Content from different reference book suggested by Prof. Prakash Sir and mentioned in CNS Syllabus file, Presentations, Notes provided in 2023

NOTES ON BASIS OF CNS PPT INTRODUCTION TO SECURITY 25 SLIDES

CHEAT SHEET - Read PPT once

Introduction to Computer Security and Privacy Cheatsheet

Textbook:
- Security in Computing, 4th edition
  Authors: Charles P. Pfleeger and Shari Lawrence Pfleeger

Content:

1. Course Goal:
   - Identify security and privacy issues in computing.
   - Design systems that enhance security and privacy.

2. Security:
   - Confidentiality: Limited access to authorized parties.
   - Integrity: Ensuring the correctness of data.
   - Availability: System/data accessibility when needed.

3. Privacy:
   - Control over personal information.
   - Control includes data visibility, usage, sharing, etc.

4. Assets, Vulnerabilities, Threats, Attacks, Controls:
   - Assets: Items to be protected (hardware, software, data).
   - Vulnerabilities: System weaknesses.
   - Threats: Potential harm to the system.
   - Attacks: Actions exploiting vulnerabilities.
   - Controls: Measures to prevent, detect, or mitigate attacks.

5. Methods of Defense:
   - Prevent: Block attacks.
   - Deter: Increase attack difficulty.
   - Deflect: Reduce attractiveness to attackers.
   - Detect: Notice attacks.
   - Recover: Mitigate attack effects.

6. Computer Criminals:
   - Amateurs, Crackers, Career Criminals.

7. Defense Techniques:
   - Cryptography: Data protection, authentication, integrity.
   - Software Controls: Access restrictions, OS separation, virus scanners.
   - Hardware Controls: Fingerprint readers, smart tokens, firewalls, IDS.
   - Physical Controls: Locks, guards, backups.
   - Policies and Procedures: Rules, training, security practices.

8. Threat Management:
   - Method: Attack skills, knowledge, tools.
   - Opportunity: Time, access for attacks.
   - Motive: Reason behind attacks.

9. Security vs. Privacy:
   - Both are not necessarily opposing forces.
   - Balancing both is crucial.

10. Recap:
    - Course goal: Identify and design for security and privacy.
    - Security: Confidentiality, Integrity, Availability.
    - Privacy: Control over personal information.
    - Attackers: Amateurs, Crackers, Career Criminals.
    - Defense: Prevent, Deter, Deflect, Detect, Recover.
    - Techniques: Cryptography, Software/Hardware Controls, Physical Controls, Policies/Procedures.

NOTES
Introduction to Computer Security and Privacy

In this course, we will delve into the realm of computer security and privacy, exploring various aspects of safeguarding information and systems in the digital age. Our primary textbook, "Security in Computing, 4th edition" by Charles P. Pfleeger and Shari Lawrence Pfleeger, will serve as our guide through this exciting journey.

1-3 Content

What is our goal in this course?
Our overarching objective is to equip you with the ability to identify security and privacy concerns across a spectrum of computing domains. This includes understanding potential vulnerabilities and threats that may compromise the integrity of:

- Programs
- Operating systems
- Networks
- Internet applications

- Databases

Additionally, we aim to cultivate your skills to design systems that prioritize security and privacy, thus contributing to a safer digital landscape.

What is security?
Security in the context of computing can be summarized in three crucial aspects:

1. Confidentiality: Ensuring that only authorized parties have access to systems or data.
2. Integrity: Guarantees that data remains accurate and unaltered, providing the "right" information when requested.
3. Availability: Ensures that systems and data are accessible and operational when needed.

A computing system can be deemed secure when it effectively embodies these three properties.

Protecting money and protecting information
While there are parallels between protecting physical assets (such as money) and digital assets (such as information), there are notable differences:

- Size and Portability: Money tends to be larger and requires substantial physical security, while digital information can be stored on portable devices.
- Ability to Avoid Physical Contact: Digital information can be handled electronically, whereas money requires direct physical contact.
- Value of Assets: Money typically has a universally high value, whereas the value of digital information can vary greatly.

Security and reliability
Security and reliability are closely intertwined. A secure system is one that users can rely on to:

- Maintain confidentiality of personal data
- Allow only authorized access or modifications
- Deliver accurate and meaningful results consistently

What is privacy?
Privacy encompasses a variety of definitions, but a practical one involves having control over your personal information. Control, in this context, includes determining who can access the information, how it can be used, who it can be shared with, and more.

Security vs. privacy
Security and privacy are not necessarily opposing forces. It's possible to achieve both, and they often complement each other rather than being mutually exclusive.

Some terminology

- Assets: Items worth protecting, including hardware, software, and data.
- Vulnerabilities: Weaknesses in a system that can be exploited to cause harm.
- Threats: Potential incidents or events that can lead to loss or harm to a system.
- Attacks: Actions that exploit vulnerabilities.
- Controls: Measures taken to prevent, deter, deflect, detect, or recover from attacks.

Method, opportunity, and motive
Understanding attacks involves considering the attacker's method, opportunity, and motive:

- Method: Skills, knowledge, and tools required for an attack.
- Opportunity: Time and access needed to execute an attack.
- Motive: The reason behind an attack.

Computer Criminals
Different types of computer criminals include amateurs, crackers, and career criminals, each with varying levels of expertise and intent.

Methods of defense
Defending against threats involves multiple strategies:

- Prevent: Blocking the attack entirely.
- Deter: Making the attack more challenging or costly.
- Deflect: Reducing attractiveness as a target.
- Detect: Noticing ongoing or past attacks.
- Recover: Minimizing the impact of an attack.

Example of defense
For instance, defending against the theft of a car involves a combination of prevention, deterrence, detection, and recovery methods.

Defense of computer systems
To protect hardware, software, and data, a multi-layered approach is crucial. Various methods of defense include:

- Cryptography: Protecting data through encryption and digital signatures.
- Software controls: Implementing access controls, separating user actions, using virus scanners, and enforcing code quality.
- Hardware controls: Utilizing fingerprint readers, smart tokens, firewalls, and intrusion detection systems.
- Physical controls: Protecting hardware and controlling physical access.
- Policies and procedures: Establishing rules and training to prevent security breaches.

Recap
This introductory overview has covered our course's goals, the fundamental concepts of security and privacy, the relationship between them, key terminology, methods of defense, and the different ways to

protect computer systems and data. This foundation will guide us through a deeper exploration of the intricacies of computer security and privacy.

SUMMARY

The course "Introduction to Computer Security and Privacy" covers the fundamental concepts of safeguarding computing systems and maintaining the confidentiality, integrity, and availability of data. The required textbook, "Security in Computing, 4th edition" by Charles P. Pfleeger and Shari Lawrence Pfleeger, serves as the foundational resource for understanding these concepts.

The course begins by outlining its goals, which include the ability to recognize security and privacy issues across various computing domains and to apply this knowledge in designing more secure systems. Security is defined as encompassing confidentiality, integrity, and availability of systems and data.

Differentiating between protecting assets like money and information, the course highlights that security is closely tied to reliability, ensuring that systems consistently deliver accurate results, safeguard personal data, and restrict unauthorized access.

Privacy is introduced as the control individuals have over their personal information, encompassing who can access, use, share, and manipulate such data. The relationship between security and privacy is explored, challenging the notion that they are opposing forces and emphasizing the need to balance both.

Key terms such as assets, vulnerabilities, threats, attacks, and controls are defined. Assets include hardware, software, and data, while vulnerabilities represent weaknesses that can be exploited. Threats encompass potential losses or harm, and attacks exploit vulnerabilities. Controls are mechanisms to prevent, deter, deflect, detect, or recover from attacks.

The course delves into various methods of defense against threats, including prevention, deterrence, deflection, detection, and recovery. Real-world examples illustrate these strategies, such as securing a car against theft.

Defending computer systems involves cryptography, which protects data and authenticates users and transactions. Software controls like access control and virus scanners, hardware controls like fingerprint readers and firewalls, and physical controls such as locks and guards are explored. Policies and procedures are also discussed to establish guidelines for secure practices within an organization.

The course concludes by reiterating its goals, emphasizing the importance of identifying security and privacy issues, understanding the nature of security (confidentiality, integrity, availability), and exploring methods of defense, including cryptographic techniques, software and hardware controls, physical safeguards, and established policies and procedures.

SUMMARY IN POINTS

Concise summary of the key points from the "Introduction to Computer Security and Privacy" course:

1. Course Overview:

- Introduction to fundamental concepts of computer security and privacy.
- Required textbook: "Security in Computing, 4th edition" by Charles P. Pfleeger and Shari Lawrence Pfleeger.

2. Goals of the Course:
- Identify security and privacy issues across computing domains.
- Design systems that enhance security and privacy.

3. Understanding Security:
- Security encompasses confidentiality, integrity, and availability of data.
- Security and reliability are closely linked; a secure system is reliable in protecting data and allowing authorized access.
- Protecting assets like money and information involves different characteristics and methods.

4. Privacy Defined:
- Privacy grants individuals control over their personal information.
- Control includes determining who can access, use, share, and manipulate data.

5. Balancing Security and Privacy:
- Security and privacy are not necessarily opposing; both need to be balanced and harmonized.
- Achieving both security and privacy goals is possible with careful design.

6. Key Terminology:
- Assets: Elements to be protected, such as hardware, software, and data.
- Vulnerabilities: Weaknesses that can be exploited in a system.
- Threats: Potential losses or harm that exploit vulnerabilities.
- Attacks: Actions that exploit vulnerabilities.
- Controls: Mechanisms to prevent, deter, detect, or recover from attacks.

7. Methods of Defense:
- Prevention: Blocking attacks from occurring.
- Deterrence: Making attacks more difficult or expensive.
- Deflection: Reducing the attractiveness as a target.
- Detection: Identifying ongoing or past attacks.
- Recovery: Minimizing the impact of an attack.

8. Defense Strategies:
- Cryptography: Protecting data, authenticating users and transactions.
- Software Controls: Access control, virus scanners, separation of user actions.
- Hardware Controls: Biometrics, firewalls, intrusion detection systems.
- Physical Controls: Locks, guards, backups.
- Policies and Procedures: Establishing guidelines for secure practices.

9. Understanding Attackers:

- Different categories of attackers, including amateurs, crackers, and career criminals.
- Consider methods, opportunities, and motives behind attacks.

10. Course Recap:
- Goals include recognizing security and privacy issues and designing more protective systems.
- Security entails confidentiality, integrity, and availability.
- Privacy grants control over personal information.
- Security and privacy are not necessarily opposing; a balance is achievable.
- Key concepts include assets, vulnerabilities, threats, attacks, and controls.
- Defense methods encompass prevention, deterrence, deflection, detection, and recovery.

This summary captures the core concepts and objectives of the "Introduction to Computer Security and Privacy" course, providing a concise overview of the covered material.

DIAGRAMS - Refer PPT Diagrams also
Create your own diagrams or from ppt

SIMULATED QA
Q1: What is the required textbook for this course?
A1: Security in Computing, 4th edition by Charles P. Pfleeger and Shari Lawrence Pfleeger.

Q2: What is the primary goal of this course?
A2: The primary goal is to identify security and privacy issues in various aspects of computing and design systems that enhance security and privacy.

Q3: How is security defined in the context of computers?
A3: Security in the context of computers generally refers to three things: confidentiality, integrity, and availability.

Q4: Define confidentiality, integrity, and availability in the context of security.
A4: Confidentiality limits access to authorized parties, integrity ensures the right data is provided, and availability ensures the system or data is accessible when needed.

Q5: What is the relationship between security and reliability?
A5: A secure system is reliable and can be trusted to keep personal data confidential, allow authorized access, and provide accurate results.

Q6: How is privacy defined?
A6: Privacy is the ability to control information about oneself, including who can see, use, and share that information.

Q7: Is security opposed to privacy?
A7: No, security and privacy are not necessarily opposing forces; they can coexist and complement each other.

Q8: Define assets, vulnerabilities, threats, attacks, and controls in the context of computer security.
A8: Assets are things to protect, vulnerabilities are weaknesses, threats are potential losses or harm, attacks exploit vulnerabilities, and controls are measures to reduce vulnerabilities.

Q9: Differentiate between threats and vulnerabilities.
A9: Threats are potential losses or harm, while vulnerabilities are weaknesses in a system that can be exploited by threats. Threats are blocked by controlling vulnerabilities.

Q10: What is an attack?
A10: An attack is an action that exploits a vulnerability in a system.

Q11: How do controls contribute to computer security?
A11: Controls are measures such as gates, walls, software, and hardware that help defend against threats by preventing, deterring, deflecting, detecting, and recovering from attacks.

Q12: Explain the concepts of method, opportunity, and motive in the context of computer security.
A12: Method refers to the skills and tools required for an attack, opportunity involves the time and access for an attack, and motive is the reason behind an attack.

Q13: What are the categories of computer criminals mentioned?
A13: Amateurs, crackers, and career criminals are categories of computer criminals.

Q14: What are the different methods of defense against threats?
A14: Methods of defense include prevention, deterrence, deflection, detection, and recovery.

Q15: Provide an example of defense against a threat and explain how it corresponds to the methods of defense.
A15: To defend against the threat of a stolen car: Prevention by using locks, Deterrence by parking in a secure facility, Deflection by using a cover, Detection through car alarms, and Recovery through insurance.

Q16: How is data protected using cryptography?
A16: Cryptography protects data by making it unreadable to attackers. It can also authenticate users and transactions and ensure data integrity.

Q17: Give examples of software controls used for computer security.
A17: Software controls include passwords, access control, operating system isolation, virus scanners, and development controls.

Q18: Provide examples of hardware controls used for computer security.
A18: Hardware controls include fingerprint readers, smart tokens, firewalls, and intrusion detection systems.

Q19: What are some examples of physical controls for computer security?

A19: Physical controls include locks, guards, and off-site backups to protect hardware and prevent unauthorized physical access.

Q20: How can policies and procedures contribute to computer security?
A20: Policies and procedures help prevent security breaches by defining rules and best practices, such as controlling access and training employees.

Q21: Summarize the goals of the course, the concepts of security, and privacy.
A21: The course aims to identify security and privacy issues, design protective systems, and promote confidentiality, integrity, availability, and control of personal information.

Q22: What is the relationship between attackers and defenders in computer security?
A22: Understanding attackers' methods helps defenders protect against threats using various controls and defense mechanisms.

Q23: Explain the concept of "defense in depth."
A23: "Defense in depth" involves layering multiple security measures to provide comprehensive protection against various threats.

These simulated Q&A pairs cover the key concepts introduced in the provided material about Introduction to Computer Security and Privacy.

QUIZ MCQ
Sure, here's a multiple-choice quiz based on the provided content. The answers are provided at the end.

Introduction to Computer Security and Privacy Quiz

Question 1: What is the primary goal of this course?
a) To learn programming languages
b) To explore different operating systems
c) To identify security and privacy issues in computing
d) To study network protocols

Question 2: What are the three properties that define a secure computing system?
a) Confidentiality, Encryption, Availability
b) Integrity, Authentication, Encryption
c) Confidentiality, Integrity, Availability
d) Privacy, Authentication, Reliability

Question 3: What does the term "privacy" mean in the context of this course?
a) Keeping personal information secret from everyone
b) Controlling information about oneself
c) Completely isolating oneself from the digital world
d) Encrypting all data for security

Question 4: Which of the following is NOT one of the major categories of threats?
a) Interception
b) Interruption
c) Modification
d) Authentication

Question 5: What is the purpose of cryptography in computer security?
a) Prevent hardware failures
b) Authenticate users
c) Make data unreadable to attackers
d) Enhance network speed

Question 6: What is the term for an action that exploits a vulnerability in a system?
a) Asset
b) Threat
c) Control
d) Attack

Question 7: How can you defend against a threat in computer security?
a) Ignore it and hope it goes away
b) Make yourself more attractive to attackers
c) Detect it and let it happen
d) Prevent, Deter, Deflect, Detect, Recover

Question 8: Which of the following is an example of a hardware control?
a) Password protection
b) Firewalls
c) Encryption
d) Security policies

Question 9: What is the goal of "Defence in depth"?
a) To prevent all attacks
b) To deter attackers with strong measures
c) To create multiple layers of defense
d) To ignore potential threats

Question 10: What is the main difference between interception and modification threats?
a) Interception involves unauthorized access, while modification involves changing data
b) Interception is a physical threat, while modification is a digital threat
c) Interception affects availability, while modification affects confidentiality
d) Interception cannot be controlled, while modification can be blocked

Answers:

1. c) To identify security and privacy issues in computing
2. c) Confidentiality, Integrity, Availability
3. b) Controlling information about oneself
4. d) Authentication
5. c) Make data unreadable to attackers
6. d) Attack
7. d) Prevent, Deter, Deflect, Detect, Recover
8. b) Firewalls
9. c) To create multiple layers of defense
10. a) Interception involves unauthorized access, while modification involves changing data

Of course! Here are some more multiple-choice questions for your quiz:

Question 11: What are the three properties that define security in the context of computer systems?
a) Authentication, Availability, Encryption
b) Confidentiality, Integrity, Availability
c) Intrusion detection, Reliability, Privacy
d) Accessibility, Modifiability, Trustworthiness

Question 12: Which term refers to a weakness in a system that may be exploited to cause harm?
a) Threat
b) Control
c) Asset
d) Vulnerability

Question 13: What is the primary goal of cryptography?
a) To prevent all cyberattacks
b) To make data indestructible
c) To ensure data confidentiality and integrity
d) To create new computer languages

Question 14: What type of control involves using biometric data like fingerprints for authentication?
a) Physical control
b) Software control
c) Hardware control
d) Network control

Question 15: What is the purpose of a firewall in computer security?
a) To block all internet access
b) To prevent software crashes
c) To protect against malware
d) To control physical access to computers

Question 16: What is the term for an unauthorized user who gains access to computer systems to exploit vulnerabilities?
a) Hacker
b) Developer
c) Moderator
d) Administrator

Question 17: Which category of threat involves adding false information to a system?
a) Interception
b) Interruption
c) Modification
d) Fabrication

Question 18: What is the concept of "least privilege" in computer security?
a) Giving every user maximum access rights
b) Restricting users' access to only what is necessary
c) Providing unlimited privileges to administrators
d) Ignoring access control altogether

Question 19: What is the term for an action that makes an attack harder or more expensive to carry out?
a) Prevention
b) Deterrence
c) Detection
d) Recovery

Question 20: Which of the following is an example of a physical control?
a) Antivirus software
b) Firewall configuration
c) Biometric access system
d) Strong password policy

Answers:
11. b) Confidentiality, Integrity, Availability
12. d) Vulnerability
13. c) To ensure data confidentiality and integrity
14. a) Physical control
15. c) To protect against malware
16. a) Hacker
17. d) Fabrication
18. b) Restricting users' access to only what is necessary
19. b) Deterrence
20. c) Biometric access system

FLASHCARDS/KEY TERMS

Here are flashcards summarizing the key points from the provided introduction to Computer Security and Privacy:

Flashcard Set: Introduction to Computer Security and Privacy

Card 1:
Term: Required Textbook
Definition: Security in Computing, 4th edition
Authors: Charles P. Pfleeger and Shari Lawrence Pfleeger

Card 2:
Term: Course Goal
Definition: Identify security and privacy issues in computing, design protective systems for security and privacy.

Card 3:
Term: Security
Definition: Protection of computer systems and data against unauthorized access, integrity compromise, and unavailability.

Card 4:
Term: Privacy
Definition: Control over personal information, including who can access, use, and share it.

Card 5:
Term: Assets, Vulnerabilities, Threats, Attacks, Controls
Definition: Elements of security including valuable resources, weaknesses, potential harm, actions, and protective measures.

Card 6:
Term: Methods of Defence
Definition: Strategies to protect against threats, including prevention, deterrence, deflection, detection, and recovery.

Card 7:
Term: Confidentiality, Integrity, Availability
Definition: Core aspects of security - limiting access, ensuring correctness, and maintaining system/data availability.

Card 8:
Term: Security and Reliability
Definition: A secure system is reliable, maintains confidentiality, allows authorized access, and provides accurate results.

Card 9:
Term: Privacy Control
Definition: Control over personal information, including its visibility, usage, and sharing.

Card 10:
Term: Security vs. Privacy
Definition: Security and privacy are not always opposing forces, finding a balance is important.

Card 11:
Term: Assets
Definition: Elements to be protected, e.g., hardware, software, data.

Card 12:
Term: Vulnerabilities
Definition: Weaknesses in a system that can be exploited for harm.

Card 13:
Term: Threats
Definition: Potential events causing harm, e.g., unauthorized access or data exposure.

Card 14:
Term: Attacks
Definition: Actions exploiting vulnerabilities to cause harm.

Card 15:
Term: Controls
Definition: Measures to prevent, deter, deflect, detect, and recover from attacks.

Card 16:
Term: Method, Opportunity, Motive
Definition: Factors contributing to an attack - skills, access, and reasons.

Card 17:
Term: Computer Criminals
Definition: Amateurs, crackers, and career criminals engaging in cybercrime.

Card 18:
Term: Defence Strategies
Definition: Prevent, deter, deflect, detect, recover - strategies to defend against threats.

Card 19:
Term: Cryptography
Definition: Protecting data through encryption and digital signatures.

Card 20:
Term: Software Controls
Definition: Passwords, access controls, user separation, virus scanning, development controls.

Card 21:
Term: Hardware Controls
Definition: Fingerprint readers, smart tokens, firewalls, intrusion detection.

Card 22:
Term: Physical Controls
Definition: Locks, guards, off-site backups - physical protection of hardware and access.

Card 23:
Term: Policies and Procedures
Definition: Rules, training, and practices to prevent security breaches.

Card 24:
Term: Recap - Course Goal
Definition: Identify security and privacy issues, design protective systems.

Card 25:
Term: Recap - Security and Privacy
Definition: Security ensures confidentiality, integrity, availability. Privacy involves control over personal information.

Feel free to use these flashcards for studying and reviewing the concepts introduced in the "Introduction to Computer Security and Privacy" section.
- Read PPT once