About the Book

Foundation of Computer Security: Cryptography, Attacks, and Emerging Technologies" is a comprehensive guide to cybersecurity in the digital age. Covering topics from cryptography to emerging technologies like IoT and blockchain, this book offers insights and practical advice for professionals, researchers, and students. It explores secure communication, network security, AI in cybersecurity, healthcare security, cloud security, and the potential of emerging technologies to enhance security measures. With a focus on theoretical understanding and practical applications, it's an essential resource for navigating the ever-evolving landscape of computer security.

About the Editors:

Dr. Manish Tiwari is serving as Associate Professor and Head, Department of Computer Science and Engineering, Career Point University, Kota, Rajasthan, India. His research interests include Artificial Intelligence, Data Mining. He has 1 books, 25 publications National, International and Conferences ,12 filed Indian patents in his credit. Till date 6 students are doing PhD work under his guidance, 12 students have successfully obtained their M.Tech degree under his sole supervision as Supervisor.

Mr. Rohit Maheshwari an esteemed academician, possesses an extensive 18 years of experience in the education sector. Currently engaged in the pursuit of a PhD in computer science, his academic interests encompass Network Security, Artificial Intelligence, and Machine Learning. Mr. Maheshwari holds the position of Assistant Professor at Career Point University in Kota, Rajasthan.

Deepak Mahawar has dedicated over 19 years to academia, showcasing versatility and a pursuit of excellence. He holds a Bachelor's in Computer Science & Engineering, a Master's in Technology, and is pursuing a Ph.D. in Computer Science and Artificial Intelligence. His career includes research roles at Indian Institute of Technology, Kanpur, with publications and presentations in international forums. As an educator, he has contributed to institutions like Poornima University, Suresh Gyan Vihar University, and Career Point University, focusing on curriculum development and student mentorship.

Ms. Preeti Gupta an esteemed academician, possesses an extensive 17 years of experience in the education sector. She has accomplished her master of technology in Computer Science. Her academic interests encompass Information Security and Artificial Intelligence. Ms. Gupta holds the position of Assistant Professor at Career Point University Kota, Rajasthan.
As an educator, she has contributed to institutions like Modi Institute of Technology Kota, Jodhpur Institute of Engineering and Technology Jodhpur and Career Point University, focusing on curriculum development and student mentorship.

CP PUBLICATION

Also Available at
amazon flipkart snapdeal

₹ 280.00

9 788197 169328

FOUNDATION OF COMPUTER SECURITY

cryptography, Attacks and Emerging Technologies

CP PUBLICATION

Editor:
Manish Tiwari
Rohit Maheswari
Deepak Mahawar
Preeti Gupta

FOUNDATION OF COMPUTER SECURITY

CRYPTOGRAPHY, ATTACKS AND EMERGING TECHNOLOGIES

CAREER POINT

CP Tower, Road No.-1, IPIA, Kota (Raj.)
Email : publication@cpil.in

Published by Career Point Ltd.
CP Tower, Road No.-1, IPIA, Kota (Raj.)
Email : publication@cpil.in

Book No. : CPP-706

Preface

In today's digital age, computer security is of utmost importance as technology pervades every aspect of our lives. This book offers a comprehensive exploration of computer security, covering topics from cryptography to emerging technologies like IoT, AI, cloud computing, and blockchain.

Beginning with cryptography, we delve into the fundamentals of secure communication, exploring classical encryption methods and modern cryptographic algorithms. We then move on to network security, discussing advancements and strategies to safeguard interconnected systems against cyber threats.

The section on IoT security addresses the unique challenges posed by the interconnectedness of devices, offering strategies for securing IoT ecosystems. AI's role in cybersecurity is examined, highlighting how machine learning can automate threat detection and response effectively.

A focus on healthcare security introduces a technique using AI for secure image watermarking to protect sensitive medical data. Cloud security best practices are outlined, covering encryption, access control, and threat detection in cloud environments.

Emerging technologies like quantum computing and blockchain are explored for their potential to enhance cloud security. Finally, we discuss blockchain's applications beyond cryptocurrency, offering transparency, immutability, and security in various industries.

This book is tailored for cybersecurity professionals, researchers, and students, providing theoretical insights and practical guidance to navigate the evolving landscape of cyberspace effectively.

Book Description

Foundation of Computer Security: Cryptography, Attacks, and Emerging Technologies" is a comprehensive guide to cybersecurity in the digital age. Covering topics from cryptography to emerging technologies like IoT and blockchain, this book offers insights and practical advice for professionals, researchers, and students. It explores secure communication, network security, AI in cybersecurity, healthcare security, cloud security, and the potential of emerging technologies to enhance security measures. With a focus on theoretical understanding and practical applications, it's an essential resource for navigating the ever-evolving landscape of computer security.

Table of Contents

Editors

Dr. Manish Tiwari

Associate Professor & HOD

Department of Computer Science and Engineering, Career Point University, Kota

Mr. Rohit Maheshwari

Assistant Professor,

Computer Science and Engineering, Career Point University, Kota

Mr. Deepak Mahawar

Assistant Professor

Department of Computer Science and Engineering, Career Point University, Kota

Ms. Preeti Gupta

Assistant Professor,

Computer Science and Engineering, Career Point University, Kota

---

About the Editors:

Dr. Manish Tiwari, is serving as Associate Professor and Head, Department of Computer Science and Engineering, Career Point University, Kota, Rajasthan, India. His research interests include Artificial Intelligence, Data Mining. He has 1 books, 25 publications National, International and Conferences, 12 filed Indian patents in his credit. Till date 6 students are doing PhD work under his guidance, 12 students have successfully obtained their M.Tech degree under his sole supervision as Supervisor.

Mr. Rohit Maheshwari, an esteemed academician, possesses an extensive 18 years of experience in the education sector. Currently engaged in the pursuit of a PhD in computer science, his academic interests encompass Network Security, Artificial Intelligence, and Machine Learning. Mr. Maheshwari holds the position of Assistant Professor at Career Point University Kota, Rajasthan.

Deepak Mahawar has dedicated over 19 years to academia, showcasing versatility and a pursuit of excellence. He holds a Bachelor's in Computer Science & Engineering, a Master's in Technology, and is pursuing a Ph.D. in Computer Science and Artificial Intelligence. His career includes research roles at Indian Institute of Technology, Kanpur, with publications and presentations in international forums.

As an educator, he has contributed to institutions like Poornima University, Suresh Gyan Vihar University, and Career Point University, focusing on curriculum development and student mentorship. Deepak has enhanced his skills in areas like entrepreneurship and mobile computing and has actively participated in organizational activities.

Ms. Preeti Gupta, an esteemed academician, possesses an extensive 17 years of experience in the education sector. She has accomplished her master of technology in Computer Science. Her academic interests encompass Information Security and Artificial Intelligence. Ms. Gupta holds the position of Assistant Professor at Career Point University Kota, Rajasthan.

As an educator, she has contributed to institutions like Modi Institute of Technology Kota, Jodhpur Institute of Engineering and Technology Jodhpur and Career Point University, focusing on curriculum development and student mentorship.

.

CHAPTER 1

Computer Security

Mr. Deepak Mahawar

ABSTRACT

This chapter provides a comprehensive overview of computer security, covering its necessity, approaches, principles, and common types of attacks. It emphasizes the critical importance of safeguarding digital information in today's interconnected world, detailing preventive, detective, corrective, and proactive security measures. Fundamental principles such as confidentiality, integrity, and availability guide the design of secure systems. The chapter explores various types of attacks, including malware, phishing, and denial-of-service, along with preventive measures such as antivirus software and email filtering. Additionally, specific threats like sniffing and spoofing, phishing, pharming, and DNS spoofing are discussed, accompanied by corresponding countermeasures to mitigate their risks.

Content-

1. Introduction

Computer security is a crucial aspect of modern computing systems. As technology becomes more integrated into our daily lives, ensuring the security and integrity of digital information is paramount. This chapter provides an overview of computer security, including the need for security, various security approaches, the principles of security, and common types of attacks on computer systems.

2. Need of Security

The need for computer security arises from the increasing reliance on digital systems for storing, processing, and transmitting sensitive information. Without adequate security measures in place, these systems are vulnerable to various threats, including unauthorized access, data breaches, malware attacks, and more. Protecting confidential data, ensuring privacy, and maintaining the availability and reliability of systems are essential components of computer security.

3. Security Approaches

There are several approaches to computer security, each addressing different aspects of protection:

Preventive Measures: These measures aim to prevent security breaches from occurring in the first place. Examples include access control mechanisms, encryption, firewalls, and intrusion detection systems.

Detective Measures: Detective measures focus on identifying security breaches after they have occurred. This includes activities such as logging and monitoring system events, conducting security audits, and employing forensic analysis techniques.

Corrective Measures: Corrective measures involve responding to security incidents and mitigating their impact. This may include patching vulnerabilities, restoring data from backups, and implementing incident response plans.

Proactive Measures: Proactive security measures anticipate and address potential security threats before they can be exploited. This includes regular security training and awareness programs, vulnerability assessments, and penetration testing.

4. Principles of Security

Several fundamental principles guide the design and implementation of secure computer systems:

Confidentiality: Ensuring that sensitive information is only accessible to authorized individuals or systems.

- Also called as privacy
- Refers to the secrecy of information
- Only the sender and the receiver should have an access to the information

Integrity: Maintaining the accuracy and consistency of data throughout its lifecycle, preventing unauthorized modifications or tampering.

- Ensures that any changes to a message are detected
- The message from sender the receiver must travel without any alterations
- Changes Need To Be Prevented, or atleast, detected

Availability: Ensuring that information and resources are available when needed, despite potential disruptions or attacks.

- Resources/applications must be available to authenticate users all the time
- Attackers Can Deny The Availability
- DenialOfService(DOS)is an example of an attack on availability

Authentication: Verifying the identity of users or systems to prevent unauthorized access.

- Identifies the sender/receiver of a message
- Required So That The Communicating Parties trust each other

- Answers Who is who

Authorization: Granting appropriate permissions and privileges to authenticated users or systems based on their roles and responsibilities.

Non-repudiation: Ensuring that actions or transactions cannot be denied by the parties involved, providing accountability and traceability.

5. Attacks on Computer

In the realm of computer security, understanding the various types of attacks that can compromise systems and data is paramount. This chapter explores attacks on computers from both general and technical perspectives, covering active and passive attacks, different types of malicious programs, and specific attack techniques. Additionally, strategies for preventing and mitigating these attacks are discussed.

Computer systems are vulnerable to a wide range of attacks, including:

Malware: Malicious software such as viruses, worms, trojans, and ransomware designed to infiltrate systems, steal data, or cause damage.

Phishing: Deceptive attempts to trick users into revealing sensitive information such as passwords or financial details.

Denial-of-Service (DoS): Attacks that disrupt the availability of services or resources, rendering them inaccessible to legitimate users.

Man-in-the-Middle (MitM): Attacks where an attacker intercepts and alters communication between two parties without their knowledge.

SQL Injection: Exploiting vulnerabilities in web applications to manipulate or access databases through SQL queries.

Cross-Site Scripting (XSS): Injecting malicious scripts into web pages viewed by other users, enabling attackers to steal information or hijack sessions.

Social Engineering: Manipulating individuals into divulging confidential information or performing actions that compromise security.

Understanding these attacks and implementing appropriate countermeasures is essential for safeguarding computer systems and protecting sensitive information.

(i) Attacks: A General and Technical View

Computer attacks can be broadly categorized into two main types: active and passive.

Active Attacks: Active attacks involve actions that directly manipulate or disrupt computer systems or networks. These attacks can include unauthorized access, data modification, or denial of service (DoS) attacks.

Passive Attacks: Passive attacks, on the other hand, involve monitoring or eavesdropping on communication channels to gather information without altering the data. These attacks aim to gather sensitive information such as passwords, financial details, or intellectual property.

Programs That Attack

Several types of malicious programs are designed to compromise computer systems and data:

Certainly! Let's delve into each of these specific types of malicious programs and techniques, along with strategies for preventing virus infections:

a) Virus:

- A virus is a type of malware that attaches itself to legitimate programs or files and replicates when those programs are executed.
- Viruses can cause damage by deleting files, corrupting data, or stealing information.

Prevention:

-]Install reputable antivirus software and keep it updated to detect and remove viruses.
- Regularly update operating systems and applications to patch known vulnerabilities.
- Exercise caution when downloading files or clicking on links from unknown sources.

b) Worm:

- Unlike viruses, worms are standalone programs that replicate themselves and spread across networks without requiring a host program.
- Worms can rapidly infect large numbers of systems and cause widespread damage.

Prevention:

- Implement network security measures such as firewalls and intrusion detection systems to monitor and block worm activity.
- Keep systems updated with the latest security patches to prevent exploitation of known vulnerabilities.
- Use strong passwords and implement access controls to prevent unauthorized access to systems.

c) Trojan Horse:

- A Trojan horse appears to be a legitimate program or file but contains malicious code that performs unauthorized actions when executed.
- Trojans are often used to steal sensitive information or provide attackers with backdoor access to systems.

Prevention:

- Exercise caution when downloading software or files from the internet, especially from untrusted sources.
- Install and maintain up-to-date antivirus software to detect and remove Trojan horse programs.
- Regularly scan systems for malware and suspicious activities.

d) Applets:

- Applets are small applications designed to run within web browsers.
- Malicious applets can exploit vulnerabilities in the browser or underlying systems to compromise security.

Prevention:

- Disable or restrict the execution of Java applets and other active content in web browsers.
- Keep web browsers and plugins updated with the latest security patches.
- Use security features such as sandboxing to limit the impact of potentially malicious applets.

e) ActiveX Controls:

- ActiveX controls are software components used to enhance functionality in Windows-based applications and web browsers.
- Malicious ActiveX controls can execute arbitrary code on users' systems and compromise security.

Prevention:

- Disable or restrict the execution of ActiveX controls in web browsers.
- Keep web browsers and operating systems updated with the latest security patches.
- Use security settings and permissions to control the execution of ActiveX controls.

f) Cookies:

- Cookies are small pieces of data stored on users' computers by websites.
- Malicious cookies can be used to track users' browsing habits or steal sensitive information.

Prevention:

- Configure web browsers to block or delete cookies from untrusted websites.
- Use browser privacy settings to control cookie behavior and limit tracking.
- Regularly clear cookies and browser cache to remove potentially sensitive information.

g) Scripts:

- Scripts, such as JavaScript, VBScript, or PowerShell, are often used to add interactivity to websites.
- Malicious scripts can exploit vulnerabilities in web browsers or execute unauthorized actions on users' systems.

Prevention:

- Disable or restrict the execution of scripts in web browsers, especially from untrusted sources.
- Keep web browsers and plugins updated with the latest security patches.
- Use browser security settings and add-ons to block or filter potentially malicious scripts.

(ii) Preventing Virus:

- Install reputable antivirus software and keep it updated with the latest virus definitions.
- Use a firewall to monitor and control incoming and outgoing network traffic.
- Keep operating systems, applications, and plugins updated with the latest security patches.
- Exercise caution when downloading files or clicking on links from unknown or untrusted sources.
- Enable email filtering and authentication mechanisms to identify and block phishing emails.
- Regularly back up important files and data to minimize the impact of a virus infection.
- Educate users about the signs of virus infections and best practices for maintaining cybersecurity hygiene.

By implementing these preventive measures and staying vigilant against potential threats, individuals and organizations can reduce the risk of virus infections and protect their systems and data from harm.

(iii) Specific Attacks: Sniffing and Spoofing, Phishing, Pharming, and DNS Spoofing

In the realm of cybersecurity, specific attacks such as sniffing and spoofing, phishing, pharming, and DNS spoofing pose significant threats to individuals, organizations, and networks. Understanding these attacks and implementing appropriate countermeasures is essential for maintaining the security and integrity of digital information.

a) Sniffing and Spoofing:

Sniffing: Sniffing, also known as packet sniffing or network sniffing, involves intercepting and monitoring network traffic to capture sensitive information such as usernames, passwords, or financial data. Attackers use specialized tools called packet sniffers to capture data packets traversing a network segment. Sniffing attacks can occur on both wired and wireless networks, and they exploit vulnerabilities in network protocols or lack of encryption to eavesdrop on communication.

Spoofing: Spoofing attacks involve impersonating legitimate entities or devices to deceive users or systems. Common types of spoofing attacks include IP spoofing, where attackers forge the source IP address of packets to appear as if they originate from a trusted source, and ARP spoofing, where attackers manipulate Address Resolution Protocol (ARP) tables to associate their MAC address with the IP address of a legitimate device on the network. Spoofing attacks can lead to various security threats, including man-in-the-middle attacks, session hijacking, and data interception.

Countermeasures: Implementing encryption protocols such as SSL/TLS can protect sensitive data from being intercepted by sniffing attacks. Additionally, deploying network intrusion detection systems (NIDS) or intrusion prevention systems (IPS) can help detect and block spoofing attempts by monitoring network traffic for suspicious behavior.

b) Phishing:

Phishing: Phishing attacks involve sending deceptive emails, text messages, or instant messages to trick users into revealing sensitive information such as passwords, usernames, or financial details. Phishing emails often impersonate trusted entities such as banks, government agencies, or popular websites and contain links to fake login pages or malicious attachments designed to steal credentials or install malware on victims' devices.

Countermeasures: Educating users about the signs of phishing attacks, such as suspicious sender addresses, spelling errors, or urgent requests for personal information, can help mitigate the risk of falling victim to phishing scams. Additionally, implementing email filtering and authentication mechanisms such as SPF, DKIM, and DMARC can help identify and block phishing emails before they reach users' inboxes.

c) Pharming or DNS Spoofing:

Pharming: Pharming attacks involve redirecting users from legitimate websites to fraudulent websites without their knowledge or consent. Attackers typically exploit vulnerabilities in the Domain Name System (DNS) or compromise DNS servers to manipulate DNS resolution and redirect users to malicious websites designed to steal sensitive information or distribute malware.

DNS Spoofing: DNS spoofing, also known as DNS cache poisoning, involves corrupting the DNS cache of a DNS server or client device to redirect domain name queries to malicious IP addresses controlled by attackers. By spoofing DNS responses, attackers can redirect users to fake websites or intercept communication between users and legitimate servers, leading to various security threats, including data theft, phishing, and malware infection.

Countermeasures: Implementing secure DNS protocols such as DNSSEC can help prevent DNS spoofing attacks by digitally signing DNS records to ensure their authenticity and integrity. Additionally, configuring firewalls and intrusion detection systems to monitor DNS traffic and detect anomalous behavior can help identify and mitigate pharming attacks in real-time.

In conclusion, understanding specific attacks such as sniffing and spoofing, phishing, pharming, and DNS spoofing is essential for safeguarding against potential security threats in the digital landscape. By implementing robust security measures and educating users about the risks associated with these attacks, individuals and organizations can better protect themselves against cyber threats and maintain the confidentiality, integrity, and availability of their digital assets.

6. Conclusion

In conclusion, this chapter provides a comprehensive overview of computer security, emphasizing the critical importance of safeguarding digital information in today's technology-driven world. It highlights the need for security measures to protect against various threats such as unauthorized access, data breaches, malware attacks, and more. The chapter explores different security approaches, including preventive, detective, corrective, and proactive measures, along with fundamental principles guiding secure system design.

Furthermore, it delves into common types of attacks on computer systems, ranging from malware and phishing to denial-of-service attacks and social engineering. It discusses both general and technical perspectives of attacks, categorizing them as active and passive, and outlines specific malicious programs and techniques used by attackers. Additionally, strategies for preventing and mitigating these attacks are provided, emphasizing the importance of user education, regular updates, and the implementation of security protocols and tools.

Overall, by understanding the various threats and implementing appropriate security measures, individuals and organizations can better protect their systems and data, ensuring confidentiality, integrity, and availability in the digital realm.