

CSE-508 Network Security (Lecture 01)

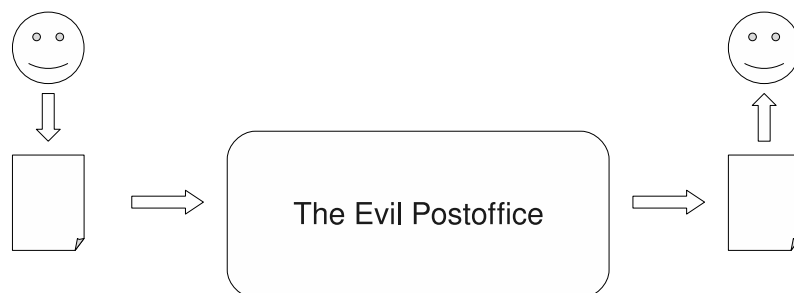
August 31, 2009

1 Goals

- Prevent unauthorized access
- Secure critical data
- Integrity
- Secrecy
- Authentication
- Non-repudiation
- Availability

2 Network as the Evil Post Office

The network and its users can be visualized as a set of people who want to send postcards to each other. The network itself is the Evil Post OfficeTM which is just there to spoil things for its users.



2.1 Stuff that an attacker can do to a message

- Read the message
- Read the source or destination address
- Change the message, or the address
- Drop the message
- Reorder a chain of messages
- Delay the message
- Replay the message

3 Cryptosystem

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

G : Key Generator

E : $Keys \times M \rightarrow C$

D : $Keys \times C \rightarrow M$

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

4 The One Time Pad

This is the only provably secure cryptographic technique that is known at present.

$$\begin{aligned} Keys = M = C &= \{0, 1\}^l \\ E(K, M) &= K \oplus M \\ D(K, C) &= K \oplus C \end{aligned}$$

Proof that it works :

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

5 Information Theoretic Security

If all that is available to an eavesdropper is the cyphertext, then

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

$$m \in M$$

$$k \in keys$$

where l is the length of the ciphertext

Theorem 1 *If (G,E,D) is information theoretically secure, then $|Keys| \geq |M|$*

Proof 1 *Let $c \in C$ and let $S = \{D(K, C) | k \in Keys\}$*

Now, $|S| \leq |Keys|$

Every plaintext must be in S because every plaintext must be a possible decryption of C . Hence proved.