

NETWORK SECURITY GOALS

SECRECY

INTEGRITY

AVAILABILITY

PREVENT UNAUTHORIZED ACCESS

AUTHENTICATE

NON REPUDIATION

SECURE CRITICAL DATA

THREAT MODELS FOR NETWORK SECURITY

1)CONTENT OF MESSAGE READABLE

2)CHANGE DESTINATION/SOURCE ADDRESS

3) READ DESTINATION/SOURCE ADDRESS

4)CHANGE MESSAGE

5)DROP MESSAGE

6)SPAM

7)MESSAGE INJECTION

8)FAKE SOURCE ADDRESS

9)REORDER

10)DELAY

11)REPLAY

Crypanalytic Attack-Deriving plaintext from ciphertext without knowing any secret information such as keys or algorithm used eg by Frequency Analysis

Note- Idea of Frequency Analysis came 1200 years back from "Kuran"

Chosen Plaintext Attack- The attacker chooses the plaintext to be encrypted and gets the corresponding ciphertext. This may reveal the key .

DEFINITION -ENCRYPTION SCHEME

An Encryption scheme is a triple(G,E,D)

G:Keys

E: keys * M-> C

D:Keys * C->M

For every K,M $D(K,E(K,M))=M$

ONE TIME PAD

KEYS=M=C={0,1}^L

$E(K,M)=K \text{ XOR } M$

$D(K,C)=K \text{ XOR } C$

$D(K,E(K,M))=K \text{ XOR } (K \text{ XOR } M)$

$(K \text{ XOR } K) \text{ XOR } M=M$

Note – key is as long as the message and is a string of random bits which is used only once

IF WE REUSE THE KEY

$C1= K \text{ XOR } M1 \quad \text{Eq1}$

$C2=K \text{ XOR } M2 \quad \text{Eq2}$

HENCE $C1 \text{ XOR } C2 = M1 \text{ XOR } M2$

Note: This comes under Known ciphertext attack

We know the relative frequency of letters in English text –

Eg letter e has a relative frequency of 12.702%

2 overlapping e has a relative frequency of $.127 * .127=0.016129$

Hence the reuse of key may lead to analysis of frequency patterns

INFORMATION THEORETIC SECURITY

$$P_{K \in \text{keys}}[M=m] = 2^{-L}$$

$$P_{k \in \text{Keys}}[M=m/C=c] = 2^{-L}$$

i.e. It should not be possible to derive any information from cipher text

Fact – If (G, E, D) is information theoretically secure,

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

Proof – if $c \in C$ and let $S = \{D(k, c) \mid k \in \text{Keys}\}$

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

Every Plaintext must be in S because every plaintext must be a possible decryption of c