

Network Security

August 31, 2009

1 Security Goals

- Prevent Unauthorized Access: The message (or a resource) should be accessed only by those people whom it is intended for.
 - Secure Critical Data: Intruders should not be able to access the data.
 - Confidentiality or Secrecy: Protection of transmitted data from passive attacks.
 - Integrity: The receiver of a message should be able to verify that the message was not modified by an intruder.
 - Availability: People who are authorized to access the message (or resource) must be able to do so all the time.
 - Authentication: The receiver of a message should be able to verify the identity.
 - Non-Repudiation: A sender should not be able to falsely deny later that he did not put a signature or he did not send a message.
- Integrity, Secrecy and Availability are considered to be the three fundamental requirements of cryptography.

2 Threat Model

A Network is considered to be an Evil Post Office.

2.1 Characteristics of a Threat Model

- Contents of a message are readable.
- Change source/destination address.
- Change message.
- Drop message.

- Spam
- Message Injection
- Fake source address
- Reordering
- Delay messages
- Replay (Access to photocopies).

3 History of Cryptography

- The history of cryptography goes back to thousands of years.
- The first applications of cryptography is believed to be in the use of recipes about 2500 years ago.
- Widely used for many Military applications.
- Ceaser Cipher
- Scholars studying Quran found out an interesting fact about frequently occurring alphabets and they thought of implementing it in cryptanalysis.
- Enigma was used by Germans in World War II. The idea was invented by Arthur Scherbius and Arvid Gerhard Damn. Alan Turing is very well know for research on breaking the Enigma.
- Recently, many companies started using cryptographic techniques for banking purposes.

4 Defintion of a Cryptosystem

A cryptosystem is a triplet (G, E, D) where:

G: Set of all possible keys (Key Space).

E: Encryption; Keys * M = C i.e. $E_K(M) = C$.

D: Decryption; Keys * C = M i.e. $D_K(M) = M$.

The main goal of a cryptosystem is to get back the original message.

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

5 One-Time Pad

A one-time pad is a nonrepeating set of random key letters. The keyspace will be the same as Message Space and Cipher space.

$$K = \mu = C$$

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

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

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

Sometimes one-time pads are used in submarines. They burn some random keys into a CD.

Q. What happens if we reuse the key?

A. Consider the following:

$$C_1 = K \oplus m_1$$

$$C_2 = K \oplus m_2.$$

By Xoring both the equations, we get: $C_1 \oplus C_2 = m_1 \oplus m_2$

Hence, if we Xor the 2 ciphertexts and then perform the frequency test, then it is very likely that we will get back the message. Further, if the intruder knows either m_1 or m_2 then it will be very easy to get back the plaintext. This is known as known-plaintext attack.

6 Information Theoretic Security

Consider two persons Alice and Bob communicating with each other. In an Ideal situation, an intruder should not be able to see the cipher text that Alice has sent to Bob. However, in reality, the intruder will have access to the ciphertext and the algorithm. Let us denote the message as M and ciphertext as C . Then, $Pr_{m \in \mu, k \in Keys}[M = m/C = c] = 2^{-l}$.

In other words, given the ciphertext, the probability that we can retrieve the actual message is 2^{-l} .

Fact:

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

Proof: Let $c \in C$ and let $S =$ set of all decryptions of that ciphertext. Then $S = D(K, c)/K \in Keys$. Hence, $|S| \leq |Keys|$.

Every plaintext must be in S because every plaintext must be a possible decryption of C . Therefore, $|\mu| \leq |S| \leq |Keys|$.