Distributed systems security

Technology, Information Technology

Distributed Systems Security

Introduction

The efficiency of internet access to the majority has paved way for new possibilities on the sharing of information. This has also been faced by several challenges in terms of scale and security. When designing a distributed file sharing system, one has to consider a design system that meets the following major challenges (Borghoff, 1992). A good distributed file sharing system has designs considerations such as:

- Untrusted storage devices
- No central manager or client communication
- Independent security domains
- Strong mutual authentication

The system being a shared file distributed system data must be stored on the network for easier access by other clients on the network. However in this system one should make sure that the data storage devices are secure and trusted. Client and data encryption are highly recommended on the storage devices which means that corresponding blocks of data corresponds both in the directory and the file but does not know content interpretation, below are the various methods of ensuring secure distributed file system.

Secure file servers

The initial secure distributed file sharing system was the use of AFS which was later followed by the use of DFS. In the AFS system, servers store data on sub trees in the file system and use the Kerberos in the provision of the authenticated access to all trees. Every server is the one in management of the meta-data which has full access to the file data. The DFS advanced in the option link in the encryption level in order to prevent the eavesdroppers from the discovery of file systems content (Kistler, 1995). This file server has improved the security of the NFS by providing the ability to encrypt the traffic in between the server and its clients by doing a strong authentication; the NFS has access to data by managing the entire file server.

Login

The security of a distributed file system calls for the use of unique and assigned id for every user in the system. This name must be used in line to a password created in the system, which helps the user to gain access in the system. This prevents unauthorized users to go into the system.

Authentication

Distributed file systems requires a security protocol to check and verify the login names and password on protection to the systems file from illegal access, this makes the system to improve its security.

Access control

Every user on the system must have a personal profile in which allows them to gain access to certain areas of the programs and files within the distributed system. This protocol assists in keeping the system’s information and data confidential.

System design

The major role of a good system design is to address the security shortcomings in a distributed file system by preserving the performance and the flexibility of a distributed file system (Swain, 1998). In the design factor, factors such as the processor speed of the systems determine the amount of time required by both the server and the client. By doing so, the distributed file system is a secure because the interaction between the client and the server is synchronous and interactive one.

References

Borghoff, U. M. (1992). Catalogue of distributed file/operating systems. Berlin: Springer-Verlag.

Kistler, J. J. (1995). Disconnected operation in a distributed file system. New York: Springer.

Swain, K. (1998, July 26). What Is Security in Distributed Systems? | eHow. com. eHow | How to Videos, Articles & More - Discover the expert in you. | eHow. com. Retrieved March 4, 2013, from http://www. ehow. com/facts_7679246_security-distributed-systems. html