Network Security

- Motivation
  - Networks are essential components of organizational processes
  - Large investments in time and money in network infrastructures
  - Time is money.
  - Information is a valuable resource that must be protected.

Network Security

- Security perspectives
  - Privacy
  - Data integrity
  - Availability
    - Keeping the systems on-line

Network Security

- Consistency
  - The system should behave as expected
- Isolation
  - Regulating access to the system
- Audit
  - Determine what was done
  - To whom
  - What was effected

Network Security

- Security requirements
  - Secrecy
  - Integrity
  - Availability
- Different environments have different security concerns
- Security considerations
  - What do you want to protect
  - How much do you want to spend
  - How much does it cost to recover losses

Network Security

Threats

- Interruption
- Interception
- Modification
- Masquerade

Network Security

Threats

- Passive threats
  - Interception
  - Release of contents
  - Traffic analysis
- Active threats
  - Denial of services
  - Modification
  - Masquerade (Authenticity)

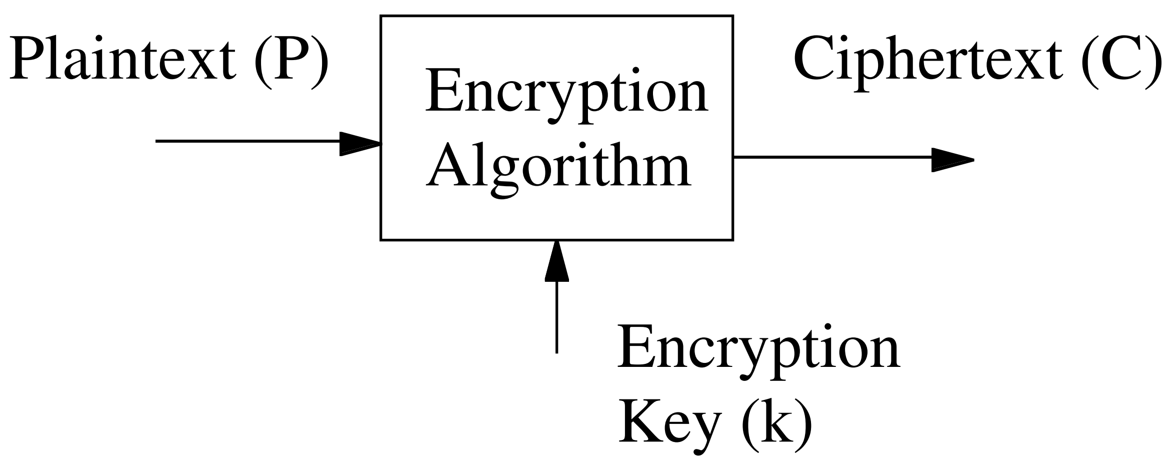
Network Security

- Approaches
  - Limit network access
  - Limit access to the physical infrastructure
  - Use fiber transmission facilities
  - Use encryption
  - Use authentication
  - Segment the system

Network Security

Encryption

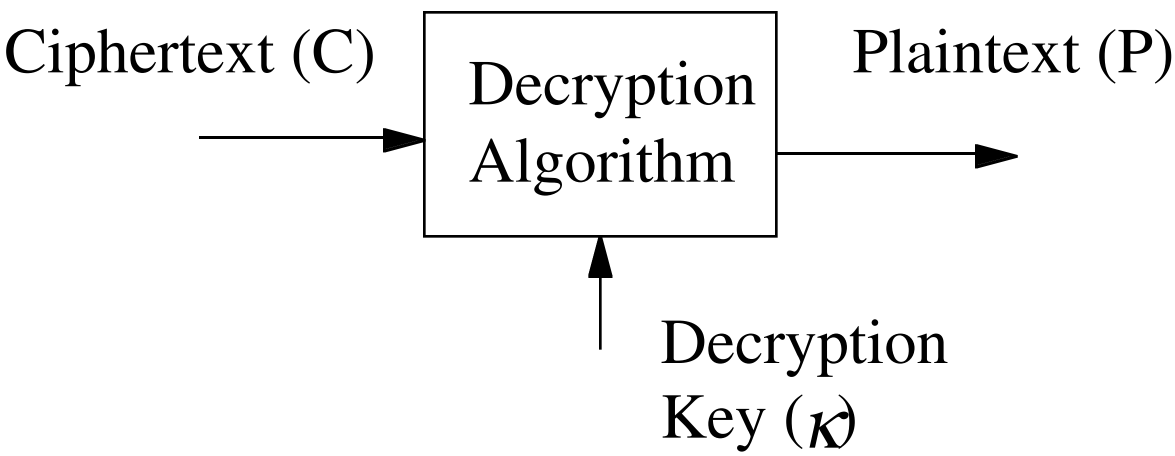
- Encryption is the process of transforming *plaintext* into *ciphertext* using and encryption algorithm and an encryption *key*.



$$C = E_k(P)$$

Network Security

Encryption



$$D_\kappa(C) = D_\kappa(E_k(P)) = P$$

Network Security

Encryption

- Encryption does:
  - Provides secrecy
  - Prevents tampering
  - Prevents forgery
- Encryption does not:
  - Keep attacker from deleting files so still need other tools

Network Security
Encryption

- Metrics of the security of an encrypted file
  - Secrecy of the key
  - Preventing successful key search
  - Breaking the encryption algorithm
  - No back doors, i.e., ways to decrypt the file without knowing the key
  - Given a partial decrypted message the ability to decrypt the entire file

Network Security
Encryption

- A simple encryption algorithm: the one-time pad
  - $C = P \oplus K$

Where P is a binary representation of the plain text and K is a random binary key the same length as P.

$$\begin{aligned}
&Let\\
&P = 011 \quad and \quad K = 101\\
&then\\
&C = 110.
\end{aligned}$$

To decrypt

$$P = C \oplus K$$

Network Security
Encryption

- Problems
  - Key can be used only once
  - The key must be *random*
  - The key must be of the same length as the plaintext

Network Security
Encryption

- Types of encryption systems
  - Private key systems
    - Same key used for both encryption and decryption algorithms
    - Data Encryption Standard (DES)
      (If available)
      - On Sun's
        des -e<infile | des -d outfile
  - Public key systems
    - One key used for encryption while another one used for decryption
    - RSA (Rivest, Shamir, Adleman)

Network Security

Public Key

- Two Keys
  - Public Key
    - Used to encrypt the message
    - Assume the encryption keys for users A and B are known publicly
    - User A forms

      $C_A = E_{k_B}(P)$

      User A sends C_A to B.

      User B decrypts C_A with a secret key κ_{B}

Network Security

Public Key

- Only user B can decrypt the message because only user B has the right key
- Requirements for a public key system
  - D(E(P)) = P
  - Very difficult to find D from E (note E will be known)
  - E cannot be broken by a *chosen plaintext* attack

(In a *chosen plaintext* attack the cryptanalyst can analyze chosen plaintext that is encrypted)

Network Security

Authentication

- Authentication
  - Receiver can verify identity of the sender
  - Sender can not later deny the message was sent
- Traditional approach is with passwords

Network Security

Authentication

- Use of public keys for authentication
  - Assume that the resource R wants to authenticate a request for services is from a user U
  - U gives R his public key
  - When U make a request, e.g., a session set up, R picks a random number, encrypts it with U's key and sends to to U

Network Security

Authentication

- U has to decode the message and return the random number to the R.
- Only U can do this.
- Copying the message and playing it back will not help an intruder because the random number is changed each time

Network Security

Digital Signatures

- Assume that
  - D(E(P))=P
  - E(D(P))=P
- User A sends
  $E_{k_B}(D_{\kappa_A}(P))$, i.e., A uses A's secret key κ_A
  as well as B's public key k_B.
  B finds $D_{\kappa_A}(P)$ using the privite key κ_{B} and
  finds P using the property that $E_{k_A}(D_{\kappa_A}(P)) = P$
  and knowing A's public key k_{A}

Network Security

Digital Signatures

- If A denies that the message was sent then B can produce
  - P
  - $D_{K_A}(P)$

The only way B could acquire a message encrypted by A is if A sent it.

Network Security

Kerberos

(The three headed watch dog of Hades)

- Kerberos is an authentication system
  - Pass sensitive information, e.g., **passwords**, over an open network
  - Add on to an existing network protocol

Network Security

Kerberos

- Elements of Kerberos
  - Users
  - Services
    - Things that user was access to
      - Computers
      - Applications
        - File service
        - mail
        - printers
    - Services have passwords

Network Security

Kerberos

- Authenticators
  - Special tokens that users sends to services to verify the right to access
  - Authenticators are encrypted and can be used only once
- Tickets
  - Tickets are cryptographic keys used to create authenticators
  - Tickets come in pairs
    - One for the user
    - One for the service
  - Tickets are encrypted

Network Security

Kerberos

- Ticket granting service
- Session Key
  - Cryptographic key used between the *ticket granting service* and the user.
  - Limited lifetime

Network Security

Kerberos

- Ticket granting ticket
  - Encrypted with the user's password
  - User gets a *ticket granting ticket* upon login
  - The ticket granting ticket contains all information needed for access to the *ticket granting service*

Network Security

Kerberos

- Kerberos Server
  - Master authentication server on the network
  - Contains the user's passwords
  - Physically secured
  - Verifies identity of users and services
  - Grants the *ticket granting ticket* that is used by the *ticket granting service*
- Passwords
  - Pick good passwords, ones not susceptible to **dictionary attacks**

Network Security

Kerberos

- Login in
  - To log into a network host the user performs same actions:
    - Login: frost
    - Password: XXXX
  - Host sends a message to the *Kerberos Server* with your user name.

Network Security

Kerberos

- If the name is in the server's data base then the server then sends a ticket back to the host that is a 'encrypted' with the user's password along other information
- The host then decrypts the ticket
  - If fails then the user can try again
  - Otherwise extracts
    - The session key
    - A ticket encrypted with the session key that will be used by the *Ticket Granting Service*
  - The server also sends a ticket (encrypted with the Ticket Granting Service's password) to the *Ticket Granting Service* with the user's name and session key
- The user is logged in

Network Security

Kerberos

- Passwords are NEVER transmitted in any form over the network
- All passwords are stored on the Kerberos Server

Network Security

Kerberos

- Access services
  - Host contacts the *Ticket Granting Service* for a ticket for the application, e.g., the file server service
  - The *Ticket Granting Service* sends the host a ticket for the application containing
    - A ticket for the application including
      - User's authenticated name
      - Expiration time
      - IP address of the host
      - All of this information is encrypted
    - The information from the *Ticket Granting Service* is encrypted so only the requesting host can read it

Network Security

Kerberos

- The host and the application server have a new key
- The exchange of information between the host and the *Ticket Granting Service* is encrypted with the Session key

Network Security

Kerberos

- The host decrypts the Application ticket using the session key and gets
  - Encryption key for communications between the host and the application
  - A ticket to present to the application which is encrypted with the application's secret key

Network Security

Kerberos

- The host then can request service from the application by sending an
  - *Authenticator*, i. e., encrypted request that contains
    - Host's IP address
    - Time of day (avoid **playback attack**)
    - Session key
    - The authenticator is encrypted with the host's secret key
  - Ticket is encrypted with the applications secret key
    - Contains the session key

Network Security

Kerberos

- The application decrypts the ticket with the applications secret key and gets the session key
- The applications decrypts the Authenticator with the session key
- If the information matches then the application provides the service