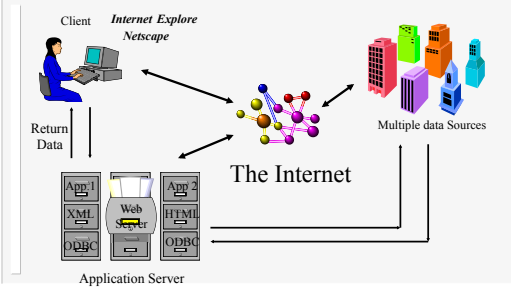
Ken Q. Yang

Data Path



Ken Yang, ECE. URI

Security Issues

- Now, Information is transferred over the Internet as opposed to Intranet/Extranet
- Do we want the information available to every one in the world?
- Who are authorized to get the information
- How is the authentication done?
- Define security policies
- Implement the policies

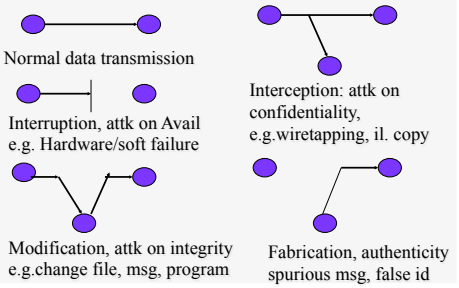
Ken Q. Yang, ECE. URI

Security Requirements

- **Secrecy**: Information is accessible to only authorized parties (Read,Print,Receive,Display)
- **Integrity**: Information can be modified by only authorized parties. (write,change,create,delete)
- **Availability:** Information is available to authorized parties

Ken Q. Yang, ECE. URI

Possible Attacks



Ken Yang, ECE. URI

Types of Attacks

- Passive attack: Interception
  - Release of message, traffic analysis
- Active attack:
  - Fabrication or Masquerade, (pretend to be some one else);
  - Modification of a msg,
  - Interruption and denial of svc,
- Data encryption, Fire Wall

Principles of Cryptography

- Plaintext---encryption-→ cypher-text,
- Cyphertext---decryption-→plaintext
- Symmetric key algorithm
- Public key algorithm

Ken Yang, ECE. URI

Traditional Encryption Methods

- Substitution Ciphers:
  - Each letter in a plaintext is replaced by another letter
  - *k-shift* shift text by k letters, k is the key
  - Random mapping with key being 26-letter string
- Transposition Ciphers:
  - Reorder the letters in a plaintext using a key rather than changing the letters

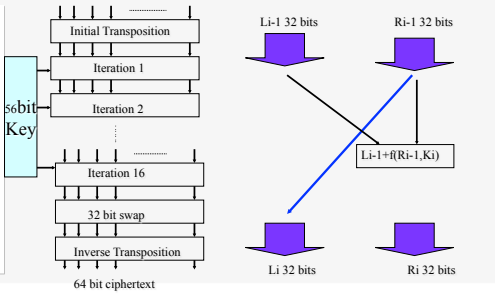
Ken Yang, ECE. URI

Examples of Traditional Encryptions

- Substitution Ciphers:
  - Key= *qwer tyui opas dfgh jklz xcvb nm*
  - *abcd efgh ijkl mnop qrst uvwx yz*
  - *attack* is transferred qzzqea
- Transposition (Permutation) Ciphers:
  - Key = MEGABUCK
  - plaintext=please send a million dollars to Q. Yang

Ken Yang, ECE. URI

Data Encryption Standard (DES)



Ken Yang, ECE. URI

Public Key Encryption

M = D (K_pub, E(K_prv, M));

and

M = D (K_prv, E(K_pub,M));

- To protect from passive attack,
  - use public key to encrypt messages, only the person with K_prv can read it
- To protect from active attach,
  - use K_prv to encrypt the message, receiver use the corresponding public key to decrypt
- To guarantee both authentic and private
  - 1st encrypt using sender's private key, 2rd encrypt using receiver's public key

Ken Yang, ECE. URI

Authentication vs Authorization

- Authentication deals with the question of whether or not you are actually communicating with a specific process
- Authorization is concerned with what that process is permitted to do

e.g. "I am Prof. Yang and I want to change Jack's grade from B to A"

- Is this actually Prof. Yang's process?
- Is Prof. Yang allowed to change Jack's grade?

Ken Yang, ECE. URI

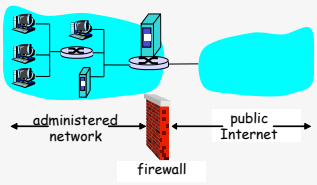
Firewalls

- To block unwanted network traffic into or out of a private network
- Packet filtering
  - Network layer
  - Transport layer
- Application Gateway
  - Application layer exam all messages and determine what messages are allowed to pass.

Firewalls

firewall

isolates organization's internal net from larger Internet, allowing some packets to pass, blocking others.



Firewalls: Why

prevent denial of service attacks:

- SYN flooding: attacker establishes many bogus TCP connections, no resources left for "real" connections.

prevent illegal modification/access of internal data.

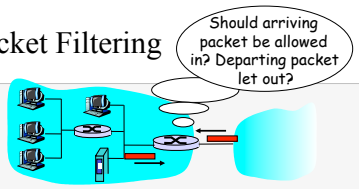
- e.g., attacker replaces CIA's homepage with something else

allow only authorized access to inside network (set of authenticated users/hosts)

two types of firewalls:

- application-level
- packet-filtering

Packet Filtering



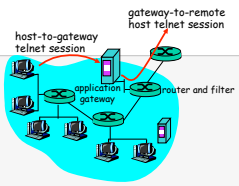
- internal network connected to Internet via router firewall
- router filters packet-by-packet, decision to forward/drop packet based on:
  - source IP address, destination IP address
  - TCP/UDP source and destination port numbers
  - ICMP message type
  - TCP SYN and ACK bits

Packet Filtering

- Example 1: block incoming and outgoing datagrams with IP protocol field = 17 and with either source or dest port = 23.
  - All incoming and outgoing UDP flows and telnet connections are blocked.
- Example 2: Block inbound TCP segments with ACK=0.
  - Prevents external clients from making TCP connections with internal clients, but allows internal clients to connect to outside.

Application gateways

- Filters packets on application data as well as on IP/TCP/UDP fields.
- Example: allow select internal users to telnet outside.



1. Require all telnet users to telnet through gateway.
2. For authorized users, gateway sets up telnet connection to dest host. Gateway relays data between 2 connections
3. Router filter blocks all telnet connections not originating from gateway.

Limitations of firewalls and gateways

- IP spoofing: router can't know if data "really" comes from claimed source
- if multiple app's. need special treatment, each has own app. gateway.
- client software must know how to contact gateway.
  - e.g., must set IP address of proxy in Web browser
- filters often use all or nothing policy for UDP.
- tradeoff: degree of communication with outside world, level of security
- many highly protected sites still suffer from attacks.