Network Security

Search this

Network Security: As millions of ordinary citizens are using networks for banking, shopping, and filling their tax returns, network security is looming on the horizon as a potentially massive problem.

Network security problems can be divided roughly into four interwined areas:

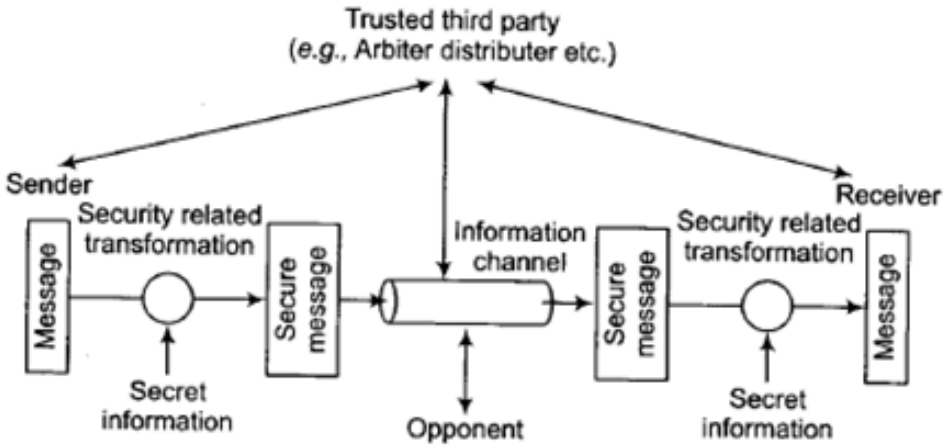
1. **Secrecy:** keep information out of the hands of unauthorized users.
2. **Authentication:** deal with determining whom you are talking to before revealing sensitive information or entering into a business deal.
3. **Nonrepudiation:** deal with signatures.
4. **Integrity control:** how can you be sure that a message you received was really the one sent and not something that a malicious adversary modified in transit or concocted?

There is no one single place — every layer has something to contribute:

- In the physical layer, wiretapping can be foiled by enclosing transmission lines in sealed tubes containing argon gas at high pressure. Any attempt to drill into a tube will release some gas, reducing the pressure and triggering an alarm (used in some military systems).
- In the data link layer, packets on a point-to-point line can be encoded.
- In the network layer, firewalls can be installed to keep packets in/out.
- In the transport layer, entire connection can be encrypted.

Model for Network Security

Network security starts with authenticating, commonly with a username and password since, this requires just one detail authenticating the username i.e., the password this is some times teamed one factor authentication.



A general Netwok Security Model (NSM)

Using this model require us to

- Design a suitable algorithm for the security transformation.
- Generate the secret in formations (keys) used by the algorithm.
- Develop methods to distribute and share the secret information.
- Specify a protocol enabling the principles to use the transformation and secret information for security service.

Cryptography

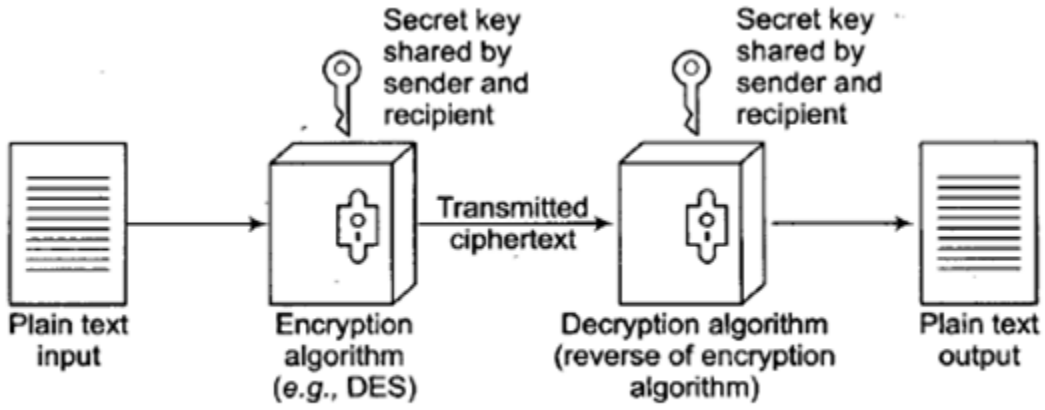
It is a science of converting a stream of text into coded form in such a way that only the sender and receiver of the coded text can decode the text. Nowadays, computer use requires automated tools to protect files and other stored information. Uses of network and communication links require measures to protect data during transmission.

Symmetric / Private Key Cryptography (Conventional / Private key / Single key)

Symmetric key algorithms are a class of algorithms to cryptography that use the same cryptographic key for both encryption of plaintext and decryption of ciphertext. The may be identical or there may be a simple transformation to go between the two keys.

In symmetic private key cryptography the following key features are involved

- Sender and recipient share a common key.
- It was only prior to invention of public key in 1970.
- If this shared key is disclosed to opponent, communications are compromised.
- Hence, does not protect sender form receiver forging a message and claiming is sent by user.



Symmetric cipher model (used in symmetric encryption)

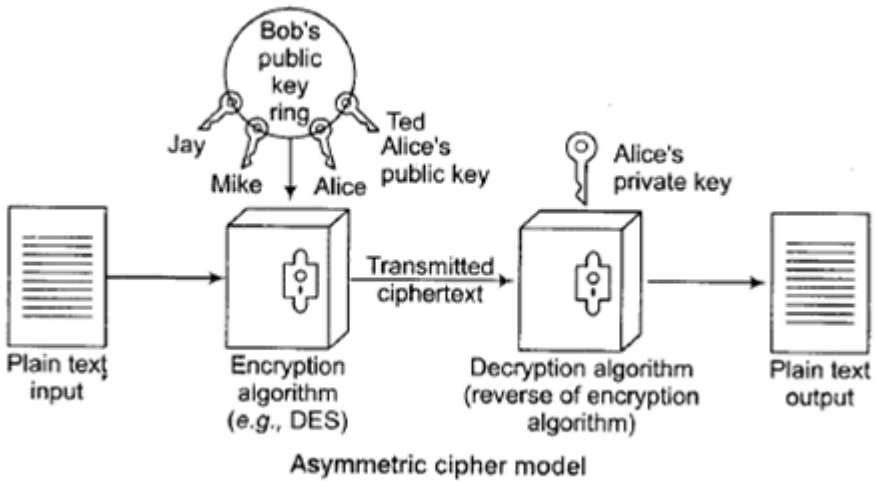
Advantage of Secret key Algorithm: Secret Key algorithms are efficient: it takes less time to encrypt a message. The reason is that the key is usually smaller. So it is used to encrypt or decrypt long messages.

Disadvantages of Secret key Algorithm: Each pair of users must have a secret key. If N people in world want to use this method, there needs to be N (N-1)/2 secret keys. For one million people to communicate, a half-billion secret keys are needed. The distribution of the keys between two parties can be difficult.

Asymmetric / Public Key Cryptography

A public key cryptography refers to a cyptogaphic system requiring two separate keys, one of which is secrete/private and one of which is public although different, the two pats of the key pair are mathematically linked.

- **Public Key:** A public key, which may be known by anybody and can be used to encrypt messages and verify signatures.
- **Private Key:** A private key, known only to the recipient, used to decrypt messages and sign (create) signatures. It is symmetric because those who encrypt messages or verify signature cannot decrypt messages or create signatures. It is computationally infeasible to find decryption key knowing only algorithm and encryption key. Either of the two related keys can be used for encryption, with the other used for decryption (in some schemes).



Asymmetric cipher model

In the above public key cryptography mode

- Bob encrypts a plaintext message using Alice’s public key using encryption algorithm and sends it over communication channel.
- On the receiving end side, only Alice can decrypt this text as she only is having Alice’s private key.

Advantages of Public key Algorithm:

1. Remove the restriction of a shared secret key between two entities. Here each entity can create a pair of keys, keep the private one, and publicly distribute the other one.
2. The no. of keys needed is reduced tremendously. For one million users to communicate, only two million keys are needed.

Disadvantage of Public key Algorithm: If you use large numbers the method to be effective. Calculating the cipher text using the long keys takes a lot of time. So it is not recommended for large amounts of text.

Message Authentication Codes (MAC)

In cryptography, a Message Authentication Code (MAC) is a short piece of information used to authenticate a message and to provide integrity and authenticity assurance on the message. Integrity assurance detects accidental and international message changes, while authenticity assurance affirms the message's origin.

A keyed function of a message sender of a message m computers MAC (m) and appends it to the message.

Verification: The receiver also computers MAC (m) and compares it to the received value.

Security of MAC: An attacker should not be able to generate a valid (m, MAC (m)), even after seeing many valid messages MAC pairs, possible of his choice.

MAC from a Block Cipher

MAC from a block cipher can be obtained by using the following suggestions

- Divide a massage into blocks.
- Compute a checksum by adding (or xoring) them.
- Encrypt the checksum.
- MAC keys are symmetric. Hence, does not provide non-repudiation (unlike digital signatures).
- MAC function does not need to be invertiable.
- A MACed message is not necessarily encrypted.

RSA Algorithm

RSA is an algorithm for public key cryptography RSA (Rivest Shamir Adleman) algorithm was publicly described in 1977.

Mathematical Background of RSA Algorithm

Extended Eucledian Algorithm: Given x, find y, such that $x \cdot y = 1 \bmod m$.

The extended Eucledian algorithm can efficiently find the solution to this problem.

Euler's Theorem: For any number, a relatively prime to

$$n = pq,\ a^{(p-1)(q-1)} = 1 \bmod pq$$

1. Why this is very useful?
2. Let $Z = k(p-1)(q-1) + r$, we have $a^2 = a^{k(p-1)(q-1)} \times a^r \ldots = a^r \bmod pq$
3. In other words, If $z = r \bmod (p-1)(q-1)$, then $a^z = a^r \bmod pq$

Special Case: If $z = 1 \bmod (p-1)(q-1)$, then $a^z = a \bmod pq$

We can use Euler's theorem to simplify $a^z \bmod pq$

RSA Algorithm

1. Let n = pq, where p and q are 2 large primes.
2. Public key (e, n), where e is relative prime to (p -1) (q -1)
3. Private key (d, n), such that $ed = 1 \bmod (p-1).(q-1)$ d can calculated using extended Eucledian Algorithm

Encryption: $c = m^e \bmod n$

Decryption: $cd = (m^e)^d = m^{ed} \bmod n$

Security of RSA: depends on the hardness of factoring.

factoring $n = p \times q$ is hard when n is large.

DES (Data Encryption Standard)

- The data encryption standard was developed in IBM.
- DES is a symmetric key crypto system.
- It has a 56 bit key.
- It is ***block cipher***, encrypts 64 bit plain text to 64 bit cipher texts.
- Symmetric cipher: uses same key for encryption and decryption
- It Uses 16 rounds which all perform the identical operation.
- Different subkey in each round derived from main key

- Depends on 4 functions: Expansion E, XOR with round key, S-box substitution, and Permutation.
- DES results in a ***permutation*** among the 2^{64} possible arrangements of 64 bits, each of which may be either 0 or 1. Each block of 64 bits is divided into two blocks of 32 bits each, a left half block **L** and a right half **R**. (This division is only used in certain operations.)

DES is a ***block cipher***–meaning it operates on plaintext blocks of a given size (64-bits) and returns cipher text blocks of the same size. Thus DES results in a ***permutation*** among the 2^{64} possible arrangements of 64 bits, each of which may be either 0 or 1. Each block of 64 bits is divided into two blocks of 32 bits each, a left half block **L** and a right half **R**. (This division is only used in certain operations.)

Authentication Protocols

Authentication: It is the technique by which a process verifies that its communication partner is who it is supposed to be and not an imposter. Verifying the identity of a remote process in the face of a malicious, active intruder is surprisingly difficult and requires complex protocols based on cryptography.

The general model that all authentication protocols use is the following:

- An initiating user A (*for Alice*) wants to establish a secure connection with a second user B (*for Bob*). Both and are sometimes called principals.
- Starts out by sending a message either to, or to a trusted **key distribution center (KDC)**, which is always honest. Several other message exchanges follow in various directions.
- As these message are being sent, a nasty intruder, T (for Trudy), may intercept, modify, or replay them in order to trick and When the protocol has been completed, is sure she is

talking to and is sure he is talking to. Furthermore, in most cases, the two of them will also have established a secret **session key** for use in the upcoming conversation.

In practice, for performance reasons, all data traffic is encrypted using secret-key cryptography, although public-key cryptography is widely used for the authentication protocols themselves and for establishing the (secret) session key.

Authentication based on a shared Secret key

Assumption: and share a secret key, agreed upon in person or by phone.

This protocol is based on a principle found in many **(challenge-response)** authentication protocols: one party sends a random number to the other, who then transforms it in a special way and then returns the result.

Three general rules that often help are as follows:

1. Have the initiator prove who she is before the responder has to.
2. Have the initiator and responder use different keys for proof, even if this means having two shared keys, and.
3. Have the initiator and responder draw their challenges from different sets.

Authentication using Public-key Cryptography

Assume that and already know each other’s public keys (a nontrivial issue).

Digital Signatures: For computerized message systems to replace the physical transport of paper and documents, a way must be found to send a “signed” message in such a way that

1. The receiver can verify the claimed identity of the sender.
2. The sender cannot later repudiate the message.
3. The receiver cannot possibly have concocted the message himself.

Secret-key Signatures: Assume there is a central authority, Big Brother (BB), that knows everything and whom everyone trusts.

If later denies sending the message, how could prove that indeed sent the message?

- First points out that will not accept a message from unless it is encrypted with.
- Then produces, and says this is a message signed by which proves sent to.
- is asked to decrypt , and testifies that is telling the truth.

What happens if replays either message?

- can check all recent messages to see if was used in any of them (in the past hour).
- The timestamp is used throughout, so that very old messages will be rejected based on the timestamp.

Public-key Signatures: It would be nice if signing documents did not require a trusted authority (e.g., governments, banks, or lawyers, which do not inspire total confidence in all citizens).

Under this condition,

- sends a signed message to by transmitting .
- When receives the message, he applies his secret key to get , and saves it in a safe place, then applies the public key to get .
- How to verify that indeed sent a message to ?
- Produces both and The judge can easily verify that indeed has a valid message encrypted by simply applying to it. Since is private, the only way could have acquired a message encrypted by it is if did indeed send it.

Another new standard is the **Digital Signature Standard (DSS)** based on the EI Gamal public-key algorithm, which gets its security from the difficulty of computing discrete logarithms, rather than factoring large numbers.

Message Digest

- It is easy to compute.
- No one can generate two messages that have the same message digest.
- To sign a plaintext, first computes, and performs , and then sends both and to .
- When everything arrives, applies the public key to the signature part to yield, and applies the well-known to see if the so computed agrees with what was received (in order to reject the forged message).