Internet and Data Security
Khalid F. Jassima, Harith A. Dawoodb
Dept. of Computer Science
Cihan University, Erbil, Iraq.
a khalid.jassim@hotmail.com, b harith.dawood@hotmail.com

ISSN: 2231-8852

ABSTRACT
Internet is the largest computer network, actually consisting of thousands, or millions of interconnected networks. People use Internet to research information, buy and sell products, and many other services. Over time, the attacks on the Internet and the attached computer systems have grown and at the same time there is an increased use of the Internet. Thus, it is important to secure Internet and the attached computers. Individual users depend on the security of the Internet, email, the web, and web-based applications. Thus, a wide range of technologies and tools are needed to face the growing threats.
In this paper, we will cover and review various security threats, attacks, requirements, and finally we will introduce proposal model for data security in order to get perfect secrecy requirements.

Keywords: security mechanisms, encryption, digital signatures, hash functions, security attack.

1. Introduction
Data security is the science and study of methods of protecting data in computers and communications systems. Data in computer systems is vulnerable to many security threats. Threats to secrecy include browsing, leakage, and inference. And threats to authenticity include tampering (such as: modifying, replaying, inserting, and deleting data) or accidental destruction. Computer systems are also vulnerable to another problem: masquerading. If an intruder can gain access to a system under another user's account, In 1982 Dorothy E. Denning (1982) introduced the first block diagram for computer security threats (as shown in Fig. 1).
Internet needs more and better security, and to secure the network infrastructure from unauthorized monitoring and control of network traffic. Many technical reports showed the security weaknesses in software, operating systems of the attached computers (windows, Linux) as well as vulnerabilities in Internet routers and other devices. For example, the denial of service attacks; Internet Protocol (IP) spoofing (Dawood, 2012), (Dawood, 2012), (Minoli & Kouns, 2009), in which intruders create packets with false IP addresses and exploit applications that use authentication based on IP; and various forms of eavesdropping and packet sniffing, in which attacks read transmitted information, including logon information and database contents (Al-Hamdani, 2008), (Denning, 1982), (Konheim, 2007), (Stamp, 2006), (Vacca, 2009).
Fig. 1: Threats to data stored in computer systems.

2. Security Attacks

Information transmitted over insecure communication channels are vulnerable to passive attack (wiretapping), which threatens secrecy, and to active attack (wiretapping), which threatens authenticity, as shown in Fig. 2.

Fig. 2: Threats to secure communication.

A passive attack attempts to learn or make use of information from the system but does not affect system resources. The active attack attempts to alter system resources or affect their operation (Denning, 1982), (Pfleeger, 2006), (Schneier, 1996), (Stallings, 2006).
2.1 Passive Attacks

Passive attacks include eavesdropping on transmissions or monitoring of transmissions. The opponent attempts to obtain information that is being transmitted. There are two types of passive attacks as follows:

- **Release of message contents:** In this case the opponent attempts to read contents of message from sender to receiver. A telephone conversation, an email message, or any transferred file may contain sensitive information. It is important to prevent an opponent from unauthorized reading the contents of these transmissions.

- **Traffic analysis:** The opponent attempts to observe pattern of transferred messages. We can use encryption technique for masking the contents of messages so that opponent could not extract the information from the message. But, the opponent could determine the location and identify of communicating hosts and could observe the frequency and length of messages being exchanged.

Passive attacks are very difficult to detect because they do not involve any alteration of the data. Here, the message traffic is sent and received in normal way, and neither the sender nor receiver is aware that a third party has read the messages or observed the traffic pattern. It is feasible to prevent the success of these attacks by means of encryption.

2.2 Active Attacks

Active attacks include some modification of the data stream and can be classified into four categories: masquerade, reply, modification of messages, and denial of service.

- **Masquerade:** It takes place when one entity pretends to be a different entity. A masquerade attack usually includes one of the other forms of active attack. For example, authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges.

- **Replay:** It involves the passive capture of data unit and its subsequent transmission to produce an unauthorized effect. For example, the opponent captures transferred message; and later replay message to receiver.

- **Modification of messages:** It means that some portion of a legitimate message is altered, or that messages are delayed or recorded, to produce an unauthorized effect. For example, a message meaning “Allow Khalid F. Jassim to read confidential file account” is modified to mean “Allow Harith A. Dawood to read confidential file account”.

- **Denial of service:** It prevents the normal use or management of communication facilities. For example, an entity may suppress all messages directed to a particular destination. Another form of service denial is the disruption of an entire network by disabling the network or by overloading it with messages so as to degrade performance.

It is quite difficult to prevent active attacks, because of the wide range of potential physical, software, and network security vulnerabilities.

3. Security Requirements

The security requirements include data confidentiality, authentication, non repudiating, access control, data availability, and integrity, as shown in Fig.3.
3.1 Confidentiality

Confidentiality is the protection of transmitted data from passive attacks. There are several levels of protection regarding the content of a data transmission. The broadest service protects all user data transmitted between two users over a period of time. For example, when a Transmission Control Protocol (TCP) connection is set up between two systems, this broad protection prevents the release of any user data transmitted over the TCP connection.

The narrow service protects a single message or specific fields within a message. The broad approach is more useful because the narrow protection is more complex and expensive to implement. The other aspect of confidentiality is the protection of traffic flow from analysis. This requires that an attacker not be able to observe the source and destination, frequency, length, or other characteristics of the traffic on a communications links (Bradley et al., 2007), (Pfleeger, 2006), (Stallings, 2006).

3.2 Authentication

The authentication service is concerned with assuring that a communication is authentic. In the case of a single message, such as a warning or alarm signal, the function of the authentication service is to assure the recipient that the message is from the source that it claims to be from. If we have a connection of a terminal to a host, two cases are involved. First, at the time of connection initiation, the service assures that the two entities are authentic. Second, the service must that the connection is not interfered with in such a way that a third party can masquerade as one of the two legitimate parties for the purpose of unauthorized transmission or reception (Anderson, 2001), (Bishop, 2004), (Stallings, 2011).

Two specific authentication services are defined as follows:

- **Peer entity authentication**: Provides for the proof of the identity of a peer entity in an association. It is provided for use at the establishment of a connection or during the data transfer phase. It attempts to provide confidence that an entity is not performing either a masquerade or an unauthorized replay of a previous connection.

- **Data origin authentication**: Provides for the proof of the source of a data unit. It does not provide protection against the duplication or modification of data units. This type of service supports applications like email where there are no prior interactions between the communicating entities.
3.3 Non-repudiation

Non-repudiation prevents the sender and receiver from denying a transmitted message. Thus, when a message is sent, the receiver can prove that the claimed sender in fact sent the message. Similarly, when a message is received, the sender can prove that the claimed receiver in fact received the message (Schneier, 1996).

3.4 Access Control

In the computers network security, access control is the ability to limit and control the access to host systems and applications via communications links. To achieve this, each entity trying to gain access must first be identified, or authenticated, so that access rights can be tailored to the individual (Ferguson & Schneier, 2003), (Lehtinen, 2006).

3.5 Availability

Availability can be defined as the property of a system or system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system. A variety of attacks can result in the loss of or reduction in availability. Some of these attacks are amenable to automated countermeasures, such as authentication and encryption, whereas others require some sort of physical action to prevent or recover from loss of availability of elements of a distributed system. An availability service is one that protects a system to ensure its availability. This service addresses the security concerns raised by denial of service attacks. It depends on proper management and control of system resources and thus depends on access control service and other security services (Anderson, 2001), (Bishop, 2004).

3.6 Integrity

Integrity can apply to a stream of messages, a single message, or selected fields within a message. The most useful approach is total stream protection. The connection-oriented integrity service, which deals with a stream of messages, assures that messages are received as sent, without duplication, insertion, modification, recording, or replays. Thus, the connection-oriented integrity service addresses both message stream modification and denial of service. On the other hand, a connectionless integrity service, one that deals with individual messages without respect to any larger context, generally provides protection against message modification only. Because the integrity service relates to active attacks, we are concerned with detection rather than prevention. If a violation of integrity is detected, then the service may simply report this violation, and some other portion of software or human intervention is required to recover from the violation. There are mechanisms available to recover from the loss of integrity of data. The incorporation of automated recovery mechanisms is the more attractive alternative (Crypto AG, 2011), (Pfleeger, 2006).

4. The Proposal Model for Data Security

A security mechanism is any process that is designed to detect, prevent, and/or recover from a security attack. And such mechanisms are encryption algorithms, digital signatures, and hash algorithms. There are some practical solutions, such as those networks can be secured by encryption and firewalls. Tight configuration management is the important aspect of a secure network, and it is important as having a reasonable firewall. Unauthorized intrusion into a computer system or network is one of the most serious threats to computer security. Thus, intrusion detection systems have been used to provide early warning of an intrusion so that defensive action can be taken to prevent or minimize damage, (Mao, 2003), (Menezes & Vanstone, 1996), (Nemati & Yang, 2011).

The basic building blocks for security mechanisms are:
Cryptographic algorithms are used to provide confidentiality, and can provide authentication and integrity.

Digital signatures are used to provide authentication, integrity protection, access control, and non-repudiation.

Hash algorithms are used to provide integrity protection, availability and can provide authentication.

Security aspects come into play when it is necessary or desirable to protect information transmission from an opponent who may present a threat to confidentiality, authenticity, and so on.

This general model shows that there are three basic building blocks in designing particular security mechanisms: (Fig. 4).

**4.1 Encryption**

Encryption is the original goal of cryptography. In general communication channels are not secure. To prevent unauthorized user (opponent) from understanding the conversation that sender and receiver are having, they use encryption as shown in Fig. 5. At first, sender and receiver agree on a secret key. They will have to do this via some communication channel that unauthorized user cannot eavesdrop on it (Konheim, 2007).
An important rule is Dorothy’s principle (Denning, 1982): the security of the encryption scheme must depend only on the secrecy of the key, and not on the secrecy of the algorithms.

In the context of using encryption to secure the Network, we suggest the following ideas:

1. First approach is to do encryption and/or authentication at the Internet Protocol layer, which is to be provided in IPv6. Internet Protocol Security (IPsec) has the potential to stop some network attacks, and to be a useful component in designing robust distributed systems.

2. Second approach is the Virtual Private Network (VPN). The idea here is that a number of branches of a company arrange for traffic between their sites to be encrypted at their firewalls. This way the Internet can link up their local networks, but without their traffic being exposed to eavesdropping.

3. In practical systems it is preferred to combine the flexibility of public key cryptography with the efficiency of symmetric-key cryptography. The public key algorithms are used to establish a secret key, and secret key algorithms are used to encrypt the actual data.

4.2. Digital Signatures

We suggest using the idea of Public Key Infrastructure (PKI). The main idea is to have a central authority called the Certificate Authority (CA). Each user takes his public key to the CA and identifies himself to the CA. The CA then signs the user’s public key using a digital signature. The signed message, or certificate, states: “the CA, have verified the public key P_Alice belongs to the user Alice.” The certificate will often include an expiration date and other useful information. In a PKI each participant only has to have the CA certify his public key, and know the CA’s public key so that he can verify the certificates of other participants.

4.3 Hash Functions

The hash functions most commonly used in applications are all related, and are based on variants of a block cipher with a 512-bit key and a block size of either 128 or 160 bits. The hash function MD4 has three rounds and a 128-bit hash value. The hash function MD5 has four rounds and a 128-bit hash value, and the U.S Secure Hash Standard SHA1 has five rounds and 160-bit hash value (Crypto AG, 2011).

The hash functions may be used as follows (Ferguson & Schneier, 2003):

1. **Message Authentication Codes (MACs)**
   Hash functions may be used to compute MACs. We hash the message with a key: \( \text{MAC}_k(m) = h(k,m) \). The accepted way of doing this, called HMAC, uses an extra step in which the result of this computation is hashed again. The two hashing operations are done using variants of the key.

2. **Timestamp a Digital Document**
   Another hash function use is to timestamp a digital document in order to establish intellectual priority, but not be willing to reveal the contents yet. In this case, we can submit a hash of the document to a commercial time stamping service.

3. **Key Updating**
   Key updating means that two or more principals who share a key K pass it through a one-way hash function at agreed times: \( K_i = h(K_{i-1}) \). The point is that if an attacker compromises one of their systems and steals the key, he only gets the current key and is unable to decrypt back traffic (back word security).
4. **Auto keying**

Auto keying means that two or more principals who share a key $K$ hash it at agreed times with the messages they have exchanged since the last key change: $K_{i+1} = h(K_i, m_{i1}, m_{i2}, \ldots)$. The point is that if an attacker compromises one of their systems and steals the key, then as soon as they exchange a message which he does not observe or guess, security will be recovered in that he can no longer decrypt their traffic (forward security).

5. **Conclusions**

Internet is growing and changing every day. Consequently, it is better to know the technology, the latest attacks, and the newest defense mechanisms. Preventing and detecting attacks that are launched over networks, and particularly over the Internet, is the most important aspect of Internet security. Therefore:

1. In order to prevent network attacks, we may use a combination of encryption techniques, the signed message, and hash functions. These techniques provide perfect secrecy and authenticity over the insecure networks channels.
2. Because IPv6 and IPv4 are both network layer protocols, many of the network layer vulnerabilities are therefore similar. It is better to implement encryption and/or authentication at the IP layer, which is to be provided in IPv6, and is available as a retrofit for the current IP protocol as IPsec. A native IPsec has the potential to stop many network attacks.

**Acknowledgements**

At first we must thank our lovely families for their support. We would like to thank our colleagues and friends, for encouragement and support.

**References**


Denning, Dorothy E., (1982), *Cryptography and Data Security*. Addison-Wesley Publishing Company,
