Week # 1 topics (as per course outline)

**The text taken from Internet to facilitate a different flavor other than the mandatory reading of these topic from the textbook and following lecture contents including (slides, whiteboard and verbal delivery)

Week #	Topic	Reference Text
1	**Information Security Foundations**: Definition of Computer Security with Examples, The Challenges of Computer Security, A Model for Computer Security, Threats, Attacks, and Assets, Functional Requirements, Security Design Principles, Attack Surfaces and Attack Trees, Security Policy, Security Implementation Assurance and Evaluation, Standards	Main Textbook, Chapter 1 Sections 1.1, 1.2, 1.4, 1,6, 1,7

Definition of Computer Security with Examples

Computer security, also known as cybersecurity, refers to the practice of protecting computer systems, networks, and data from various threats and unauthorized access in order to ensure their confidentiality, integrity, and availability. It involves the implementation of measures, processes, and technologies to safeguard digital information and prevent cyberattacks.

There are several aspects to computer security, each addressing different types of threats and vulnerabilities. Here are some examples of computer security concepts and their corresponding examples:

1. **Authentication and Authorization:**
   - **Example:** A user logging into an online banking application using their username and password. The system verifies their credentials (authentication) and grants access to specific account information based on their privileges (authorization).

2. **Encryption:**
   - **Example:** Before transmitting sensitive data (such as credit card information) over the internet, the data is encrypted using protocols like SSL/TLS. This ensures that even if intercepted, the data remains unreadable to unauthorized parties.

3. **Firewalls:**
   - **Example:** A network firewall is set up to block unauthorized incoming traffic while allowing approved outgoing traffic. This prevents external attackers from gaining access to internal network resources.

4. **Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS):**
   - **Example:** An IDS monitors network traffic for suspicious activities or patterns that might indicate a cyberattack. An IPS, if integrated, can take automated actions to block or prevent those attacks in real-time.

5. **Malware Protection:**
   - **Example:** Antivirus software scans files and programs for known malware signatures. If it detects a match, it quarantines or deletes the infected file to prevent further spread.

6. **Patch Management:**
   - **Example:** Software developers release patches and updates to fix security vulnerabilities in their products. Regularly applying these patches to operating systems, applications, and software helps prevent exploitation by attackers.

7. **Social Engineering Awareness:**
   - **Example:** Employees receive training to recognize and resist social engineering tactics, such as phishing emails or phone calls. This prevents attackers from manipulating individuals into divulging sensitive information.

8. **Access Control:**
   - **Example:** An organization restricts access to its sensitive databases to authorized personnel only. Employees have access to data relevant to their roles, minimizing the risk of data breaches.

9. **Backup and Recovery:**
   - **Example:** Regularly backing up critical data and systems ensures that if a cyberattack or system failure occurs, data can be restored from a previous state, reducing downtime and loss of information.

10. **Multi-Factor Authentication (MFA):**
    - **Example:** After entering a password, a user is prompted to provide an additional authentication factor, such as a fingerprint scan or a time-based code from a mobile app. This adds an extra layer of security beyond just a password.

These examples showcase the diverse strategies and practices that comprise computer security. In an increasingly digital world, maintaining strong cybersecurity measures is essential to protect against a wide range of threats and vulnerabilities.

The Challenges of Computer Security

Computer security, also known as cybersecurity, refers to the practice of protecting computer systems, networks, and data from various threats and unauthorized access. There are several key challenges in the field of computer security that organizations and individuals face:

1. **Cyberattacks and Threats**: Cyberattacks come in various forms, such as viruses, malware, ransomware, phishing, and more. Attackers constantly develop new techniques to exploit vulnerabilities in software and systems, making it challenging to stay ahead of evolving threats.

2. **Vulnerability Management**: Software and systems often have vulnerabilities that can be exploited by attackers. Identifying and addressing these vulnerabilities before they are exploited is crucial but can be challenging due to the complexity of modern software and the sheer number of potential vulnerabilities.

3. **Complexity of Systems**: Modern computer systems are incredibly complex, often composed of numerous interconnected components and layers. Each component can introduce potential security weaknesses, making it difficult to ensure comprehensive security across the entire system.

4. **Human Factor**: People remain a significant source of security challenges. Human errors, lack of cybersecurity awareness, and social engineering attacks can lead to data breaches and compromises. Insider threats, whether intentional or accidental, also pose a significant risk.

5. **Insufficient Authentication and Authorization**: Weak or inadequate authentication methods can lead to unauthorized access. Similarly, improper authorization can allow legitimate users to access resources beyond their intended scope, potentially leading to data breaches.

6. **Mobile and IoT Security**: The proliferation of mobile devices and Internet of Things (IoT) devices has expanded the attack surface. These devices often have limited security features and are susceptible to various forms of exploitation.

7. **Data Privacy**: Protecting sensitive and personal data is crucial, especially with the increasing amount of data stored and processed online. Data breaches can have serious financial, legal, and reputational consequences.

8. **Cloud Security**: As more services and data are moved to cloud environments, ensuring the security of cloud platforms becomes a challenge. Organizations need to understand the shared responsibility model and implement appropriate security measures within their cloud infrastructure.

9. **Regulatory Compliance**: Many industries are subject to regulations and compliance standards that require specific security measures to be in place. Meeting these requirements while also ensuring overall security can be complex.

10. **Patch Management**: Keeping software and systems up to date with the latest security patches is essential for preventing known vulnerabilities from being exploited. However, the process of patch management can be time-consuming and disruptive.

11. **Emerging Technologies**: New technologies such as artificial intelligence, machine learning, and quantum computing introduce both opportunities and challenges to cybersecurity. Adapting security practices to these technologies requires ongoing research and development.

12. **Global Nature of Attacks**: Cyberattacks can come from anywhere in the world, making it difficult to track down and prosecute attackers. Additionally, the interconnected nature of the internet means that an attack on one entity can have ripple effects across the digital landscape.

Addressing these challenges requires a multi-faceted approach, involving technical solutions, policies and procedures, user education, collaboration among stakeholders, and ongoing vigilance to stay ahead of evolving threats.

A Model for Computer Security

A model for computer security is a structured representation or framework that defines the concepts, principles, and components involved in ensuring the confidentiality, integrity, and availability of computer systems, networks, and data. These models provide a systematic way to understand, analyze, and manage security risks and measures.
Several models have been developed over time to help organizations and individuals address computer security concerns effectively. Here are a few notable ones:

1. **CIA Triad Model:**
   This is one of the fundamental models in computer security. It focuses on three key principles: Confidentiality, Integrity, and Availability (CIA). Confidentiality ensures that data is only accessible to authorized parties, integrity ensures that data remains accurate and unaltered, and availability ensures that data and services are accessible when needed.
2. **AAA Model:**
   The AAA model stands for Authentication, Authorization, and Accounting. It is commonly used in access control systems. Authentication verifies the identity of users or systems, authorization defines what actions or resources they are allowed to access, and accounting tracks the actions taken by users for auditing purposes.
3. **Bell-LaPadula Model:**
   This model is based on access control policies and enforces confidentiality. It defines mandatory access controls and access levels through security labels. The model emphasizes the "no read up, no write down" principle, which prevents users from accessing data at higher security levels than their own.
4. **Zero Trust Model:**
   The Zero Trust model challenges the traditional perimeter-based security approach and assumes that threats may exist within an organization's network. It enforces strict identity verification and access controls regardless of the user's location.

These models serve as frameworks for designing and implementing effective security strategies. It's important to note that different models may be more appropriate for different scenarios, and organizations often combine aspects of multiple models to create a comprehensive security posture. Additionally, the field of computer security continues to evolve, and new models and approaches may emerge over time.

Threats, Attacks, and Assets

In the context of cybersecurity and information security, the terms "Threats," "Attacks," and "Assets" are crucial concepts. They are fundamental to understanding and managing risks to an organization's digital infrastructure and sensitive information.

1. **Threats:**
Threats refer to potential dangers or harmful events that have the potential to exploit vulnerabilities in a system, network, or organization. These can be both intentional, like cyberattacks conducted by hackers, or unintentional, such as natural disasters or hardware failures. Threats can come from various sources, including malicious actors, software vulnerabilities, environmental factors, and more.

2. **Attacks:**
An attack is an actual attempt to exploit a vulnerability or take advantage of a weakness in a system's security. It's the execution of a threat with the intent to cause harm, steal information, disrupt services, or otherwise compromise the integrity, confidentiality, or availability of data and resources. Attacks can take many forms, including but not limited to malware infections, phishing scams, denial of service (DoS) attacks, and social engineering.

3. **Assets:**
Assets are the valuable resources that organizations aim to protect. These can include physical assets like servers and computers, as well as intangible assets like sensitive data, intellectual property,

customer information, financial records, and more. Understanding and categorizing assets is essential for prioritizing security efforts and allocating resources effectively.

In summary, threats are potential dangers, attacks are actual attempts to exploit vulnerabilities, and assets are the valuable resources that organizations aim to safeguard from those threats and attacks. Managing cybersecurity effectively involves identifying potential threats, assessing vulnerabilities, implementing protective measures, and responding to attacks in a timely and effective manner to mitigate risks and protect assets.

Security Functional Requirements

Functional requirements for security define the specific features and capabilities that a system or application must possess to ensure the security of its users, data, and resources. These requirements outline the functionalities that enable the system to protect against unauthorized access, data breaches, cyberattacks, and other security threats. Here are some common functional security requirements:

1. **User Authentication and Authorization:**
   - The system must support secure user authentication using methods like passwords, multi-factor authentication (MFA), biometrics, etc.
   - Role-based access control should be implemented to ensure that users have appropriate permissions and access rights based on their roles and responsibilities.

2. **Data Encryption:**
   - Sensitive data, both in transit and at rest, must be encrypted using strong encryption algorithms and protocols.
   - Encryption keys and certificates must be properly managed and protected.

3. **Access Control:**
   - Access to resources, functionalities, and data should be restricted based on the principle of least privilege.
   - Access control mechanisms should prevent unauthorized users from accessing critical functions or data.

4. **Audit Trails and Logging:**
   - The system should maintain comprehensive audit logs of user activities, system events, and security-related actions.
   - Logs must include relevant details such as timestamps, user identities, and actions performed.

5. **Secure Communication:**
   - The system must use secure communication protocols (e.g., HTTPS, TLS) to protect data transmitted between users and the system.

6. **Vulnerability Management:**
   - Regular security assessments and vulnerability scans should be conducted to identify and address potential weaknesses in the system.
   - Timely patching and updates should be applied to fix known vulnerabilities.

7. **Intrusion Detection and Prevention:**

- The system should be equipped with intrusion detection and prevention mechanisms to identify and respond to unauthorized access attempts or suspicious activities.

8. **Malware Protection:**
   - The system should have anti-malware mechanisms to detect and mitigate the risk of malicious software infections.

9. **Secure Configuration Management:**
   - Default settings should be secure, and the system should not expose unnecessary services or functionalities.
   - Configuration changes should follow secure practices and be well-documented.

10. **Secure Session Management:**
    - Sessions should be properly managed to prevent session hijacking or fixation attacks.
    - Logout mechanisms should be implemented to terminate sessions securely.

11. **Backup and Recovery:**
    - Regular backups of critical data should be taken and securely stored to facilitate data recovery in case of incidents.

12. **Incident Response and Management:**
    - A well-defined incident response plan should be in place to address security breaches, including steps for containment, mitigation, and communication.

13. **Secure API and Integration:**
    - If the system interacts with other systems or services via APIs, those interfaces must be designed and implemented with security in mind.

14. **Secure Software Development Lifecycle (SDLC):**
    - Security should be integrated throughout the software development process, including design, coding, testing, and deployment.

15. **User Training and Awareness:**
    - The system should provide user education and awareness about security best practices to help users understand their roles in maintaining security.

These functional security requirements are just a starting point. Depending on the nature of the system, industry regulations, and potential threats, additional requirements might be necessary to ensure comprehensive security.

Security Design Principles

Security design principles are fundamental guidelines and concepts that help in creating systems, applications, and environments that are secure, resilient, and able to defend against various threats and risks. These principles provide a framework for designing security measures that protect data, assets, and individuals from unauthorized access, breaches, and attacks. Here are some key security design principles:

1. **Least Privilege:** Grant users and processes only the minimum permissions necessary to perform their tasks. This reduces the potential damage that could occur if compromised.

2. **Defense in Depth:** Implement multiple layers of security controls to prevent a single point of failure. Even if one layer is breached, other layers can still provide protection.

3. **Fail-Safe Defaults:** Systems should be configured with secure defaults. If a user or administrator doesn't explicitly configure a setting, the most secure option should be in place.

4. **Economy of Mechanism:** Keep security mechanisms as simple and straightforward as possible. This reduces the potential for errors and vulnerabilities that can arise from complex designs.

5. **Complete Mediation:** Ensure that every access to a resource is checked for authorization. Avoid shortcuts that might bypass security checks.

6. **Open Design:** Security through obscurity is not effective. Security mechanisms should not rely on keeping their designs secret, but rather on their robustness against known and unknown attacks.

7. **Separation of Duties:** Divide tasks among multiple individuals to prevent any single person from having complete control over critical systems or processes.

8. **Least Common Mechanism:** Avoid sharing components or resources among different users or processes whenever possible. This reduces the potential for one user's actions affecting another user's security.

9. **Psychological Acceptability:** Security measures should be designed in a way that they are not too burdensome for users. If security is too difficult or frustrating, users might find ways to bypass it.

10. **Secure the Weakest Link:** Identify and address the most vulnerable components or areas in your system. Attackers often target the weakest points.

11. **Isolation:** Isolate different components or services from each other to contain breaches and limit the potential damage.

12. **Minimize Attack Surface:** Reduce the number of entry points and avenues an attacker could exploit. Disable unnecessary services, ports, and functionalities.

13. **Regular Updates:** Keep software, systems, and devices up to date with the latest security patches to address known vulnerabilities.

14. **Auditing and Monitoring:** Implement thorough logging, auditing, and monitoring mechanisms to detect and respond to suspicious activities in real-time.

15. **Incident Response Planning:** Have a well-defined plan in place for responding to security incidents. This minimizes the impact of an attack and speeds up recovery.

16. **Secure Communication:** Ensure that data in transit is encrypted and protected from eavesdropping and tampering.

17. **Authentication and Authorization:** Implement strong authentication mechanisms to ensure users are who they claim to be, and enforce proper authorization controls to restrict access based on roles and permissions.

18. **Data Protection:** Use encryption to protect sensitive data at rest and in transit. Implement data retention policies and secure data disposal practices.

19. **Physical Security:** Don't overlook the importance of physical security measures, such as access controls, surveillance, and environmental protections for critical infrastructure.

20. **Continuous Improvement:** Regularly assess and update security measures to adapt to new threats, vulnerabilities, and technologies.

These principles should guide the design and implementation of security measures to create a robust and effective security posture for systems and applications. Keep in mind that security is an ongoing process that requires vigilance and adaptation to evolving threats and technologies.

Computer Security Strategy

Developing a comprehensive computer security strategy is crucial for protecting your digital assets, sensitive information, and ensuring the continuity of your operations. Here's a structured approach to creating an effective computer security strategy:

1. **Assessment and Risk Management:**
   - Identify your organization's critical assets, systems, and data that require protection.
   - Conduct a thorough risk assessment to understand potential threats, vulnerabilities, and potential impacts.
   - Prioritize risks based on their likelihood and potential impact on the organization.

2. **Security Policies and Procedures:**
   - Develop and document clear security policies that outline acceptable use, access controls, data handling, incident response, and more.
   - Create procedures for various security scenarios, such as password management, device management, and data backup.

3. **Access Control:**
   - Implement strong authentication mechanisms, such as multi-factor authentication (MFA), to enhance user access security.
   - Define roles and permissions for users based on their job responsibilities.
   - Regularly review and update access privileges to ensure the principle of least privilege is followed.

4. **Network Security:**
   - Implement firewalls, intrusion detection/prevention systems, and network segmentation to control and monitor network traffic.
   - Encrypt network traffic using protocols like HTTPS and VPNs, especially for remote access.
   - Regularly update and patch network devices to address known vulnerabilities.

5. **Endpoint Security:**
   - Deploy antivirus, anti-malware, and endpoint protection software to safeguard individual devices.
   - Enforce device encryption and strong password policies for all endpoints.

6. **Data Security:**
   - Classify and label data based on its sensitivity and regulatory requirements.
   - Apply encryption to sensitive data both at rest and during transit.
   - Implement data loss prevention (DLP) mechanisms to prevent unauthorized data leakage.

7. **Incident Response:**
   - Develop a well-defined incident response plan that outlines the steps to be taken in the event of a security breach.
   - Regularly conduct drills and simulations to ensure the team is prepared to handle security incidents effectively.

8. **Security Awareness Training:**
   - Provide regular security training to employees, contractors, and stakeholders to educate them about security risks and best practices.
   - Raise awareness about phishing, social engineering, and other common attack vectors.

9. **Vendor and Third-Party Management:**
   - Assess the security practices of third-party vendors before integrating their services into your infrastructure.
   - Establish security requirements and monitoring mechanisms for third-party relationships.

10. **Continuous Monitoring and Improvement:**
    - Implement security monitoring tools and practices to detect and respond to potential threats in real-time.
    - Regularly review and update your security strategy to incorporate new technologies, threats, and lessons learned from incidents.

11. **Regulatory Compliance:**
    - Ensure that your security strategy aligns with industry-specific regulations and compliance standards that apply to your organization.

12. **Backup and Disaster Recovery:**
    - Maintain regular data backups and test the restoration process to ensure business continuity in case of data loss or system failures.

Remember that a security strategy is not a one-time effort; it requires continuous assessment, adaptation, and improvement to effectively mitigate evolving security threats.

Computer Security Standard

Computer security standards are guidelines, best practices, and specifications developed to establish a baseline level of security for computer systems, networks, and software. These standards are created by various organizations, government bodies, and industry groups to ensure the confidentiality, integrity,

and availability of digital information and resources. They help organizations and individuals in setting up effective security measures and reducing the risk of cyberattacks and data breaches.

Here are some well-known computer security standards:

1. **ISO/IEC 27001 and 27002**: These standards provide a comprehensive framework for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System (ISMS). ISO/IEC 27002 specifically outlines security controls and guidelines.

2. **NIST SP 800-53**: Published by the U.S. National Institute of Standards and Technology (NIST), this document provides guidelines for security and privacy controls for federal information systems and organizations. It covers a wide range of security topics.

3. **PCI DSS (Payment Card Industry Data Security Standard)**: This standard is aimed at organizations that handle credit card transactions. It outlines security requirements to protect cardholder data and prevent data breaches.

4. **HIPAA (Health Insurance Portability and Accountability Act)**: HIPAA sets standards for the protection of sensitive patient health information, mandating security measures to ensure confidentiality and privacy in the healthcare sector.

5. **FISMA (Federal Information Security Management Act)**: This U.S. federal law mandates information security practices for federal agencies and their contractors. It requires agencies to implement risk-based cybersecurity programs.

6. **GDPR (General Data Protection Regulation)**: Although not exclusively a computer security standard, GDPR establishes data protection and privacy requirements for handling personal data of EU citizens. It has implications for how organizations secure and process data.

7. **CIS Critical Security Controls**: Formerly known as the SANS Top 20 Critical Security Controls, these are a prioritized set of actions designed to improve computer security. They are regularly updated to address emerging threats.

8. **OWASP (Open Web Application Security Project)**: While not a standard in the traditional sense, OWASP provides a collection of resources, tools, and guidelines for web application security. It highlights the top web application security risks.

9. **IEEE 802.1X**: This standard defines port-based network access control for Ethernet networks. It is often used for securing Wi-Fi networks and authenticating devices before granting access to the network.

10. **ISO/IEC 15408 (Common Criteria)**: This international standard specifies criteria for evaluating the security of IT products and systems. It defines security requirements and evaluation methodologies.

These are just a few examples, and there are many other standards that cater to specific industries, technologies, and security aspects. Organizations often adopt a combination of these standards to create a comprehensive security posture that aligns with their needs and regulatory requirements.