

NETWORK SECURITY

August 31, 2009

Goals

- To prevent unauthorized access
- To secure critical data
- Integrity : Only authorized persons should be allowed to modify the data
- Secrecy : Only authorized persons should be allowed to read the data
- Authentication : Verifying the identity of the user
- Non-repudiation : Proof that a message/document was sent/signed by the specified person.
- Availability : Authorized persons should be able to access and use the data at all times

Integrity, secrecy and availability of data are the three most important goals of network security.

Threat Model

Let Alice be the sender and Bob, the receiver of a message. The network through which the message gets routed is considered to be an Evil Post Office.

The following are the threats –

- Change of source and destination addresses
- The message, source and destination addresses can be read
- The message can be changed/modified.
- The message can be dropped.
- The addresses can be used for spamming.
- Message injection
- If a sequence of messages is being sent, the order of messages can be changed.
- The delivery of messages to the recipient can be delayed.
- The messages can be replayed at a later time (with modification)

History of cryptography

- To indicate the chemicals included in recipes
- In warfare
- Caesar cipher : Replacing each letter of the alphabet with the letter three places further down.
- Random Substitution : To infer the plaintext, the relative frequency of the letters in the ciphertext is compared to the standard frequency of English alphabets. This technique was developed by analysing the text in Quran.
- Rotor machines : Enigma used invented during the World War. Turing is known for his efforts in breaking the Enigma.

Chosen Plaintext attack

The attacker chooses the plaintext, which is then encrypted. Hence the attacker knows the plaintext and the ciphertext. This information could help in revealing the key.

Definitions

Cryptosystem : An encryption scheme is a triple (G,E,D) where

G : Key generator

E : Encryption :- key X M \rightarrow C

D : Decryption :- key X C \rightarrow M

$\forall K, M \ D(K, E(K, M)) = M$

The One-Time Pad

This scheme uses a key that is as long as the message, with no repetitions.

Key = μ = C = $\{0,1\}^l$

Encryption :

$E(K, M) = K \oplus m = C$

Decryption :

$D(K, C) = K \oplus C = m$

$D(K, E(K, M)) = K \oplus (K \oplus M)$

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

$= M$

If the key is reused, then

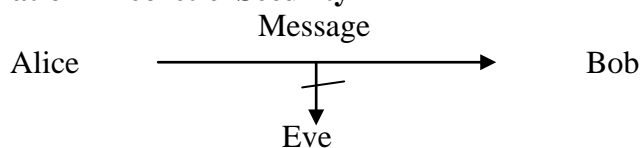
$C_1 = K \oplus m_1$

$C_2 = K \oplus m_2$

$C_1 \oplus C_2 = m_1 \oplus m_2$

So, if the two ciphertexts are XORed, and the frequency distribution statistics is applied, it is possible to obtain the plaintext.

Information Theoretic Security



If the encrypted message sent by Alice to Bob is accessible to the intruder, then the probability of the plaintext being retrieved is

$\Pr_{m \in \mu, k \in \text{Keys}}[M = m | C = c] = 2^{-l}$

Where l = length of ciphertext

Fact : If (G,E,D) is information theoretically secure, then $|\text{keys}| \geq |\mu|$

Proof :

Let $c \in C$ and $S = \{D(K, C) | K \in \text{keys}\}$

$|S| \leq |\text{Keys}|$

Every plaintext must be an element of S because every plaintext must be a possible decryption of C .

Therefore,

$|\mu| \leq |S| \leq |\text{Keys}|$

Hence proved.