Cyber Security Essentials For Engineers

Author :	Parveen A.
ISBN 13 :	978-93-55388-52-0
ISBN 10 :	93-55388-52-7
E-ISBN 13 :	978-93-55388-52-0
Edition :	First
Pages :	72
Type of book :	Paperback
Year :	2025
Language :	English
Publisher :	Khanna Publishing House
M.R.P :	Rs 148.00
Categories :	Satyabhama Series
Condition Type :	New
Country Origin :	India

Product Description

Cyber Security Essentials For Engineers In today's interconnected world, security is not an add-on; it is an essential engineering discipline. Cybersecurity Essentials for Engineers is the practical, hands-on guide built specifically for engineers, developers, and IT professionals who need to do more than define security—they need to build it. This book provides a robust foundation, starting with the core security principles: Confidentiality, Integrity, and Availability (CIA Triad), supplemented by critical mechanisms like Authentication and Non-repudiation. It then dives into the technical details of securing communications, exploring the evolution of protocols like SSL/TLS, WPA2, S/MIME, and PGP. Moving beyond theory, the text focuses on real-world implementation, teaching you to analyze cipher suite negotiations, identify potential attack vectors, and navigate the crucial trade-offs between security and system performance. Packed with practical insights, ethical hacking exercises, and case studies, this resource ensures you are equipped to design, implement, and maintain truly resilient digital systems.**Salient Features:**

- **Engineering-Centric Foundation**: Master the CIA Triad (Confidentiality, Integrity, Availability) and the importance of robust Authentication and Non-repudiation mechanisms.
- **Protocol Mastery**: Detailed examination of secure communication protocols, tracing their evolution from early standards (SHTTP, WEP, SET) to modern essentials (SSL/TLS, WPA, WPA2).
- **Secure Email and Trust Models**: In-depth coverage of S/MIME, PEM, and PGP, contrasting the PKI and Web of Trust models and addressing key management challenges.
- **Practical Attack Analysis**: Learn through packet analysis and ethical hacking exercises to understand implementation details and uncover real-world vulnerabilities.
- **Performance vs. Security**: Explore the critical trade-offs between high security, performance, and usability in system design.
- **Dispelling Myths**: Directly addresses and corrects common security misconceptions, such as "encryption alone guarantees security" or "hiding the SSID is enough."
- **Best Practices**: Emphasizes the need for strong passwords/passphrases and the continuous imperative to stay current with emerging threats and protocol updates.

Table of Contents

Preface

Author

Parveen A., Associate Professor, Dept of CSE, Sathyabhama Institute of Science and Technology   **S. Priya**
Associate Professor, Dept of CSE, Sathyabhama Institute of Science and Technology