

Cybersecurity: Technology and Governance

Audun Jøsang

Textbook at bachelor and master levels

Springer Nature

**Chapter 1: Basic concepts of cybersecurity**

- Cybersecurity terminology
- What is security and cybersecurity?
- Threats, vulnerabilities, incidents and impacts
- Cybersecurity objectives
- Information security controls
- Sources of requirements for cybersecurity
- Cyber risk
- CIA security goals

Chapter 2: Attack vectors and malware

- Attack vectors
- Supply-chain attacks
- Malware
- Exploits

Chapter 3: System security

- System architecture
- Vulnerability management for systems and software
- Privilege levels for processes in the microprocessor
- Buffer overflow vulnerabilities, exploits and countermeasures
- Virtualization
- Trusted computing and secure boot
- Side channels and covert channels

Chapter 4: Cryptography

- What is cryptography?
- Symmetric algorithms
- Block cipher modes of operation
- Hash functions and MAC
- Diffie-Hellman key exchange
- Asymmetric algorithms
- Digital signature
- The history of cryptography
- Post-quantum cryptography
- Blockchains, Bitcoin and energy consumption

Chapter 5: Key management and PKI

- Key types, key sizes and key lifecycle
- Key management and crypto periods
- PKI: Public Key Infrastructure
- The challenges of key distribution
- Public-key certificates
- Trust models for PKI
- Verifiable credentials in blockchains

Chapter 6: Network security

- Computer networks and the Internet
- DNS: The Domain Name System
- The Internet stack and communication security
- TLS and IPSec
- VPN (Virtual Private Networks)
- Computer network security
- Firewalls
- Intrusion Detection
- Network architecture for security
- TLS Inspection

Chapter 7: Wireless security

- Radio communication
- Security in Wi-Fi
- Security in Bluetooth
- Mobile network security

Chapter 8: User authentication

- User authentication methods
- Passwords
- Tokens
- Biometrics
- MFA: Multi-factor authentication
- e-Authentication frameworks

Chapter 9: IAM: Identity and access management

- The silo model and federated identity management models
- IAM protocols, OpenIdConnect and OAuth
- eID in India, the EU, and the USA
- ID federations around the world
- Access authorization and access control

Chapter 10: Information privacy

- Privacy in the digital age
- Privacy-invasive technologies
- Anti-tracking
- GDPR: The EU General Data Protection Regulation
- DPIA: Data Protection Impact Assessment
- Notification of personal-data breach

Chapter 11: Secure by design

- Privacy by design and secure by design
- The seven phases of secure by design
- Secure software development
- Threat modelling
- Application security
- Security in the cloud

Chapter 12: Physical information security

- Physical security goals and threats
- Safety of staff and their environment
- Controlled authorized access
- Shielding of sites and equipment
- Continuity of technical support services

Chapter 13: Security culture

- Building the security culture
- The insider threat and management's responsibility
- Personal integrity
- Social engineering
- Physical social engineering
- Security usability and security learning

Chapter 14: Cybersecurity readiness, security testing and audit

- Contingency planning principles
- Technical concepts of contingency planning
- Cyber contingency planning
- Cyber incident management
- Digital forensics
- Security audit

Chapter 15: AI and cybersecurity

- What is AI?
- Offensive use of AI
- Deepfakes
- Defensive use of AI
- Vulnerabilities and exploitation of AI systems

Chapter 16: Cyber operations

- Advanced cyber threats
- CTI: Cyber threat intelligence
- MITRE ATT&CK
- Cyber warfare

Chapter 17: Cyber organizations and regulation

- The importance of cybersecurity regulation
- Hierarchy of regulations
- Cyber-organizations in the USA, EU, Russia and China
- Cyber regulation in the USA, EU, Russia and China

Chapter 18: Governance and information security management

- Levels of information security governance and management
- NIST Cybersecurity Framework 2.0
- The cyber defence matrix
- CIS Critical Security Controls
- ISO/IEC 27000 series of information security standards
- ISMS – Information Security Management System
- Maturity in information security governance

Chapter 19: Cyber risk management

- What is risk and risk management?
- The risk management process
- Risk assessment
- Risk identification
- Risk analysis
- Risk evaluation and reporting