Assignment (Lec. 17 & 18): Distributed Operating System Principles (COP5615)

Name: Vikas Chaubey**, UFID:** 3511 5826**, Email:** vikas.chaubey@ufl.edu

1) **Security Threats:** Different types of security threats to the system:

   a. **Interception:** when an unauthorized party, person or different computing system gains access to the asset then it is called interception. for example, the intruder can steal the program or valuable data, also networks could be wiretapped to obtain the data. Sometimes the intruding party do not leave any trace hence it becomes very difficult to trace interception.

   b. **Interruption:** An interruption occurs in the system when any service or asset of the system is unusable or unavailable. For example, an operating system manager is not able to find a file on the disk could be counted as interruption.

   c. **Modification:** In case of interception when an unauthorized intruder gets access to a system asset and then it tempers with it then the threat is categorized as modification. For example, data from database could be stolen and could be changed.

   d. **Fabrication:** In this case an intruder might put or insert counterfeit objects in computing system. For example, a data base could be tempered, and fake records or transactions could be inserted.

2) **Intrusion Detection:** An intrusion detection system could be used to detect the intrusions made in the computing system network in order to avoid security threats. These types of system monitor the network for any possible security issue and issue alerts in case of any detection. This reporting is done to the system administrator or they are collected using a management system called security information and event management. This system uses filtering techniques to differentiate between the activity from false alarms. There might be some cases of false alarms. Hence these systems need to be fine-tuned with the system in order to identify the threats, The IDS should clearly identify a normal functioning system from a breached system.

3) **Encryption:** Encryption is a way of encoding original data or scrambling data which is called "plain text" into a form which is unreadable by another entity who does not know how to decode it. The encoded data is called "cipher text". Encryption helps securing the digital data from security threats. An encryption algorithm uses a pseudo random encryption key to encode data. On the reception end the key is known in advance and could be used to decrypt the data.

   a) **PGP Encryption:** PGP is Pretty Good Privacy encryption technique which is used to secure online communication such as emails, text and other files. PGP does data encryption using a mix of data compression, hashing and public key. For data encryption It also uses symmetric and asymmetric keys to encrypt the computation data. PGP compresses the plain text before encrypting it. After public keys have been traded among partners, the private keys are used to digitally sign the encrypted content.

b) **Deffie Hellman Algorithm:** In the secured encrypted communication, It is required that the two communicating ends first exchange the encryption keys in order to decode the encoded data. However, deffie hellman algorithm allows two parties to share the encryption key over a channel which is not secure without having prior knowledge of each other by the parties. This key can then be used to encrypt subsequent communications using a symmetric key cipher.

4) **Symmetric encryption:** In this type of data encryption electronic data is encrypted and decrypted using the same key. But since the same key is used in both processes at both ends hence the parties involved in communication need to exchange the key in advance in order to encrypt and decrypt the data. This encryption is different than asymmetric encryption where a pair of public and private keys are used for data encryption.

a) AES (Advanced Encryption Standard): AES – 128 uses 128 bits long key to encrypt and decrypt the data. Like AES 128, other variants like AES 192, AES 256 also use 192 bits and 256 bits long keys however the encryption and decryption of data takes place in size of 128 bits. There are several rounds of processing steps involved in conversion of plain text to cipher text. These rounds consist of processes like substitution. transposition and mixing techniques to get the final encoded cipher data.

b) DES (Data Encryption Standard): DES uses 64-bit long encryption keys, however only 56 bits are used by the DES algorithm. every 8th bit is used as a parity bit. This encryption process first divides the data into 64 bits of blocks. There are several rounds of processing steps involved in conversion of plain text to cipher text. These rounds consist of processes like substitution. transposition and mixing techniques to get the final encoded cipher data.

5) Secure Hash Algorithms: Secure Hash Algorithms are also called SHA, these algorithms are used to secure the data. These algorithms encode the plain text using the hash functions, the encoding process involves bitwise operations, compression functions and modular additions. SHA is a one-way algorithm that means once the data is encrypted or transformed it cannot be transformed into its original forma. Few examples of SHA algorithms which are used are SHA1, SHA2, SHA3 etc. SHA algorithms are commonly used to encode the passwords.

6) Public Key Cryptography: Public key cryptography is also known as asymmetric cryptography. It involves the encryption algorithm which uses two separate keys to encrypt and decrypt the data. In the network when a user wants to encrypt the data then it obtains the public key from the directory and encrypts the data. This encrypt key is used to encrypt the message and send it to the recipient. once the data is received by the recipient then it decrypts the data using the private key.