

Network Security

Sumeet P Dash

August 31, 2009

Key Goals of Network Security

The three key goals of Network Security are as follows.

1. Data Integrity

The wholeness of data should be maintained during any operation.
In other words the data must be consistent and correct at all times.

2. Data Secrecy

The original data should only be accessible to the intended user.
Anyone eavesdropping on a network link shouldn't be able to get hold on any information exchanged between the communicating parties.

3. Data Availability

The network should be immune to node failures. It should be able to cater to the needs of its users with impressively high probability.
In simple terms the data must be available at the time of need.

Other concerns of security include Non-repudiation (The receiver of a message should be able to establish the identity of the sender), preventing unauthorized access, authentication etc. . .

Network as Evil Post Office

A computer network can be perceived as an evil post office which is constantly eavesdropping on every communication which passes through it. Given a chance it can harm the communicating parties in a number of ways like altering the message, changing its content, dropping the message, altering the recipient or the sender etc. . . The goal of network security is to ensure secure and timely communication in this hostile environment.

Threat Model

In computer security Threat Modelling deals with identifying the vulnerabilities of the system from an attacker's perspective. A threat model is defined for a piece software to help optimize its security features.

Crypto System

A cryptosystem can be defined as a triple (G,E,D) so that

G : Key Generator

E : M * Key \rightarrow C

D : C * Key \rightarrow M

where M = Plain Text; C = Cipher Text; K = Key and

$\forall Key, M : M = D_k(E_k(M))$

The One Time Pad

The One Time Pad(OPD) is arguably the most secure cryptosystem. The length of the key is essentially same as the length of message being transmitted. To ensure perfect secrecy the key or pad should be used only once. The encryption scheme is as follows: Keys = M = C = $\{0,1\}^l$

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

$D_k(C) = K \oplus C$

Proof of its Working:

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

Information Theoretic Security

For a given ciphertext of length l available to an intruder, the probability that the original text can be retrieved of it is

$$P_r[M = m|C = c] = 2^{-l}$$

Theoram

If (G,E,D) is information theoretically secure, then $|Keys| \geq |M|$.

Proof

Let $c \in C$ and $S = \{D_k(c)|k \in Keys\}$

By definition, $|S| \leq |Keys|$

and, since each message must be a possible decryption of c, $M \subseteq S$. Hence $|M| \leq |S| \leq |Keys|$. \square