Information and Network Security

Satvik Gupta

September 27, 2023

Contents

Information and Network Security

Symmetric Cryptography	Asymmetric Cryptography
Secret Key/Private Key Cryptography	Public Key Cryptography
1 key	2 keys
Faster	Slower
Less complex, less computationally expensive	More complex and more computationally expensive
Used to transfer bulk data	Used to exchange keys
Key sharing is unsafe	Key sharing is safe because of private key concept

Security Fundamentals

Security Goals

Confidentiality, Integrity, Availability (CIA)

Confidentiality

Allows authorized users to access sensitive data. Unauthz'd users shouldn't be able to access it.

Integrity

Changes in data should be done by authz'd entities,using authz'd mechanisms. Nobody else should be able to modify any data.

Availability

Data should be available to authorized users. Information is useless if we can't access it.

Security Attacks

Passive Attacks	Active Attacks
Makes use of system's information without harming it	May change or harm the system's data or resources
Goal is to obtain information. Difficult to detect.	Easier to detect than passive.
Attacks that threaten confidentiality are passive.	Attacks on integrity or availability are active.
Can be prevented by encipherment	
Snooping, Traffic Analysis	Masquerading, modification, repudiation, replaying, DoS

Attacks on Confidentiality

Snooping

Unauthorized access to or interception of data. Can be prevented by encipherment.

Traffic Analysis

Using pattern analysis, attacker can gain information about the sender/receiver, such as IP addresses. With enough data, they can also launch ciphertext-only attacks against the encryption algorithms used.

Attacks on Integrity

Modification

Changing information after intercepting it, before the receiver reads it. Deleting/delaying the message is also modification

Masquerading

Attacker impersonates someone else. Attacker can pretend to be sender or receiver.

Replaying

> The attacker obtains a copy of a message sent by a user and later tries to replay it. For example, a person sends a request to her bank to ask for payment to the attacker, who has done a job for her. The attacker intercepts the message and sends it again to receive another payment from the bank.

Repudiation

Denial by sender/receiver about having sent/received a message. For e.g, a sender may claim she did not ask the bank to transfer money.

Attacks on Availability

Denial of Service

Slow down or completely stop a system's service. Can be done by overwhelming a server, or intercepting a response so that it never reaches the recipient.

Security Services

- **Data Confidentiality**
- **Data Integrity** - prevents against modification as well as replaying
- **Authentication** - Authenticates sender/receiver in connection-based communication, and authenticates source of data in connectionless communication.
- **Non-repudiation** - Provides proof of origin and proof of delivery services.
- **Access-Control** -Protects against unauthz'd access of data.

Security Mechanisms

- **Encipherment**
- **Digital Signature**
- **Data Integrity** - add a checkvalue to the data.
- **AuthN Exchange** - exchange a message to prove identities. Eg - by sharing a secret only they're supposed to know.
- **Traffic Padding** - insert bogus data into data traffic to foil traffic analysis attempts
- **Routing Control** - keep on changing routes btw sender and receiver.
- **Access Control** - passwords, PINs, etc.
- **Notarization** - select a trusted third party to control communication. This is used to prevent repudiation.

Cryptography

Block vs Stream Cipher

Block Ciphers	Stream Ciphers
Take plaintext blocks at a time	Take plaintext 1 bit/1 byte at a time
Simple	Complex
Confusion + Diffusion	Only confusion
Reversing encrypted text is hard	Reversing encrypted text is easy
ECB, CBC	CFB, OFB

Shannon's Theory of Confusion and Diffusion

Diffusion

Relationship btw plaintext and ciphertext. Each symbol in plaintext should be dependent on some or all symbols in plaintext.

Confusion

Relationship btw key and ciphertext. If single bit in key is changed, most/all bits of cipher text should also change.

Feistel Cipher Structure

- Most block ciphers follow this.
- n rounds

One single round:

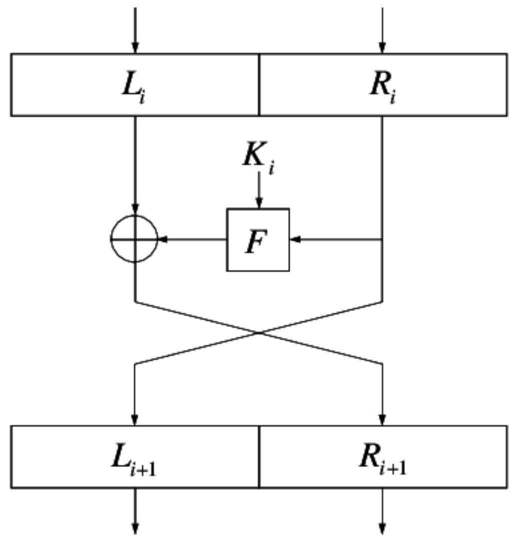

Figure 1: Illustration of a round in a Feistel network

K_i is a round key generated from the master key.

Security increases when:

- Block size is large
- Key size is large (which may decrease speed)
- No of rounds is more
- Subkey generation algorithm is complex
- Function F is complex.

DES

- Symmetric
- Block Cipher
- 16-round, 64-bit block size, 64-bit (which gets reduced to 56-bit) key, 48-bit round key Feistel cipher.

Steps:

- Initial permutation
- 16 rounds
- Swap left/right
- Final permutation (inverse of initial permutation)

Function F of DES

- L_i and R_i are 32-bit each.
- R_i is expanded to 48-bit using a Expansion p-box.
- Expanded R_i is XORed with K_i. The output produced (say B) is written as the concatenation of eight 6-bit strings ($B_1B_2B_3B_4B_5B_6B_7B_8$)
- DES has 8 S-boxes that convert each 6-bit B_i to a 4-bit value. This is done by the following process.
  - Suppose $B_i = 101110$.
  - First and last bit $10 = 2$ is the row number
  - All other 4 bits $0111 = 7$ is the column number
  - Row number 2 and Column number 7 will give the output for B_i.

S-box

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
1	00	15	07	04	14	02	13	10	03	06	12	11	09	05	03	08
2	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
3	15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13

Figure 2: S box

  - 2nd row (1) and 7th column (6) will give us value 13 = 1011
- This is done for all B_i. The output is concatenated, let's call it C
- C is passed through a straight permutation box that shuffles the 32-bits around. This is designed so that bits from output of each S-box are spread across 4 different S-boxes in the next round.
- The output of this P-box is the output of function F

Subkey-Generation Algorithm

- We take a 64-bit key and convert it to 56-bit.
  - Divide 64-bits into 8 parts of 8 bits each.
  - From each part, drop the last bit.
  - i.e, drop bit number 8,16,24…64
  - Use a P-box called Permuted-Choice 1 on the remaining bits to get a 56-bit key.
- This 56-bit key is used as a master key for generating subkeys.
- Subkey-gen algorithm works in 16 rounds to produce 16 subkeys.
- 56-bit key is divided into 2 parts - left and right, each of 28-bits.
- Each part is shifted left by 1 or 2 bits. In rounds 1,2,9,16 the shift is of 1 bit. In all other rounds it is of 2 bits.
- Through another P-box (Permuted-Choice 2), 48 of those 56 bits are selected and they form the round key.

Cryptanalysis of DES

Avalanche Effect

- Small change in plain text should create significant change in cipher text.
- DES is strong with this topic.

Completeness Effect

- Each bit in ciphertext should depend on many bits of plaintext.
- Confusion and Diffusion created by D-box and S-box shows very strong completeness effect.

Weaknesses

- Key size is only 56-bit (effectively). Can be brute-forced with modern computers.
- **Weak keys**

  - 4 out of 2^{56} keys are **weak**. These are keys which consists of all 0's or all 1's, or half 0's and half 1's (after the parity drop)
    * Encrypting with a weak key twice results in the **same block**
  - **Semi-weak keys** - 6 key-pairs are semi-weak. These create only 2 different round keys, each one being repeated 8 times.
  - **Possibly weak keys**- 48 such keys exist. Creates only 4 round keys. 16 round keys are divided into 4 groups, each group has 4 identical keys.

- **Key clustering** - 2 or more keys can create the same ciphertext.
- **Weakness in cipher design** - Two specifically chosen inputs to S-box can create same output.

Double DES

- $ciphertext = DES_{encrypt}(k_2, DES_{encrypt}(k_1, plaintext))$

Attack on Double DES (Meet in Middle Attack):

- DES is breakable through brute-force, i.e we can brute force 2^{56} keys
- Suppose we know plaintext p and ciphertext c
- Encrypt p with all possible values of k_1.
- Decrypt c with all possible values of k_2
- When the outputs for these match, we have found our keys.
  - Multiple key-pairs may match, but the number will be very small and we can brute-force it again.
- Therefore, double DES is only twice as secure as single DES.

Security of DES $=2^{56}$

Security of double DES $= 2^{57}$

Triple DES

- 2 or 3 keys
- Much stronger than double DES.

2-keys

$ciphertext = DES_{encrypt}(k_1, DES_{decrypt}(k_2, DES_{encrypt}(k_1, plaintext)))$

$plaintext = DES_{decrypt}(k_1, DES_{encrypt}(k_2, DES_{decrypt}(k_1, plaintext)))$

3-keys

$ciphertext = DES_{encrypt}(k_3, DES_{decrypt}(k_2, DES_{encrypt}(k_1, plaintext)))$

$plaintext = DES_{decrypt}(k_3, DES_{encrypt}(k_2, DES_{decrypt}(k_1, plaintext)))$