Network and Computer Security

Summary

Contents

Chapter 1

Network Security

1.1 Cryptography

It is a widespread and dangerous belief that encrypting everything provides protection against anything. In reality, when the algorithm is known it is necessary to prevent several types of attacks, such as ciphertext-only, known-plaintext, chosen-plaintext or chosen-ciphertext. Cryptography must, then, protect the information against unauthorized insertion of information, modification of information in transit, replay of information and access to information.

1.1.1 Cryptographic Services

To this end, we need the following cryptographic services:

- Confidentiality: a service used to keep the content of the information from all, but those entities authorized to have it. Has the drawbacks of making debugging harder and may lead to information loss if the key is lost. Can be assured through symmetric of assymetric cipher.
- Integrity: a service that detects data manipulation by unauthorized entities (not the same thing as error detection codes). An intruder should not be able to substitute a false message for a legitimate one. Can be assured through MIC or a digital signature.
- Authenticity: a service used to ascertain the identity or the origin of a message. Can be assured through MIC or a digital signature, tough freshness requires adding a nonce to the message.
  - Entity authentication: verify the identity of an entity
  - Data origin authentication: confirm the creator of the message
  - Non-repudiation: a service which prevents an entity from denying. Can be assured by a digital signature. previous commitments or actions

1.1.2 Cryptographic Building Blocks

Symmetric Cipher

Uses the same key to cipher and decipher. In cryptographic function notation:

- $E(M, K)$: cipher message M with key K
- $D(C, K)$: decipher cryptogram C with key K

Asymmetric Cipher

A public/private pair of keys is used (KU/KR). In cryptographic function notation:

- $AE(M, KR)$: cipher message M with private key KR
- $AD(C, KU)$: decipher cryptogram C with public key KU

It is also possible to cipher with the public key and then decipher with the private key.

Cryptographic Hash

A cryptographic hash function does not use a key, instead receives an input message and returns a digest of the data. In cryptographic function notation:

- $H(M)$: hash of message M

The digest value is deterministic, has fixed size, a unique representation, is non-reversible and sensible to input changes.

Composite Building Blocks

- Hybrid cipher: a random symmetric key is generated and used to cipher the message. This key is then ciphered with the public key of the receiver and is sent along with the ciphered message. The receiver must decipher the symmetric key with its private key and use it do decipher the message
- Message integrity code: the MIC is created by creating the digest of the message and ciphering the result. It can then be used to check the integrity of the message by generating a new hash and comparing to the sent one.
- Digital signature: a digital signature is created by ciphering a digest with the private key. The receiver can then decipher with the public key and verify the identity of the sender.