Assignment (Week 11/9-11/13): Distributed Operating System Principles (COP5615)

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

1) **Hardware encryption:** Encryption is a way of increasing security and making the data safe from external threats of theft and security breach. Encryption could be done using software or hardware implementation. The question is what kind of implementation should be used in what situation, generally it depends on how much security is required in the distributed system. When large volumes of data need to be secured and protected then in that case hardware encryption makes more sense than software encryption. In case of hardware encryption if a fast microcontroller is used for encryption, then data processing is even faster than software encryption. Hardware encryption can avoid the problems of data processing by the core. Hardware encryption can provide better real time system performance. A hardware encryption costs more than a software encryption. hence system should be evaluated for tradeoffs among time, space and cost to choose a specific scheme. However, in general hardware encryption is used to secure large volumes of data on the other hand software encryption could be used in case of authentication, keys exchanges and protocols setups.

    a) **AES Encryption Algorithm:** AES stands for advanced encryption standard; AES is used in both software and hardware type of encryption. Nowadays the more popular and widely used symmetric encryption algorithm is AES algorithm. AES is faster many times than DES (Data Encryption Standard). AES is an iterative cipher. It consists of various operations which involve replacing the inputs with specific outputs and it also involves shuffling of bits. AES performs all its operations on bytes rather than performing them on bits. It treats 128 bits of plaintext as 16 bytes. These 16 bytes are arranged in four rows and columns to process it as a matrix. AES algorithm makes use of 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and then 14 rounds for 256-bit keys. In Each round AES makes use of a different 128-bit round key, this round key is calculated using original AES key.

    b) **AES Instruction Set:** An Advanced Encryption Standard instruction set is integrated with different processors to perform encryption and decryption of data. The main purpose of the AES instruction set is to improve the performance and speed of the applications which are performing encryption and decryption using AES algorithm. These instructions implement the single round of AES algorithm. for example, instructions like AESENC, AESENCLAST performs one round and last round of an AES encryption, AESDEC and AESKEYGENASSIST performs one round and last round of an AES decryption flow, AESKEYGENASSIST is used to generate AES round key and AESIMC is used to inverse mix columns

2) **Public key authentication:** 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.

3) **Digital Signatures:** Digital signatures are used to validate and authenticate the integrity of software, message or digital documents. Digital signatures work in similar fashion as handwritten signature or stamps, but they are used in the case of digital documents and they offer better security. In digital communication the problem of documents tampering could be solved using digital signatures. In various countries the digital signatures are considered to be legal bindings that means they are legally accepted in various legal processes. The digital signatures make use of public key cryptography. Public key authentication could be used to generate two mathematically related public and private keys. Digital signature makes use of these keys to perform authentication. The person who is creating the digital signature uses their own private key to encrypt the digital data and this data could only be decrypted using the public key of that person. However, in order for digital signatures to remain unique the users have to keep their personal key private. if it is accessed by any other person it could be used to create fraudulent digital signatures.

4) **Zero-day exploits:** A zero-day vulnerability is basically a software, firmware or hardware flaw which is there since its release, but it is unknown to the parties creating or fixing that unit. These vulnerabilities if exploited by hackers could produce serious harms to the software or firmware systems before anyone realizes that they exist or fix them. A zero attack happens when the hackers exploit the zero-day vulnerability of the system and release the malware to hack the system before the developers could create a patch and fix the problem. These types of zero-day exploits are very dangerous because they might be hidden for days, months or sometimes years before the exploit or threat is actually detected.

5) **MapReduce: simplified data processing:** MapReduce is a programming model which is used to process or generate large datasets, these datasets could be used in large number of real worlds tasks.in this model the computations are represented in terms of map and a reduce function. A map function can process a key value pair and generates a set of intermediate key value pairs, on the other hand a reduce function can merge all the intermediate values which are associated with same intermediate key. The run time system can parallelize the computation across the cluster to make efficient use of network computation capacity.

6) **Distributed File System:** A distributed file system is a system which is distributed across multiple machines in a cluster in different locations. DFS system allows the programs to store or access a file stored across the machines in cluster network. This system allows users from physically distributed systems to share their data and resources by using a common file system. Location transparency and redundancy are the main two components of distributed file systems. In case of any failure these components provide data availability by sharing data in different locations to be logically grouped under one folder, this folder locations is called “DFS root”. The main features of DFS systems are transparency, high availability , high performance and simplicity and ease of use.

References:

1) https://www.crucial.com/support/articles-faq-ssd/overview-hardware-encryption
2) https://www.maximintegrated.com/en/design/technical-documents/tutorials/5/5421.html
3) https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm
4) https://searchsecurity.techtarget.com/definition/digital-signature
5) https://www.fireeye.com/current-threats/what-is-a-zero-day-exploit.html
6) https://static.googleusercontent.com/media/research.google.com/en//archive/mapreduce-osdi04.pdf
7) http://cacs.usc.edu/education/cs653/Dean-MapReduce-CACM08.pdf
8) https://www.geeksforgeeks.org/what-is-dfsdistributed-file-system/