**Unit 3: Operating and Distributed System Security**

Welcome to Week 3. This week, you will be introduced to several different models and tools used to secure distributed systems and operating systems, with a view to appreciating the ways in which technologies are deployed, and therefore the security mechanisms required.

We will review several security models – including the Saltzer and Schroeder model – and look at how it has affected the security tools utilized to secure modern systems.

**On completion of this unit, you will be able to:**

Understand the core objectives of implementing secure mechanisms to support communications in distributed systems, including confidentiality, integrity, and availability.

**Reflection:**

A **distributed system** is one in which the various system components reside on separate computers that are networked together. These computers may coordinate their actions and communicate with one another by exchanging messages from any system.

**Security models** are employed to design the guidelines and procedures that ensure data is kept private, secure, and in its original form. A security model explains crucial features of security and how they influence the overall efficiency of the operating system. Without reliable and efficient security models, no company can guarantee the safety of their confidential data and information (National Computer Security Center (U.S, 1993).

A distributed system's primary objective is to facilitate the secure and convenient sharing of remote resources among multiple users. Resources might be everything from printers and storage spaces to databases, files, websites, and networks.

When building and deploying systems, it is important to keep in mind the obstacles that ensuring security in a distributed system presents. Information may be at danger not only on a hacked computer or network, but also on other devices or networking devices (Bos, 2020).

As we know that between the communication, we must need security of the specific medium or transmission resource through which the data is passing. While transmitting the data we must keep the following mechanism UNF. (n.d.).

* **Confidentiality:** To protect the privacy of the information, only authorized parties are able to view it.
* Data **integrity** demands that only authorized users can make modifications to the data.
* **Availability:** Data must be made available to the right people or groups in order to be considered "available."

**References:**

Bos, S. (2020). *What Is a Distributed Application?* [online] JRebel by Perforce. Available at: https://www.jrebel.com/blog/distributed-application [Accessed 20th Aug. 2022].

National Computer Security Center (U.S (1993). *A Guide to understanding security modeling in trusted systems.* Fort George G. Meade, Md: National Computer Security Center.

Splunk. (n.d.). What Are Distributed Systems? Retrieved from Splunk website: https://www.splunk.com/en\_us/data-insider/what-are-distributed-systems.html

UNF. (n.d.). Distributed System Security. Retrieved August 20, 2022, from www.unf.edu website: https://www.unf.edu/~sahuja/cis6302/security.html#:~:text=Confidentiality%3A%20Requires%20that%20the%20data  [Accessed 20th Aug 2022].