OVERVIEW OF SECURITY METHODS

Common solutions that can protect computer communication networks from attacks are classified as cryptographic techniques or authentication techniques (verification).

Cryptographic Techniques

Cryptography has a long and fascinating history. Centuries ago, cryptography was used as a tool to protect national secrets and strategies. Today, network engineers focus on cryptography methods for computer communication networks. Cryptography is the process of tranforming a piece of information or message shared by two parties into some sort of code. The message is scrambled before transmission so that it is undetectable by outside watchers. This kind of message needs to be decoded at the receiving end before any further processing.

The main tool that network security experts are using to encrypt a message M is a secret key K; the fundamental operation often used to encrypt a message is the Exclusive-OR ($\oplus$). Suppose that we have one bit, M, and a secret bit, K. A simple encryption is carried out using M $\oplus$K. To decrypt this message, the second partyif he/she has the key, Kcan easily detect M by performing the following:

Equation 10.1

$$(M \oplus K) \oplus K = M.$$

In computer communication networks, data can travel between two users while it is encrypted. In Figure 5.14, two servers are exchanging data while two types of encryption devices are installed in their communication network. The first encryption device is end-to-end encryption, whereby secret coding is carried out at both end systems.

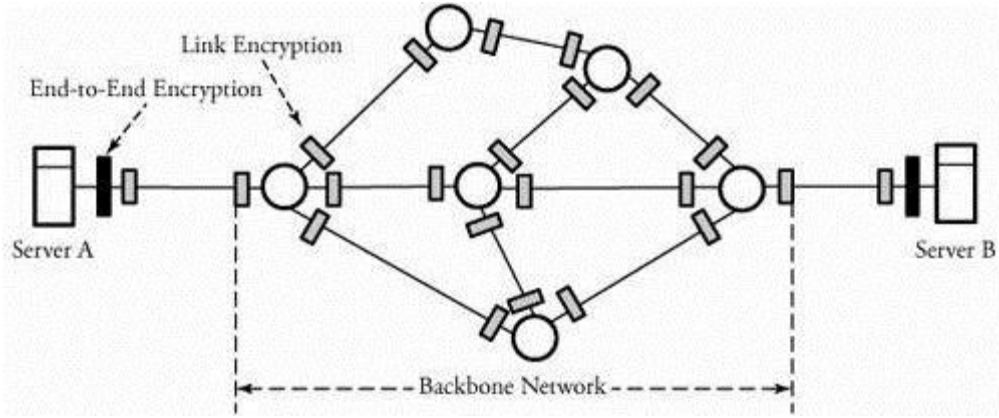

Figure 5.14. Overview of encryption points in a communication network

In this figure, server A encodes its data, which can be decoded only at the other end server. The second phase of encryption is link encryption, which secures all the traffic passing over that link.

The two types of encryption techniques are secret-key encryption and public-key encryption. In a secret-key model, both sender and receiver conventionally use the same key for an encryption process. In a public-key model, a sender and a receiver each use a different key. The public-key

system is more powerful than the secret-key system and provides better security and message privacy. But the biggest drawback of public-key encryption is speed. The public-key system is significantly more complex computationally and may not be practical in many cases. Hence, the public-key system is used only to establish a session to exchange a session key. Then, this session key is used in a secret-key system for encrypting messages for the duration of the session.

Authentication Techniques

Encryption methods offer the assurance of message confidentiality. However, a networking system must be able to verify the authenticity of the message and the sender of the message. These forms of security techniques in computer networks are known as authentication techniques and are categorized as authentication with message digest and authentication with digital signature. Message authentication protects a user in a network against data falsification and ensures data integrity. These methods do not necessarily use keys.

Source : http://elearningatria.files.wordpress.com/2013/10/cse-vi-computer-networks-ii-10cs64-notes.pdf