1.Data is two type

Moving data (ssl, tsl)

Static Data

2. Integrity, Authentication, confidentiality, non-reputation

3. Access control

1. security Services

i. confidentiality: Confidentiality is the protection of transmitted data from passive attacks. With respect to release of message contains several levels of protection can be identified.

ii. Authentication: the authentication service is concerned with assuring that a communication is authentic. In case of single message such as a warning or alarm signal is to assure the recipient that the message is from the source that it claims to be from.

iii. Integrity: Integrity says that the contain of the message is not changed in middle at the time of communication.

iv. non-repudiation: non-repudiation either sender or the receiver from denying a transmitted message thus when a message is sent. the receiver can prove that the message was in fact send by the alleged sender. Similarly, when a message is received. the send can prove the message was in fact received by the alleged receiver.

Bastion Host

A bastion host is system identified by the firewall administrator as a critical strong point in the network's security. Typically

the bastion host serves as a platform for an application level or circuit level gateway.

The following are the common characteristic of a bastion host

1. The bastion host hardware platform executes a secure version of its operating system. Making it a trusted system.

2. Only the services that the network administrator consider essential are installed on the bastion host.

3. The bastion host may require additional authentication before a user is allowed to access to the proxy services. In addition, each proxy

service may require its own authentication before granting user access.

4. Each proxy is configured to support only a subset of the standard applications and command sets.

6. Each proxy maintains detail audit information by logging all traffic. The audit log is a essential tool for discovery and terminating

intruder attacks.

Trusted Systems

One way to enhance the ability of a system to defend against intruders and malicious programs is to implement trusted system

technology. To provide trusted system, we need to know some basic concept of data access control.

Data Access Control

Following successful logon, the user has been granted to access to one or many hosts and applications.

Book cryptography and network security principal and practice William Stolin.

apaine

caseer

hill cipher