Introduction to Network Security – Part 1

Posted by Alejandro G. Carlstein Ramos Mejia on October 26, 2010 October 28, 2010 About Programming / Network Security

NOTIFICATION: These examples are provided for educational purposes. The use of this code and/or information is under your own responsibility and risk. The information and/or code is given 'as is'. I do not take responsibilities of how they are used.

Network Security

What do we considerate as network security? Network security is a system in which:

1. There is a level of confidentiality. This means that only authorised system or personnel is allowed to access
2. There is a level of integrity: This means that from the origin to the destination, the data is authentic and correct.
3. There is a level of availability: This means that a system or personnel can use the information and/or resource.

In 1982, the International Organization for Standartization (ISO) along with the International Telecommunication Union, Telecommunication Standartization Section (ITU-T), created the Open System Interconnection (OSI) with the purpose of standardize networking.

This system is a systematic way for the definition of levels of security such as:

1. Security against attacks
2. Security mechanisms
3. Security Devices

Security against Attacks

A security attack is any action in which the security of a system or information owned by an individual or organization is compromised.
How to detect and prevent an attack on information based system is called information security.

Security attacks are divided in passive and actives attacks.

Passive Attacks

We considerate an attack passive when the attacker try to obtain and/or use information from a system but do not affect the system and/or the system resources. A passive attack is difficult to detect; therefore, instead of focusing in detection, we are better off by

focusing our energies in prevention.

There exist to main type of passive attacks:

1. Release of message contents: This means that the attacker monitor (listen) to the transmissions between the client and the server.
2. Traffic Analysis: When the information is encrypted, the attacker may not be able to obtain the information; however, the attacker may be able to observe the pattern of the messages. Due the frequency and the length of the message, the attacker may get an idea of how to decrypt the message or perform a different active/passive attack.

Active Attacks

We considerate an attack active when the attacker try to alter the system and/or system resource by affecting its operation. The basic type of active attacks are masquerade attack, replay attack, modification of message attack, and denial of service attack.

1. Masquerade attack: When the attacked pretend to be a different entity. For example, an attack could get into a system by pretending being one of the members of an organization.
2. Replay attack: When the attacker intercept a transmission from a sender, and then use the information to produce an authorized effect on the receiver.
3. Modification of message attack: When the attacker intercept a transmission form the sender, alter, delay, or reorder the information in the transmission, and then resend the altered transmission to the receiver.
4. Denial of Service (DoS) attack: When the attacker perform an attack in such a way that interrupt the communication between the sender and the receiver. An example can be found in the New York Times when Yahoo! was shut-down due a denial of service attack: http://www.nytimes.com/2000/02/08/business/yahoo-blames-a-hacker-attack-for-a-lengthy-service-failure.html

Security Services

Security services have the purpose of counter any security attack done to a resource system by an attacker.
The recommendation done by the International Telecommunication Union, Telecommunication Standartization Section (ITU-T), X.800 (Security architecture for Open Systems Interconnection for CCITT applications) found at <http://www.itu.int/rec/T-REC-X.800/en> establish a division of these services into 5 specific categories and 14 specific services:

1. Authentication: Verify that the entity to which the communication is establish is indeed the one that claim to be.
2. Access Control: Verity that the user have authorization to access and use a resource

system

3. Data Confidentiality: Prevent an attacker to unauthorised disclose the data being transmitter between the user/system and a resource system by:
    1. Protecting the transmitter data from a passive attack.
    2. Protecting all data between two ends over a period of time (also known as Broader Services).
    3. Protecting a single chunk of data inside a message (also known as Narrower Services).
4. Data Integrity: Verify that the data received is the same as the data being send and assure that it was not modified by an unauthorized entity.
    1. Verify the integrity of a single chunk of data inside a message.
    2. Provide total stream protection
    3. Verify that the messages are received are the same and the one send and prevent duplications, modifications, and/or denial of services (DoS). This is also know as Connection Oriented Integrity Services.
5. No Repudiation: Provide protection to a communication being done by any number of ends against denial services to anyone of them.
    1. Verify that the message send by an specific entity was send by that entity and not other.
    2. Verify that the message received by an specific entity was send by that entity and not other.

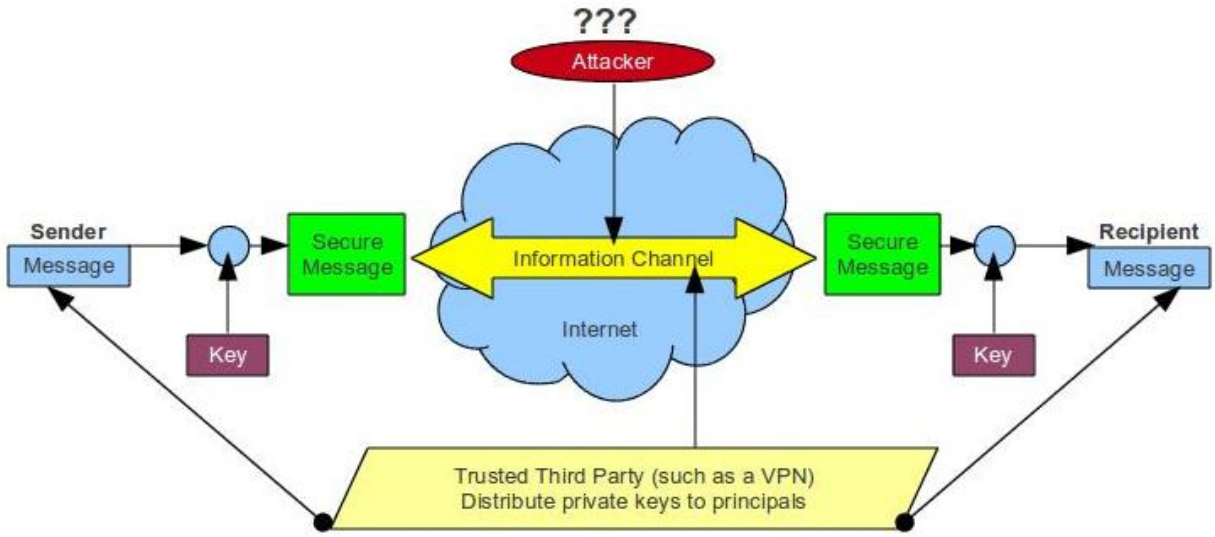
Security Mechanisms

A security mechanism is a single feature for a single support that prevent, recover, delete a form of security attack.There are different specifict security mechanism such as:

1. Encipherment: The transformation of a readable message to an illegible message by the use of mathematical algorithms.
2. Access Control: Security mechanisms that provide a way to enforce access right to resources. For example, in Linux, every file, folder, and/or resource have three set of permissions. These permissions indicate who have the right to read, write, and/or execute an specific file, folder, and/or resource.
3. Digital Signatures: A digital signature is a data chuck that will be append to the message before sending it to the receiver. When the receiver obtain the message, it can verify the authenticity of the message by checking the digital signature. This help to prevent forgery of the message by an attacker.
4. Data Integrity: Security mechanism that verify the integrity of the chuck of data or a data stream.
5. Traffic padding: This is a security mechanism which insert or append bits of information inside the gaps between streams or chucks of data making harder to the attacker to perform a traffic analysis.
6. Authentication Exchange: By exchanging certain information, this security mechanisms can verify if the entity is not an attacker.

Model for Network Security

Lets assume a sender which to send a message to a recipient and the sender wish to use the Internet. We could establish an information channel that could secure the message to arrive secure to the recipient. There are third parties programs that would let us do this such as a Virtual Private Network (VPN) and/or Point to Point (P2P) network.



A trusted third party is the one responsible for the distribution of the secret information needed for both ends. This secret information is the one needed to assure the authenticity of the message transmitted.

This kind of model requires:

1. A secure algorithm for the security transformation
2. A generation of keys (secret information) using an algorithm that will be provided to the principals
3. A method of distribution and share of the key.

Model for Network Access Security

When creating a network access security, we have to have in consideration the enemy of our network such as hackers, crackers, virus, trojans, and worms.

1. A hacker and/or cracker is a person who will try to break the access security of our network.
2. A virus is a software that try to multiply itself inside our computer systems by making copies of itself in different programs. It required to be inside a program in order to be executed and/or propagate.
3. A worm is a program by itself that have the purpose of copy itself and disperse thought the network.
4. Trojans are programs that have an hidden functionality inside them that is unknown to the user and have nefarious purposes.

Some security mechanism that we need to use in order to deal with any unwanted access are:

1. Gatekeeper Functions: A gateway can be represented as a door. Here are two examples of a kind of gateways
    1. A password-base login procedure (such as used in Linux). A user or system that do not have the password is going to be denied access.
    2. Screening controls designed to search, detect, and reject/delete viruses, worms, trojans, and any other similar type of attacks.
2. Internal Controls: They help to monitor and analyze the activity inside the system and the stored information. It intended to try to detect and stop an unwanted intruder.