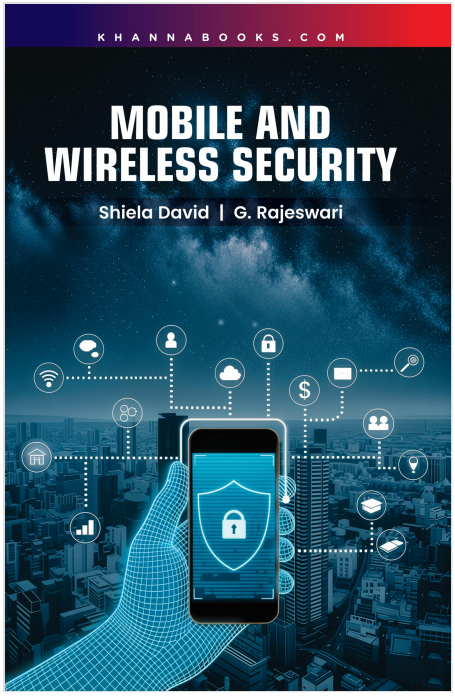

Mobile and Wireless Security

by Shiela David, G. Rajeswari

ISBN-13	9789355389039
ISBN-10	9355389035
Edition	1
Format	Both
Publishing Year	2026
Categories	New Arrivals, Computer Science Engineering, Book Store, Sathyabama Series
Original Price	~~₹148.00~~
Discounted Price	**₹125.80**
Stock Status	**In Stock (5 available)**

Description

In our modern, interconnected world, where wireless networks and mobile devices have become ubiquitous tools for communication, business, and daily life, the imperative for robust security has never been greater. This handbook, Mobile and Wireless Security, serves as an essential guide, providing an in-depth understanding of this dynamic and critical field, from foundational principles to the newest industry trends.

The core purpose of this material is to illuminate the underlying systems of wireless technology and expose the resultant security threats they face. The book's major goals are to enable readers to grasp the basic features of wireless systems, meticulously examine the necessary security protocols and cryptographic methods, and confidently implement effective security practices across various wireless devices. It thoroughly addresses the vast array of threats, such as unauthorized access, data intrusion, and Denial of Service (DoS) attacks, that compromise modern wireless environments.

This resource is designed for a broad target audience, including IT professionals, cybersecurity experts, academics, students, and any individual or organization—from enterprises to governments—who must proactively safeguard sensitive data and defend against unauthorized access in a mobile-first landscape. By the end of this journey, you will possess the practical knowledge required to apply sophisticated security measures to mobile wireless systems with the confidence needed to secure wireless networks in real-world applications.

Salient Features:

• Foundational Network Models: Delivers a clear overview of the OSI and TCP/IP models, establishing the fundamental theoretical frameworks necessary for understanding how various network protocols interact during end-to-end communication.

• Wireless Protocol Evolution: Provides a comprehensive examination of essential WLAN security protocols, detailing the weakness of WEP and the evolution through WPA and WPA2 to the robust security standards offered by WPA3.

• Core Cryptography Methods: Covers symmetric and asymmetric cryptography schemes, hash functions, and key secure protocols like SSL/TLS and IPSec, which are crucial for securing data confidentiality, integrity, and non-repudiation.

• Device Security Analysis: Dedicated content analyzes security problems specific to wireless devices, including Laptops and Handsets, covering topics like physical security, application security, and the risks of information leakage.

• Cellular System Defense: Explores security considerations for cellular networks, detailing threats, types of Cellular Fraud, and the security mechanisms employed within systems like GSM and data networks such as GPRS.

• Wireless Threat Landscape: Defines and provides mitigation techniques for pervasive wireless threats, including Eavesdropping, Communication Jamming, Rogue Client Attacks, and vulnerabilities arising from weak cryptographic algorithms.

• Practical LAN Implementation: Offers practical security guidance on deploying Wireless LANs in various organizational structures, including Large Enterprise Campuses, Wireless ISP Designs, and Small Office/Home Office (SOHO) environments.

• Security Best Practices: Outlines actionable strategies for a proactive security stance, emphasizing the need for robust Authentication, ongoing Network Monitoring, regular Firmware/Software Patching, and stringent physical access controls.

About the Author(s)

Shiela David

G. Rajeswari