



Network Security

Gaurav S. Kasbekar

Dept. of Electrical Engineering

IIT Bombay

NPTTEL

Introduction

- Communication networks being extensively used by a large number of users for various applications
 - ❑ e.g., email, web browsing, Internet telephony, financial transactions
- However, malicious or hostile users seek to attack networks by:
 - ❑ stealing secret information (e.g., passwords, credit card information),
 - ❑ installing malware,
 - ❑ disrupting communications, etc.
- Goals of the field of network security are to:
 - ❑ understand how malicious users can attack networks, and
 - ❑ design mechanisms for defending networks against such attacks
- Objective of this course is to provide a detailed exposure to this important field

Who will Benefit

- Students, faculty members, and industry practitioners in Electrical Engineering and Computer Science

NPTTEL

Prerequisites

- An understanding of the basics of communication networking and programming will be helpful
 - required background from communication networking will be reviewed in this course

NPTTEL

Course Contents

- Review of Basics of Communication Networks
- Different Types of Attacks on Networks
- Mathematical Background for Cryptography
- Principles of Cryptography: Symmetric Key Cryptography and Public Key Cryptography
- Message Integrity, Cryptographic Hash Functions, and Digital Signatures
- Authentication
- Public Key Infrastructure, Certificates
- Securing Email
- Transport-Layer Security
- Network-Layer Security and Virtual Private Networks

Course Contents (contd.)

- Security in Wireless Local Area Networks
- Wireless Cellular Network Security
- Firewalls and Intrusion Detection Systems
- Cryptocurrencies and Blockchain
- Cloud Security
- Security of the Internet of Things (IoT), Hardware Security
- Anonymous Connections and Onion Routing
- Post-Quantum Cryptography

NPTTEL

References

- C. Kaufman, R. Perlman, M. Speciner, R. Perlner, “*Network Security: Private Communication in a Public World*”, Pearson Education, 3rd edition, 2024
- J. Kurose, K. Ross, “*Computer Networking: A Top Down Approach*”, 8th Edition, Pearson Education, 2022
- B.L. Menezes, R. Kumar, “*Cryptography, Network Security, and Cyber Laws*”, Cengage Learning India Pvt. Ltd., 2018
- J. Edney, W.A. Arbaugh, “*Real 802.11 Security: Wi-Fi Protected Access and 802.11i*”, Pearson Education, 2004
- W. Stallings, “*Cryptography and Network Security: Principles and Practice*”, Pearson Education, 8th edition, 2023
- L. Peterson, B. Davie, “*Computer Networks: A Systems Approach*”, 6th Edition, Morgan Kaufmann, 2021
- Research Papers