Information Security : An Introduction

Harshvardhan Aggarwal
Student, Maharaja Surajmal Institute of Technology

Abstract
This paper presents a tutorial introduction to basic understanding of information security. It gives the basic information about the goals of information security, attacks threatening them and the security services and mechanisms provided to counter these attacks. The paper concludes with a practical technique to implement the security goals.

Keywords
Confidentiality, Integrity, Availability, Masquerade, Repudiation, Notarization, Cryptography

I. Introduction

Until a few decades ago, the information collected by an organization was stored on physical files. To secure this information, it needs to be hidden from unauthorized access (confidentiality), protected from unauthorized change (integrity), and available to an authorized entity when it is needed (availability). The confidentiality of the files was achieved by restricting the access to a few authorized and trusted people in the organization. In the same way, only a few authorized people were allowed to change the contents of the files [1].

With the advent of computers, information storage has become electronic. The files stored in computers require confidentiality, integrity and availability.

In this paper, we will first see the three goals of information security. We then see how attacks can threaten these goals. We then discuss the security services in relation to these goals. Finally we define mechanisms to provide security services and introduce techniques that can be used to implement these mechanisms[2].

II. Security Goals

The three security goals are : confidentiality, integrity, and availability (Fig. 1) [1].

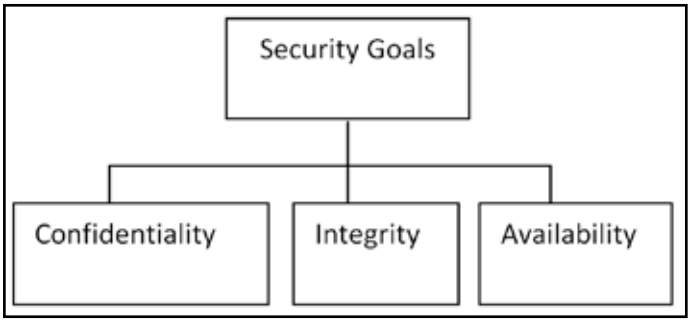

Fig. 1: Taxonomy of Security Goals

A. Confidentiality

Confidentiality is the concealment of information or resources. The need for keeping information secret arises from the use of computers in sensitive fields such as government and industry. For example, military and civilian institutions in the government often restrict access to information to those who need that information.

Confidentiality not only applies to the storage of the information, it also applies to the transmission of information. When we send a piece of information to be stored in a remote computer or when we retrieve a piece of information from a remote computer, we need to conceal it during transmission[1].

Access control mechanisms support confidentiality. One access control mechanism for preserving confidentiality is cryptography, which scrambles data to make it incomprehensible. A cryptographic key controls access to the unscrambled data, but then the cryptographic key itself becomes another datum to be protected [3].

B. Integrity

Integrity refers to the trustworthiness of data or resources, and it is usually phrased in terms of preventing improper or unauthorized change. Integrity includes data integrity (the content of the information) and origin integrity (the source of the data, often called authentication).

Integrity means that changes need to be done only by authorized entities and through authorized mechanisms. Integrity violation is not necessarily the result of a malicious attack; an interruption in the system, such as power surge, may also create unwanted changes in some information [1].

C. Availability

Availability refers to the ability to use the information or resource desired. Availability is an important aspect of reliability as well as of system design because an unavailable system is at least as bad as no system at all. The aspect of availability that is relevant to security is that someone may deliberately arrange to deny access to data or to a service by making it unavailable. Imagine what would happen to a bank if the customers could not access their accounts for transactions [1].

III. Attacks

Our three goals of security – confidentiality, integrity and availability – can be threatened by security attacks. These attacks are divided into three groups (Fig. 2) [1].

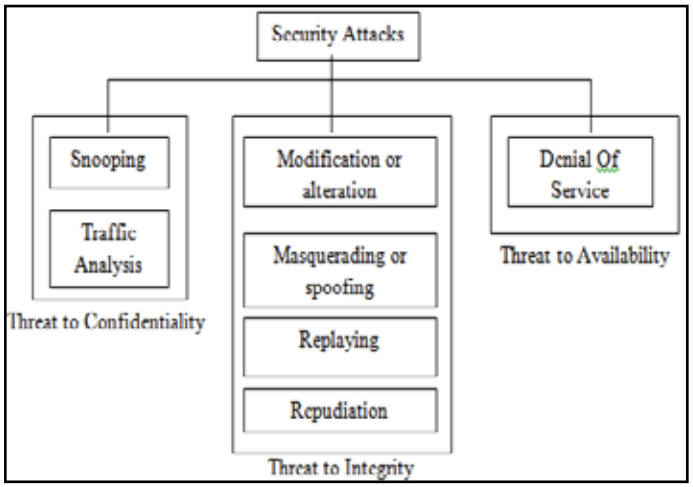

Fig. 2: Taxonomy of Attacks with Relation to Security Goals

A. Attacks Threatening Confidentiality

In general, two types of attacks threaten the confidentiality of information: snooping and traffic analysis.

1. Snooping
Snooping, the unauthorized interception of information, is a form of disclosure. It is passive, suggesting simply that some entity is listening to (or reading) communications or browsing through files or system information. Wiretapping, or passive wiretapping, is a form of snooping in which a network is monitored. To prevent snooping, the data can be made nonintelligible to the interceptor by using encipherment techniques.

2. Traffic Analysis
It is the process of intercepting and examining messages in order to deduce information from patterns in communication. An attacker can gain important information by monitoring the frequency and timing of network packets.

B. Attacks Threatening Integrity
The integrity of data can be threatened by several kinds of attacks: modification, masquerading, replaying, and repudiation.

1. Modification
After intercepting or accessing information, the interceptor modifies the information to make it beneficial to itself. For example, a customer sends a message to a bank to do some transaction. The attacker intercepts the message and changes the type of transaction to benefit itself.

2. Masquerading
Masquerading, or spoofing, happens when the attacker impersonates somebody else. It is a type of attack where the attacker pretends to be an authorized user of a system in order to gain access to it or to gain greater privileges than they are authorized for. For example, an attacker might steal the bank card and PIN of a bank customer and pretend that she is that customer. Sometimes, the attacker pretends instead to be the receiver entity. For example, a user tries to contact a bank, but another site pretends that it is the bank and obtains some information from the user.

3. Replaying
It is an attack in which a service already authorized and completed is forged by another "duplicate request" in an attempt to repeat authorized commands. For example, a person sends a request to her bank to ask for payment to the attacker, which has done a job for her. The attacker intercepts the message and sends it again to receive another payment from bank.

4. Repudiation
This type of attack is different from others because it is performed by one of the two parties in communication: the sender or the receiver. The sender of the message might later deny that he has sent the message; the receiver of the message might later deny that he has received the message [1].

C. Attacks Threatening Availability
There is one attack threatening availability: denial of service.

1. Denial of Service
It is an attempt to make a machine or network resource unavailable to its intended users. The denial may occur at the source (by preventing the server from obtaining the resources needed to perform its function), at the destination (by blocking the communications from the server), or along the intermediate path (by discarding messages from either the client or the server, or both). The attacker may also intercept requests from the clients, causing the clients to send requests many times and overload the system [1].

IV. Passive Versus Active Attacks

A. Passive Attacks
In a passive attack, the attacker's goal is just to obtain information. This means that the attack does not modify or harm the system. The system continues with its normal operation. Attacks that threaten confidentiality – snooping and traffic analysis – are passive attacks.

B. Active Attacks
An active attack may change the data or harm the system. Attacks that threaten the integrity and availability are active attacks. Active attacks are normally easier to detect than to prevent, because an attacker can launch them in variety of ways.

The table given (Table 1) categorizes the attacks into two groups : passive and active.

Table 1 : Categorization of Passive and Active Attacks

Attacks	Passive/ Active	Threatening
Snooping Traffic Analysis	Passive	Confidentiality
Modification Masquerading Replaying Repudiation	Active	Integrity
Denial of Service	Active	Availability

V. Services and Mechanisms
The International Telecommunication Union-Telecommunication Standardization Sector (ITU-T) provides some security services and some mechanisms to implement those services[1].

A. Security Services
ITU-T has defined five services related to the security goals and attacks we defined in the previous sections (fig. 3).

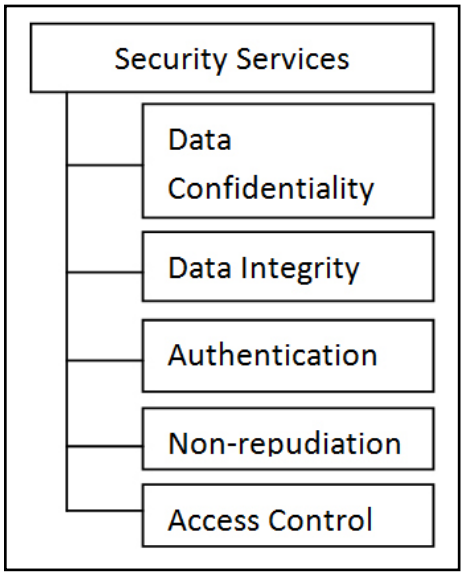

Fig. 3: Security Services

1. Data Confidentiality
It is designed to protect data from disclosure attack. The service is very broad and encompasses confidentiality of the whole message or part of a message and also protection against traffic analysis.

2. Data Integrity
Data integrity is designed to protect data from modification, insertion, deletion, and replaying by an adversary. It may protect the whole message or part of the message.

3. Authentication
This service provides the authentication of the party at the other end of the line. In connection-oriented communication, it provides authentication of the sender or receiver during the connection establishment (peer entity authentication). In connection communication, it authenticates the source of the data (data origin authentication).

4. Non-repudiation
Non-repudiation service protects against repudiation by either the sender or the receiver of the data. In non-repudiation with proof of the origin, the receiver of the data can later prove the identity of the sender if denied. In non-repudiation with proof of delivery, the sender of data can later prove that data were delivered to the intended recipient.

5. Access Control
Access control provides protection against unauthorized access to data,. The term access can involve reading, writing, modifying, executing programs, and so on.

B. Security Mechanisms
ITU-T also recommends some security mechanisms to provide the security services defined earlier. Fig. 4, gives the taxonomy of these mechanisms [1].

1. Encipherment
Encipherment, hiding or covering data, can provide confidentiality. It can also be used to complement other mechanisms to provide other services. Today two techniques – cryptography and steganography – are used for enciphering.

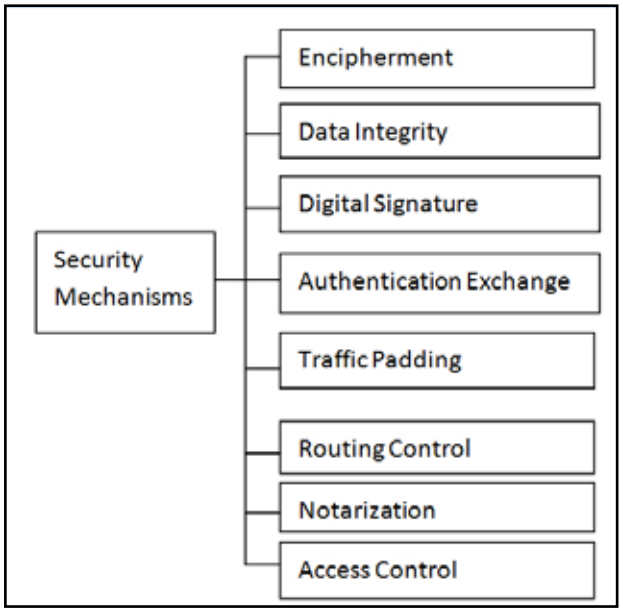

Fig. 4: Security Mechanisms

2. Data Integrity
The data integrity mechanism appends to the data a short checkvalue that has been created by a specific process from the data itself. The receiver receives the data and checkvalue. He creates a new checkvalue from the received data and compares the newly created checkvalue with the one received. If the two checkvalues are same, then the integrity of data has been persevered.

3. Digital Signature
A digital signature is a means by which the sender can electronically sign the data and the receiver can electronically verify the signature. The sender uses a process that involves showing that she owns a private key related to the public key that she has announced publicly. The receiver uses the sender's public key to prove that the message is indeed signed by the sender who claims to have sent the message.

4. Authentication Exchange
In authentication exchange, two entities exchange some messages to prove their identity to each other. For example, one entity can prove that she knows a secret that only she is supposed to know.

5. Traffic Padding
Traffic padding means inserting some bogus data into the data traffic to thwart the interceptor's attempt to use the traffic analysis.

6. Routing Control
Routing control means selecting and continuously changing different available routers between the sender and the receiver to prevent the opponent from eavesdropping on a particular route.

7. Notarization
Notarization means selecting a third trusted party to control the communication between two entities. This can be done to prevent repudiation. The receiver can involve a trusted party to store the sender request in order to prevent the sender from later denying that she has made such a request.

8. Access Control
Access control uses methods to prove that a user has access right to the data or resources owned by a system. Examples of proofs are passwords and PINs.

The Table 2, shows the relationship between the security services and the security mechanisms. The table shows that three mechanisms (encipherment, digital signature, and authentication exchange) can be used to provide authentication.

VI. Techniques
Mechanisms discussed in the previous sections are only theoretical recipes to implement security. The actual implementation of security goals needs some techniques. The most prevalent technique today is cryptography [1].

A. Cryptography
Cryptography, a word with Greek origins, means "secret writing".

Table 2 : Relation Between Security Services and Security Mechanisms

Security Service	Security Mechanism
Data Confidentiality (Snooping and Traffic Analysis)	Encipherment and routing control
Data Integrity (Modification, masquerade, replaying and repudiation)	Encipherment, digital signature, data integrity
Authentication	Encipherment, digital signature, authentication exchange
Non-repudiation	Digital signature, data integrity and notarization
Access Control	Access Control mechanism

Although in the past cryptography referred only to the encryption and decryption of messages using secret keys, today it is defined as involving three distinct mechanisms: symmetric-key encipherment, asymmetric-key encipherment, and hashing.

1. Symmetric-Key Encipherment

In symmetric-key encipherment, an entity, say Alice, can send a message to another entity, say Bob, over an insecure channel with the assumption that an adversary, say Eve, cannot understand the contents of the message by simply eavesdropping over the channel. Alice encrypts the message using an encryption algorithm; Bob decrypts the message using a decryption algorithm. Symmetric-key encipherment uses a single secret key for both encryption and decryption. Encryption/decryption can be thought of as electronic locking. In symmetric-key enciphering, Alice puts the message in a box and locks the box using the shared secret key; Bob unlocks the box with the same key and takes out the message.

2. Asymmetric-Key Encipherment

In asymmetric-key encipherment, we have the same situations as the symmetric-key encipherment, with a few exceptions. First, there are two keys instead of one: one public key and one private key. To send a secured message to Bob, Alice first encrypts the message using Bob's public key. To decrypt the message, Bob uses his own private key.

3. Hashing

In hashing, a fixed-length message digest is created out of a variable-length message. Te digest is normally much smaller than the message. To be useful, both the message and the digest must be sent to Bob. Hashing is used to provide checkvalues, which were discussed earlier in relation to providing data integrity.

References

[1] Forouzan, Behrouz A.,"Cryptography and Network Security", Tata McGraw Hill, New Delhi, India, 2007.

[2] Diffie, Whitfield, Hellman, Martin E.,"Privacy and Authentication: An Introduction to Cryptography", in Proceedings of The IEEE, Vol. 67, No. 3, March 1979.

[3] Dowd, P.W. , McHenry J.T.,"Network security: it's time to take it seriously", IEEE Computer Society, Vol. 31, No. 9, 1998.

Harshvardhan Aggarwal is currently pursuing his B.Tech. in Computer Science and Engineering from Maharaja Surajmal Institute Of Technology, Janakpuri, New Delhi, India from 2009 – 2013, affiliated to Guru Gobind Singh Indraprastha University, Delhi. His research interest includes computer networks, network security, wireless sensor networks, and database management systems.