware and Software Vulnerabilities

- 5G MEC Infrastructure and Transport Vulnerabilities

Table of Contents

Virtualization Threat Vectors

5G MEC API Vulnerabilities

DDoS Attacks

Securing 5G MEC

Physical Security

Hardening Hardware and Software

MEC Infrastructure and Transport Security

Securing Virtualized Deployments in 5G MEC

Securing API

Validating Both Read and Write Requests

DDoS Protection

Real Scenario Case Study: MEC Threats and Their Mitigation

Threats: Case Study

Mitigation Examples

Summary

Acronym Key

References

Chapter 6: Securing Virtualized 5G Core Deployments

A Brief Evolution of Virtualization in Telecommunications

Threats in Virtualized 5G Packet Core Deployments

5GC Container Vulnerabilities

Insecure Container Networking

Container Host and HW Vulnerabilities

Securing Virtualized 5G Packet Core Deployments

Secure CI/CD

Securing 5GC NFs and 5GC NF Traffic

Securing 5GC NF Orchestration and Access Controls

Securing 5GC CNF in Roaming Scenarios

Securing the Host OS and Hardware

Real Scenario Case Study: Virtualized 5GC Threats and Mitigation

Threats Case Study

Mitigation Examples

Table of Contents

Summary

Acronym Key

References

Chapter 7: Securing Network Slice, SDN, and Orchestration in 5G

Network Slicing and Its EnablersSDN and Orchestration

Threat Surfaces in 5G Network Slice, SDN, and Orchestration Deployments

Threats in the SDN Controller Layer

Threats in the SDN Data Plane

Threats in Orchestration Layer

Insufficient Slice-Level Isolation

Threats in NSaaS Deployments

Mitigation of Threats

Trusted Components

Securing Orchestration

Securing the Software-Defined Network (SDN)

Mitigating Data Exfiltration

Securing Network Slices

Securing NSaaS Deployments

Real Scenario Case Study: Threats in the 5G Network Slice, SDN, and
Orchestration Deployments and Their Mitigation

Threats: Case Study

Mitigations: Case Study

Summary

Key Acronyms

References

Chapter 8: Securing Massive IoT Deployments in 5G

Massive IoTBased Threats in 5G

Device Vulnerabilities Due to Weak Built-in Security

Securing mIoT Deployments in 5G Networks

Built-in Hardening of the Device

Real Scenario Case Study: mIoT Threats and Their Mitigation

Table of Contents

Threats Example

Mitigation Example

Summary

Key Acronyms

References

Chapter 9: Securing 5G Use Cases

Secure 5G Smart Factory and Manufacturing

Threats in 5G Smart Factory Deployments

Securing the 5G Smart Factory

Application-Level Security Controls

Critical Infrastructure

5G Energy Utility

Threats in the 5G-Enabled Energy Utility

Securing 5G-Enabled Energy Utility

5G Vehicle-to-Everything (5G-V2X)

Threats in 5G-V2X Deployments

Securing 5G-V2X Deployments

Standards and Associations

Summary

Key Acronyms

References

Part III: End-to-End 5G Security Architecture and Prioritizing Security Investments

Chapter 10: Building Pragmatic End-to-End 5G Security Architecture

Foundations of 5G Security

Securing 5G and Evolving Network Deployments

Securing IT and OT

Securing Consumers of 5G and Evolving Technologies

Key Tenets of 5G Security Architecture

Supply Chain Security

Table of Contents

Securing User and Device Access Using Zero-Trust Principles

Secure Intra/Inter-Network Connectivity

Application-Level Security

Vulnerability Management and Forensics

Enhanced Visibility, Monitoring, and Anomaly Detection

Slice-Level Security

Secure Interoperability

Summary

Acronyms Key

References

Chapter 11: Prioritizing 5G Security Investments

Method of Prioritizing Security Controls

Scenario 1

Scenario 2

Summary

Acronyms Key

References

Part IV: Emerging Discussions

Chapter 12: 5G and Beyond

Adoption and Adaptability of 5G and Evolving Technologies

Convergence of Wi-Fi and Evolving Cellular Technologies

Use of AI and ML in Securing 5G and Evolving Networks

Crypto Agility in 5G and Evolving Technologies

Summary

Acronym Key

References

Index