Security in Distributed System

P K Mudholkar
Lecturer,TIMSCDR
University of Mumbai, Mumbai-400101
Mob. No. 9324600672
pankaj.mudholkar@thakureducation.org

M Mudholkar
Lecturer, TCET
University of Mumbai, Mumbai-400101
Mob. No.9220703083
megha.kunte@thakureducation.org

ABSTRACT

Security is the very important principle of distributed systems. Security in distributed systems can be divided into two parts. One part concerns the communication between users and processes, possibly residing on different machines. The principal mechanism for ensuring secure communication is that of a secure channel and via authorization.

In this research paper, we focus on the study of several encryption algorithms for security in distributed systems. The RSA algorithm has some important parameters affecting its level of security. It is shown here that increasing the modules length plays an important role in increasing the complexity of decomposing it into its factors.

This will increase the length of the public key and the length of the encrypted message making it more difficult to be decrypted without knowing the decryption key. However the public key length has no major affect on the private key length. When the length of the message is changed then the length of the encrypted message will proportionally change, hence larger chunks are selected to obtain larger encrypted message to increase the security of the data in use.

Categories and Subject Descriptors

C.2.4 [**Computer-Communication Networks**]: Distributed Systems – *Client/ Server*.

General Terms

Security.

Keywords

TCB, RISSC.

1. INTRODUCTION

Security in computer systems is strongly related to the notion of dependability. Informally, a dependable computer system is one that we justifiably trust to deliver its services. Dependability includes availability, reliability, safety, and maintainability. However, if we are to put our trust in a computer system, then confidentiality and integrity should also be taken into account.

When data is transmitted over a certain channel, it is possible that someone else can receive and listen to it. This may include some confidential data like password or so. In wireless communications, this interference is more probable than it is in wired communications, especially if the third party is within the range of transmission.

2. SECURITY – WHY?

To protect your data throughout the channel, we need a security. A way of looking at security in computer system is that we attempt to protect the services & data it offers against **security threats.** There are four types of security threats to consider, Interception, Interruption, Modification and Fabrication.

A **security policy** describes precisely which actions the entities in a system are allowed to take & which ones are prohibited. Entities include users, services, data, machines & so on. Once a security policy has been laid down, it becomes possible to concentrate on the **security mechanisms** by which a policy can be enforced. Important security mechanisms we are generally using are: Encryption, Authentication, Authorization and Auditing.

3. DISTRIBUTION OF SECURITY MECHANISMS

Dependencies between services regarding trust lead to the notion of a **Trusted Computing Base (TCB).** A TCB is a set of all mechanisms in a (distributed) computer systems that are needed to enforce a security policy. The smaller the TCB, the better. If a distributed system is built as middleware on existing network operating system, its security may depend on the security of the underlying local operating systems at various hosts.

Consider a file server in a distributed file system. Such a server may need to rely on the various protection mechanisms offered by its local operating system. Such mechanisms include not only those for protecting files against accesses by processes other than the file server, but also mechanisms to protect the file server from being maliciously brought down. Middleware-based distributed systems thus require trust in the existing local operating systems they depend on. If such trust does not exist, then part of the functionality of the local operating systems may need to be incorporated into the distributed system itself. This separation effectively reduces the TCB to a relatively small number of machines and software components. By subsequently protecting those machines against security attacks from the outside, overall trust in the security of the distributed system can be increased. Preventing clients and their applications direct access to critical services is followed in the Reduced Interfaces for Secure System Components (RISSC) approach.

ICWET'10, February 26–27, 2010, Mumbai, Maharashtra, India.
Copyright 2010 ACM 978-1-60558-812-4…$10.00.

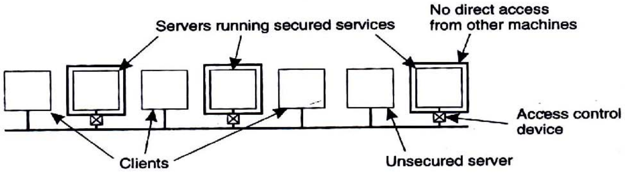
Servers running secured services
No direct access from other machines
Access control device
Clients
Unsecured server

Figure 1: The principle of RISSC as applied to secure distributed systems

4. PROPOSED WORK

Fundamental to security in distributed systems is the use of cryptographic techniques. The basic idea of applying these techniques is simple. Consider a sender S wanting to transmit message m to a receiver R. To protect the message against security threats, the sender first encrypts it into an unintelligible message m', and subsequently sends m' to R. R, in turn, must decrypt the received message into its original form m.

Encryption and decryption are accomplished by using cryptographic methods parameterized by keys, as shown in figure. The original form of the message that is sent is called the plaintext, shown as P and the encrypted form is referred to as the ciphertext, illustrated as C.

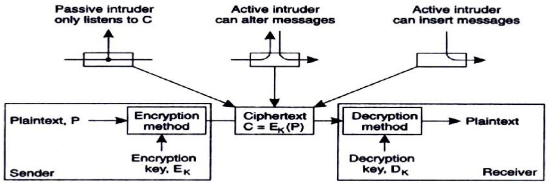

Figure 2: Intruders and eavesdroppers in communication

To describe the various security protocols that are used in building security services for distributed systems, it is useful to have a notation to relate plaintext, ciphertext, and keys. Following the common notational conventions, we will use C = Ek(P) to denote that the ciphertext C is obtained by encrypting the plaintext P using key K. Likewise, P = Dk(C) is used to express the decryption of the ciphertext C using key K, resulting in the plaintext P.

As shown in figure, while transferring a message as ciphertext C, there are three different attacks that we need to protect against, and for which encryption helps. First, an intruder may intercept the message without either the sender or receiver being aware that eavesdropping is happening. Of course, if the transmitted message has been encrypted in such away that it cannot be easily decrypted without having the proper key, interception is useless; the intruder will see only unintelligible data.

The second type of attack that needs to be dealt with is that of modifying the message. Modifying plaintext is easy; modifying ciphertext that has been properly encrypted is much more difficult because the intruder will first have to decrypt the message before it can meaningfully modify it.

The third type of attack is when an intruder inserts encrypted messages into the communication system, attempting to make R believe these messages came from S. Again, encryption can help protect against such attacks. Note that if an intruder can modify messages, he can also insert messages. There is a fundamental distinction between different cryptographic systems, based on whether or not the encryption and decryption key are the same. In a symmetric cryptosystem, the same key is used to encrypt and decrypt a message.

In other words,

$$P = Dk(Ek(P))$$

Symmetric cryptosystems are also referred to as secret-key systems, because the sender and receiver are required to share the same key, and to ensure that protection works, this shared key must be kept secret; no one else is allowed to see the key. We will use the notation $K_{A,B}$ to denote a key shared by A and B.

In an asymmetric cryptosystem, the keys for encryption and decryption are different, but together form a unique pair. In other words, there is a separate key K_E for encryption and one for decryption, K_D, such that

$$P = D_{KD}(E_{KE}(P))$$

One of the keys in an asymmetric cryptosystem is kept private, the other is made public. For this reason, asymmetric cryptosystems are also referred to as public key systems.

One final application of cryptography in distributed systems is the use of hash functions. A hash function H takes a message m of arbitrary length as input and produces a bit string h having a fixed length as output:

$$h = H(m)$$

A hash h is comparable to the extra bits that are added to a message in communication systems to allow for error detection, such a cyclic-redundancy check (CRC).

Hash functions that are used in cryptographic systems have a number of perties. First, they are one-way functions, meaning that it is computationally infeasible to find the input m that corresponds to a known output h. On the other hand, computing h from m is easy. Second, they have the weak collision resistance property, meaning that given an input m and its associated output h = H(m), it is computationally infeasible to find another, different input m' = m, such that H(m) = H(m'). Finally, cryptographic hash functions also have the strong collision resistance property, which means that, when given only H, it is computationally infeasible to find why two different input values m and m', such that H(m) = H(m').

Similar properties apply to any encryption function E and the keys that are used. Furthermore, for any encryption function E, it should be computationally infeasible to find the key K when given the plaintext P and associated ciphertext C = $E_K(P)$. Likewise, analogous to collision resistance, when given a plaintext P and a key K, it should be impossible to find another key K' such that $E_K(P) = E_{K'}(P)$.

5. CONCLUSION

The paper only discusses on the issues related to security in distributed systems. On working of several security algorithms a feasibility analysis is done by comparing the time taken for encryption and decryption by various algorithms. It shows that, in most of the cases, when we increase the number of bits of information to be encrypted together the total time including encryption and decryption steadily decreases. It must always be kept in mind that the integer representation of the message to be encrypted should lie within the range specified by the modules, that lies in the range of [0,n-1], which poses a limitation on the maximum number of characters that can be encrypted at a single time.

6. REFERENCES

[1] Behrouz A. Forouzan, “Data Communications and Networking”, Tata McGraw-Hill Publishing, 2004. pp. 821-822.

[2] Willian Stallings, “Data and Computer Communications”, Pearson Education, 2001. pp. 673-675.

[3] Matthew Strebe, Charles Perkins, “Firewalls”, BPB Publication, 2000. pp. 115- 241.