Chapter VI

Integrity and Authentication

In this chapter, methods that can check if a message was modified are explained; this includes the Message Authentication Code (MAC), hash functions, and the Keyed-Hash Message Authentication Code (HMAC). Also discussed are ways to verify a sender’s identity by using digital signatures.

Objectives

- Understand the SHA-1 and MD5 hash algorithms
- Learn how digital signatures are used to verify the message sender’s identity
- Understand how digital certificates are used to validate public keys
Introduction

In the world of communications, it is very important to ensure that messages are not modified by unauthorized persons.

The mechanism for ensuring that data is not altered when transmitted from source to destination, or when it is stored, is called *integrity*. Message Digest 5 (MD5), Secure Hash Standards (SHA-1, SHA-256, SHA-384, and SHA-512), Message Authentication Codes (MACs), and Keyed-Hash Message Authentication Codes (HMAC) are mechanisms that check the integrity of a message.

Encryption provides intrinsic integrity because if a ciphertext block has been modified, the block will not be deciphered properly. Digital signature also provides integrity because it uses hash functions.

Message Authentication Code (MAC)

The mechanisms that provide integrity checks based on a secret key are usually called *Message Authentication Codes* (MACs). Typically, Message Authentication Codes are used between two parties who share a secret key in order to authenticate information transmitted between these parties.

MAC is a key-dependent one-way hash function. One popular way to construct a MAC algorithm is to use a block cipher in conjunction with the Cipher Block Chaining (CBC) mode of operation with the $IV = 0$. The Message Authentication Code is the ANSI standard DES-based checksum, also known as the U.S. Government Standard Computer Data Authentication Code, FIPS PUB 113 (Federal Information Processing Standards (FIPS), 1985).

The integrity provided by the MAC is based on the fact that it is not possible to generate a MAC without knowing the cryptographic key. An adversary without knowledge of the key will not be able to modify data and then generate an authentic MAC on the modified data.

Figure 6-1. Secure mechanisms for integrity