OSI Security Architecture

Session 1

LEARNING OBJECTIVES

On completion of this session, you should be able to:

- Appreciate the importance of network security
- Understand the security requirements and the OSI Security Architecture (X.800 standard)
- Be familiar with the basic security model
- Understand security management to handle the OSI security services and mechanisms

Contents

1.0 Introduction
1.1 Importance of Network Security
1.2 OSI Security Architecture
1.3 Network Security Model
1.4 Security Management
1.5 Conclusion
1.6 References

Reading

Prescribed readings

Reading 1: Read W. Stallings, Network Security Essentials – Application and Standard, 4th edition, Prentice Hall, 2010, pp. 16 to 22.

Reading 2: Read W. Stallings, Network Security Essentials - Application and Standard, 4th edition, Prentice Hall, 2010, pp. 22 to 32.

Reading 3: Read W. Stallings, Network Security Essentials - Application and Standard, 4th edition, Prentice Hall, 2010, pp. 33 to 35.

Consult: OSI Security Architecture standard
http://fag.grm.hia.no/IKT7000/litteratur/paper/x800.pdf

1.0 Introduction

Over the past two decades, there has been tremendous growth of the use of computers in every sphere of life, from private use to small to large organizations. Computers within an organization are connected in a network for information and resource sharing, for increased productivity and smoother operation. Organizations are again connected through either proprietary network or the Internet. With businesses going global, a networked system allows everyone to access information quickly, communicate efficiently with partners at reduced cost, provide improved customer services and conduct commerce electronically.

However, with the ease of access to information, particularly access to a shared system over a public telephone network, the requirement of information security is crucial than ever. Security measures are needed to protect data and to thwart hackers, to ensure integrity of data during transmission, and to maintain privacy of communication. A security breach

to an organization can be devastating in terms of financial loss, market reputation, discloser of sensitive information and legal implication.

1.1 Importance of Network Security

Form an organization's point of view, network security is a highly important issue because it depends on computer networks for its day-to-day operations, to store critical financial and business data, and to provide access to users internally within an organization and externally to customers and suppliers. An information security survey conducted by the UK Department of Trade and Industry in 2000 revealed the followings [2, pp. 2-3]

- About 70% of the organizations surveyed hold sensitive or critical information on their networks. They placed high value on the information and considered potential loss of customer confidence in the event of discloser.
- About 60% of the organizations reported a security breach between 1998 to 2000.
- Those organizations suffered a financial loss of $20,000 to in excess of $100,000 per breach. The loss would be much higher when full impact of security breach on the loss of productivity and customer confidence is taken into account.
- Most importantly, the number of security breaches is on the rise.

Today's software/hardware products are designed in a way that people with little computing expertise can install and operate them. However, most of the people do not have the knowledge to configure them securely which certainly makes their systems vulnerable. On the other hand, hackers come up with new ideas everyday to launch an attack. With computer system growing more and more complex gradually, system administrators find it difficult to keep the system updated with the latest bug fixes. As pointed by J. H. Allen, "Thus, even vigilant, security-conscious organizations discover that the security starts to degrade immediately after fixes, workarounds, and new technology are installed" [3]. Widespread availability and use of intrusion tools and exploit scripts have made an attacker's job easy and encourage them to do it more frequently.

Even though the implementation of network security is the responsibility of the IT department within an organization, it is utmost important that the management board be convinced that the increasing frequency of security

breaches is a serious issue that can potentially cost huge amount of money and hard-built reputation. Sixty percent of the respondent organizations in the above-mentioned survey lay the responsibility with IT department. However, technical solution is only a part of the overall security strategy. The other aspect of the strategy, i.e., proper workplace behaviour can be best implemented through a well-formulated security policy adopted and enforced by the management. The survey reported that only a small percentage (14%) of organizations in the UK has a formal security policy [2, pp. 5]. With the current networking environment in which the organizations operate, it is very important that the management assess the risks and threats associated with security breaches and formulate a security policy to protect information assets and ensure guaranteed services.

Reading 1:
Read W. Stallings, Network Security Essentials - Application and Standard, 4th edition, Prentice Hall, 2010, pp. 16 to 22.

1.2 OSI Security Architecture

The ITU (International Telecommunication Union) recommends OSI Security Architecture (X.800 standard) that defines a systematic approach to identify the requirements for security and the approaches that satisfy those requirements. The benefit of such standardization is that all vendors can incorporate features in their products that satisfy those security requirements. The OSI Security Architecture focuses on the followings [1],[4]

- Security attack: an attack is an action that tends to compromise the security of the organization's network. An attack can be passive or active. An active attack affects or attempts to affect the system whereas a passive attack does not affect it.

    - Passive attack: this type of attacks eavesdrop or monitor any transmission of messages between the two parties. It may try to capture the content of the communication, i.e., tapping the telephone conversation, reading an email or file that contains sensitive information (the information may not be revealed to the attacker if it is encrypted). In another form, it may try to analyze the traffic, i.e., locating the host, frequency and duration of communication etc.

- Active attack: this type of attack is more severe in the sense that it attempts to alter the data streams. It can modify a message in transition, hijack a session, replay a message to produce an unauthorized effect, or even launch a denial of service attack to prevent normal use of a service.

- Security service: In X.800, a security service is defined as "a service, provided by a layer of communicating open systems, which ensures adequate security of the systems or of data transfers." These services are provided in six categories and implemented in fourteen specific mechanisms. These categories are described briefly in the following.

Category	Description
Authentication	This service is provided for use at the establishment of, or at times during, the data transfer phase of a connection to confirm the identities of one or more of the entities connected to one or more of the other entities.
Access control	This service provides protection against unauthorized use of resources accessible via OSI. These may be OSI or non-OSI resources accessed via OSI protocols. This protection service may be applied to various types of access to a resource (e.g., the use of a communication resource; the reading, the writing, or the deletion of an information resource; the execution of a processing resource) or to all accesses to a resource.
Data confidentiality	These services provide for the protection of data from unauthorized disclosure and protect data from traffic analysis.
Data Integrity	These services counter active threats and ensure that messages are

	received as sent, with no duplication, insertion, modification, reordering or replays.
Nonrepudiation	This service ensures that sender or receiver can not later deny sending or receiving a message.
Service availability	Availability of the system to legitimate users.

- Security mechanism: X.800 defines a number of security mechanisms. It includes encipherment, digital signature, access control, data integrity, authentication etc. among others. Some of these mechanisms are implemented in specific protocol layer. In practice, they will be invoked at appropriate layers and in appropriate combinations, usually with non-OSI services and mechanisms, to satisfy security policy and/or user requirements. Particular security mechanisms can be used to implement combinations of the basic security services. These topics will be covered in details in later study guides.

Reading 2:
Read W. Stallings, Network Security Essentials - Application and Standard, 4th edition, Prentice Hall, 2010, pp. 22 to 32.

1.3 Network Security Model

A model for network security is illustrated in Fig. 1.5, page 17 of the textbook. The two parties (sender and receiver) communicate over a communication channel which is made virtually secure using cryptography and other related techniques. To ensure security, all the aspects defined in the OSI security architecture are considered. All the security techniques have the following first two components, and may also have the third component.

- Transformation of the message to be sent in a form that can not be retrieved by an unintended party.

- Some secret information is shared by the two parties. Safe distribution of the secret information between the parties is important.
- A trusted third party may be needed, e.g., for distribution of the secret information.

The security model has the four basic tasks to perform [1]:

- Design an algorithm to perform the security related transformation of the message. The algorithm should be such that an opponent should not be able to retrieve the original message.
- Generate the secret information to be used with the algorithm.
- Develop secure method for the distribution and sharing of the secret information among the parties.
- Specify a protocol to be used by the parties to achieve a particular security service making use of algorithm and secret information.

Reading 3:
Read W. Stallings, Network Security Essentials - Application and Standard, 4th edition, Prentice Hall, 2010, pp. 33 to 35.

1.4 Security Management

OSI security management is concerned with the management of OSI security services and mechanisms. The OSI security architecture identifies three areas of security management [4]:

- System security management: system security management is concerned with the management of security aspects of the overall distributed computing environment. Activities include overall security policy management, interaction with security service management and security mechanism management etc.
- Security service management: security service management is concerned with the management of particular security services. This service provides for invocation of specific security mechanisms via the appropriate security mechanism management function.

- Security mechanism management: security mechanism management is concerned with the management of particular security mechanisms. This is responsible for encryption keys and digital certificate management, access control management etc.

Consult:
OSI Security Architecture standard
http://fag.grm.hia.no/IKT7000/litteratur/paper/x800.pdf

1.5 Conclusion

In this study guide, we briefly discuss the importance of network security, especially in the Internet environment. An overview of the OSI security architecture and model is also presented. Regarding the OSI security architecture, we should be aware that it has been developed not to solve a particular network security problem, but to provide a framework that can be commonly used to describe and discuss security-related problems and solutions.

1.6 References

[1] W. Stallings, Network Security Essentials - Application and Standard, 4th edition, Prentice Hall, 2010.

[2] Owen Poole, Network Security ? A Practical Guide, Butterworth-Heinemann, 2003, pp7-11.

[3] J. H. Allen, The CERT Guide to System and Network Security Practices, Addison-Wesley, 2001, pp 3-5.

[4] OSI Security Architecture standard