

Network Security - CSE 508 - Fall 09

Faculty - Rob Johnson

Monday August 31, 2008

1 Goals of Network Security

1.1 Primary

- Integrity
- Secrecy
- Availability

1.2 Secondary

- Prevent unauthorized access
- Secure Critical data
- Authentication
- Non-repudiation

2 Threat Model - Scope of attack

- Content is readable
- Change destination/source address
- Read destination/source address
- Alter the message
- Drop message
- Spam nodes on the network
- Message injection
- Fake source address
- Re-order messages
- Delay messages
- Replay messages
- Any combination of the above

3 Chosen Plaintext attack

- In this form of attack, the attacker chooses the specific portions of the plain-text and hence obtains the corresponding cipher-text. The attacker obtains information about the encryption system from this.

4 Mathematical definition of a Cryptosystem

A cryptosystem is an encryption scheme which is a triple (G, E, D) where

- Key generator G
- Encryption function $E : Keys * M \rightarrow C$
- Decryption function $D : Keys * C \rightarrow M$

For a system to work, $D(K, E(K, M)) = M$

5 One Time Pad

- $Keyspace(K) = Mesg(M) = Ciphertext(C) = \{0, 1\}^l$
Encryption: $E(K, M) = K \oplus M = C$
Decryption: $D(K, C) = K \oplus C = M$
Hence : $D(K, E(K, M)) = K \oplus (K \oplus M) = (K \oplus K) \oplus M = M$

6 Information Theoretic Security

- In the situation that the eavesdropper knows only the ciphertext c ,
 $Pr[M = m | C = c] = 2^{-l}$
where $m \in M$ and $k \in Keys$

7 Theorem

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

- Proof: Let $c \in C$, then the set of all decryptions,

$$S = \{D(K, C) | K \in Keys\}$$

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

$$\text{and } |M| \subseteq |Keys|$$

$$\text{Hence } |Keys| \geq |M|$$