Computer Security DD2395

http://www.csc.kth.se/utbildning/kth/kurser/DD2395/dasakh11/

Fall 2011

Sonja Buchegger
buc@kth.se

Lecture 9

Firewalls, Multilevel Security

Course Admin

- Master's:
  - Lab 1: 3 CORRECT mails means passed, results in RAPP later this week
  - Lab 2: prepare before lab session, sign up
  - Lab 3: prepare: webgoat, gruyere; instructions
  - Lab 4:
    - sign up for topics and presentation times
    - finding group partners: meet here during break

Firewalls

- Stop fire from spreading
- History:
  - Separate kitchen from rest
  - Castles, moats
  - Chinese wall
  - Coal-powered trains

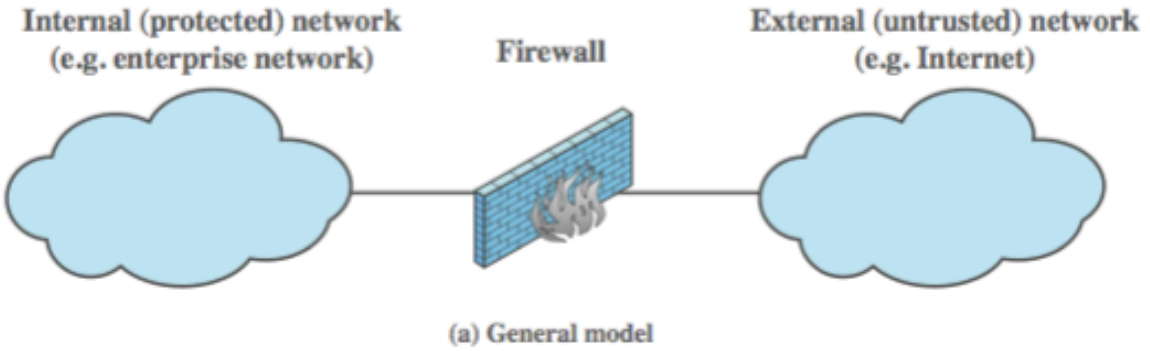
Firewalls and Intrusion Prevention Systems

- effective means of protecting LANs
- internet connectivity essential
  - for organization and individuals
  - but creates a threat
- could secure workstations and servers
- also use firewall as perimeter defence
  - single choke point to impose security

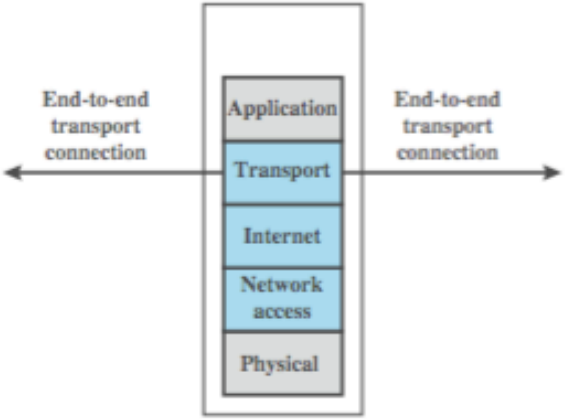
Firewall Capabilities & Limits

- capabilities:
  - defines a single choke point
  - provides a location for monitoring security events
  - convenient platform for some Internet functions such as NAT, usage monitoring, IPSEC VPNs
- limitations:
  - cannot protect against attacks bypassing firewall
  - may not protect fully against internal threats
  - improperly secure wireless LAN
  - laptop, PDA, portable storage device infected outside then used inside

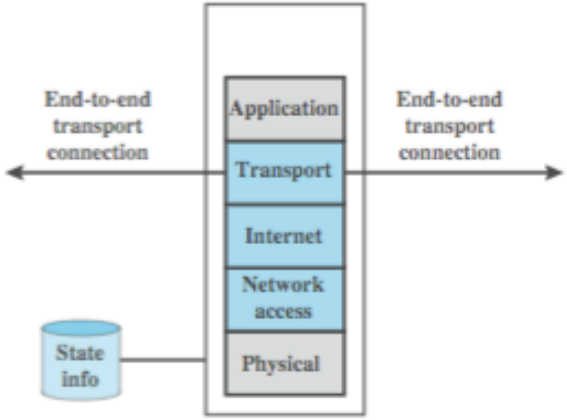
Types of Firewalls



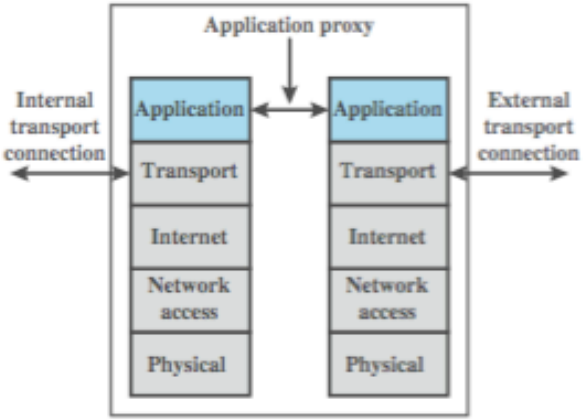
(a) General model



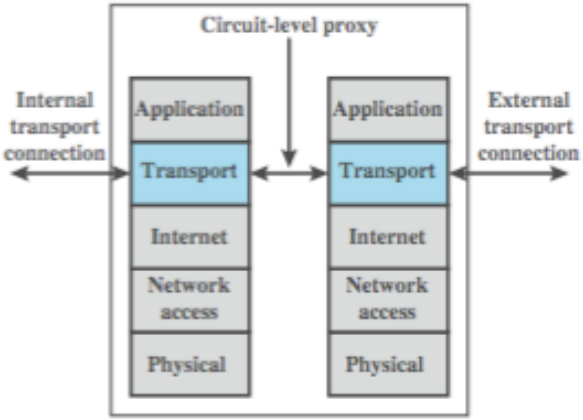
(b) Packet filtering firewall



(c) Stateful inspection firewall



(d) Application proxy firewall



(e) Circuit-level proxy firewall

Packet Filtering Firewall

- applies rules to packets in/out of firewall
- based on information in packet header
  - src/dest IP addr & port, IP protocol, interface
- typically a list of rules of matches on fields
  - if match rule says if forward or discard packet
- two default policies:
  - discard - prohibit unless expressly permitted
    - more conservative, controlled, visible to users
  - forward - permit unless expressly prohibited
    - easier to manage/use but less secure

Packet Filter Rules

Rule Set A

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

Rule Set B

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

Rule Set C

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

Rule Set D

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

Rule Set E

action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	*		our outgoing calls
allow	*	*	*	*	ACK	replies to our calls
allow	*	*	*	>1024		traffic to nonservers

Packet Filter Weaknesses

- weaknesses
  - cannot prevent attack on application bugs
  - limited logging functionality
  - do no support advanced user authentication
  - vulnerable to attacks on TCP/IP protocol bugs
  - improper configuration can lead to breaches
- attacks
  - IP address spoofing, source route attacks, tiny fragment attacks

Stateful Inspection Firewall

- reviews packet header information but also keeps info on TCP connections
  - typically have low, “known” port no for server
  - and high, dynamically assigned client port no
  - simple packet filter must allow all return high port numbered packets back in
  - stateful inspection packet firewall tightens rules for TCP traffic using a directory of TCP connections
  - only allow incoming traffic to high-numbered ports for packets matching an entry in this directory
  - may also track TCP seq numbers as well

Application-Level Gateway

- acts as a relay of application-level traffic
  - user contacts gateway with remote host name
  - authenticates themselves
  - gateway contacts application on remote host and relays TCP segments between server and user
- must have proxy code for each application
  - may restrict application features supported
- more secure than packet filters
- but have higher overheads

Circuit-Level Gateway

- sets up two TCP connections, to an inside user and to an outside host
- relays TCP segments from one connection to the other without examining contents
  - hence independent of application logic
  - just determines whether relay is permitted
- typically used when inside users trusted
  - may use application-level gateway inbound and circuit-level gateway outbound
  - hence lower overheads

Firewall Basing

- several options for locating firewall:
- bastion host
- individual host-based firewall
- personal firewall

Bastion Hosts

- critical strongpoint in network
- hosts application/circuit-level gateways
- common characteristics:
  - runs secure O/S, only essential services
  - may require user auth to access proxy or host
  - each proxy can restrict features, hosts accessed
  - each proxy small, simple, checked for security
  - each proxy is independent, non-privileged
  - limited disk use, hence read-only code

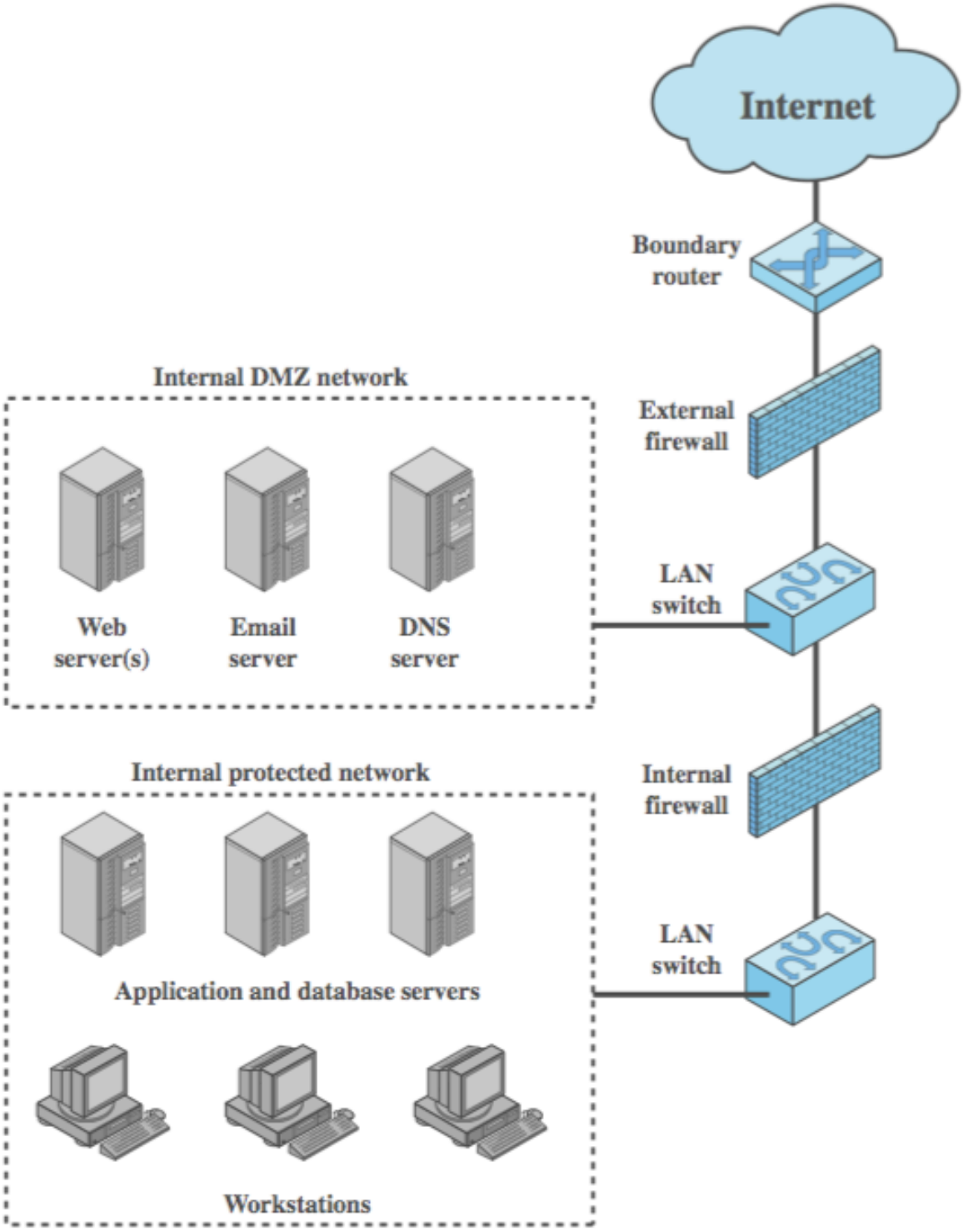
Host-Based Firewalls

- used to secure individual host
- available in/add-on for many O/S
- filter packet flows
- often used on servers
- advantages:
  - taylored filter rules for specific host needs
  - protection from both internal / external attacks
  - additional layer of protection to org firewall

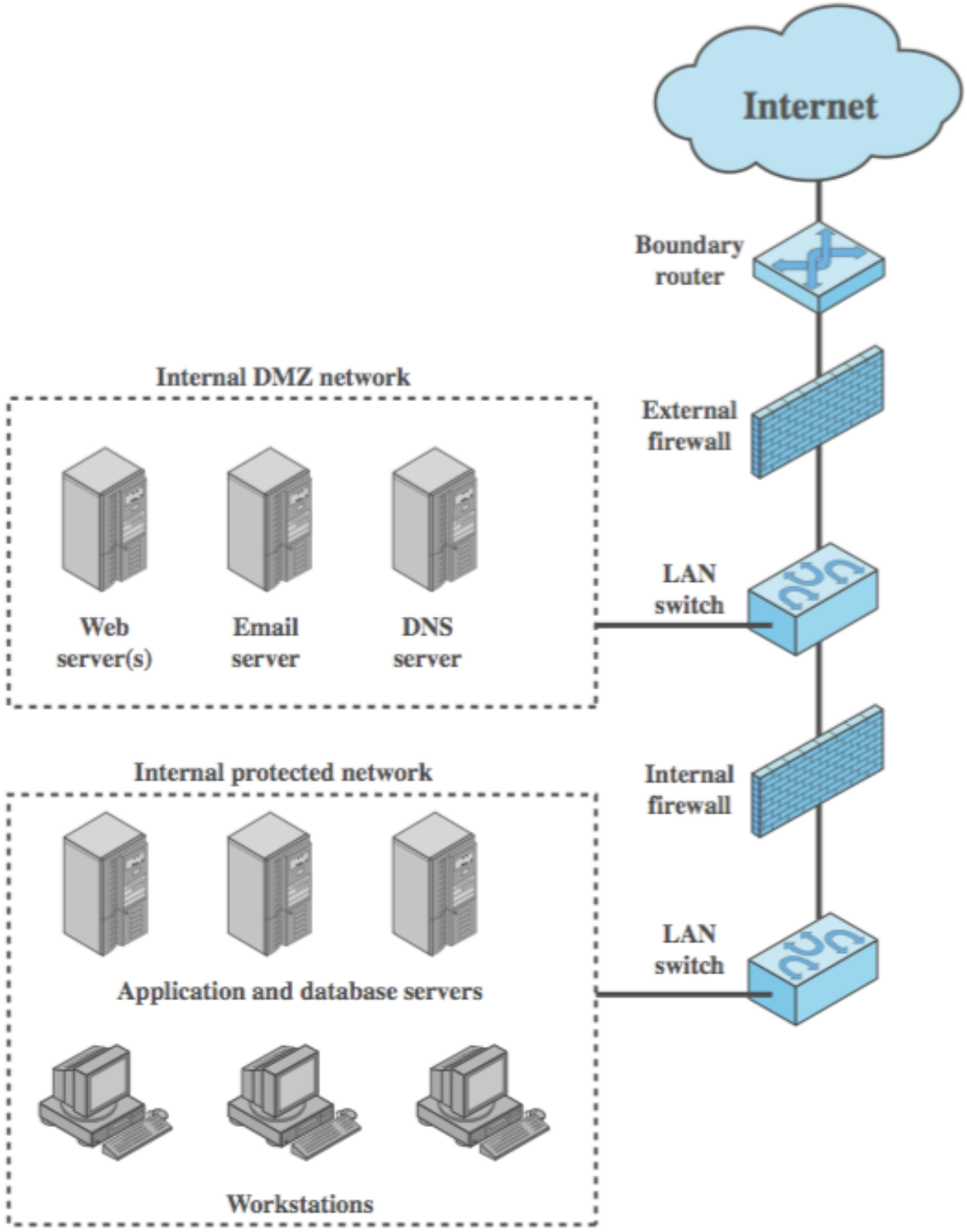
Personal Firewall

- controls traffic flow to/from PC/workstation
- for both home or corporate use
- may be software module on PC
- or in home cable/DSL router/gateway
- typically much less complex
- primary role to deny unauthorized access
- may also monitor outgoing traffic to detect/block worm/malware activity

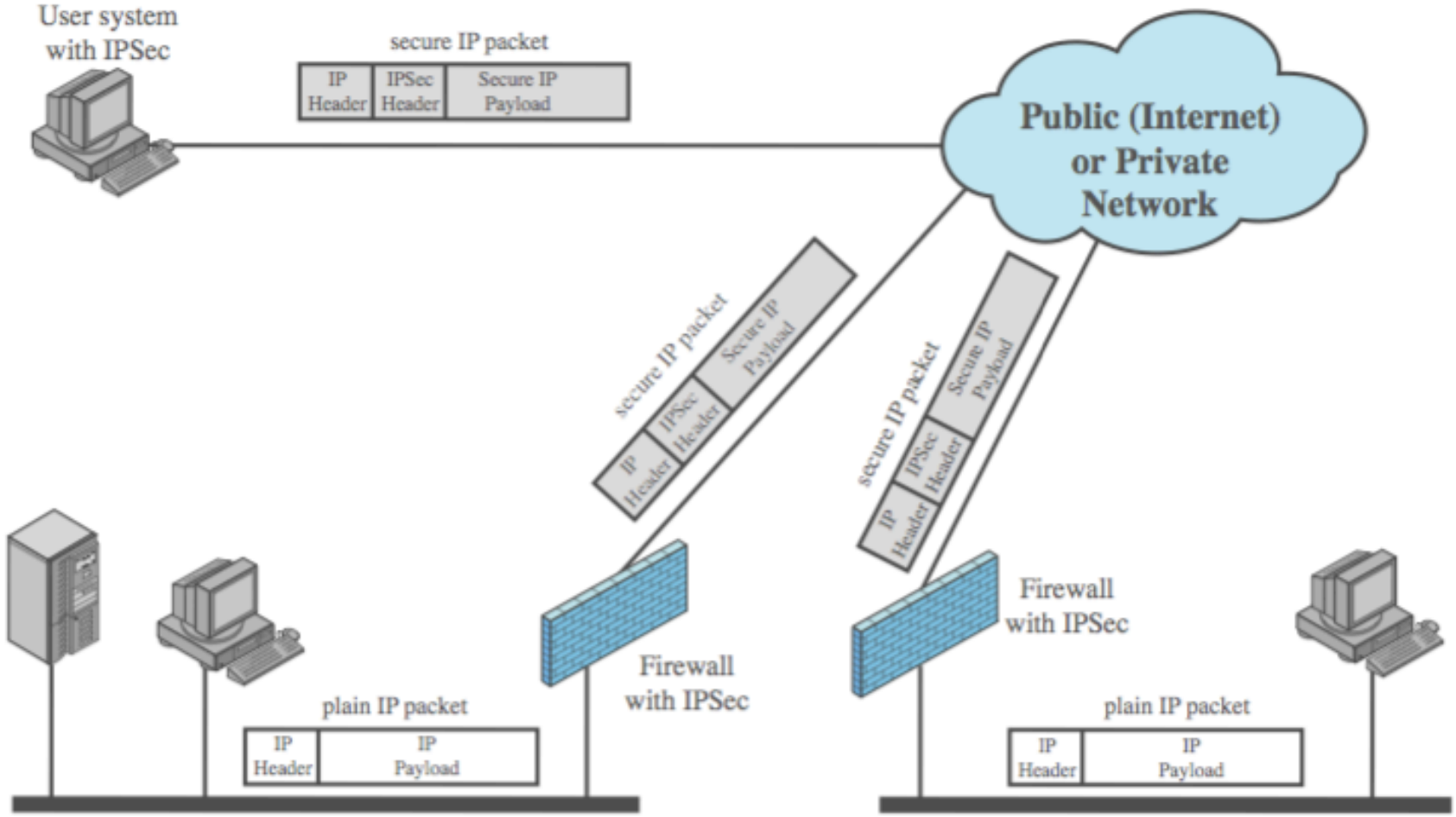
Firewall Locations



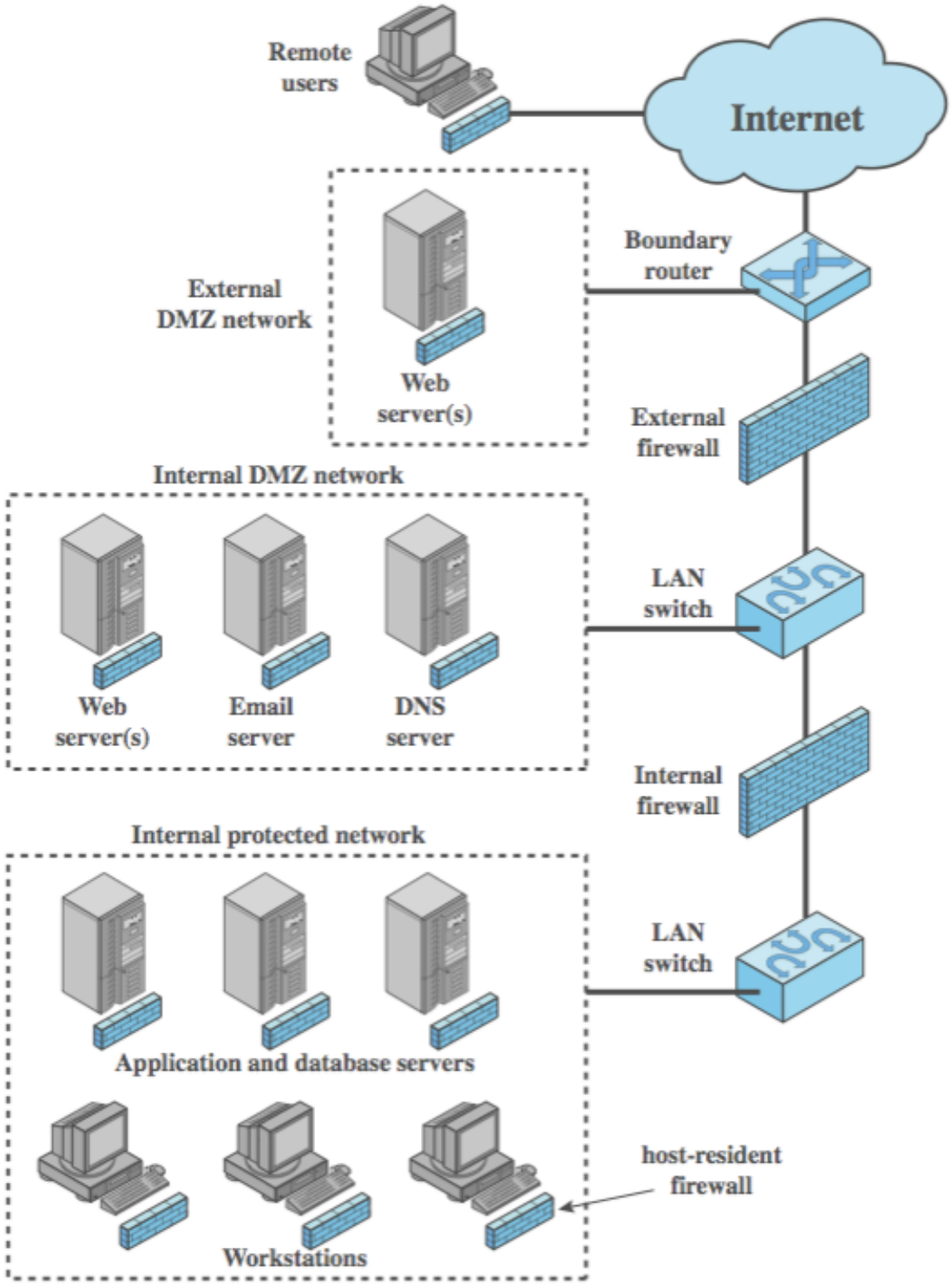
Firewall Locations: Advantages, Disadvantages ?



Virtual Private Networks



Distributed Firewalls



Firewall Topologies

- host-resident firewall
- screening router: packet filtering
- single bastion inline between routers
- single bastion T, with DMZ
- double bastion inline: DMZ between bastions
- double bastion T
- distributed firewall configuration

Intrusion Prevention Systems (IPS)

- recent addition to security products which
  - inline net/host-based IDS that can block traffic
  - functional addition to firewall that adds IDS capabilities
- can block traffic like a firewall
- using IDS algorithms
- may be network or host based

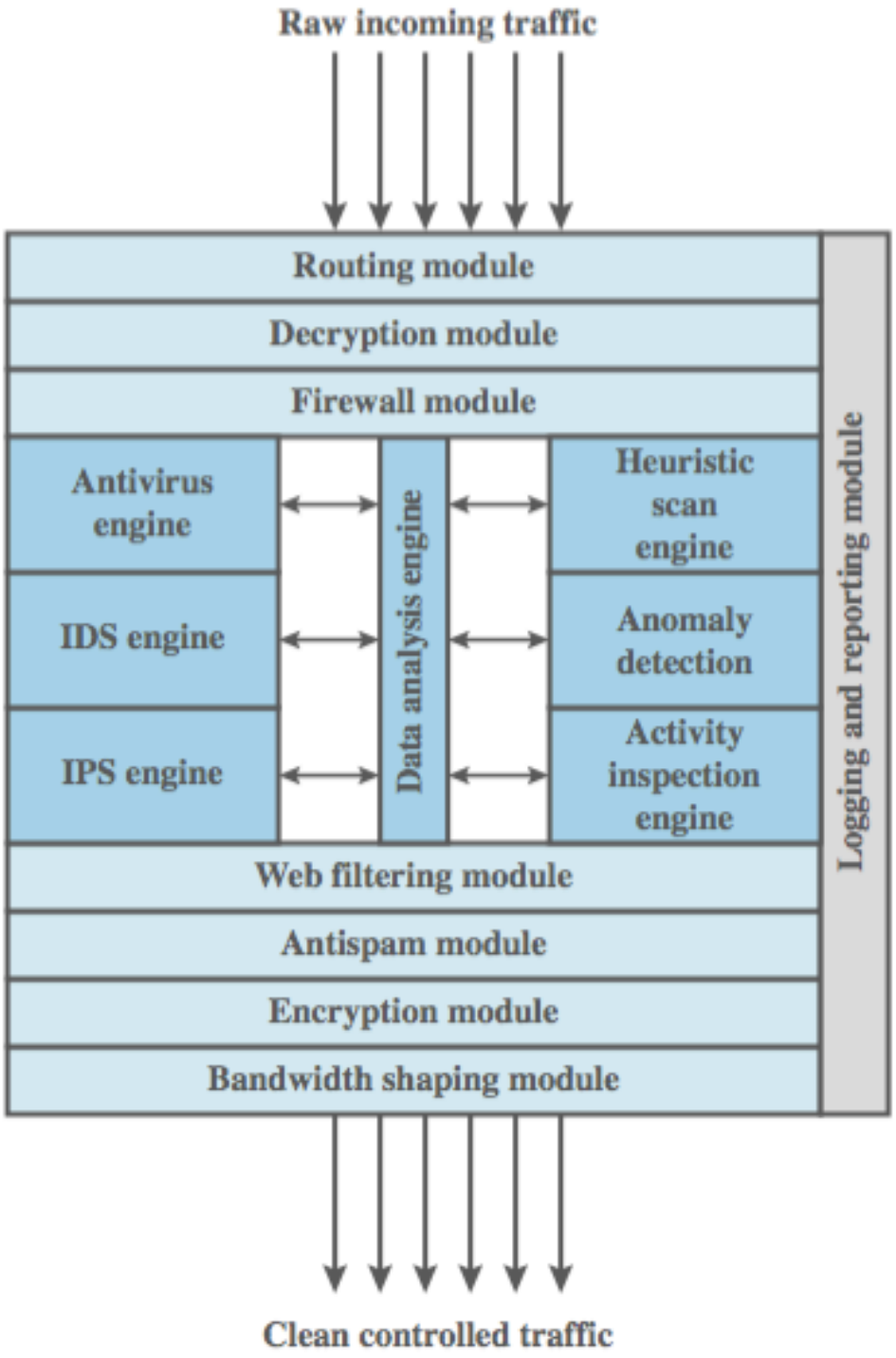
Host-Based IPS

- identifies attacks using both:
  - signature techniques
    - malicious application packets
  - anomaly detection techniques
    - behavior patterns that indicate malware
- can be tailored to the specific platform
  - e.g. general purpose, web/database server specific
- can also sandbox applets to monitor behavior
- may give desktop file, registry, I/O protection

Network-Based IPS

- inline NIDS that can discard packets or terminate TCP connections
- uses signature and anomaly detection
- may provide flow data protection
  - monitoring full application flow content
- can identify malicious packets using:
  - pattern matching, stateful matching, protocol anomaly, traffic anomaly, statistical anomaly
- cf. SNORT inline can drop/modify packets

Unified Threat Management Products



Summary

- introduced need for & purpose of firewalls
- types of firewalls
  - packet filter, stateful inspection, application and circuit gateways
- firewall hosting, locations, topologies
- intrusion prevention systems

Multilevel Security

Trusted Computing and Multilevel Security

- present some interrelated topics:
  - formal models for computer security
  - multilevel security
  - trusted systems
  - mandatory access control

Formal Models for Computer Security

- two fundamental computer security facts:
  - all complex software systems have flaw/bugs
  - is extraordinarily difficult to build computer hardware/ software not vulnerable to attack
- hence desire to prove design and implementation satisfy security requirements
- led to development of formal security models
  - initially funded by US DoD
- Bell-LaPadula (BLP) model very influential

Bell-LaPadula (BLP) Model

- developed in 1970s
- as a formal access control model
- subjects and objects have a **security class**
  - top secret > secret > confidential > unclassified
  - subject has a **security clearance** level
  - object has a **security classification** level
  - class control how subject may access an object
- applicable if have info and user categories

BLP Formal Description

- based on current state of system (b, M, f, H):

  (current access set *b,* access matrix *M,* level function *f,* hierarchy *H)*

- three BLP properties:

  ss-property: (S_i, O_j, read) has $f_c(S_i) \geq f_o(O_j)$.

  *-property: $(S_i, O_j, \text{append})$ has $f_c(S_i) \leq f_o(O_j)$ and

  (S_i, O_j, write) has $f_c(S_i) = f_o(O_j)$

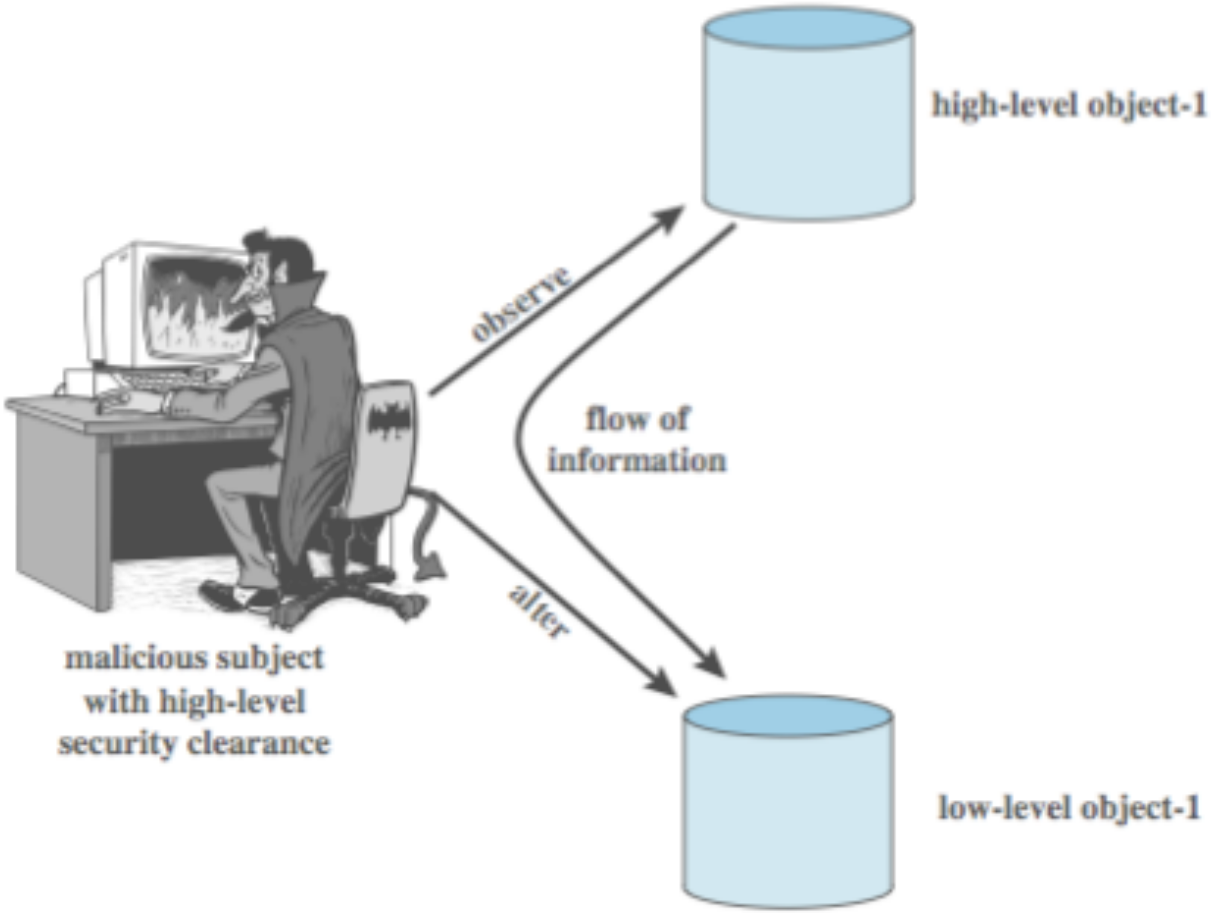
  ds-property: (S_i, O_j, A_x) implies $A_x \in M[S_i, O_j]$

- BLP give formal theorems
  - theoretically possible to prove system is secure
  - in practice usually not possible

BLP

- No read up.
- No write down – why?

Multi-Level Security



Confidentiality

- Current state (b,M, f, H) is secure if and only if every element of b satisfies the 3 properties
- The security state of the system is changed by any operation that causes a change of any of the 4 components b, M, f, H
- A secure system remains secure so long as any state change does not violate the 3 properties

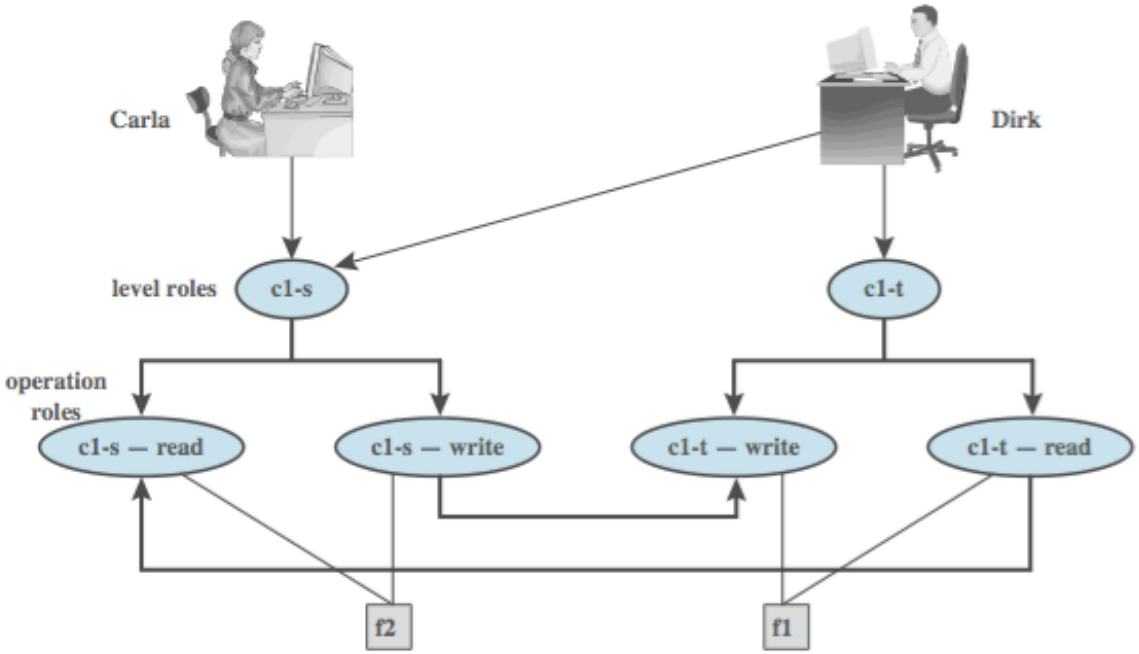
BLP Additional Properties

- Strong * property: only same level
- Tranquility
  - Strong: security levels do not change during the normal operation of the system
  - Weak: security levels may never change in such a way as to violate a defined security policy

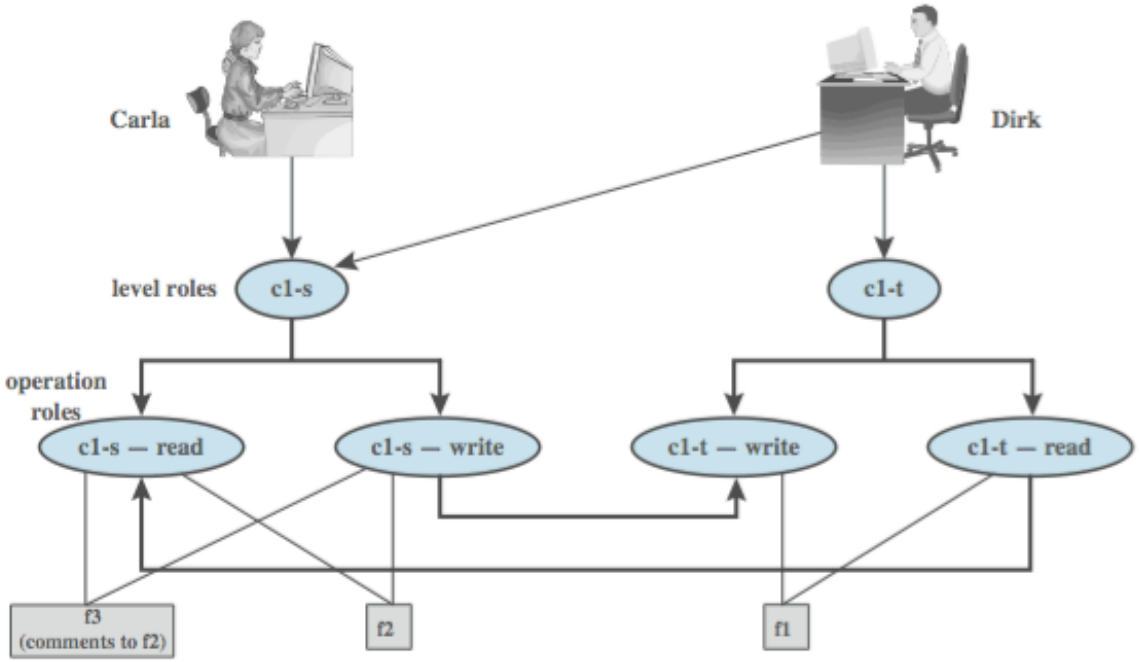
BLP Rules

1. get access: add a triple S, O, A to b
2. release access: remove triple from b
3. change object level
4. change current level of subject
5. give access permission
6. rescind access permission
7. create an object: add a leaf in H
8. delete a group of objects

BLP Example

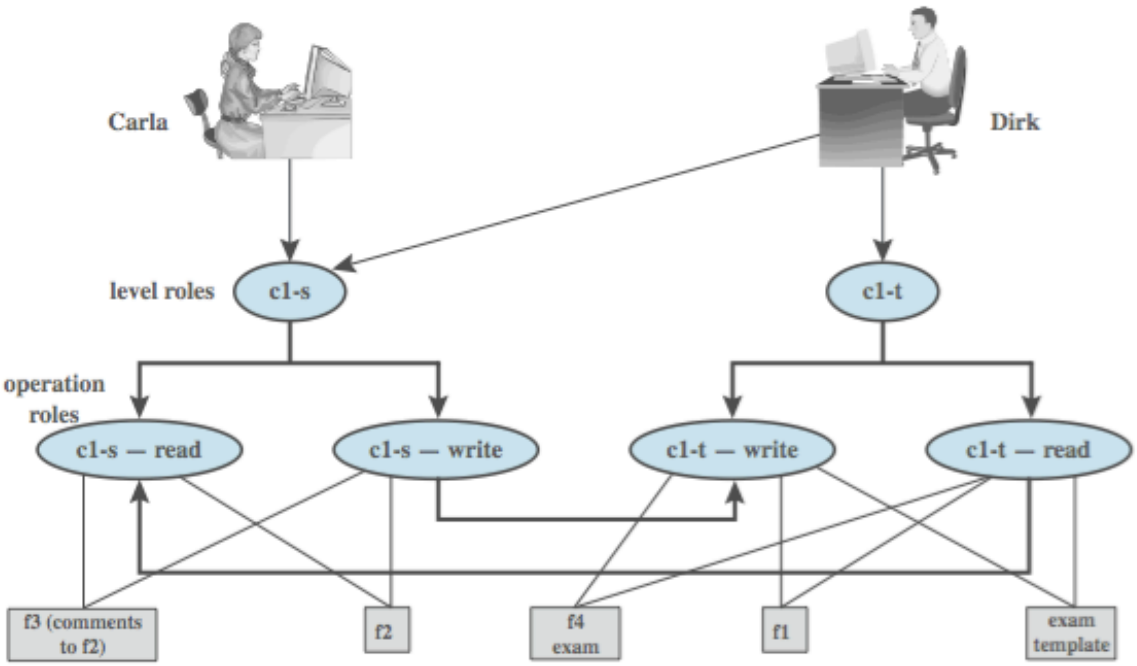


(a) Two new files are created: f1: c1-t; f2: c1-s

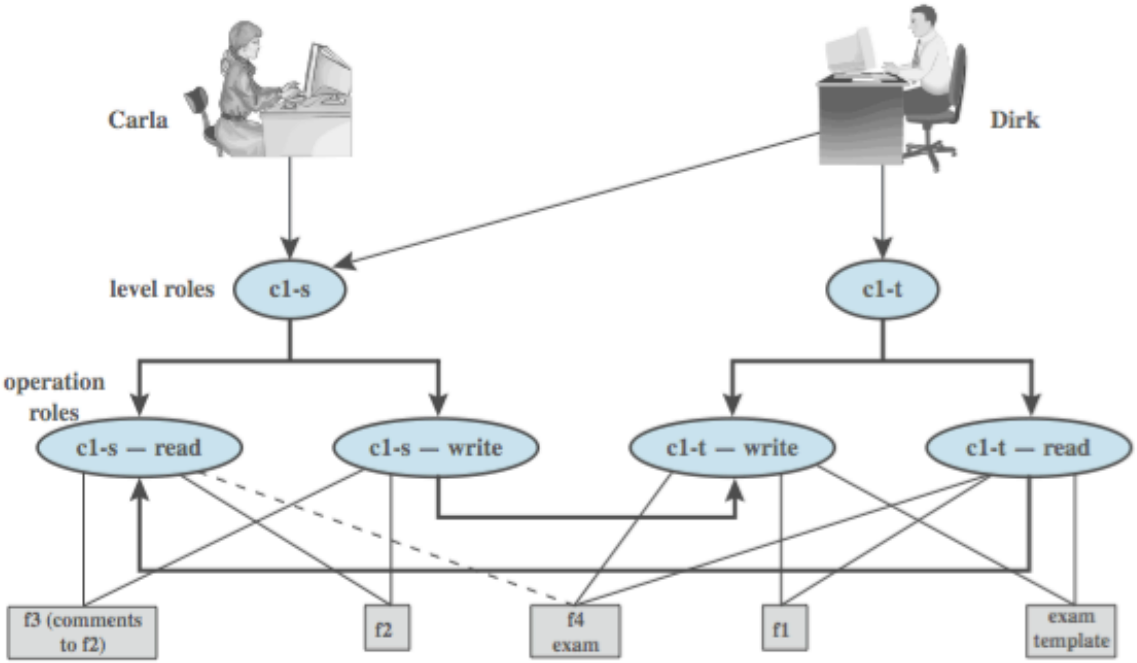


(b) A third file is added: f3: c1-s

BLP Example cont.

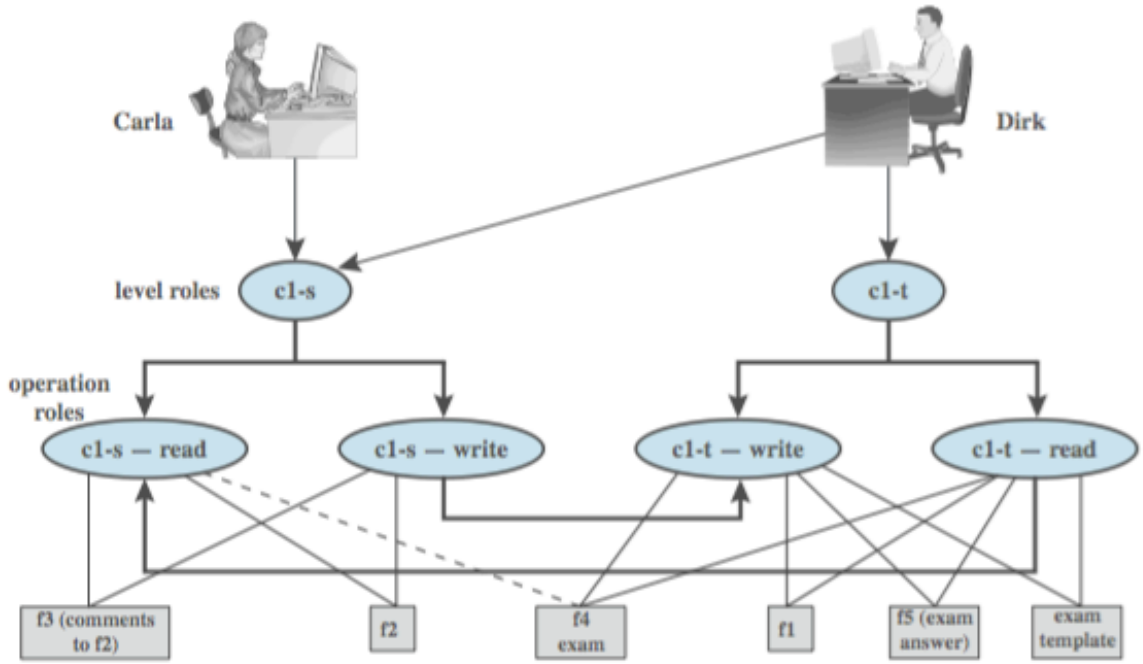


(c) An exam is created based on an existing template: f4: c1-t



(d) Carla, as student, is permitted acess to the exam: f4: c1-s

BLP Example cont.



(e) The answers given by Carla are only accessible for the teacher: f5: c1-t

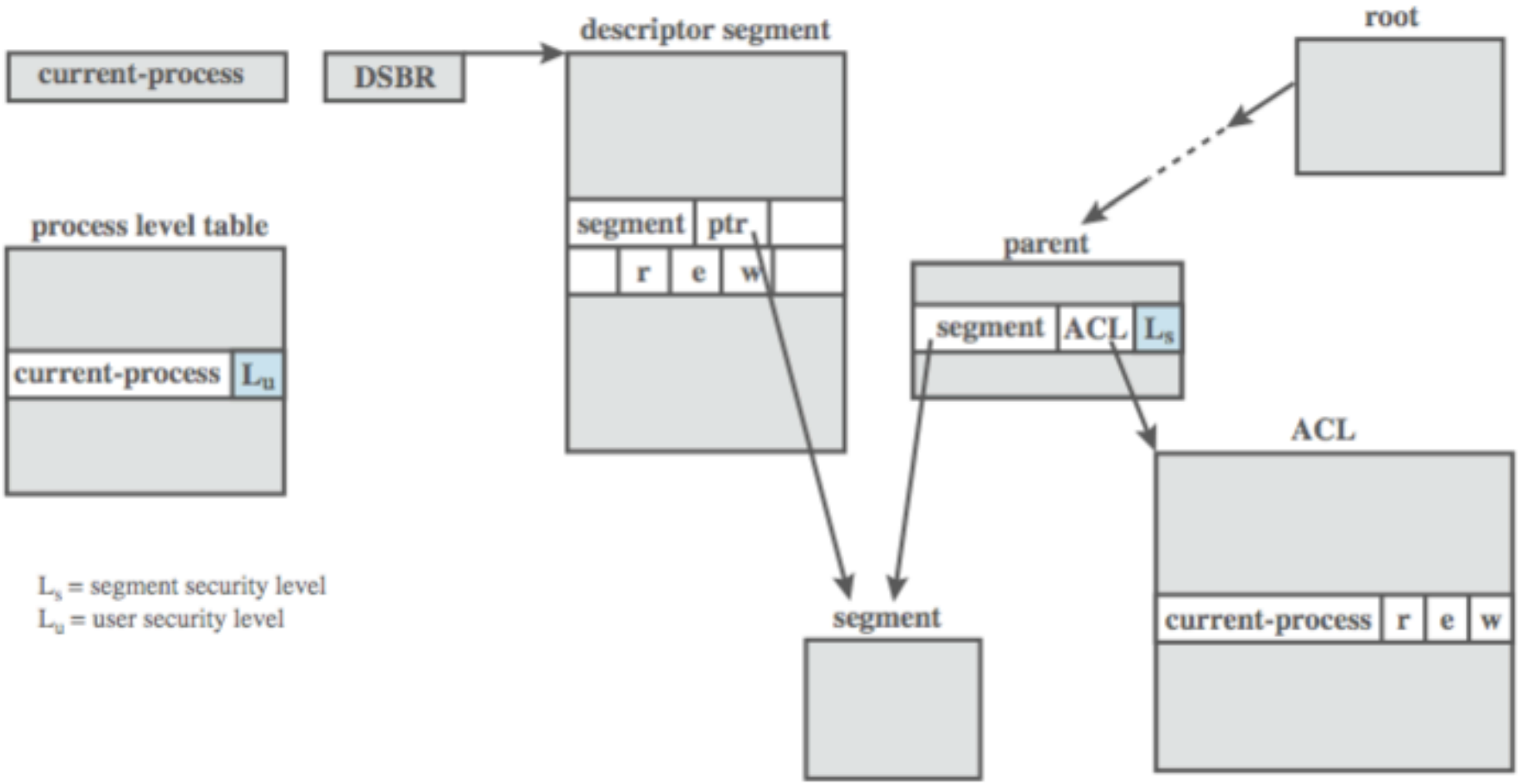
BLP limitations

- In this example, what problems show up?

BLP limitations

- No provision for downgrading
- Can only edit at one level while reading at same or lower level
- Classification creep by consolidation of documents from different sources and levels

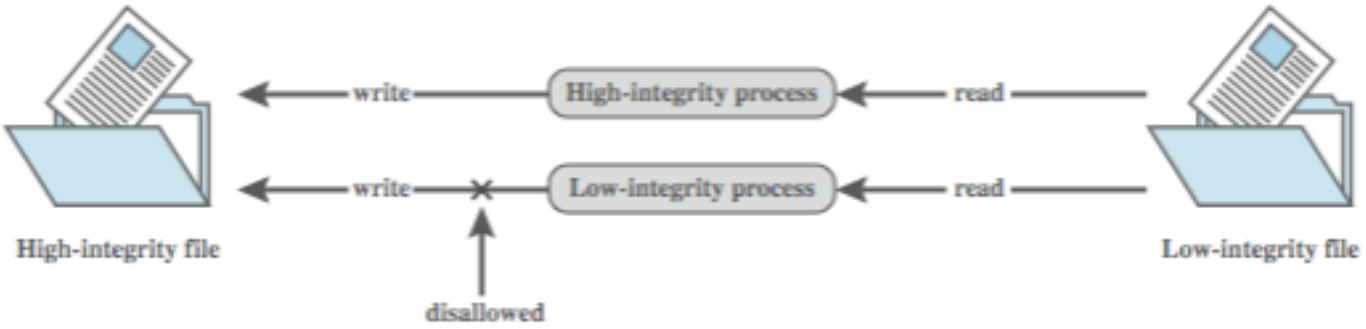
MULTICS Example



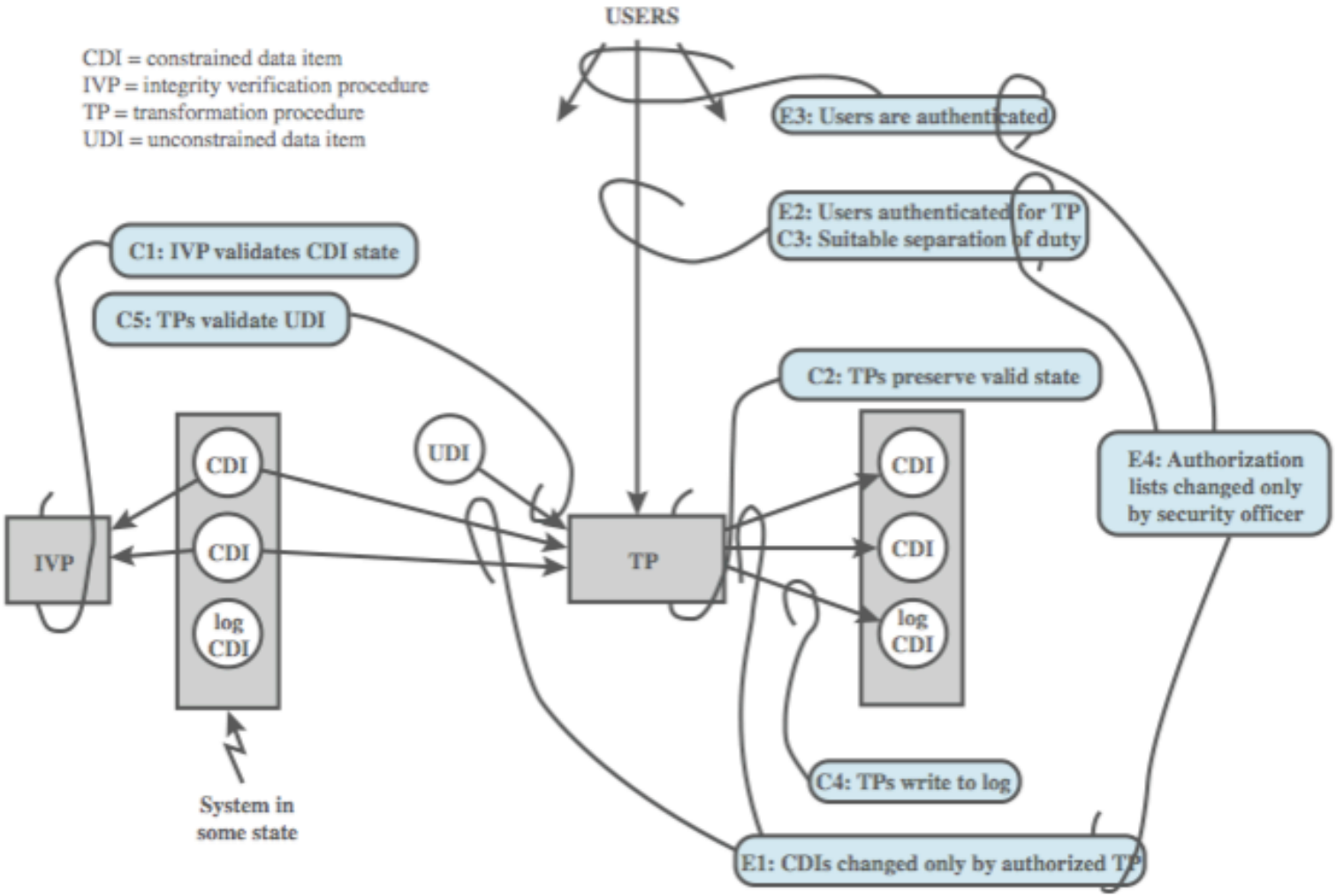
Biba Integrity Model

- various models dealing with integrity
- "no read down, no write up”
- strict integrity policy:
  - simple integrity: modify if $I(S) \geq I(O)$
  - integrity confinement: read if $I(S) \leq I(O)$
  - invocation property: $I(S_1) \geq I(S_2)$

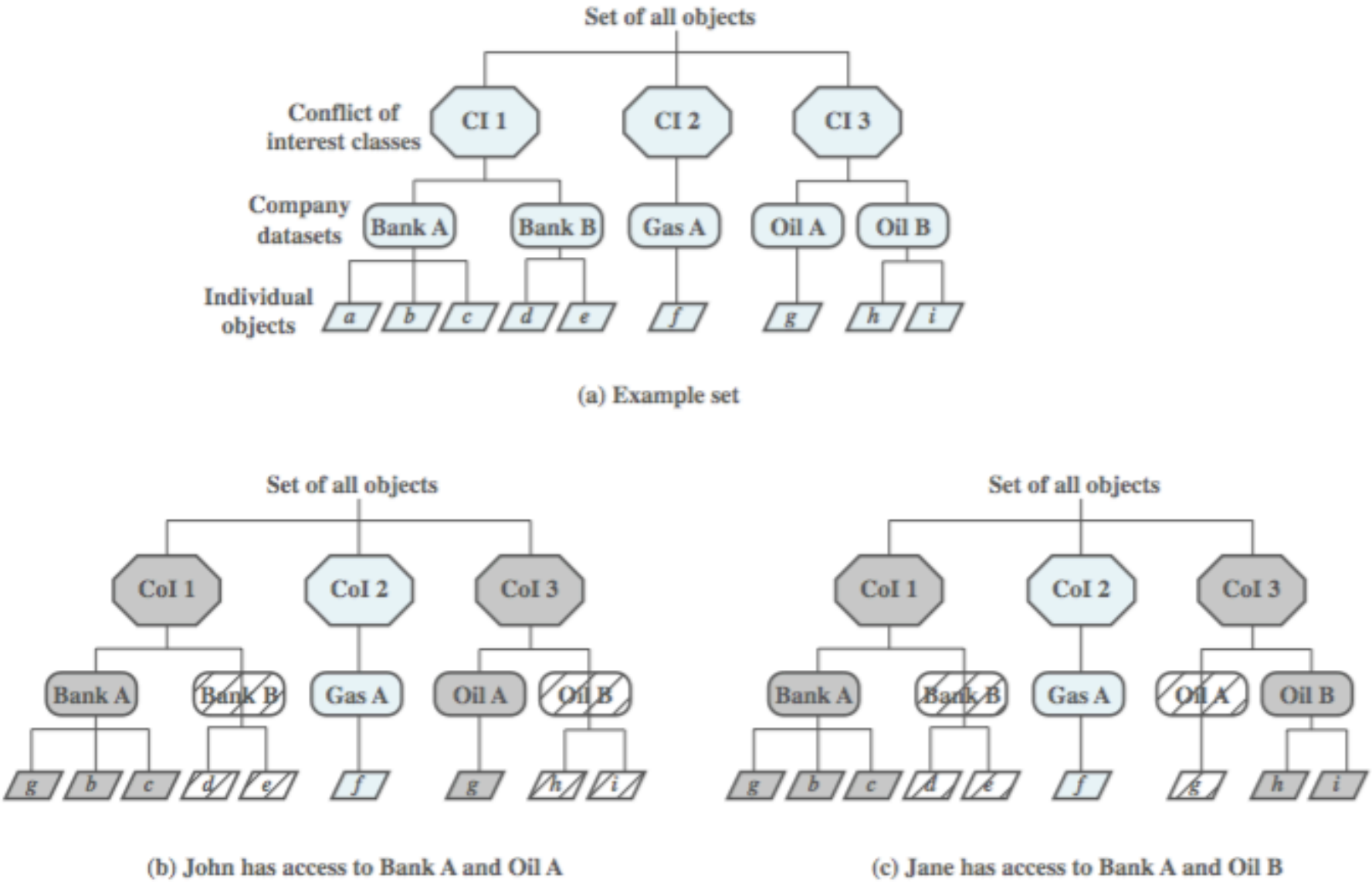
  Contamination with simple integrity only:



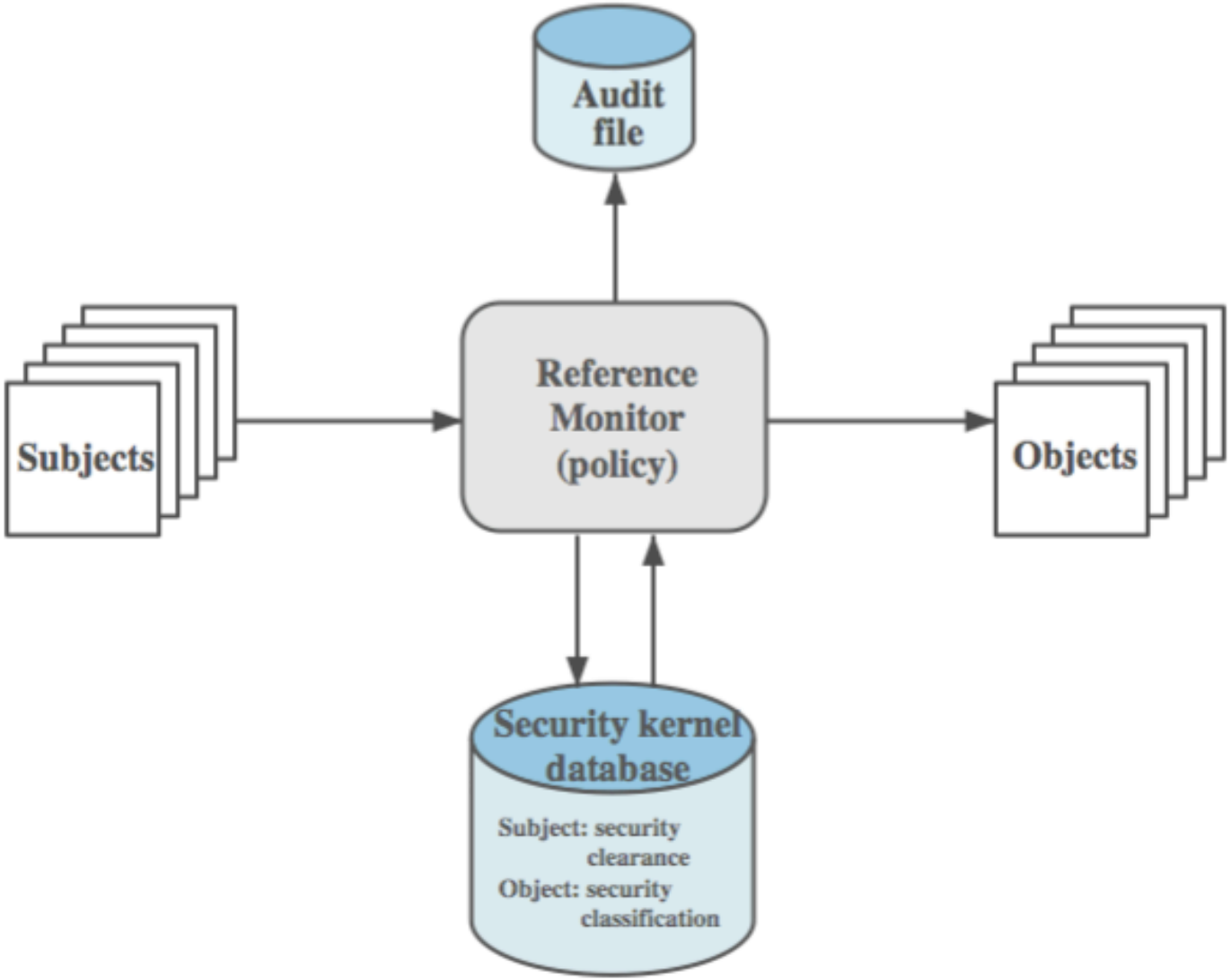
Clark-Wilson Integrity Model



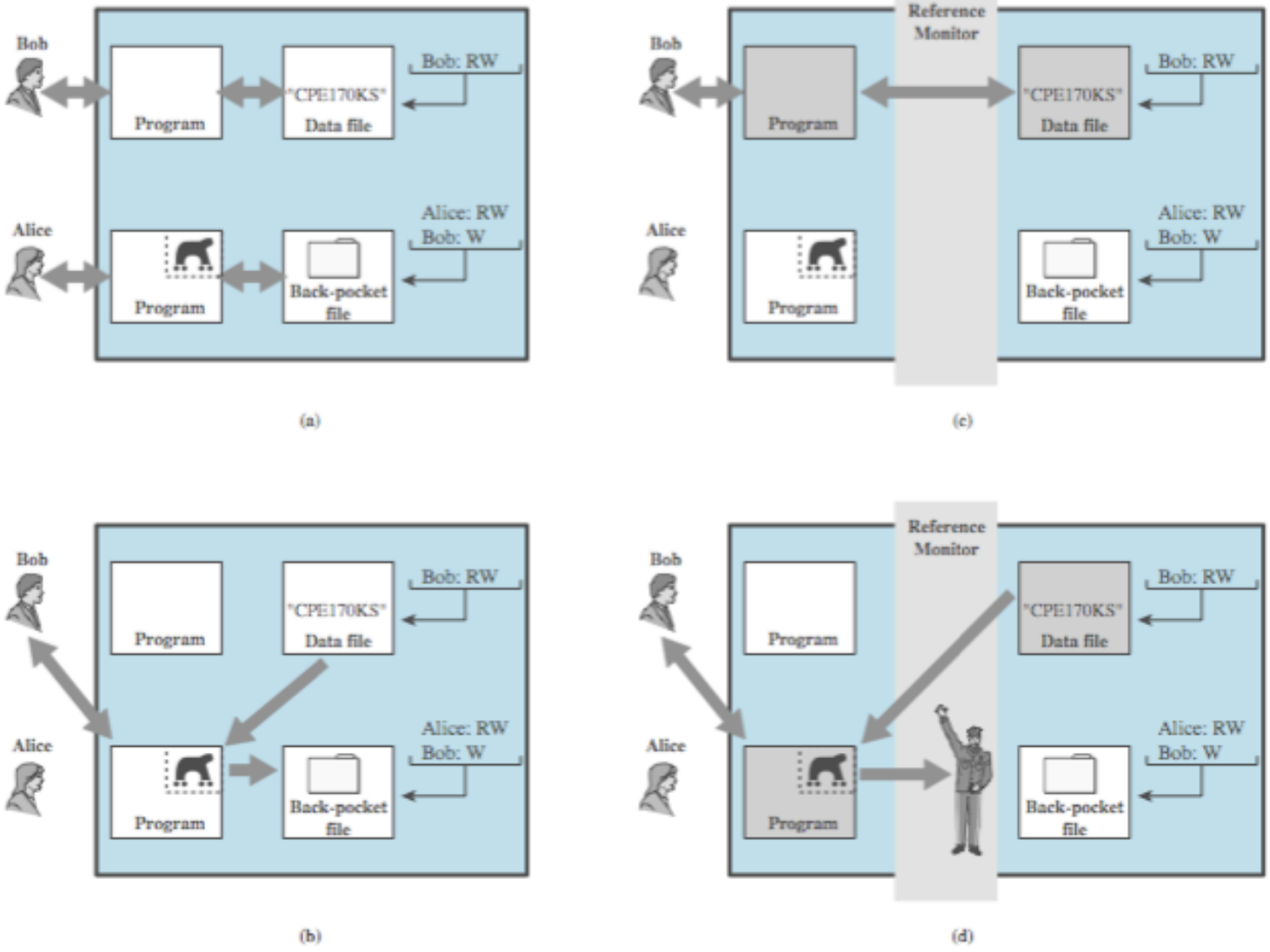
Chinese Wall Model



Reference Monitors



Trojan Horse Defence



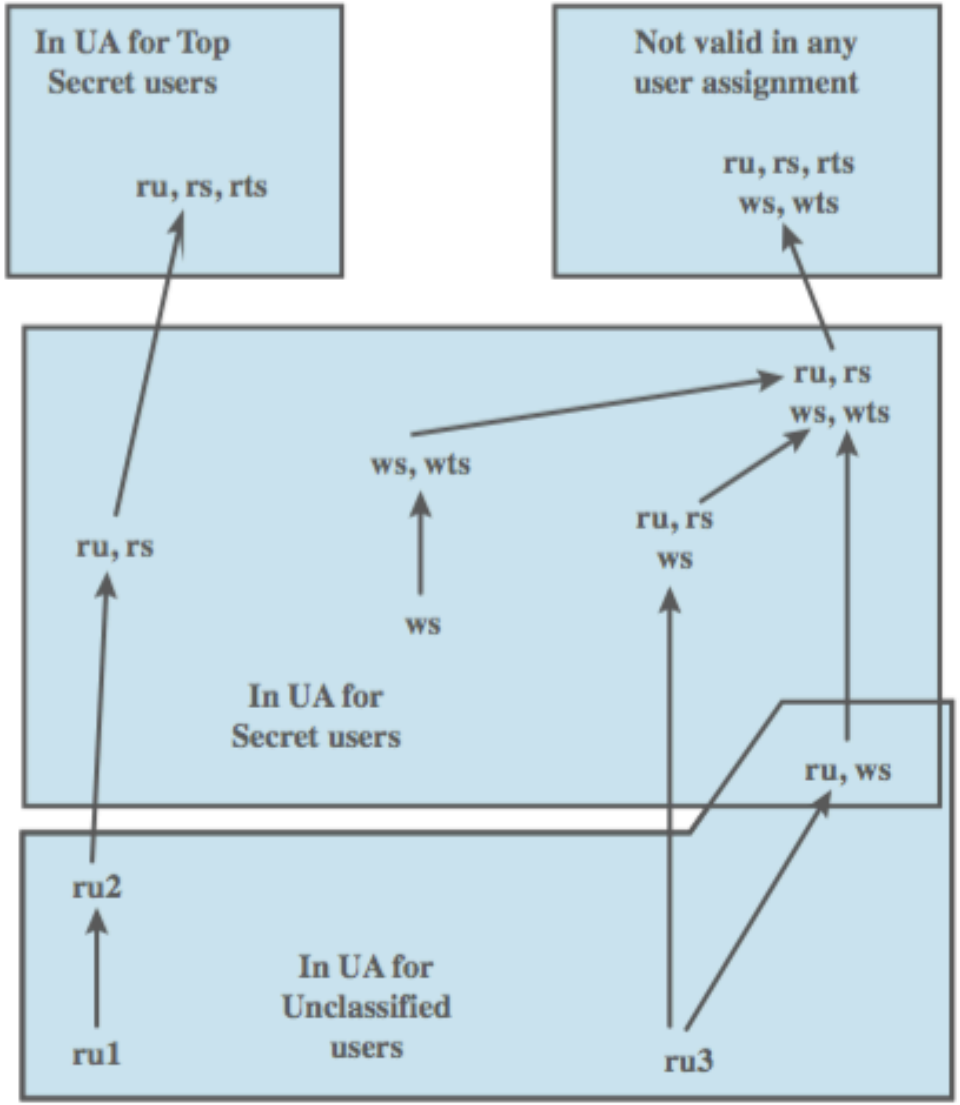
Multilevel Security (MLS)

- a class of system that has system resources (particularly stored information) at more than one security level (i.e., has different types of sensitive resources) and that permits concurrent access by users who differ in security clearance and need-to-know, but is able to prevent each user from accessing resources for which the user lacks authorization.

MLS Security for Role-Based Access Control

- rule based access control (RBAC) can implement BLP MLS rules given:
  - security constraints on users
  - constraints on read/write permissions
  - read and write level role access definitions
  - constraint on user-role assignments

RBAC MLS Example



MLS Database Security

Department Table - U		
Did	Name	Mgr
4	accts	Cathy
8	PR	James

Employee - R			
Name	Did	Salary	Eid
Andy	4	43K	2345
Calvin	4	35K	5088
Cathy	4	48K	7712
James	8	55K	9664
Ziggy	8	67K	3054

(a) Classified by table

Department Table		
Did -U	Name -U	Mgr -R
4	accts	Cathy
8	PR	James

Employee			
Name -U	Did -U	Salary -R	Eid -U
Andy	4	43K	2345
Calvin	4	35K	5088
Cathy	4	48K	7712
James	8	55K	9664
Ziggy	8	67K	3054

(b) Classified by column (attribute)

MLS Database Security

Department Table			
Did	Name	Mgr	
4	accts	Cathy	R
8	PR	James	U

Employee				
Name	Did	Salary	Eid	
Andy	4	43K	2345	U
Calvin	4	35K	5088	U
Cathy	4	48K	7712	U
James	8	55K	9664	R
Ziggy	8	67K	3054	R

(c) Classified by row (tuple)

Department Table		
Did	Name	Mgr
4 - U	accts - U	Cathy - R
8 - U	PR - U	James -R

Employee			
Name	Did	Salary	Eid
Andy - U	4 - U	43K - U	2345 - U
Calvin - U	4 - U	35K - U	5088 - U
Cathy - U	4 - U	48K - U	7712 - U
James - U	8 - U	55K - R	9664 - U
Ziggy - U	8 - U	67K - R	3054 - U

(d) Classified by element

MLS Database Security
Read Access

- DBMS enforces simple security rule (no read up)
- easy if granularity entire database / table level
- inference problems if have column granularity
  - if can query on restricted data can infer its existence
    - `SELECT Ename FROM Employee WHERE Salary > 50K`
  - solution is to check access to all query data
- also have problems if have row granularity
  - null response indictes restricted/empty result
- no extra concerns if have element granularity

MLS Database Security
Write Access

- enforce *-security rule (no write down)
- have problem if a low clearance user wants to insert a row with a primary key that already exists in a higher level row:
  - can reject, but user knows row exists
  - can replace, compromises data integrity
  - can polyinstantiation and insert multiple rows with same key, creates conflicting entries
- same alternatives occur on update
- avoid problem if use database / table granularity

Summary

- Bell-Lapadula security model
- other models
- reference monitors & trojan horse defence
- multilevel secure RBAC and databases