**IT Infrastructure Management**

**Week 8 Assignment**

1. List the classification of various Trojan horses.

## Answer 1: Trojan Horses

Trojan horses are malicious programs that disguise themselves as legitimate or useful software to trick users into installing or running them. They can perform various harmful actions on the infected computer, such as stealing data, deleting files, opening backdoors, installing other malware, etc. Unlike viruses or worms, Trojan horses do not have the ability to self-replicate or spread to other computers.

**Classification of Trojan Horses**

There are different ways to classify Trojan horses based on their characteristics, functions, or behaviors. One possible classification is:

* **Backdoor Trojans**: These are Trojans that create a hidden access point on the infected computer that allows remote attackers to control or monitor the system. They can also download or upload files, execute commands, launch attacks, etc.
* **Exploit Trojans**: These are Trojans that exploit a known vulnerability in an application or an operating system to gain access or privileges on the infected computer. They can also deliver other malware or payloads to the system.
* **Rootkit Trojans**: These are Trojans that hide themselves or other malware from detection by modifying the system files, processes, registry, or drivers. They can also intercept system calls, network traffic, or user input.
* **Downloader/ Dropper Trojans**: These are Trojans that download or drop other malware onto the infected computer. They can also update themselves or other malware remotely.
* **Banking Trojans**: These are Trojans that target online banking users and try to steal their credentials, account information, or money. They can also modify web pages, redirect traffic, capture keystrokes, etc.

Some other types of Trojans are:

* **Ransom Trojans**: These are Trojans that encrypt or lock the user’s files or system and demand a ransom for their decryption or release.
* **Spyware Trojans**: These are Trojans that collect and send the user’s personal or sensitive information, such as passwords, credit card numbers, browsing history, etc., to a remote server.
* **Clicker Trojans**: These are Trojans that generate fraudulent clicks on online advertisements or links to generate revenue for the attackers.
* **Notifier Trojans**: These are Trojans that notify the attackers when the infected computer is online or when certain events occur on the system.
* **Proxy Trojans**: These are Trojans that use the infected computer as a proxy server to relay or hide the source of malicious traffic.

2. List the categories of cryptographic algorithms and explain them.

## Answer 2: Cryptographic Algorithms

Cryptographic algorithms are mathematical procedures that are used to perform encryption and decryption of data. Encryption is the process of transforming plain text (readable data) into cipher text (unintelligible data) using a key (a secret value). Decryption is the reverse process of transforming cipher text back into plain text using the same or a different key.

There are three main categories of cryptographic algorithms:

* **Symmetric-key algorithms**: These are algorithms that use the same key for both encryption and decryption. The key must be shared securely between the sender and the receiver of the message. Symmetric-key algorithms are fast and efficient, but they have the drawback of key distribution and management. Some examples of symmetric-key algorithms are Data Encryption Standard (DES), Advanced Encryption Standard (AES), Triple DES (3DES), Blowfish, etc.
* **Asymmetric-key algorithms**: These are algorithms that use a pair of keys for encryption and decryption. One key is called the public key, which can be shared openly, and the other key is called the private key, which must be kept secret. The public key is used to encrypt the message, and the private key is used to decrypt it. Alternatively, the private key can be used to sign the message, and the public key can be used to verify it. Asymmetric-key algorithms are more secure and flexible than symmetric-key algorithms, but they are slower and more complex. Some examples of asymmetric-key algorithms are Rivest-Shamir-Adleman (RSA), Diffie-Hellman, Elliptic Curve Cryptography (ECC), etc.
* **Hash functions**: These are algorithms that map any input data (of any size) to a fixed-length output data (called a hash or a digest). Hash functions are one-way functions, which means that it is easy to compute the hash from the input, but it is hard to find the input from the hash. Hash functions are used to ensure the integrity and authenticity of data, but not to encrypt or decrypt it. Some examples of hash functions are Message Digest 5 (MD5), Secure Hash Algorithm 1 (SHA-1), SHA-2, SHA-3, etc.

3. Highlight the importance of cryptography.

## Answer 3: Cryptography

Cryptography is the science and art of designing and using methods to protect information and communication from unauthorized access, modification, or disclosure. Cryptography relies on mathematical principles and algorithms to transform plain text (readable data) into cipher text (unintelligible data) and vice versa. Cryptography also provides mechanisms to ensure the integrity, authenticity, and non-repudiation of data.

**Importance of Cryptography**

Cryptography is important for various reasons, such as:

* **Privacy and confidentiality**: Cryptography enables individuals and organizations to keep their data and conversations private and confidential from prying eyes or eavesdroppers. By encrypting the data with a secret key, only the intended recipient can decrypt it with the same or a different key. For example, messaging apps like WhatsApp use end-to-end encryption to secure the communication between users.
* **Authentication and identity**: Cryptography enables individuals and organizations to verify the identity and authenticity of the sender and receiver of data. By using digital signatures, certificates, or public-key encryption, one can prove that they are who they claim to be and that the data has not been tampered with. For example, websites use SSL/TLS certificates to establish a secure connection between the browser and the server.
* **Integrity and non-repudiation**: Cryptography enables individuals and organizations to ensure that the data has not been altered or corrupted during storage or transmission. By using hash functions, checksums, or digital signatures, one can detect any changes or errors in the data. Cryptography also prevents the sender or receiver from denying their involvement in the communication or transaction. For example, blockchain technology uses cryptography to create an immutable ledger of transactions that cannot be disputed or reversed.
* **Key exchange and distribution**: Cryptography enables individuals and organizations to securely share and distribute cryptographic keys that are needed for encryption and decryption. By using protocols such as Diffie-Hellman, RSA, or ECC, one can generate and exchange keys without exposing them to third parties or adversaries. For example, VPNs use cryptography to create encrypted tunnels between devices that share a common key.

4. Compare any Four antivirus software and list all the features and functionalities supported by them.

## Answer 4: Antivirus Software

Antivirus software is a type of software that protects your computer from various types of malware, such as viruses, worms, ransomware, spyware, etc. Antivirus software can perform various functions, such as scanning, detecting, removing, blocking, or preventing malware infections. Antivirus software can also offer additional features, such as firewall, VPN, password manager, parental control, etc.

**Antivirus Software Comparison**

Here is a table that compares four popular antivirus software based on their features and functionalities. The table is based on the information from the websites of the antivirus software and the reviews from PCMag, TechRadar, Forbes Advisor, and SafetyDetectives.

| **Antivirus Software** | **Features** | **Functionalities** |
| --- | --- | --- |
| Norton | - Real-time protection against malware - Firewall and network protection - Secure VPN - Password manager - Cloud backup - Parental control - Dark web monitoring - Identity theft protection - SafeCam - LifeLock identity alert system (US only) | - Scans files, folders, drives, and removable media for malware - Detects and removes malware infections - Blocks malicious websites, downloads, and phishing emails - Encrypts and anonymizes online traffic with VPN - Stores and autofills passwords securely - Backs up important files to the cloud - Monitors and controls children’s online activities - Alerts users of personal information exposed on the dark web - Protects users from webcam hacking - Alerts users of potential identity theft and offers restoration services |
| Bitdefender | - Real-time protection against malware - Firewall and network protection - Secure VPN - Password manager - Anti-tracker - Webcam protection - Microphone monitor - File shredder - Safe online banking - Parental control | - Scans files, folders, drives, and removable media for malware - Detects and removes malware infections - Blocks malicious websites, downloads, and phishing emails - Encrypts and anonymizes online traffic with VPN - Stores and autofills passwords securely - Blocks online trackers and ads - Protects users from webcam hacking - Alerts users of microphone access by apps - Deletes files permanently without leaving traces - Secures online transactions with a dedicated browser - Monitors and controls children’s online activities |
| McAfee |  |  |

* Real-time protection against malware
* Firewall and network protection
* Secure VPN
* Password manager
* Identity theft protection
* Safe web browsing
* Performance optimization
* Encrypted storage
* Home network security
* Parental control

|

* Scans files, folders, drives, and removable media for malware
* Detects and removes malware infections
* Blocks malicious websites, downloads, and phishing emails
* Encrypts and anonymizes online traffic with VPN
* Stores and autofills passwords securely
* Alerts users of potential identity theft and offers recovery services
* Warns users of risky websites and downloads
* Boosts PC speed and battery life
* Protects sensitive files with encryption
* Secures home Wi-Fi network from intruders
* Monitors and controls children’s online activities