Notes on Network Security - Introduction

Security comes in all shapes and sizes, ranging from problems with software on a computer, to the integrity of messages and emails being sent on the Internet. Network Security is a term to denote the security aspects attributed to the use of computer networks. This involves the protection of the integrity of the communications that are sent over the network, who is able to access the network or information system present, and also what can be sent over the network. There are a multitude of scenarios and areas that a network and its use can be exploited.

The problem is that given the OSI Network Model of: **Application**, **Transport**,**Network**, **Datalink** and **Physical**, where amongst this can security be deployed? Should everything be concentrated at the data link or network or transport… layers? or should a **Defense in Depth** strategy be employed? These notes details the various ways in which networks can be made secure. The remainder of this chapter provides some introductory material in relation to networks and their security. First, some terminology:

- **Security Attack**: Any action that compromises the security of information exchanges and systems.
- **Security Service**: A service that enhances the security of information exchanges and systems. A sercurity service makes use of one or more security mechanisms.
- **Security Mechanism***: A mechanism that is designed to detect, prevent or recover from a security attack.

2.1. Security Attacks

There exist several attack types and they can be divided into two distinct category's: **Passive** and **Active**, they denote the amount of work that an attacker must do.

2.1.1. Passive Attacks

A **Passive Attack** is one that involves either the eavesdropping or monitoring of data communications. The goal of the malicious entity is to acquire the information or learn more about the communication.

- **Release of Message Contents**: This is when during the transmission of data from one party to another, a third and malicious party intercepts the message and learns its contents.
- **Traffic Analysis**: Traffic analysis is concerned with the analysis of patterns generated by the actions of the parties involved. This may simply involve the detection of an encrypted message being sent from a single party.

Such attacks are difficult to detect, due to their inherent nature. Though one can use encryption in order to inhibit the success-fullness of such attacks.

2.1.2. Active Attacks

Active Attacks are those that involve the modification of the communication channel or the data being sent across the channel.

- **Masquerade**: This is simply the impersonation of a legitimate entity in order to abuse or access the resources accessible by the entity.
- **Replay**: Involves the retransmission of existing and already transmitted data in order to produce an unauthorized effect.
- **Message Modification**: The delay, modification, reorder on a legitimate message such that it produces an unauthorized effect.
- **Denial of Service**: This involves the prevention of or reduction in quality, of a legitimate service. Such attacks may target specific hosts or entire networks.

In contrast to passive attacks, active ones are easy to detect but harder to counter, as it would involve the protection of **all** the communication services offered.

2.2. Security Services

A **Security Service**, as defined by X.800, is a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or data transfers. There are five categories mentioned, together with availability:

Availability
: The property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system.

Access Control
: The prevention of unauthorised use of a resource.

Authentication

This is the assurance that the communicating entity is the one that it claims to be. There are two classes of authentication:

- **Peer Entity** — involves the authentication of a logical entity in a communication process; and
- **Data Origin** — involves assurances relating to the origin of the source of received data.

Data Confidentiality

The protection of data from unauthorised disclosure. This can be further specified as:

- **Connection Confidentiality** — The protection of all user data on a connection.
- **Connectionless Confidentiality** — The protection of all user data in as single data block.
- **Selective-Field Confidentiality** — The confidentiality of selected fields within the user data on a connection or in a single data block.
- **Traffic-Flow Confidentiality** — The protection of the information that might be derived from observation of traffic flows.

Data Integrity

The assurance that data received is in the exact same format as it was when sent by an authorised entity. This can be considered in terms of **Connection Integrity**:

- **Connection Integrity with Recovery** — Provided for the integrity of all user data on a connection and detects any modification, insertion, deletion or replay of any data within an entire data sequence, with recovery attempted.
- **Connection Integrity without Recovery** — As previously but provides only detection without recovery.
- **Selective-Field Connection Integrity** — Provides for the integrity of selected field within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted or replayed.
- **Connectionless Integrity** — Provides for the integrity of a single connectionless data block and may take the form of a detection of data

modification. Additionally a limited form of replay detection may be provided.

- **Selective-Field Connectionless Integrity** — Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.

Non-repudiation

Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication. This can imply:

- **Origin Non-repudiation** — Proof that the message was sent by the specified party.
- **Destination Non-repudiation** — Proof that the message was received by the specified party.

2.3. Security Mechanisms

Security Mechanisms refer to tools and techniques that can be implemented within a specific protocol layer or outwith the layer that provided some form of security. Some examples are listed below.

Specific Mechanisms

Encryption, Digital Signatures, Access Control, Data Integrity, Authentication Exchange, Traffic Padding, Routing Control, Notarisation

Pervasive Mechanisms

Trusted Functionality, Security Label, Event Detection, Security Audit Trail, Security Recovery

2.4. Security Models

There are two main security models that are used when dealing with network security: **Secure Communication** and **Secure Systems**.

2.4.1. Secure Communication

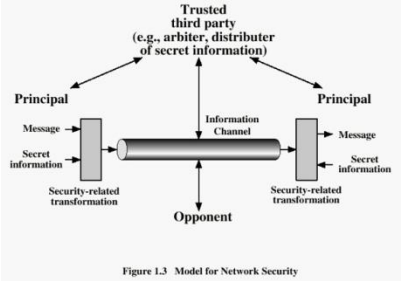

Figure 1. Secure Communication

In this model, there are two principal agents i.e. Alice and Bob, who wish to send a message via a information channel to each other that contains some secret information. In order to protect the secret information the parties involved will perform some form of **Security Related Transformation** on the information to be sent, using some form of **shared secret** that is known only by the parties involved. Such activities may involve the use of a **Trusted Third Party** to whom some responsibilities such as distribution of secret information or authorisation/authentication, are entrusted to. This is summarised in the figure above. This model is used for most areas of network security when the transmission of data is concerned. [Stallings2008] mentions that there are four basic task involved in designing a security service using this model:

1. Design an algorithm for performing the security related transformation.
2. Generate the secret information that is to be used.
3. Develop method for distribution and sharing of the secret information.
4. Specify a protocol to be used by the two principals that utilises the security algorithm and secret information to achieve a particular security service.

2.4.2. Secure Systems

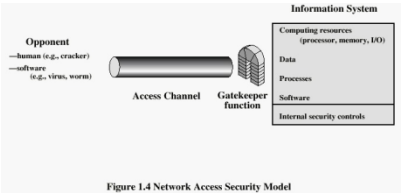

Figure 2. Secure System

The other model reflects the remainder of the security problems that are associated with the protection of an information system i.e. a network, from malicious entities. Such entities can be a hacker that aims to gain access to a system for **fun and profit**, a disgruntled employee who wishes to cause damage or a criminal who wishes to exploit the resources for financial gain. Furthermore this model incorporates the

notion of additional software that aims to exploit vulnerabilities in the system and targets applications and utility programs. They can be classed as: **Information access threats** — interception/modification of data; and **Service Threats**-- exploitation of service flaws. Moreover in order to protect the information system a **Gatekeeper Function** is used to perform access control and restrict the accessibility of the system. If this fails then some form of internal security controls are needed to identify any, stop the actions of and repair any damage as caused by, intruders. This is summarised in Figure fig:secure:sys.

2.5. Outline of Notes

The notes are organised into two distinct parts:

- **Part One: Security Protocols**
    - this looks at the various protocols and techniques used to ensure security of networks. This utilises the Secure Communication Model and will look at topics such as Wireless and Wired network security and protocols such asSSH and **SSL/TLS**.
- **Part Two: System Security**
    - this looks at the ways in which an information system can be attacked and defended. This utilises the Secure System Model and will look at topics such in relation to both **Attacking** and **Defending** information systems.
- **Part Three: Guest Lectures**
    - during the course three guest lectures were given by security professionals from **KPMG** and **Quarantainenet**, looking at **Covert Channels**, **Eavesdropping on DECT Communication** and **Quarantining**. This topics, as given by them will be addressed.

Source: http://jfdm.host.cs.st-andrews.ac.uk/notes/netsec/#_security_attacks