Assignment (Lec. 19 & 20): Distributed Operating System Principles (COP5615)

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

1) **Secure Channels:** In the distributed system communication between client and server machines could be protected using secured channels. These channels could be adjusted by the transmitter and receiver processes as per requirement. Secure channels provide protection against cyber-attacks such as information tracking by third parties, forged messages, and message interception. Secure channels provide confidentiality for the communication happening between two processes hence it improves privacy and security of the distributed system's communication line. In order to implement secure channel communication line, the transmitter and receivers have to follow certain protocols for mutual authentication and message integrity.

2) **Mutual Authentication and Message Integrity:** Authentication and message integrity are the two very important factors of secure communication among clients and servers in distributed system. A communication channel is not fully secure till it incorporates both of these features. For example, suppose if a channel provides message integrity i.e. encrypted messages but not authentication then such system is prone to security issues. Similarly, a system without message integrity that only incorporates authentication cannot guarantee safety of communicated messages among the transmitters and receivers. Generally, message integrity is maintained by encryption, the messages are encrypted using an encryption key, this key is again used by the receivers to decode the messages, message encryption protects messages from being interpreted by cyber attackers in case even if they are intercepted. Authentication is generally done by a session key, both transmitter and receiver share this secret session key, this key is used to establish and authenticate the communication channel.

3) **Different Authentication Methods:** Below are different types of authentication method used in distributed system:

    a. **Authentication Using Shared key:** This authentication utilizes the wired equivalent privacy (WEP) protocol. In this protocol a WEP encryption key should be matched in order to authenticate the connecting clients with the server. This encryption key is stored at both ends, transmitter and receiver. In order to establish a connection, a client send a request to the sever, when the server receives the connection request by the client then the server responds to client by sending a character sequence message to the receiver, this message is called a "challenge". When this message sequence is received by the receiver access point then it encrypts the sequence using its WEP encryption key and send the encrypted sequence to the transmitter. When transmitter receives the sequence, it decrypts it using the WEP encryption key again. If the decrypted character sequence matches the original character sequence which was sent by the transmitter previously then the transmitting server accepts the connection request made by the access point at the receiving end. If the character sequence is not matched with original, then connection request is declined.

b. **Authentication Using Key distribution center:** In a distributed system a key distributed system could be used in order to manage secure communication channels among the different end points. that takes away the overhead of managing the encryption keys and communication channel from the endpoints. A key distribution center is a standalone component in the access control system, this system can assign resources by giving tickets and session keys to different participating machines in the system. This system uses cryptographic techniques to authenticate users, obtain the permissions given to that user machines and grant them tickets and session keys as per requests. In this authentication method an access point A which wants to communicate with access point B first connects with KDC system and requests a connection with end point B. Then KDC respond to the end point A sends an encryption key to the end point in order to communicate with machine end point B. This key is also sent to machine B by KDC.

c. **Authentication using public key encryption:** The public key encryption method of authentication is based on public key or asymmetric cryptography. In this cryptography technique the messages are. Encrypted and decrypted using different keys unlike other authentication methods which utilize only one encryption key. The main drawback of previous methods of authentication is that the keys encryption key is shared among the end points. This same key could be used to encrypt and decrypt the messages. Sharing of these encryption keys on unreliable networks is not a good idea. Public key encryption provides a solution for this problem, in this type of authentication each access point in distributed system has to generate a pair of keys, one public key and another one is a private key. The public keys are used to encrypt the message and private keys are used to decrypt the messages. The public keys associated with each end points could easily be shared among the machines without any concern. Private keys are private to specific access points, they are never shared. The access points encrypt the messages by using the public keys of other end points to which message has to be conveyed, then these messages could only be decrypted by using the private keys of the receiving machines. Hence any other machine other than actual recipient cannot decrypt the message.

4) **Secure group communication:** A secure group communication allows the group members to establish multicast or point to point communication with other members in the group. Different processes or members might join or leave the group. As group members leave the group or new members join the group this information is given to all the existing members. In a secure group only, those members are allowed to join which are trusted and authenticated. In the secure group communication, the integrity and confidentiality of the messages is maintained. The group keys are switched and changed every single time the new members join, or when the members leave the group. Different members of the group write their trust policy to a list called access control list. Members should be allowed to change their access control list. This communication maintains the forward and backward confidentiality policy i.e. the past members cannot access the future keys

used in the system for communication similarly future members can not access the past keys used by past members.

References:

1) http://www.hrpub.org/download/20150301/CSIT3-13503378.pdf
2) https://www.ssh.com/manuals/server-zos-product
3)https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.186.8532&rep=rep1&type=pdf
4) https://www.khanacademy.org/computing/computers-and internet/