Computer Security

1. Computer Security: Overview

- **Computer/Network Security**: Protects data, devices, and networks from threats, misuse, and unauthorized access.
- **Threats** exploit vulnerabilities to cause harm, steal data, or damage reputation.
- **Total isolation** (offline, not connected) is 100% safe, but not practical today.

2. Malware and Its Types

- **Malware**: MALicious softWARE. Software designed to infiltrate, damage, or steal from systems without user consent.
- **Categories**:
  - **Virus**: Needs a host, spreads by user action (e.g., ILOVEYOU, CryptoLocker).
  - **Worm**: Standalone, spreads itself via network (e.g., Morris Worm, Code Red).
  - **Ransomware**: Locks/encrypts data, demands payment (e.g., WannaCry).
  - **Trojan Horse**: Pretends to be useful, user installs it, opens backdoor.
  - **Spyware**: Secretly collects and sends user data.
  - **Adware**: Displays ads, may lead to more malware.
  - **Keylogger**: Records keystrokes to steal data.
  - **Rootkit**: Hides malware, enables root/admin access.
  - **Logic Bomb/Time Bomb**: Triggers on specific condition or date/time.
  - **Backdoor/Trapdoor**: Secret method for unauthorized access.
  - **Zombie**: Infected machine controlled for attacks (e.g., botnet).
  - **Macro Virus**: Infects files using macros (Word, Excel).
  - **File System Virus**: Alters file directory/path.
  - **Polymorphic Virus**: Changes its code to avoid detection.
  - **Multipartite Virus**: Spreads via multiple methods.
  - **Web Scripting Virus**: Spreads via malicious web code.
  - **Auto-rooter**: Tool for remotely breaking into new machines.
  - **Kit (virus generator)**: Set of tools for creating new viruses.
  - **Spammer/Flooder**: Sends unwanted emails/attacks.

Note: Viruses need a host program; worms do not.

3. Malware Distribution Modes

- **Internet downloads** (often disguised as free software)
- **Spam email** (attachments/links)
- **Removable devices** (USB, SSD, phones)
- **Network propagation** (worms spread automatically)

4. Combating Malware

Signs of infection: Pop-ups, homepage changes, slow PC, unknown programs, missing files, spam from your account.

Prevention:

- Install/update antivirus.
- Configure browser security.
- Use HTTPS for sensitive data.
- Avoid pirated software.
- Regular backups.
- Enable firewalls.
- Don't use public computers for sensitive info.
- Don't click unknown email links/attachments.

- Scan removable devices before use.
- Remove unknown programs.
- Never share passwords/PINs.

5. Antivirus

- **Software** that detects, prevents, removes malware.
- **Detection methods**:
  - Signature-based (matches known virus code).
  - Sandbox (runs suspicious files in isolation).
  - Data mining/AI (classifies by patterns).
  - Heuristics (detects suspicious code).
  - Real-time protection (monitors running programs).

Popular Antivirus: AVG, Avast, Kaspersky, Norton, Bitdefender, McAfee, Panda, Quick Heal.

6. Network Security Threats

- **Denial of Service (DoS)**: Overloads a resource to make it unavailable.
- **Distributed DoS (DDoS)**: Multiple infected computers (botnet) attack together.
- **Snooping**: Secretly records/analyzes network traffic for later use.
- **Eavesdropping**: Real-time interception of private communications.
- **Phishing/Smishing/Whaling**: Deceive users to reveal info.
- **Spoofing**: Fakes identity (IP, DNS, email, website, caller ID).
- **Salami Technique**: Diverts small amounts from many accounts.
- **Hacking/Cracking**: Unauthorized access or breaking protections.
- **Skimming**: Steals card data at ATMs or POS terminals.
- **Spooling**: Temporary storage for execution.

7. HTTP vs HTTPS

- **HTTP**: No encryption; data can be stolen.
- **HTTPS**: Encrypts data (SSL certificate); safe for transactions.

8. Firewall

- **Barrier** (software/hardware) filters traffic between trusted/untrusted networks.
  - **Network Firewall**: Protects networks.
  - **Host-based Firewall**: Protects individual devices.
- Can block/allow by user, device, app.

9. Cookies

- **Small files** stored by websites for session management, preferences, autofill, etc.
- **Risks**: Tracking, supercookies, zombie cookies (reappear after deletion).

10. Hackers and Crackers

- **White hats**: Ethical hackers (test, secure).
- **Black hats**: Unethical, harm/gain.
- **Grey hats**: Hack for fun/challenge.

11. Other Security Terms

- **Botnet**: Group of infected computers (zombies) used for attacks.
- **Piggybacking/War driving**: Unauthorized use of Wi-Fi.
- **Pharming**: Redirects user to fake sites.
- **Patch**: Update to fix security flaws.
- **Brute-force**: Tries many passwords rapidly.
- **IDS**: Intrusion Detection System.

12. Security Solutions

- **Antivirus**: Detects/removes malware.
- **Digital Certificate**: Verifies sender/receiver identity.
- **Digital Signature**: Authenticates sender/ensures content integrity.
- **Firewall**: Monitors/filters network traffic.
- **Passwords**: User authentication.
- **File Access Permissions**: Restricts read/write/execute rights.

13. Types of Attacks

Passive Attack:

- Does not affect system resources.
- Goal: Eavesdrop, monitor, traffic analysis.

Active Attack:

- Alters system resources/data (masquerade, replay, message modification, DoS).

14. Glossary

- **Authentication**: Confirming user/device identity.
- **Encryption/Decryption**: Coding/decoding data.
- **Piracy**: Unauthorized copying/distribution of software.
- **Pen-testing**: Authorized hacking to test security.
- **Sanitization**: Removing sensitive data before disposal.

15. Questions and Answers

A. Short Q&A

1. **Malicious software that replicates itself without a host program?**
   Answer: Worm
2. **Which malware encrypts user data and demands payment?**
   Answer: Ransomware
3. **Safest way to ensure no external attack?**
   Answer: Isolation (offline computer)
4. **Software that detects/removes viruses?**
   Answer: Antivirus
5. **Unwanted emails sent in bulk?**
   Answer: Spam
6. **Protocol that encrypts browser-server data?**
   Answer: HTTPS
7. **Ethical hacker?**
   Answer: White hat
8. **Unethical hacker for gain/harm?**
   Answer: Black hat
9. **Small files that websites store to remember info?**
   Answer: Cookies
10. **Barrier between trusted/untrusted networks?**
    Answer: Firewall
11. **Program that records keystrokes?**
    Answer: Keylogger
12. **Malware disguised as legitimate software?**
    Answer: Trojan
13. **Real-time interception of private communication?**
    Answer: Eavesdropping

14. **Unauthorized analyzing/storing of network traffic?**
    Answer: Snooping
15. **Malware that shows unwanted ads?**
    Answer: Adware
16. **Common email-based malware distribution?**
    Answer: Attachment
17. **Firewall on individual device?**
    Answer: Host-based firewall
18. **Spam that tricks users for info?**
    Answer: Phishing
19. **Flooding server with requests from many computers?**
    Answer: DDoS
20. **Collection of infected computers for attack?**
    Answer: Botnet
21. **Unauthorized viewing of computer screen/keyboard?**
    Answer: Shoulder-surfing
22. **Coding data to prevent unauthorized access?**
    Answer: Encryption
23. **Opposite of encryption?**
    Answer: Decryption
24. **Unauthorized network access?**
    Answer: Intruder
25. **Unique string for authentication?**
    Answer: Password
26. **Fake email to steal info?**
    Answer: Phishing
27. **Program that appears useful but is malicious?**
    Answer: Trojan
28. **Malware that replicates/spreads to other computers?**
    Answer: Virus
29. **Security software for network access control?**
    Answer: Firewall
30. **Person who explores systems for fun/challenge?**
    Answer: Hacker

B. Multiple Choice Questions (MCQ)

1. Name the recent spyware that can stealthily enter a smart phone and gain access to everything?

(1) Ransomware (2) Trojan Horse (3) Wannacry (4) Pegasus

Answer: (4) Pegasus

2. Pegasus spyware enters which OS?

(1) Android (2) Blackberry (3) iOS (4) All of these

Answer: (4) All of these

3. Who developed Pegasus spyware?

(1) DARPA (2) ISO (3) NSO (4) CERN

Answer: (3) NSO

4. Pegasus discovered in?

(1) 2014 (2) 2015 (3) 2016 (4) 2019

Answer: (3) 2016

5. Unethical hacker/security cracker?

(1) Black Hat Hacker (2) White Hat Hacker (3) Grey Hat Hacker (4) Orange Hat Hacker

Answer: (1) Black Hat Hacker

6. Ethical hacker/penetration tester?
(1) Black Hat Hacker (2) White Hat Hacker (3) Grey Hat Hacker (4) Orange Hat Hacker
Answer: (2) White Hat Hacker

7. Hacks systems for challenge, never harms?
(1) Black Hat Hacker (2) White Hat Hacker (3) Grey Hat Hacker (4) Orange Hat Hacker
Answer: (3) Grey Hat Hacker

8. Malware that does not self-replicate?
(1) Worms (2) Trojans (3) Viruses (4) Rootkits
Answer: (2) Trojans

9. Key logger is?
(1) Firmware (2) Antivirus (3) Spyware (4) Firmware
Answer: (3) Spyware

10. Firewalls protect against?
(1) Data driven attacks (2) Fire attacks (3) Virus attacks (4) Unauthorized access
Answer: (4) Unauthorized access

11. Logic bomb activated by time event is?
(1) Virus (2) Trojan horse (3) Hacking (4) Time bomb
Answer: (4) Time bomb

12. Altering data so it's unusable unless undone?
(1) Ergonomics (2) Compression (3) Biometrics (4) Encryption
Answer: (4) Encryption

13. VIRUS stands for?
(1) Very Intelligent Result Until Source
(2) Very Interchanged Resource Under Search
(3) Vital Information Resource Under Seize
(4) Viral Important Record User Searched
Answer: (3) Vital Information Resource Under Seize

16. Important One-Liners

- **First computer virus**: Creeper (1971, Bob Thomas)
- **First ransomware**: AIDS Trojan (1989, Joseph L. Popp)
- **ILOVEYOU virus**: Love Bug, 2000, Onel De Guzman
- **First boot sector virus in India**: Brain (1986)
- **Popular antivirus HQs**:
  AVG/Avast: Prague, Kaspersky: Moscow, Norton: USA, Bitdefender: Romania, Quick Heal: Pune (India)
- **Most ATMs use**: AES/Triple DES encryption
- **WPA2**: Used for Wi-Fi security