Computer Security and Cryptography

CS381

Access Control and Firewall

来学嘉
计算机科学与工程系 电院3-423室
34205440 1356 4100825 laix@sjtu.edu.cn
2016-05

Organization

- Week 1 to week 16 (2016-02-24 to 2016-06-08)
- 东上院502
- Monday 3-4节; week 9-16
- Wednesday 3-4节; week 1-16
- lecture 10 + exercise 40 + random tests 40 + other 10
- Ask questions **in** class – counted as points
- Turn ON your mobile phone (after lecture)
- Slides and papers:
  - http://202.120.38.185/CS381
    - **computer-security**
  - http://202.120.38.185/references
- TA: '薛伟佳' icelikejia@qq.com，'黄格仕' <huang.ge.shi@foxmail.com>
- Send homework to: laix@sjtu.edu.cn and to TAs

Rule: do not disturb others!

2

Contents

- Introduction -- What is security?
- Cryptography
  - Classical ciphers
  - Today's ciphers
  - Public-key cryptography
  - Hash functions/MAC
  - Authentication protocols
- Applications
  - Digital certificates
  - Secure email
  - Internet security, e-banking

Network security
- SSL
- IPSEC
- Firewall
- VPN

Computer security
- Access control
- Malware
- DDos
- Intrusion

Examples
- Bitcoin
- Hardware
- Wireless

3

overview

IT-security
- Definition
- 5 services
- 1-way function →

Classical Shannon

Security Un/condition

Integer factor Discrete log

Block cipher Stream cipher | **Hash MAC** | **PKC signature**

Key-manage →

Kerberos

Certificate PKI

Intrusion Malware

Firewall

IPSEC VPN

SSL TLS

PGP S/MIME

applications

4

contents

- Access Control
- Firewall
  - Firewall characteristics
  - Types of Firewall
  - Firewall Architecture

- ISO7498-2 defines five security services:
  - Authentication
  - **Access Control**
  - Data Confidentiality
  - Data Integrity
  - Non-repudiation

Access Control

- Access control refers to exerting control over who can interact with a resource.
  - What you are allowed to do.
  - Focus is policy
- The goal of access control
  - protect resources from unauthorized access
- Basic rule [Bell-LaPadula Confidentiality Model]
  - no read up
  - no write down

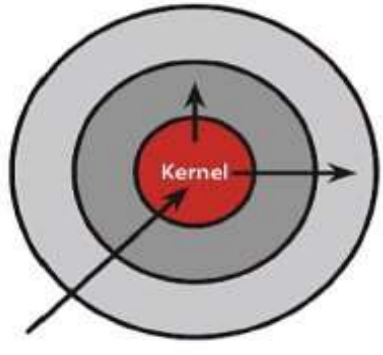
Bell–LaPadula model

- **Bell–LaPadula** (**BLP**) **Model** is a state machine model used for enforcing access control in government and military applications
- a formal state transition model of computer security policy
- focuses on data confidentiality and controlled access to classified information, the entities in system are divided into subjects and objects
- Mandatory rules
  1. a subject at a given security level may not read an object at a higher security level (**no read-up**).
  2. a subject at a given security level must not write to any object at a lower security level (**no write-down**).
- Discretionary rules
  - use of an access matrix to specify the access control
- Limitation: Only addresses confidentiality and control of writing

8

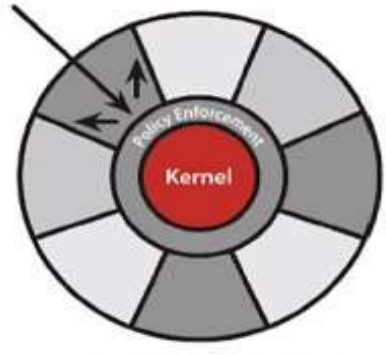
Access Control

- Discretionary Access Control
  - Restrict access to objects based on the identity of subjects and/or groups to which they belong.
  - allows users the ability to make policy decisions and/or assign security attributes.
  - flexibility
- Mandatory Access Control
  - Whenever a subject attempts to access an object, an authorization rule enforced by the operating system kernel examines these security attributes and decides whether the access can take place.
  - More secure



Discretionary Access Control

Once a security exploit gains access to priveleged system component, the entire system is compromised.



Mandatory Access Control

Kernel policy defines application rights, firewalling applications from compromising the entire system.

Access Control : Access Matrix

- A set of subjects S
- A set of objects O
- A set of rights R
- An access control matrix
  - one row for each subject
  - one column for each subject/object
  - elements are right of subject on another subject or object

	File 1	File 2	File 3	File 4	Account 1	Account 2
John	Own R W		Own R W		Inquiry Credit	
Alice	R	Own R W	W	R	Inquiry Debit	Inquiry Credit
Bob	R W	R		Own R W		Inquiry Debit

Access Control Issues

- Preventing Access
  - Prevent users form accessing privileged data or resources
- Limiting Access
  - Need to allow some access but not full access
- Granting Access
  - Give new access or greater access.
- Revoking Access
  - Take back some or all of granted access.

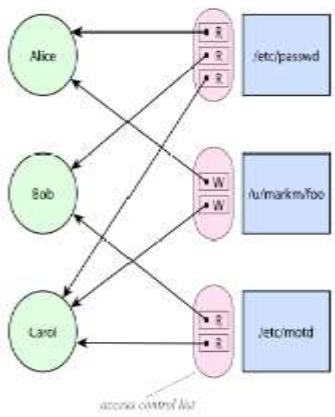
Methods of Access Control

- Access Control Lists
  - Access control associated with the resource
  - Can prevent and revoke access
  - Cannot limit or grant access
- Capability Lists
  - Access control associated with the user
  - Can prevent , limit , and grant access
  - Can revoke but not likely expected

Access Control

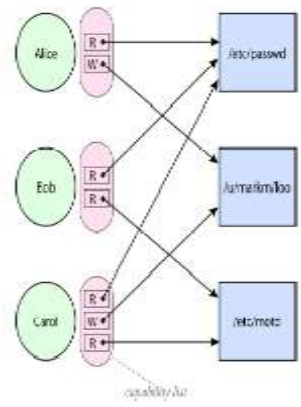
ACL Diagram

from resources to subjects

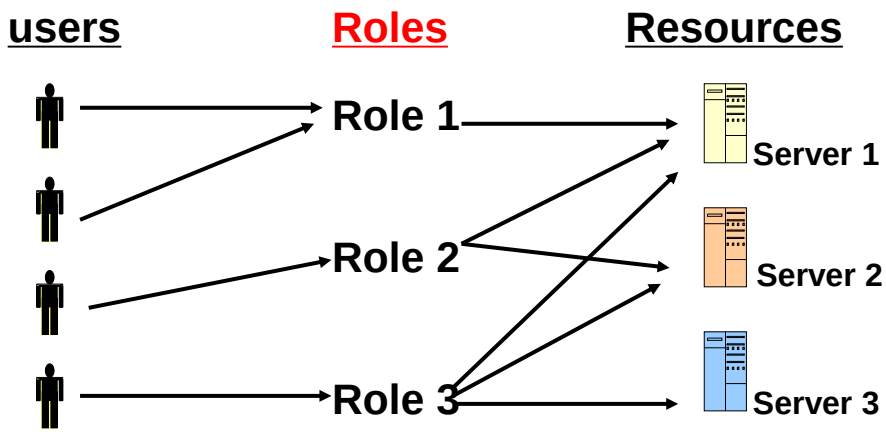


Capability Diagram

- from subjects to resources



RBAC Role-Based-Access-Control



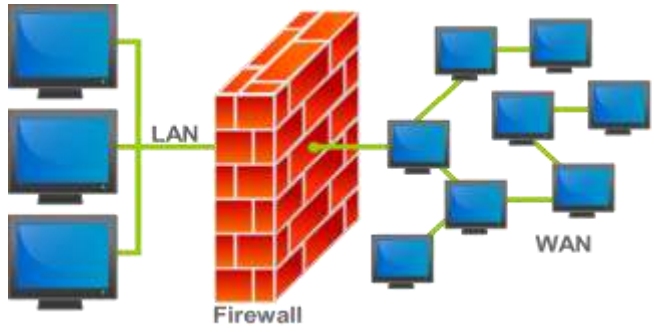
User's change frequently, Roles don't

Access Control

- Access Control
- Firewall
  - Firewall characteristics
  - Types of Firewall
  - Firewall Architecture

Firewall

- Access control are the rules to be implemented for security
- while firewall is the complete setup or mechanism.



Firewall

- An example of a user interface for a firewall on Ubuntu

- Access Control
- Firewall
  - Firewall characteristics
  - Types of Firewall
  - Firewall Architecture

Firewall characteristics

1. All traffic from inside to outside, and vice versa, must pass through the firewall.
   - This is achieved by physically blocking all access to the local network except via the firewall.
2. Only authorized traffic, as defined by the local security policy, will be allowed to pass.
   - Various types of firewalls are used, which implement various types of security policies.

The firewall itself is immune to penetration.

- This implies the use of a hardened system with a secured operating system.

Firewall characteristics

control abilities

- **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 may be initiated and allowed to flow through the firewall
- **User control**
  - Controls access to a service according to “who is attempting to access it”.
- **Behavior control**
  - Controls how particular services are used.

Firewall characteristics

Capabilities:

- choke point
- monitor security-related events
- a convenient platform for several other functions
- serve as the platform for IPSec/VPN

Limitations

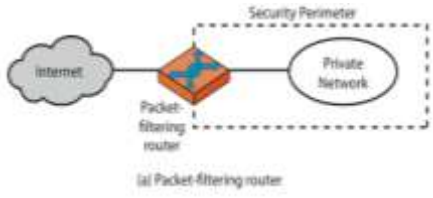
- **1- against attacks that bypass the firewall?** ✗
- **2- against internal threats?** ✗
- **3- guard against wireless communications between local systems on different sides of the internal firewall?** ✗
- **4- protect against the transfer of virus-infected programs or files?** ✗

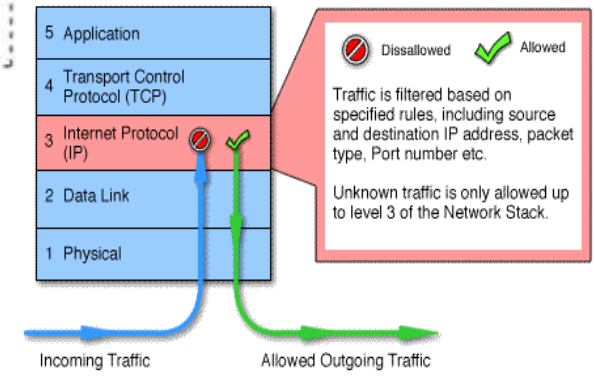
Types of Firewall

- Access Control
- Firewall
  - Firewall characteristics
  - Types of Firewall
    - Packet Filtering Firewall
    - Stateful Inspection Firewalls
    - Application-level gateways
    - Circuit-level gateways
  - Firewall Architecture

Types: Packet Filtering Firewall

- Apply a set of rules to each incoming and outgoing IP packet and then forwards or discards the packet





For example
Allow all outgoing traffic
Block all incoming traffic
It's 1-way!

Types: Packet Filtering Firewall

- Filtering rules are based on information contained in a network packet:
  - Source IP address
  - Destination IP address
  - Source and destination transport-level address
  - IP protocol field
  - Interface

Types: Packet Filtering Firewall

- Two default policies
  - Default=forward
    - what is not expressly prohibited is permitted.
  - Default=discard
    - what is not expressly permitted is prohibited.

action	ourhost	port	theirhost	port	comment
block	*	*	*	*	*default*

Example1

- allow inbound mail (SMTP, port 25) but only to our gateway machine.
- But mail from some particular site SPIGOT is to be blocked.

action	ourhost	port	theirhost	port	comment
block	*	*	SPIGOT	*	*we don't trust these people*
allow	OUR-GW	25	*	*	*connection to our SMTP port*

Types: Packet Filtering Firewall

Example 2

- If we want to implement the policy "any inside host can send mail to the outside".

action	ourhost	port	theirhost	port	comment
allow	*	*	*	25	*connection to their SMTP port*

This solution allows calls to come from any port on an inside machine, and will direct them to port 25 on the outside.

Types: Packet Filtering Firewall

action	ourhost	port	theirhost	port	comment
allow	*	*	*	25	*connection to their SMTP port*

The problem with this rule:

- Our defined restriction is based solely on the outside host's port number, which we have no way of controlling.
- Now an enemy can access any internal machines and port by originating his call from port 25 on the outside machine.

What can be a better solution ?

Types: Packet Filtering Firewall

action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	25		*our packets to their SMTP port*
allow	*	25	*	*	ACK	*their replies*

- The ACK signifies that the packet is part of an ongoing conversation
- Packets without the ACK are connection establishment messages, which we are only permitting from internal hosts

Types: Packet Filtering Firewall

Advantage

- simple
- transparent
- fast

Disadvantage

- do not examine upper-layer data
- limited logging functionality
- do not support advanced user authentication schemes
- Vulnerable to attacks and exploits that take advantage of problems within the TCP/IP specification and protocol stack
- Susceptible to security breaches caused by improper configurations

Types: Packet Filtering Firewall

Attacks

- IP address spoofing
  - fake source address to be trusted
  - *add filters on router to block*
- source routing attacks
  - attacker sets a route other than default
  - *block source routed packets*
- tiny fragment attacks
  - split header info over several tiny packets
  - *either discard or reassemble before check*

Types : Stateful Inspection Firewall

- stateful packet filters examine each IP packet in context
  - keep track of client-server sessions
  - check each packet validly belongs to one
- hence are better able to detect bogus packets out of context

Example

- SMTP server(25) ←→SMTP client(1024-65533)

- packet filtering firewall: permit inbound network traffic on all these high-numbered ports for TCP-based traffic to occur

Types: Stateful Inspection Firewall

Stateful inspection firewall:

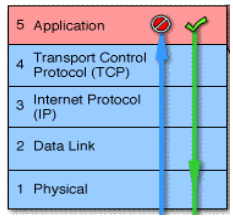
- allow incoming traffic to high-numbered ports only for those packets that fit the profile of one of the entries in the directory

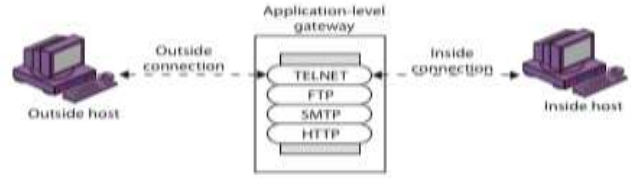
Table 11.2 Example Stateful Firewall Connection State Table [WACK02]

Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	210.22.88.29	80	Established
192.168.1.102	1031	216.32.42.123	80	Established
192.168.1.101	1033	173.66.32.122	25	Established
192.168.1.106	1035	177.231.32.12	79	Established
223.43.21.231	1990	192.168.1.6	80	Established
2122.22.123.32	2112	192.168.1.6	80	Established
210.922.212.18	3321	192.168.1.6	80	Established
24.102.32.23	1025	192.168.1.6	80	Established
223.21.22.12	1046	192.168.1.6	80	Established

Types: Application-level gateway

- Gateway that is configured to be a web proxy will not allow any ftp, gopher, telnet or other traffic through





(b) Application-level gateway

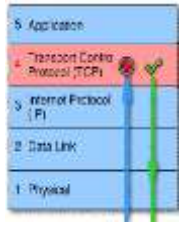
- acts as a relay of application-level traffic
  - User: provide a valid user ID and authentication information
  - Gateway: contact the application on the remote host; relay TCP segments containing the application data between the two endpoints

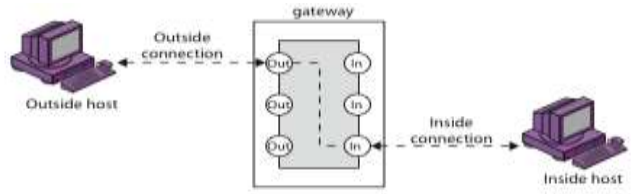
Types: Application-level gateway

- Advantage
  - more secure than packet filters
  - only scrutinize a few allowable applications
  - easy to log and audit all incoming traffic at the application level
- Disadvantage
  - Additional processing overhead on each connection

Types: Circuit-level gateway

- set up two TCP connections:
  - between itself and a TCP user on an inner host
  - between itself and a TCP user on an outside host





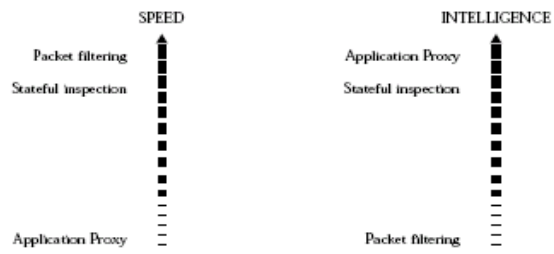
(c) Circuit-level gateway

- once created usually relays traffic without examining contents
- typically used when trust internal users by allowing general outbound connections

Types of Firewall: comparison

FIREWALL PERFORMANCE SUMMARY

Technology	Speed	Flexibility	Intelligence
Packet filtering	V. Good	V.Good	Low
Application Proxy	Low	Low	V. Good
Stateful inspection	Good	Good	Good
Circuit gateway	Low	Low	Low

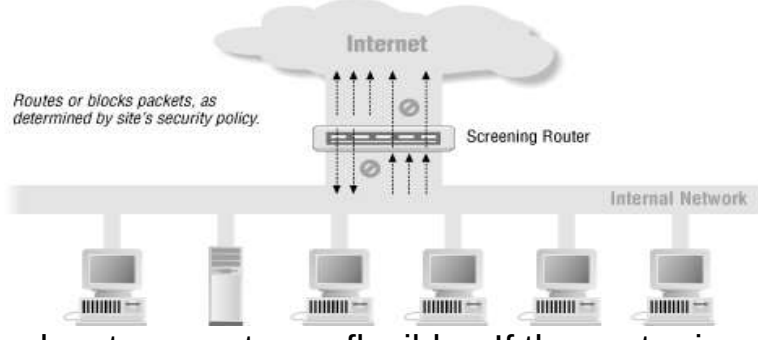


contents

- Access Control
- Firewall
  - Firewall characteristics
  - Types of Firewall
    - Packet Filtering Firewall --Stateful Inspection Firewalls
    - application-level gateways --circuit-level gateways
  - Firewall Architecture
    - Screening Router
    - Dual-Homed Host
    - Screened Host
    - Screened Subnet

Screening Router Architecture

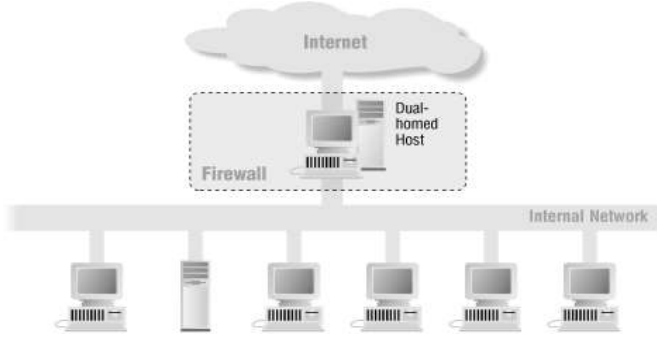
- The communication is restricted to the type that is allowed by a screening router



Disadvantage: not very flexible; If the router is compromised, you have no further security

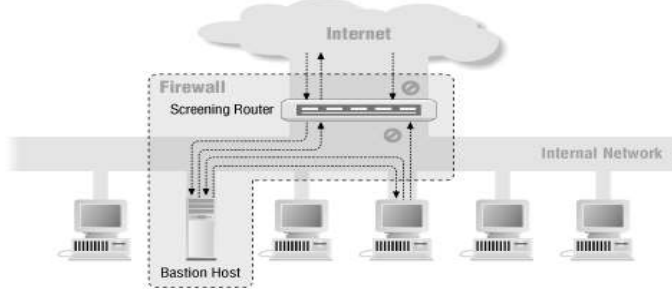
Dual-Homed Host Architecture

– One port connects to the *Local Network* and the other port/ports connects to the Internet.
– provide services by proxying them



Screened Host Architecture

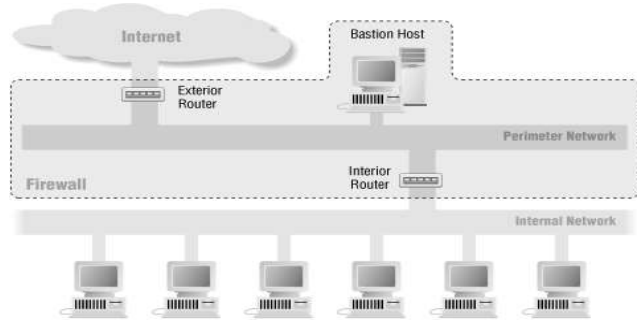
– the bastion host is the only system on the internal network that hosts on the Internet can open connections to



– Disadvantage: If someone successfully breaks into the bastion host in a screened host architecture, that intruder has hit the jackpot.

Screened Subnet Architectures

– add a perimeter network that further isolates the internal network from the Internet.



– By isolating the bastion host on a perimeter network, you can reduce the impact of a break-in on the bastion host.

Summary

- Access Control
  - – Access matrix; ACL; Capability list
- Firewall
  - – Firewall characteristics
  - – Types of Firewall
    - Packet Filtering Firewall --Stateful Inspection Firewalls
    - application-level gateways --circuit-level gateways
  - – Firewall Architecture
    - Screening Router --Dual-Homed Host
    - Screened Host --Screened Subnet

Exercise 16

1. What is the purpose of access control?
2. Describe the different methods of access control
3. Describe the different types of firewall

Deadline: before next lecture