Outline

- Firewall Design Principles
  - Firewall Characteristics
  - Types of Firewalls
  - Firewall Configurations
- Trusted Systems
  - Data Access Control
  - The Concept of Trusted systems
  - Trojan Horse Defense
Firewalls

- Effective means of protecting a local system or network of systems from network-based security threats while affording access to the outside world via a WAN or the Internet.

Threat:

> While Internet provides benefits to organizations, it exposes the organizations’ systems to the outside world.
Firewall Design Principles

• Information systems undergo a steady evolution (from small LAN`s to Internet connectivity)
• Strong security features (like intrusion protection) for all workstations and servers is not a practical approach.
• Firewall is a popular approach to protect the assets.
Firewall Design Principles

• The firewall is inserted between the premises network and the Internet.

• Aims:
  - Establish a controlled link
  - Protect the premises network from Internet-based attacks
  - Provide a single choke point. (to keep the unauthorized users out of the protected network.)
Firewall Characteristics

- Design goals:
  - All traffic from inside to outside and outside to inside must pass through the firewall (physically blocking all access to the local network except via the firewall)
  - Only authorized traffic (defined by the local security policy) will be allowed to pass
  - The firewall itself is immune to penetration
Firewall Characteristics

Four general techniques to control access:

• Service control
  - Determines the types of Internet services that can be accessed, inbound or outbound

• Direction control
  - Determines the direction in which particular service requests are allowed to flow
Firewall Characteristics

• User control
  - Controls access to a service according to which user is attempting to access it

• Behavior control
  - Controls how particular services are used (e.g., it may enable external access to only a portion of local information).
Types of Firewalls

- Four common types of Firewalls:
  - Packet-filtering routers
  - Application-level gateways
  - Circuit-level gateways
  - Bastion hosts.
Types of Firewalls

- Packet-filtering Router
Types of Firewalls

• Packet-filtering Router
  - Applies a set of rules to each incoming IP packet and then forwards or discards the packet.
  - Filters packets going in both directions.
  - The packet filter is typically set up as a list of rules based on matches to fields in the IP or TCP header.
  - Two default policies (discard or forward).
Types of Firewalls

- Advantages:
  - Simplicity
  - Transparency to users
  - High speed

- Disadvantages:
  - Difficulty of setting up packet filter rules
  - Lack of Authentication (IP spoofing attacks possible)
Types of Firewalls

• Possible attacks and appropriate countermeasures

1. IP address spoofing
   //discard outside packets that contain an inside source address.//

2. Source routing attacks
   > Source specifies a route that a packet should take.
   > May bypass security measures.
   > Discard all packets with this option.
Types of Firewalls

• Possible attacks and appropriate countermeasures.

3. Tiny Fragment attacks:
   > Intruder uses IP fragmentation option to create extremely small fragments.
   > Forces TCP header information into a separate packet fragment.
   > Only the first fragment will be examined by the filtering router.
   >> Discard all such packets.
Types of Firewalls

• Application-level Gateway
Types of Firewalls

• Application-level Gateway
  - Also called proxy server
  - Acts as a relay of application-level traffic
Types of Firewalls

• Advantages:
  - Higher security than packet filters
  - Only need to scrutinize a few allowable applications
  - Easy to log and audit all incoming traffic

• Disadvantages:
  - Additional processing overhead on each connection (gateway as splice point)
Types of Firewalls

• Circuit-level Gateway
Types of Firewalls

- Circuit-level Gateway
  - Does not permit an end-to-end TCP connection.
  - Sets up two TCP connections
    > One between itself and inner TCP user.
    > Second between itself and outside TCP host.
  - The gateway typically relays TCP segments from one connection to the other without examining the contents.
Types of Firewalls

• Circuit-level Gateway
  - The security function consists of determining which connections will be allowed
  - Typically use is a situation in which the system administrator trusts the internal users.

  //low processing overheads.//
Types of Firewalls

• Bastion Host
  - A system identified by the firewall administrator as a critical strong point in the network’s security
  - The bastion host serves as a platform for an application-level or circuit-level gateway
Firewall Configurations

• In addition to the use of simple configuration of a single system (single packet filtering router or single gateway), more complex configurations are possible.

• Three common configurations.
Firewall Configurations

- Screened host firewall system
  (single-homed bastion host)
Firewall Configurations

Firewall consists of two systems:

- A packet-filtering router
- A bastion host

>Only packets from and to the bastion host are allowed to pass through the router.

- From Internet, only IP packets destined for the bastion host are allowed.
- From internal network, only IP packets from bastion host are allowed out.
Firewall Configurations

• Greater security than single configurations because of two reasons:
  - This configuration implements both packet-level and application-level filtering (allowing for flexibility in defining security policy).
  - An intruder must generally penetrate two separate systems.
Firewall Configurations

• Provides flexibility in having direct access from Internet.
• Internal network may include an information server for which tighter security is not required (like a Web server).
• The router can allow direct traffic between the Internet and the information server.
Firewall Configurations

- Screened host firewall system (dual-homed bastion host)
Firewall Configurations

- Traffic between the Internet and other hosts on the private network has to flow through the bastion host.

- If the packet-filtering router is completely compromised, traffic will not flow freely between Internet and protected network.
Firewall Configurations

- Screened-subnet firewall system
Firewall Configurations

> Most secure configuration of the three.
> Two packet-filtering routers are used.
> Creation of an isolated sub-network.
Firewall Configurations

• Advantages:
  - Three levels of defense to thwart intruders.
  - The outside router advertises only the existence of the screened subnet to the Internet (internal network is invisible to the Internet)
  - Inside router advertises only the existence of the screened subnet to the internal network. (an inside host can not construct direct route to the Internet.)
Trusted Systems

- One way to enhance the ability of a system to defend against intruders and malicious programs is to “implement trusted system technology”.

32
Data Access Control

• Through the user access control procedure (log on), a user can be identified to the system.

• Associated with each user, there can be a profile that specifies permissible operations and file accesses.

• The operating system can enforce rules based on the user profile.
Data Access Control

- General models of access control:
  - Access matrix
  - Access control list
  - Capability list
Data Access Control

- Access Matrix

<table>
<thead>
<tr>
<th></th>
<th>Program1</th>
<th>SegmentA</th>
<th>SegmentB</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process1</td>
<td>Read</td>
<td>Read</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Process2</td>
<td>Execute</td>
<td>Write</td>
<td>Read</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

Page 34.
Data Access Control

- **Access Matrix**: Basic elements of the model
  - **Subject**: An entity capable of accessing objects. The concept of subject equates with that of process.
  - **Object**: Anything to which access is controlled (e.g. files, programs).
  - **Access right**: The way in which an object is accessed by a subject (e.g. read, write, execute).
Data Access Control

• Access Control List: Decomposition of the matrix by columns

| Access Control List for Program1:          |
| Process1 (Read, Execute)                  |
| Access Control List for SegmentA:         |
| Process1 (Read, Write)                    |
| Access Control List for SegmentB:         |
| Process2 (Read)                           |
Data Access Control

• Access Control List
  - An access control list lists users and their permitted access rights.
  - The list may contain a default or public entry.
Data Access Control

- Capability list: Decomposition of the matrix by rows

<table>
<thead>
<tr>
<th>Capability List for Process 1:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Program 1 (Read, Execute)</td>
</tr>
<tr>
<td>Segment A (Read, Write)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Capability List for Process 2:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Segment B (Read)</td>
</tr>
</tbody>
</table>
Data Access Control

• Capability list
  - A capability ticket specifies authorized objects and operations for a user.
  - Each user have a number of tickets.
  - Capabilities are not forgeable.
The Concept of Trusted Systems

• Levels of Security
  - Protection of data and resources on the basis of levels of security (e.g., military, unclassified, confidential, secret, top secret.)
  - Users can be granted clearances to access certain categories of data.
The Concept of Trusted Systems

• Multilevel security
  - Definition of multiple categories or levels of data

• A multilevel secure system must enforce:
  - No read up: A subject can only read an object of less or equal security level (Simple Security Property)
  - No write down: A subject can only write into an object of greater or equal security level (*-Property)
The Concept of Trusted Systems

• Reference Monitor Concept: Multilevel security for a data processing system
The Concept of Trusted Systems
The Concept of Trusted Systems

- Reference Monitor
  - Controlling element in the hardware and operating system of a computer that regulates the access of subjects to objects on basis of security parameters
  - The monitor has access to a file (security kernel database)
  - The monitor enforces the security rules (no read up, no write down)
The Concept of Trusted Systems

• Properties of the Reference Monitor
  - Complete mediation: Security rules are enforced on every access.
  - Isolation: The reference monitor and database are protected from unauthorized modification.
  - Verifiability: The reference monitor’s correctness must be provable (mathematically).
Trojan Horse Defense

• Secure, trusted operating systems are one way to secure against Trojan Horse attacks
Trojan Horse Defense
Trojan Horse Defense