Dr.Mahalingam College of Engineering and Technology

CCET- II Answer Key

**Name of the Programme:** Mech, Mechatronics, Auto, Civil, ECE

**Semester:** 7

**Course Code & Course Name:** 19ITOC1004 / Cyber Law and Information Security

# Section-A

## 1. Define 802.11 networking standards.

802.11 networking standards: Institute of Electrical and Electronics Engineers (IEEE)-802.11 is a family of standards for wireless local area network (WLAN), stating the specifications and/or requirements for computer communication in the 2.4, 3.6 and 5 GHz frequency bands.

## 2. Justify how 2- way Handshaking is implemented in real time network Communication system.

- Client sends synchronize (syn) packet to web server
- Server sends synchronize acknowledgment (syn-ack)
- Client replies with an acknowledgment packet, the connect is established

## 3. Predict the steps to secure the wireless Network.

- Avoid providing the network a name which can be easily identified
- Connect only to secured wireless network {i.e., do not auto connect to open Wi-Fi hotspots).
- Enable WPA/WEP encryption
- Upgrade router's firmware periodically

## 4. State the purpose of SDLC.

The goal of SDLC is to minimize project risks through forward planning so that software meets customer expectations during production and beyond. This methodology outlines a series of steps that divide the software development process into tasks you can assign, complete, and measure.

## 5. Compare Information security and Cyber security

**Information Security:**

- Keeps information safe, accurate, and available when needed.
- Uses various methods like passwords, locks, and rules to protect all types of information.

**Cybersecurity:**

- Protects computers, networks, and data from online bad things like viruses and hackers.
- Uses special tools like firewalls and antivirus software to keep everything safe online.

## 6. How does authenticity of information play a crucial role in ensuring data integrity and security?

- Authenticity: Authenticity of information is the quality or state of being genuine or original, rather than a reproduction or fabrication.
- Information is authentic when it is in the same state in which it was created, placed, stored, or transferred.

## 7. Specify the need for cyber Security Policies.

- It increases efficiency.
- It upholds discipline and accountability

- It can make or break a business deal
- It helps to educate employees on security literacy

8. **Justify the needs for security.**

- The primary mission of an information security program is to ensure that systems and their contents remain the same.
- Protecting Confidential Information
- Protecting Employee Information
- Protecting Customer Trust

9. **State CFA act.**

- The CFAA is the leading federal law that protects digital information from unauthorized access. The law governs every computer connected to the internet and non-network computers used by the federal government or financial institutions.

**10.Specify the types of law and explain it in short**

- **Civil law** comprises a wide variety of laws that govern a nation or state and deal with the relationships and conflicts between organizational entities and people.
- **Criminal law** addresses activities and conduct harmful to society, and is actively enforced by the state.
- Law can also be categorized as **private or public**.
- **Private law** encompasses family law, commercial law, and labor law, and regulates the relationship between individuals and organizations.
- **Public law** regulates the structure and administration of government agencies and their relationships with citizens, employees, and other governments.

**Section-B**

**11ai) Explain DDoS attack and how to protect from it.**

- In a DDoS attack, an attacker may use your computer to attack another computer.
- By taking advantage of security vulnerabilities or weaknesses, an attacker could take control of your computer.
- He/she could then force your computer to send huge amounts of data to a website or send Spam to particular E-Mail addresses.
- The attack is "distributed" because the attacker is using multiple computers, including yours, to launch the Do$ attack.
- A DDoS attack is a distributed DoS wherein a large number of zombie systems are synchronized to attack a particular system. The zombie systems are called "secondary victims" and the main target is called "primary victim."

**Protect from DDoS attack**

- Implement router filters. This will lessen your exposure to certain DoS accacks.

- If such filters are available for your system, install patches to guard against TCP SYN flooding.
- Disable any unused or inessential network service. This can limit the ability of an attacker to take advantage of these services to execute a DoS attack.
- Enable quota systems on your OS if they are available.
- Observe your system's performance and establish baselines for ordinary activity. Use the baseline to gauge unusual levels of disk activity, central processing unit (CPU) usage or network traffic.

**11.a ii) Describe International Law and Law bodies and its Agreement on Trade related aspects of Intellectual Property Rights.**

The Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), created by the World Trade Organization (WTO) and negotiated over the years 1986–1994, introduced intellectual property rules into the multilateral trade system. It is the first significant international effort to protect intellectual property rights. It outlines requirements for governmental oversight and legislation of WTO member countries to provide minimum levels of protection for intellectual property.

**The WTO TRIPS agreement covers five issues:**

- How basic principles of the trading system and other international intellectual property agreements should be appliedHow to give adequate protection to intellectual property rights
- How countries should enforce those rights adequately in their own territories
- How to settle disputes on intellectual property between members of the WTO
- Special transitional arrangements during the period when the new system is being introduced.

**11.b. i) Predict the steps to secure the wireless Network.**

- Change the default settings of all the equipment's/components of wireless network (e.g., [P address/ user IDs/administrator passwords. ere.).
- Enable WPA/WEP encryption.
- Change the default SSID.
- Enable MAC address filtering.
- Disable remote login.
- Disable SSID broadcast.
- Disable the features that are not used in the AP (e.g., printing/music support).
- Avoid providing the network a name which can be easily identified
- Connect only to secured wireless network {i.e., do not auto connect to open Wi-Fi hotspots).
- Upgrade router's firmware periodically.

- Use Tripwire or a similar tool to detect changes in configuration information or other files

- Invest in and maintain "hot spares" - machines that can be placed into service quickly if a similar machine is disabled.
- Invest in redundant and fault-tolerant network configurations.
- Establish and maintain regular backup schedules and policies, particularly for important configuration information.

**11.b.ii) Explain Software license infringement with an example.**

- software license infringement, or piracy, is routinely covered by the popular press.
- Among study participants, attitudes toward piracy were generally similar; however, participants from the United States and the Netherlands showed significant differences in attitudes from the overall group.
- Participants from the United States were significantly less tolerant of piracy, while those from the Netherlands were significantly more permissive.
- Although other studies have reported that the Pacific Rim countries of Singapore and Hong Kong are hotbeds of software piracy, this study found tolerance for copyright infringement in those countries to be moderate, as were attitudes in England, Wales, Australia, and Sweden.
- This could mean that the individuals surveyed understood what software license infringement was, but felt either that their use was not piracy, or that their society permitted this piracy in some way.
- Peer pressure, the lack of legal disincentives, the lack of punitive measures, and number of other reasons could a explain why users in these alleged piracy centers disregarded intellectual property laws despite their professed attitudes toward them.
- Even though participants from the Netherlands displayed a more permissive attitude toward piracy, that country only ranked third in piracy rates of the nations surveyed in this study.

**12a) Explain the components of Information Security.**

**Software**

- The software component of the IS comprises applications, operating systems, and assorted command utilities. Software is perhaps the most difficult IS component to secure.
- The exploitation of errors in software programming accounts for a substantial portion of the attacks on information.
- The information technology industry is rife with reports warning of holes, bugs, weaknesses, or other fundamental problems in software.
- In fact, many facets of daily life are affected by buggy software, from smartphones that crash to flawed automotive control computers that lead to recalls.
- Software carries the lifeblood of information through an organization. Unfortunately, software programs are often created under the constraints of project management, which limit time, cost, and manpower.
- Information security is all too often implemented as an afterthought, rather than developed as an integral component from the beginning. In this way, software programs become an easy target of accidental or intentional attacks.

**Hardware**

- Hardware is the physical technology that houses and executes the software, stores and transports

the data, and provides interfaces for the entry and removal of information from the system.

- Physical security policies deal with hardware as a physical asset and with the protection of physical assets from harm or theft.
- Applying the traditional tools of physical security, such as locks and keys, restricts access to and interaction with the hardware components of an information system.
- Securing the physical location of computers and the computers themselves is important because a breach of physical security can result in a loss of information.
- Unfortunately, most information systems are built on hardware platforms that cannot guarantee any level of information security if unrestricted access to the hardware is possible.

**Data**

- Data stored, processed, and transmitted by a computer system must be protected.
- Data is often the most valuable asset possessed by an organization and it is the main target of intentional attacks.
- Systems developed in recent years are likely to make use of database management systems. When done properly, this should improve the security of the data and the application.
- Unfortunately, many system development projects do not make full use of the database management system's security capabilities, and in some cases the database is implemented in ways that are less secure than traditional file systems.

**People**

- Though often overlooked in computer security considerations, people have always been a threat to information security.
- People can be the weakest link in an organization's information security program.
- And unless policy, education and training, awareness, and technology are properly employed to prevent people from accidentally or intentionally damaging or losing information, they will remain the weakest link.
- Social engineering can prey on the tendency to cut corners and the common place nature of human error. It can be used to manipulate the actions of people to obtain access information about a system.

**Procedure**

- Another frequently overlooked component of an IS is procedures. Procedures are written instructions for accomplishing a specific task.
- When an unauthorized user obtains an organization's procedures, this poses a threat to the integrity of the information.
- For example, a consultant to a bank learned how to wire funds by using the computer center's procedures, which were readily available.
- By taking advantage of a security weakness (lack of authentication), this bank consultant ordered millions of dollars to be transferred by wire to his own account.
- Lax security procedures caused the loss of over ten million dollars before the situation was corrected.
- Most organizations distribute procedures to their legitimate employees so they can access the information system, but many of these companies often fail to provide proper education on the protection of the procedures.
- Educating employees about safeguarding procedures is as important as physically securing the information system.
- After all, procedures are information in their own right. Therefore, knowledge of procedures, as

with all critical information, should be disseminated among members of the organization only on a need-to-know basis.

**Network**

- The IS component that created much of the need for increased computer and information security is networking.
- When information systems are connected to each other to form local area networks (LANs), and these LANs are connected to other networks such as the Internet, new security challenges rapidly emerge.
- The physical technology that enables network functions is becoming more and more accessible to organizations of every size.
- Applying the traditional tools of physical security, such as locks and keys, to restrict access to and interaction with the hardware components of an information system are still important, but when computer systems are networked, this approach is no longer enough.
- Steps to provide network security are essential, as is the implementation of alarm and intrusion systems to make system owners aware of ongoing compromises.

**12.b.) Enumerate the various phase involved in SDLC.**

**Investigation phase**

- The investigation phase begins with an examination of the event or plan that initiates the process.
- During the investigation phase, the objectives, constraints, and scope of the project are specified.
- A preliminary cost-benefit analysis evaluates the perceived benefits and the appropriate levels of cost for those benefits.
- At the conclusion of this phase, and at every phase following, a feasibility analysis assesses the economic, technical, and behavioral feasibilities of the process and ensures that implementation is worth the organization's time and effort.

**Analysis phase**

- The analysis phase begins with the information gained during the investigation phase.
- This phase consists primarily of assessments of the organization, its current systems, and its capability to support the proposed systems.
- Analysts begin by determining what the new system is expected to do and how it will interact with existing systems.
- This phase ends with the documentation of the findings and an update of the feasibility analysis.

**Logical design phase**

- In the logical design phase, the information gained from the analysis phase is used to begin creating a systems solution for a business problem.
- In any systems solution, it is imperative that the first and driving factor is the business need.
- Based on the business need, applications are selected to provide needed services, and then data support and structures capable of providing the needed inputs are chosen.
- Finally, based on all of the above, specific technologies to implement the physical solution are delineated. The logical design is, therefore, the blueprint for the desired solution.
- The logical design is implementation independent, meaning that it contains no reference to specific technologies, vendors, or products
- At the end of this phase, another feasibility analysis is performed.

**Implementation phase**

- In the implementation phase, any needed software is created. Components are ordered, received, and tested. Afterward, users are trained and supporting documentation created.
- Once all components are tested individually, they are installed and tested as a system. Again a feasibility analysis is prepared, and the sponsors are then presented with the system for a performance review and acceptance test.

**Maintenance and change phase**

- The maintenance and change phase is the longest and most expensive phase of the process.

- This phase consists of the tasks necessary to support and modify the system for the remainder of its useful life cycle.
- Even though formal development may conclude during this phase, the life cycle of the project continues until it is determined that the process should begin again from the investigation phase.
- At periodic points, the system is tested for compliance, and the feasibility of continuance versus discontinuance is evaluated. Upgrades, updates, and patches are managed.
- As the needs of the organization change, the systems that support the organization must also change.
- It is imperative that those who manage the systems, as well as those who support them, continually monitor the effectiveness of the systems in relation to the organization's environment.
- When a current system can no longer support the evolving mission of the organization, the project is terminated and a new project is implemented.