Securing a Distributed System

Distributed systems have been becoming more and more popular and widely used in different domains. At the same time, the security and reliability of distributed systems has become more important. The security considerations for a distributed system can be categorized as follows:

- Hardware: computers
- Software: software applications

Although hardware security methods—like keys, locks, security cards, and so on—are important, they are not the main focus. The main focus is on how to develop a secure distributed application.

Common Requirements

A distributed system may have security requirements. Often times, these will be application dependent and depend upon business needs. A small retail store is going to have different security needs than a large national chain. However, there are still some common requirements or methods that should be considered when building a securely distributed system.

Dedicated functionality is the first consideration or requirement for a security system. For example, if the database server is installed on a client’s interface/application server, the data can very easily be attacked.

A distributed system should be developed and deployed around the services or functions of the distributed environment. For instance, a database server should be built to offer database services and only accessed through a specific interface. Thus, enhanced security can be provided based on server customization.

Confidentiality is another common security requirement for distributed systems. In a distributed environment, there is a lot of communication between the distributed components over the network. The messages exchanged between the distributed components must not be readable to unintended entities. The common method used to secure data confidentiality is cryptography. Through this method, data are encrypted into unreadable data (secret-form data) and then delivered through a public network. This process is called encryption. The encrypted data are unreadable without prior knowledge of a secret key. When the secret-form data arrives at the destination, it can be decrypted into original readable data by using the secret key. This reverse process is called decryption.

Access control refers to the process with which the system only grants suitable access rights to legitimate users and is an important requirement or method for distributed system security. Therefore, it is important to figure out who should be allowed access to the system. Also, the system should have an authentication process to verify a
claimed identity. For example, passwords may be set up, and the system will check the passwords before allowing access to anyone.