

---

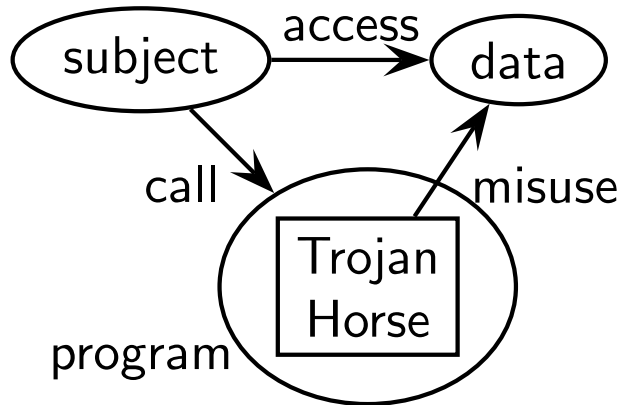
# **Mandatory Access Control Multilevel Security**

Simon Foley

January 12, 2016

# Trojan Horses

▷ Trojan Horses  
MAC and DAC  
MLS  
Security Classes  
Compartments  
Bell LaPadua  
BLP Axioms  
Clearance  
MLS File System  
French History  
Covert Channels  
Security Criteria  
Chinese Wall



```
# Trojan /tmp/ls
#Steal rights
#/bin/sh
chmod a+rw $HOME
/usr/bin/ls
```

Trojan Horse masquerades as a friendly program, is used by trusted people to do what they believe is legitimate work.

Trojan Horse can be found in games, 'useful' software, malware or effectively in trusted code that contains a vulnerability that can be exploited.

Example. Create a script with path `/tmp/ls` on a Unix system and do `chmod uoga+rx /`.

Wait for an unsuspecting user with '.' at start of PATH? to do an `ls` in `/tmp`.

Attacker could 'improve' `/tmp/ls` by concealing its existence (how?).

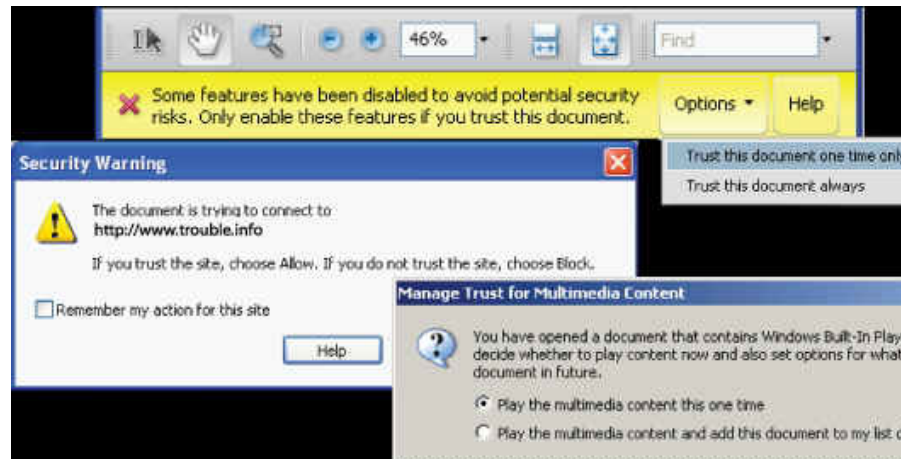
# Malicious code installation

▷ Trojan Horses  
MAC and DAC  
MLS  
Security Classes  
Compartments  
Bell LaPadua  
BLP Axioms  
Clearance  
MLS File System  
French History  
Covert Channels  
Security Criteria  
Chinese Wall

May unwittingly install software containing trojan horse/malicious code.



But its not always obvious...

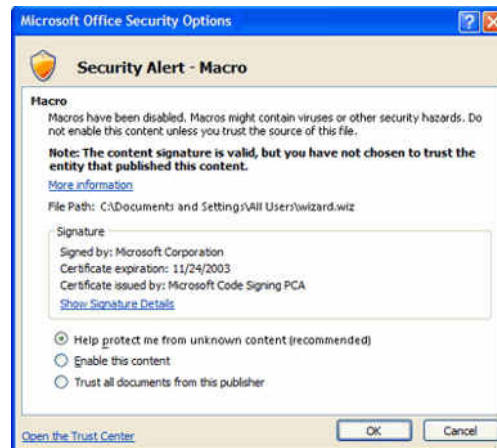


# Malicious code installation

▷ Trojan Horses  
MAC and DAC  
MLS  
Security Classes  
Compartments  
Bell LaPadua  
BLP Axioms  
Clearance  
MLS File System  
French History  
Covert Channels  
Security Criteria  
Chinese Wall

Trojan Horse may be included in any executable content.

- ☐ A VB macro in an office document (Word, Excel, ...).
- ☐ A Java applet in a webpage executed by browser.
- ☐ A  $\text{\LaTeX}$  source file.
- ☐ Javascript embedded within an pdf document.
- ☐ Javascript embedded within data supplied to HTML form.
- ☐ ...



# Malicious code installation

▷ Trojan Horses  
MAC and DAC  
MLS  
Security Classes  
Compartments  
Bell LaPadua  
BLP Axioms  
Clearance  
MLS File System  
French History  
Covert Channels  
Security Criteria  
Chinese Wall

Installation of Trojan Horse may require exploiting a vulnerability in existing software.

- ☐ A buffer-overflow in service provides a route to Trojan Horse installation.
- ☐ Guessing a weak password provides account access.
- ☐ ...
- ☐ Having compromised workstation, Torpig (botnet) installs Trojan Horse in browser software.
- ☐ ...

# Aside: Software Features as Trojan Horses

▷ Trojan Horses  
MAC and DAC  
MLS  
Security Classes  
Compartments  
Bell LaPadua  
BLP Axioms  
Clearance  
MLS File System  
French History  
Covert Channels  
Security Criteria  
Chinese Wall

Sometimes software features provide a Trojan Horse.

- ☐ Maintaining history of revisions in a document.
- ☐ MS Word fast save does not save a fresh copy of the file, instead it simply appends a journal of the changes to make on the current file when next opened. On opening the file, the file is loaded and changes applied. User is able to view old versions of document by inspecting the .doc source.
- ☐ Improper redaction of pdf files by placing black-bars over the existing text in pdf document. Easy to remove black-bars and discover original text.

*See Redacting with Confidence: How to Safely Published Sanitized Reports Converted from Word to PDF.* US National Security Agency, [www.fas.org/sgp/othergov/dod/nsa-redact.pdf](http://www.fas.org/sgp/othergov/dod/nsa-redact.pdf)

BBC NEWS | Europe | Readers 'declassify' US document

http://news.bbc.co.uk/2/hi/euro documents sit

BBC Home News Sport Radio TV Weather Languages

UK version International version | About the versions

Low graphics | Accessibility help

**BBC NEWS**

Watch One-Minute World News

News services  
Your news when you want it

News Front Page


Africa  
Americas  
Asia-Pacific  
**Europe**  
Middle East  
South Asia  
UK  
Business  
Health  
Science & Environment  
Technology  
Entertainment  
Also in the news  
Video and Audio  
Have Your Say  
In Pictures  
Country Profiles  
Special Reports

Last Updated: Monday, 2 May 2005, 17:18 GMT 18:18 UK

E-mail this to a friend Printable version

## Readers 'declassify' US document

When news started circulating in Italy that a heavily censored Pentagon report into the death of secret agent Nicola Calipari had been decrypted, many thought it must be the work of some top-notch hacker.



Someone found a simple cut-and-paste job could restore the text

In fact, it turned out that the classified document, containing top-secret details - such as the name of the soldier who fired the deadly rounds of ammunition - could be made readable with two simple clicks of your computer mouse.

A few hours after the Pentagon published the report on its website, a few Italian readers found they could make the blacked-out paragraphs reappear by cutting and pasting them from the site into a Word document.

Salvatore Schifani, a 30-year-old IT worker, spotted the document at about 0300 local time (0100 GMT) on Saturday night.

He said he had just come home from a night out and wanted

### VIDEO AND AUDIO NEWS

How the censored parts of the report were made public

Watch

### STRUGGLE FOR IRAQ

#### KEY STORIES

- Women banned from shrine
- New US embassy opens
- Iraq takes control of Green Zone
- New charges for Saddam loyalists
- Iraq signs foreign troops deals

#### FEATURES AND ANALYSIS

**Pullout 'met with relief'**

Analysis of the announcement on the withdrawal of British troops from Iraq

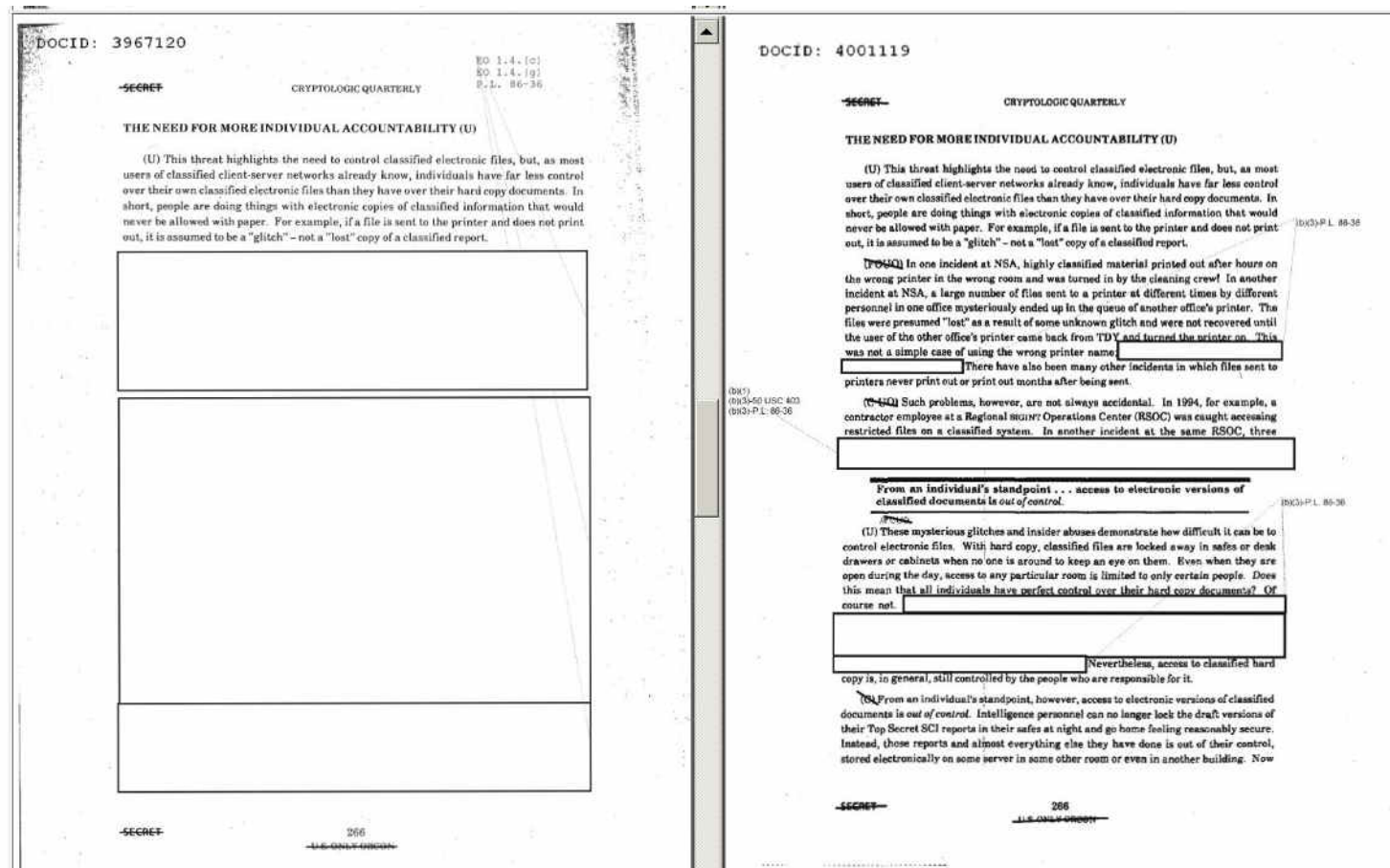
- History lesson
- Bush shoe-ing worst Arab insult
- Analysis: Kirkuk faultline
- Iraq translators' mask ban dropped
- Inside Baghdad's Rusafa prison

Find: web Next Previous Highlight all Match case



# If you are going to redact, then be consistent

▷ Trojan Horses  
MAC and DAC  
MLS  
Security Classes  
Compartments  
Bell LaPadua  
BLP Axioms  
Clearance  
MLS File System  
French History  
Covert Channels  
Security Criteria  
Chinese Wall



[Reference: Author's name redacted, "Out of Control," Cryptologic Quarterly 15 (Special Edition, 1996), 263-269, Declassified from SECRET]

Article about dangers of unfettered power possessed by intelligence agency IT system administrators.

Right hand version from [www.nsa.gov/public\\_info/\\_files/cryptologic\\_quarterly/Out\\_of\\_Control.pdf](http://www.nsa.gov/public_info/_files/cryptologic_quarterly/Out_of_Control.pdf)

Left hand version from <http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB424/docs/Cyber-009.pdf>



# MAC and DAC

Trojan Horses  
▷ MAC and DAC  
MLS  
Security Classes  
Compartments  
Bell LaPadua  
BLP Axioms  
Clearance  
MLS File System  
French History  
Covert Channels  
Security Criteria  
Chinese Wall

Does the unexpected behavior of the above software violate security?

Access control in these examples is *discretionary*: owners may choose to grant access/broadcast data if they wish.

Strictly speaking, the 'Trojan Horse' in the script for /tmp/ls above does not violate the Unix security policy.

- ☐ *Discretionary Access Control (DAC)*: subjects and objects have security attributes that can be changed by the user.
- ☐ *Mandatory Access Control (MAC)*: subjects and objects have security attributes that can not be changed by the user.

While Unix access control is generally regarded as DAC (owners can decide whether to give away access), Unix group membership is MAC.



Resident Shield alert

The horsey is infected



### Threat detected!

**File name:**  
C:\Turkey\Troad\Dardanus\Troy\WoodenHorse.exe

**Threat name:** Trojan Horse full of Soldiers  
Detected outside of walls  
[More information about this threat...](#)

☐ Remove threat as Cassandra



Burn

Let Horse In

Ignore



Hide details

Process name: C:\Achaean\Mycenae\Agamemnon.exe  
Process ID: 1184

# Multilevel Security (MLS)

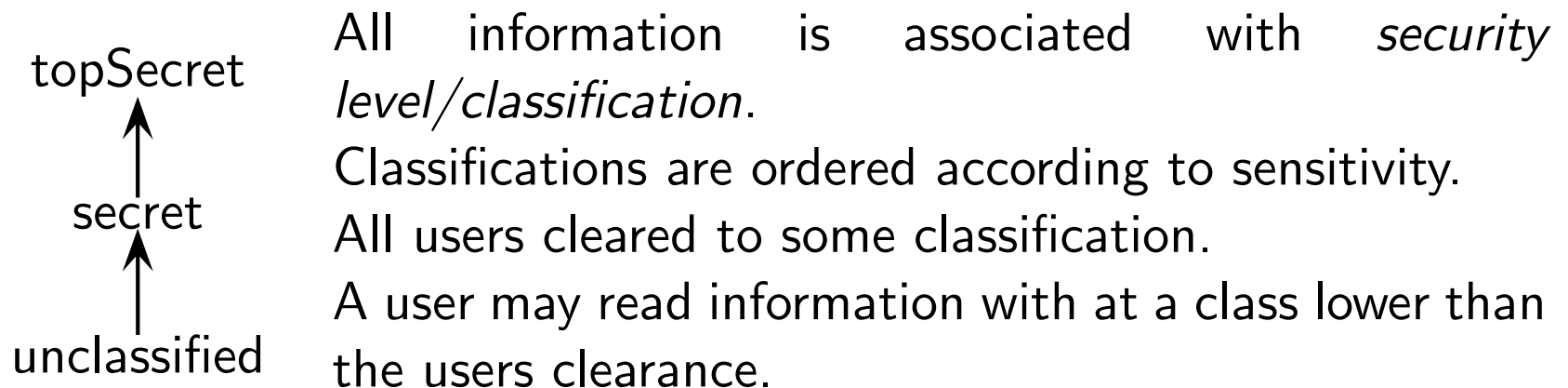
Trojan Horses  
MAC and DAC  
▷ MLS  
Security Classes  
Compartments  
Bell LaPadua  
BLP Axioms  
Clearance  
MLS File System  
French History  
Covert Channels  
Security Criteria  
Chinese Wall

MAC model of confidentiality dating back to 1970's.

Quite restrictive; used in situations when security is critical.

Originated from requirements for managing military documents.

For example, prevent the contents of a top-secret document from being read by a secret or unclassified user.



# Multilevel Security Classifications

Trojan Horses  
MAC and DAC  
MLS  
▷ Security Classes  
Compartments  
Bell LaPadua  
BLP Axioms  
Clearance  
MLS File System  
French History  
Covert Channels  
Security Criteria  
Chinese Wall

A MLS system has a set of security classifications  $SC$  and an ordering relation  $\leq$  defined over this set.

Given classifications  $a, b \in SC$  then  $a \leq b$  means that information at class  $a$  is less sensitive (or equal to) than information at class  $b$ .

Intuitively, information about  $a$  is permitted flow to classification  $b$ .

For example:  $SC = \{\text{unclassified}, \text{secret}, \text{topSecret}\}$ , with  $\text{unclassified} \leq \text{secret} \leq \text{topSecret}$ ; secret information is permitted to flow to top-secret, but not vice-versa.

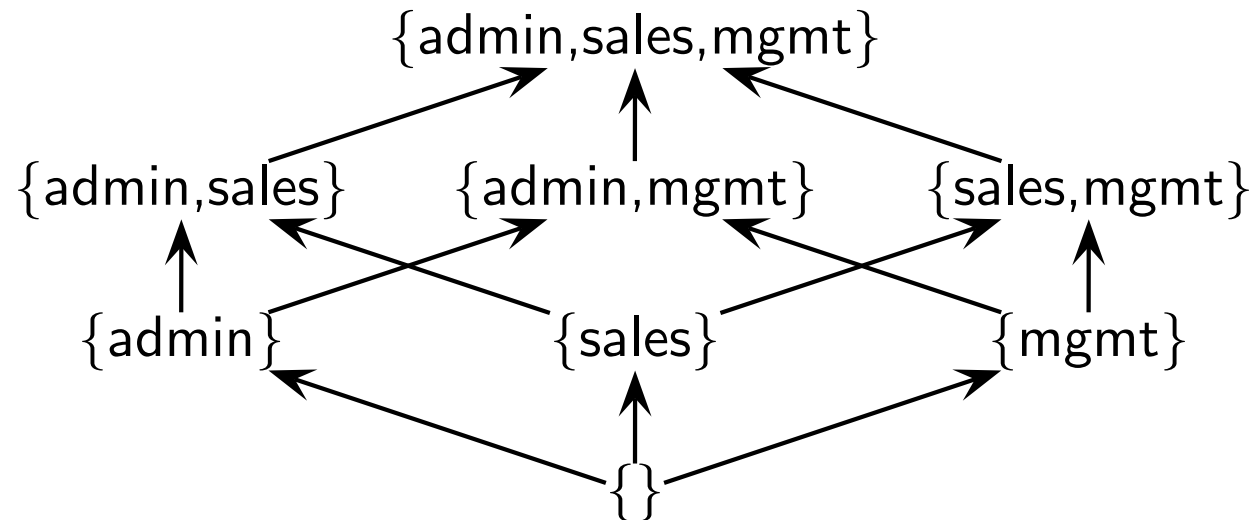
$(SC, \leq)$  is a *partially ordered set*: given  $a, b, c \in SC$ , then

- Reflexive:  $a \leq a$ .
- Antisymmetric:  $a \leq b \wedge b \leq a \Rightarrow a = b$ .
- Transitive:  $a \leq b \wedge b \leq c \Rightarrow a \leq c$ .

# Security Classification Example 'Compartment Ordering'

Trojan Horses  
MAC and DAC  
MLS  
Security Classes  
▷ Compartments  
Bell LaPadua  
BLP Axioms  
Clearance  
MLS File System  
French History  
Covert Channels  
Security Criteria  
Chinese Wall

We have compartments for sales, admin and mgmt information.  
Set of subsets of  $\{\text{sales}, \text{admin}, \text{mgmt}\}$  forms partial order under  $\subseteq$ .



A document  $S$  that contains only sales information has classification  $\{\text{sales}\}$ . A report  $R$  that contains both sales and administration information has security classification  $\{\text{sales}, \text{admin}\}$ .

It should be permitted for information in document  $S$  to be contained in report  $R$ , since  $\{\text{sales}\} \subseteq \{\text{sales}, \text{admin}\}$ , but not vice-versa.

# The Bell LaPadula (BLP) Model of Multilevel Security

Trojan Horses  
MAC and DAC  
MLS  
Security Classes  
Compartments  
▷ Bell LaPadua  
BLP Axioms  
Clearance  
MLS File System  
French History  
Covert Channels  
Security Criteria  
Chinese Wall

BLP is an abstract model for mandatory access control, providing a model of the security mechanisms of a system.

Provides an interpretation of what it means for a system to be MLS.

Model Components:

- Partial order of security classifications  $(SC, \leq)$ .  
For  $a, b \in SC$ , then  $a \leq b$  means that information at class  $a$  may flow to class  $b$ .
- set of objects  $O$ : the set of protected entities that have state, for example, directories, files, memory segments, ... Each object  $o$  has security classification  $\underline{o}$ .
- set of subjects  $S$ : the set of active entities, for example, users, processes, ... Each subject  $s$  has security classification  $\underline{s}$ .
- Access Matrix  $M$  giving current access state  $M[s, o] \subseteq \{R, W\}$ .  
 $R \in M[s, o]$  means that subject  $s$  currently has  $R$  access to object  $o$ .  
 $W \in M[s, o]$  means that subject  $s$  currently has  $W$  access to object  $o$ .
- Security Axioms that define what is means by a secure state.



# What is a Secure (Access) State $M[s, o]$ ?

Trojan Horses  
MAC and DAC  
MLS  
Security Classes  
Compartments  
▷ Bell LaPadua  
BLP Axioms  
Clearance  
MLS File System  
French History  
Covert Channels  
Security Criteria  
Chinese Wall

subjects/objects	$x$	$\underline{x}$
Process owned by Simon	Ps	top-secret
Process owned by student Alice	Pa	unclassified
Process owned by tutor Tony	Pt	secret
File of exam results	rsIts	top-secret
File of practical solutions	pract	secret
File of lecture notes	notes	unclassified

topSecret  
↑  
secret  
↑  
unclassified

$M$	Ps	Pt	Pa	rsIts	pract	notes
Ps				$RW$	$R$	$R$
Pt			$R$		$RW$	
Pa						$RW$

A Secure state.

Tutor Tony (process) may read the state of student Alice's process.

$M$	Ps	Pt	Pa	rsIts	pract	notes
Ps				$RW$	$R$	$R$
Pt			$R$		$RW$	
Pa				$R$		$RW$

Alice attempts to read results.

State is not secure.  $\underline{rsIts} \not\leq \underline{Pa}$

May not read up.

$M$	Ps	Pt	Pa	rsIts	pract	notes
Ps				$RW$	$R$	$RW$
Pt			$R$		$RW$	
Pa						$RW$

A Trojan Horse run by Simon copies results into notes

State is not secure.  $\underline{Ps} \not\leq \underline{notes}$   
No Write Down

Security mechanism implementation must ensure that its not possible for the system to be in an insecure state.

# Bell LaPadua Axioms for Secure State

Trojan Horses  
MAC and DAC  
MLS  
Security Classes  
Compartments  
Bell LaPadua  
▷ BLP Axioms  
Clearance  
MLS File System  
French History  
Covert Channels  
Security Criteria  
Chinese Wall

Axioms that define the set of all states that are permitted by the MLS security policy. Given the current security state  $M$  then:

- Simple Security Condition (SS condition): “No Read up”  
For all subjects  $s$  and objects  $o$ , then

$$R \in M[s, o] \Rightarrow \underline{o} \leq \underline{s}$$

- Confinement Property ( $\star$  property): “No Write Down”  
For all subjects  $s$  and objects  $o$ , where  $\underline{o} \leq \underline{s}$ , then

$$W \in M[s, o] \Rightarrow \underline{s} \leq \underline{o}$$

Axioms on State Transitions (how the access matrix may change).

- Tranquility: Partial order and classification bindings may not change with a state transition.

# Distinguishing Subjects and Users in MLS

Trojan Horses  
MAC and DAC  
MLS  
Security Classes  
Compartments  
Bell LaPadua  
BLP Axioms  
▷ Clearance  
MLS File System  
French History  
Covert Channels  
Security Criteria  
Chinese Wall

User Simon is cleared to top-secret. He can read and write exam results. He should also be able to read and write lecture notes. But if 'he' can simultaneously read and write *rslts* and *notes* he may violate the BLP axioms and be subject to a Trojan Horse attack by untrusted software.

We need to distinguish between user and process. If a user is cleared to class  $a$ , the user may own/launch any process (subject) with a classification dominated by  $a$ .

Ps = top-secret

Psx = unclassified

rslts = top-secret

pract = secret

notes = unclassified

$M$	Ps	Pt	Pa	rslts	pract	notes
Ps				<i>RW</i>	<i>R</i>	<i>R</i>
Psx				<i>W</i>		<i>RW</i>
Pt			<i>R</i>		<i>RW</i>	
Pa						<i>RW</i>

User Simon is cleared to top-secret and owns two processes *Ps* and *Psx*. The BLP axioms are upheld, and Trojan Horse attack is not possible.

# Distinguishing Subjects and Users in MLS

Trojan Horses  
MAC and DAC  
MLS  
Security Classes  
Compartments  
Bell LaPadua  
BLP Axioms  
▷ Clearance  
MLS File System  
French History  
Covert Channels  
Security Criteria  
Chinese Wall

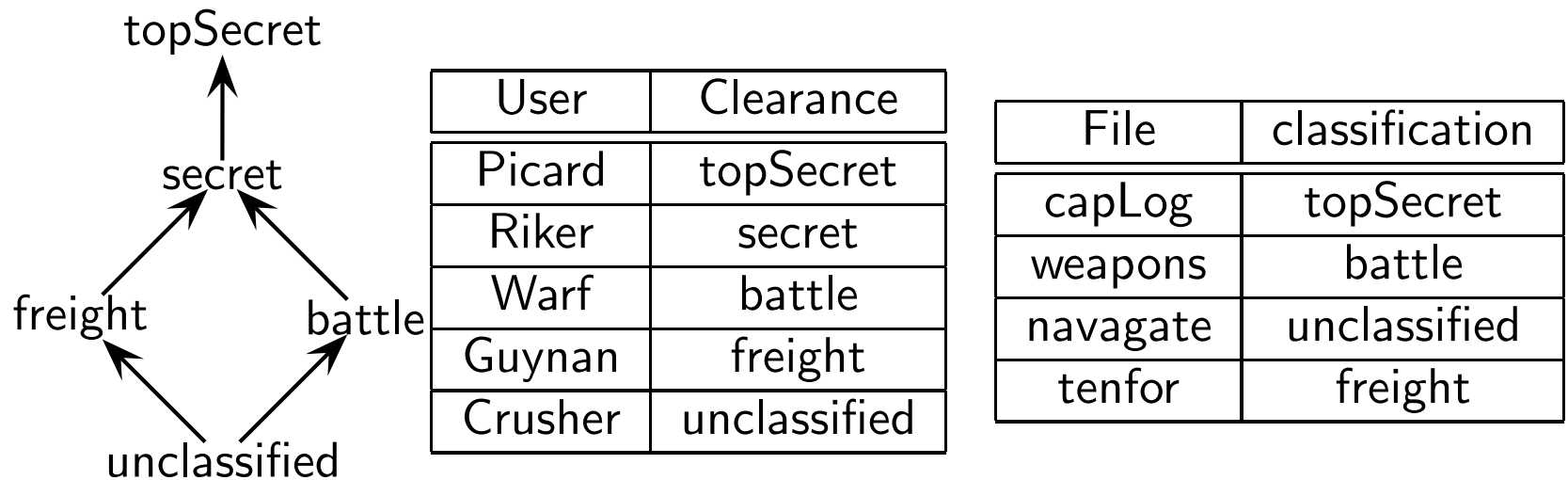
Can be supported in a number of ways.

- Single Level workstation. A user logs on at class  $a$  (dominated by user's clearance). All processes for that session are at class  $a$ . Working set is flushed between sessions.
- Multilevel workstation. A user logs-on and the workstation permits user to have simultaneous processes running at different classifications. For example, a Trustworthy “Compartmented Mode” Workstation. May also provide multilevel windowing system where different windows labeled with different security classes.
- Multilevel System/Server. Supporting multiple users/processes at different clearances.

# MLS Example

Trojan Horses  
MAC and DAC  
MLS  
Security Classes  
Compartments  
Bell LaPadua  
BLP Axioms  
▷ Clearance  
MLS File System  
French History  
Covert Channels  
Security Criteria  
Chinese Wall

The computer on the starship Enterprise handles unclass, secret, topsec, battle and freight data. Note that battle and freight is *disjoint*: information at one level may not flow to the other.



Picard can login at topSecret (a process at that level) to edit the capLog.

Picard can login at freight to check the menu in tenfor.

There's nothing that Guynan can do to learn anything about the contents of the weapons file.

# Clearances and Compartments

Trojan Horses  
MAC and DAC  
MLS  
Security Classes  
Compartments  
Bell LaPadua  
BLP Axioms  
▷ Clearance  
MLS File System  
French History  
Covert Channels  
Security Criteria  
Chinese Wall

Multilevel secure systems typically offer a combination of both compartments and a partial ordering.

For example, combining the  $\{\text{sales}, \text{admin}, \text{mgmt}\}$  compartment ordering example with security levels unclassified, secret, topSecret allows clearances, etc., to be given as a pair  $(l, s)$ , where  $s$  is a set of compartments and  $l$  a level.

User	Clearance
SalesManager	(secret, {sales, mgmt})
President	(topsecret, {sales, mgmt, admin})
SalesPerson	(unclassified, {sales})

The BLP model can be generalized for these extended orderings. Intuitively, a subject with class  $(\text{secret}, \{\text{sales}, \text{mgmt}\})$  can read an object with class  $(\text{unclassified}, \{\text{sales}\})$ , but cannot read an object with class  $(\text{secret}, \{\text{sales}, \text{admin}\})$ .



# MLS/BLP and Trojan Horses

- Trojan Horses
- MAC and DAC
- MLS
- Security Classes
- Compartments
- Bell LaPadua
- BLP Axioms
- ▷ Clearance
- MLS File System
- French History
- Covert Channels
- Security Criteria
- Chinese Wall

The BLP model regards all application s/w and most OS s/w as *untrusted*, that is, the BLP axioms are implemented by a security mechanism in a low-level security kernel that mediates all access.

For example, an editor containing a Trojan Horse cannot copy topSecret data down to secret: it cannot violate the MLS policy.

While this may prevent a malicious Word macro from violating the policy, the word macro can still interfere with other files/objects at the same level (or higher) than the executing subject.

MLS/MAC mechanisms are useful for partitioning critical data/systems (according to policy), but they do not wholly solve the problem of the spread of a Trojan Horse or other malicious code

# Its not just these systems that are critical

- Trojan Horses
- MAC and DAC
- MLS
- Security Classes
- Compartments
- Bell LaPadua
- BLP Axioms
- ▷ Clearance
- MLS File System
- French History
- Covert Channels
- Security Criteria
- Chinese Wall



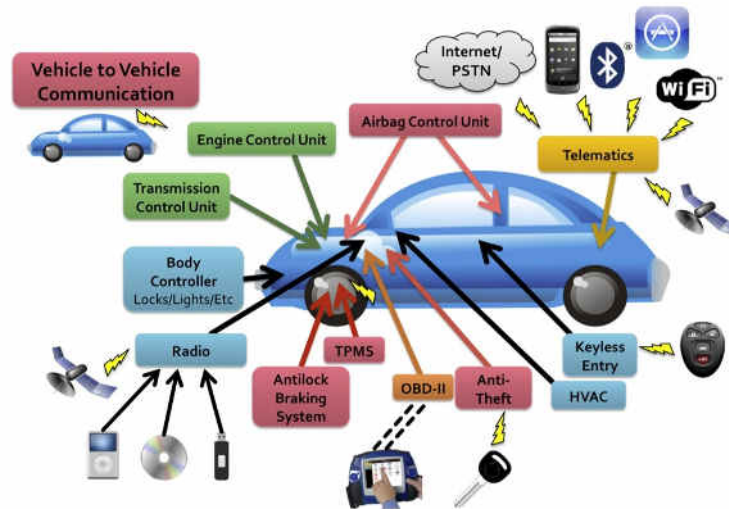
Any scenario where strict data separation must be preserved.

For example, a system running a mail server and public web server. Use an information flow policy based on subsets of  $\{\text{mail}, \text{web}\}$ . Web-server has class  $\{\text{web}\}$  and email-server has class  $\{\text{mail}\}$ .

If one of the applications is compromised, MLS policy ensures separation of damage from other application.

# Its not just these systems that are critical

Trojan Horses  
MAC and DAC  
MLS  
Security Classes  
Compartments  
Bell LaPadua  
BLP Axioms  
▷ Clearance  
MLS File System  
French History  
Covert Channels  
Security Criteria  
Chinese Wall



Any scenario where strict data separation must be preserved.

For example, a system running a mail server and public web server. Use an information flow policy based on subsets of  $\{\text{mail}, \text{web}\}$ . Web-server has class  $\{\text{web}\}$  and email-server has class  $\{\text{mail}\}$ .

If one of the applications is compromised, MLS policy ensures separation of damage from other application.

# Its not just these systems that are critical

- Trojan Horses
- MAC and DAC
- MLS
- Security Classes
- Compartments
- Bell LaPadua
- BLP Axioms
- ▷ Clearance
- MLS File System
- French History
- Covert Channels
- Security Criteria
- Chinese Wall



Any scenario where strict data separation must be preserved.

For example, a system running a mail server and public web server. Use an information flow policy based on subsets of  $\{\text{mail}, \text{web}\}$ . Web-server has class  $\{\text{web}\}$  and email-server has class  $\{\text{mail}\}$ .

If one of the applications is compromised, MLS policy ensures separation of damage from other application.

# Its not just these systems that are critical

- Trojan Horses
- MAC and DAC
- MLS
- Security Classes
- Compartments
- Bell LaPadua
- BLP Axioms
- ▷ Clearance
- MLS File System
- French History
- Covert Channels
- Security Criteria
- Chinese Wall



Any scenario where strict data separation must be preserved.

For example, a system running a mail server and public web server. Use an information flow policy based on subsets of  $\{\text{mail}, \text{web}\}$ . Web-server has class  $\{\text{web}\}$  and email-server has class  $\{\text{mail}\}$ .

If one of the applications is compromised, MLS policy ensures separation of damage from other application.

Worthwhile putting a lot of effort into assuring the security of the system.

# Building MLS Systems is not easy

Trojan Horses  
MAC and DAC  
MLS  
Security Classes  
Compartments  
Bell LaPadua  
BLP Axioms  
▷ Clearance  
MLS File System  
French History  
Covert Channels  
Security Criteria  
Chinese Wall

Suppose we wanted to implement a multilevel Secure Unix.

Every user has a security clearance. Subjects are processes. Objects are files. The security mechanisms enforce the BLP axioms.

Possible 'Covert Channels':

- ☐ Trojan Horse (executing at top-secret) emails unclassified accomplice.
- ☐ Trojan Horse (TS) writes to a socket readable by unclassified accomplice.
- ☐ Trojan Horse (TS) reads launch-codes from top-secret file; submits a print-job with name given by the launch codes. Unclassified accomplice checks print queue.
- ☐ Trojan Horse (TS) checks top-secret file `exam.txt` for keyword MLS. If found, it performs 1M write operations to disk, otherwise nothing. Unclassified user keeps track of disk performance.



# Challenges Implementing MLS Systems: Simple File System I

Trojan Horses  
MAC and DAC  
MLS  
Security Classes  
Compartments  
Bell LaPadua  
BLP Axioms  
Clearance  
▷ MLS File System  
French History  
Covert Channels  
Security Criteria  
Chinese Wall

Suppose we want to build a file system that upholds the BLP Axioms.

- Single level file system: easy as all files are at same class.
- Multilevel file system: Each file  $\underline{f}$  is an object and has a single security class, denoted  $\underline{f}$ . Each process is a subject. File system operations include OpenRead and OpenWrite. The security state is defined by matrix  $M$  and can be changed by the transition operations OpenRead and OpenWrite.

OpenRead( $s, \underline{f}$ )

if  $\underline{f} \leq \underline{s}$

then enter  $R$  into  $M[s, \underline{f}]$ .

OpenWrite( $s, \underline{f}$ )

if  $\underline{s} \leq \underline{f}$

then enter  $W$  into  $M[s, \underline{f}]$ .

Easy enough to show that this abstract model corresponds to BLP model. However, the abstract model is too abstract and does not properly correspond to the implementation (recall the covert channels described earlier).

# Challenges Implementing MLS Systems: Simple File System II

Trojan Horses  
MAC and DAC  
MLS  
Security Classes  
Compartments  
Bell LaPadua  
BLP Axioms  
Clearance  
▷ MLS File System  
French History  
Covert Channels  
Security Criteria  
Chinese Wall

Consider a flat filing system (only one directory):

- ☐ Each file uniquely identified by file identifier  $fid$
- ☐ Security classification of file is  $fid$ .
- ☐ Each file has a unique name given by  $name(fid)$ .
- ☐ A subject  $s$  opens a file named  $fname$  for access defined by  $mode \subseteq \{R, W, C\}$  by invoking operation  $open(s, fname, mode)$ . If successful it returns the file's  $fid$ .
- ☐ Given an open file, other operations include  $read(fid, buff)$ ,  $write(fid, buff)$ ,  $close(fid)$ .

For simplicity we assume that a file-id is like a handle and cannot be forged. Therefore, the only way a file may be accessed is by first opening it, obtaining the file-id, and then reading/writing. Thus, we need to model how transition Open changes the access state.

From the description on the next slide, it seems clear that the abstract model is secure. However, ...

# Simple File System II: File Open

Trojan Horses  
MAC and DAC  
MLS  
Security Classes  
Compartments  
Bell LaPadua  
BLP Axioms  
Clearance  
▷ MLS File System  
French History  
Covert Channels  
Security Criteria  
Chinese Wall

```
Op Open(s, fname, mode)
{
  if  $C \in \text{mode}$  and no fid exists with  $\text{name}(\text{fid}) = \text{fname}$ 
  then create new fid with  $\underline{\text{fid}} = \underline{s}$  and  $\text{name}(\text{fid}) = \text{fname}$ ;

  if  $R \in \text{mode}$  and fid exists with  $\text{name}(\text{fid}) = \text{fname}$  and  $\underline{\text{fid}} \leq \underline{s}$ 
  then read access OK;

  if  $W \in \text{mode}$  and fid exists with  $\text{name}(\text{fid}) = \text{fname}$  and  $\underline{s} \leq \underline{\text{fid}}$ 
  then write access OK;

  if access OK
  then return fid
  else return null
}
```

# File system example: some French History c1600

Trojan Horses  
MAC and DAC  
MLS  
Security Classes  
Compartments  
Bell LaPadua  
BLP Axioms  
Clearance  
MLS File System  
▷ French History  
Covert Channels  
Security Criteria  
Chinese Wall



Louis XIV

- ☐ Wife M'dAutriche;
- ☐ Lover 1 Mme de la Valiere; child Louis le Dauphin.
- ☐ Lover 2 Madame de Montespan; child duc duMaine (apparent father Marquis deMontspan); child M'elle de Blois

# Covert Channels in our File System

Trojan Horses  
MAC and DAC  
MLS  
Security Classes  
Compartments  
Bell LaPadua  
BLP Axioms  
Clearance  
MLS File System  
French History  
▷ Covert Channels  
Security Criteria  
Chinese Wall

King Louis XIV (secret clearance) keeps a diary in a secret file diary.

His Queen M. d'Autriche (unclassified) plants a Trojan Horse in editor to find out if Mme deMontespan is mentioned

Loius XIV logs in at secret, runs editor, Trojan Horse executes:

```
☐ inspect diary for occurance of string "deMontespan" (lover 1).  
☐ if found then create (secret) file called MYES else do nothing.
```

Later M. d'Autriche logs in at unclassified:

```
☐ attempts to create (unclassified) file MYES  
☐ if failure then King is seeing his mistress...
```

A simple covert channel with a small capacity (1 bit: YES/NO).

Easy to extend to communicate secret m-bit value to unclassified by creating/checking for multiple files, each one corresponding to one bit position.

# Removing File Creation Covert Channel

Trojan Horses  
MAC and DAC  
MLS  
Security Classes  
Compartments  
Bell LaPadua  
BLP Axioms  
Clearance  
MLS File System  
French History  
▷ Covert Channels  
Security Criteria  
Chinese Wall

**Strategy 1.** Permit duplicate filenames at different classifications.

However, this can be problematic:

☐ King Louis XIV maintains secret diary.txt.  
☐ Queen M. d'Autriche creates file diary.txt (unclassified).  
☐ Louis XIV running at unclassified now sees two diaries and accidentally writes about Melle deLaValiere (lover 2) in the wrong one!

Strategy 1 is good if the file's existence and contents are sensitive.

This has an integrity issue since it may not be clear to the king which file diary.txt is the true diary.



# Removing File Creation Covert Channel

Trojan Horses  
MAC and DAC  
MLS  
Security Classes  
Compartments  
Bell LaPadua  
BLP Axioms  
Clearance  
MLS File System  
French History  
▷ Covert Channels  
Security Criteria  
Chinese Wall

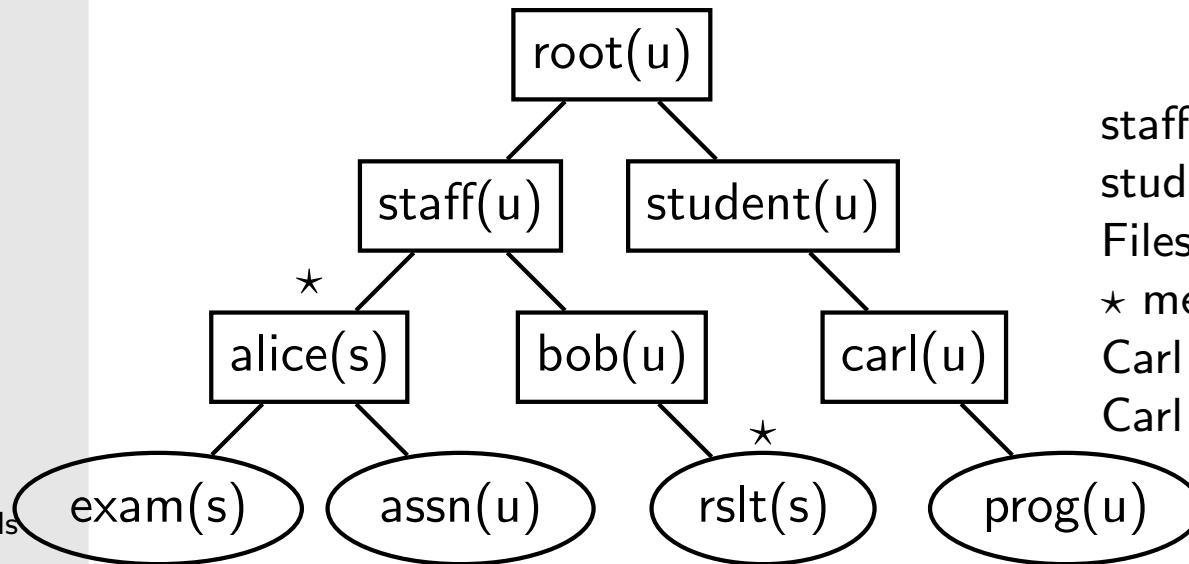
**Strategy 2.** No duplicate file names, but all file creations done at the level of the directory in which they occur. Once created, the classification is *upgraded* to the required classification.

- ☐ Louis XIV wants to create a birthday book (secret).
- ☐ Louis XIV Logs in at unclassified:  
creates `bbook.txt` (unclassified)  
upgrade `bbook.txt` to secret.
- ☐ Louis XIV logs in at secret:  
enter birthday details of Duc duMaine (child of deMontspan).
- ☐ The queen may test for the existence of the birthday book but may not read it.

Strategy 2 is good if just the contents are sensitive, and suffers no integrity problems.

# MLS File Systems in Practice

Trojan Horses  
MAC and DAC  
MLS  
Security Classes  
Compartments  
Bell LaPadua  
BLP Axioms  
Clearance  
MLS File System  
French History  
▷ Covert Channels  
Security Criteria  
Chinese Wall



staff cleared to secret.  
students cleared to unclassified.  
Files created at the level of directory.  
★ means the file was then upgraded.  
Carl can test result file existence  
Carl cannot test existence of exam file.

Other potential covert channels:

- directory listing in increasing/decreasing order.  
If *fid* values are generated sequentially then a high level Trojan horse can signal a low-level process by creating a large number of files. A solution is to use a *secure* pseudo-random number generator to generate fids.

# Security Criteria

Trojan Horses  
MAC and DAC  
MLS  
Security Classes  
Compartments  
Bell LaPadua  
BLP Axioms  
Clearance  
MLS File System  
French History  
Covert Channels  
▷ Security Criteria  
Chinese Wall

Criteria to judge system security. USA “*Orange Book*” [1983] used assurance levels (high)  $A1 > B2 > B2 > B1 > C3 > C2 > C1 > D$  (low). Levels  $A\&B$  used for MLS/MAC and  $C$  for DAC.

High assurance requires mathematical models of protection mechanisms and property proofs (eg that BLP axioms upheld), TCB code demonstrated to implement model, extensive testing and auditing. Low assurance relies on more informal methods.

Orange book superseded by the Common Criteria and other criteria such as FIPS (criteria for cryptographic modules).

Common criteria is most widely used and provides evaluation levels ranging from EAL1 (most basic) to EAL7 (highest assurance). Evaluation is done relative to a protection profile which defines the requirements. This is unlike the orange book which effectively had BLP-MLS as its only ‘profile’.

# Some Evaluated Systems

Trojan Horses  
MAC and DAC  
MLS  
Security Classes  
Compartments  
Bell LaPadua  
BLP Axioms  
Clearance  
MLS File System  
French History  
Covert Channels  
▷ Security Criteria  
Chinese Wall

- ☐ Key Management Systems: IBM Tivoli Directory Server version 6.1 (EAL4+), ...
- ☐ Firewalls: Sidewinder 7.0.0.02 (EAL4+), ...
- ☐ General Purpose OS: PR/SM for IBM System z10 EC GA1 (EAL5), Oracle Enterprise Linux Version 5 Update 1 (EAL4+), Microsoft Windows Vista and Windows Server 2008 (EAL1), XTS-400 (linux-like) (EAL5+; Orange Book B3), Apple Mac OS X v10.3.6 and Apple Mac OS X Server V10.3.6 (EAL3), Smart MX multi-application smartcard (EAL5+).
- ☐ Digital Signature Devices: Sign Live! CC Version 3.2.3 (EAL3+),...
- ☐ See <http://www.commoncriteriaportal.org/products/>

A problem with evaluation criteria is that it can take a long time (many months) to carry out an evaluation on a specific version of a system. A new system version release requires re-evaluation.

# Its all relative to the protection profile

Trojan Horses  
MAC and DAC  
MLS  
Security Classes  
Compartments  
Bell LaPadua  
BLP Axioms  
Clearance  
MLS File System  
French History  
Covert Channels  
▷ Security Criteria  
Chinese Wall

For example, MS Windows 2003 evaluated to CAPP/EAL4

It is relative to the Controlled Access Protection Profile (CAPP) protection profile that assumes non-hostile and well-managed user community requiring protection against threats of inadvertent or casual attempts to breach the system security.

The CAPP profile is not intended to be applicable to circumstances in which protection is required against determined attempts by hostile and well funded attackers to breach system security.

CAPP does not fully address the threats posed by malicious system development or administrative personnel.

# Other Contemporary uses: Language based security

Trojan Horses  
MAC and DAC  
MLS  
Security Classes  
Compartments  
Bell LaPadua  
BLP Axioms  
Clearance  
MLS File System  
French History  
Covert Channels  
▷ Security Criteria  
Chinese Wall

Check for information flows between variables in programs at compile time.  
For example, given `lo` and `hi` level variables, then

```
if hi >= 10 {lo := 0} else {lo := 1;}
```

contains an implicit flow of information from `hi` to `lo`.

For example, Java tools such as Jif have been used to check information flows in the implementation of security protocols, electronic voting systems and other security-critical systems.

# Chinese Wall (MAC) Security Policy

- Trojan Horses
- MAC and DAC
- MLS
- Security Classes
- Compartments
- Bell LaPadua
- BLP Axioms
- Clearance
- MLS File System
- French History
- Covert Channels
- Security Criteria
  - ▷ Chinese Wall

Stock Market analyst must maintain confidentiality of organizations that she consults for; she is not permitted to advise an organization given insider knowledge of another competing organization.

Define a conflict-of-interest relation ( $_ \wr _$ ) between organizations.  $a \wr b$  means that  $a$  is in competition with  $b$ . A system enforces a Chinese Wall policy if it ensures that it is not possible for a consultant (user) to access information about  $a$  and  $b$ , with  $a \wr b$ .

$_ \wr _$	esso	elf	aib	boi
esso		×		
elf	×			
aib				×
boi			×	

Consultant, Smith, working for aib, may not have access to boi information. Similarly, consultant, Jones, working for bank, boi, may not access bank aib information. But both have the potential to access oil company esso or elf information, but not both.

Define zones of non-communication (email, IM, etc) between different departments are a form of chinese wall

## [-] **How Does Exchange 2010 Help You Implement Ethical Walls?**

Exchange 2010 uses transport rules configured on Hub Transport servers. Correctly configured transport rules support ethical walls by helping to prevent e-mail messages from being sent between specific groups of recipients within your organization.

### ◆ **Important:**

Exchange 2010 includes features that may help you prevent breaches of an ethical wall. However, Exchange 2010 doesn't prevent individuals from using other methods of communication, such as private e-mail accounts located outside the Exchange organization, network file shares, or phone calls, to share information. Consider Exchange 2010 transport rules as part of an overall suite of tools or processes that you deploy throughout your organization to help enforce an ethical wall policy.



# Chinese Wall Policy Requirements

- Trojan Horses
- MAC and DAC
- MLS
- Security Classes
- Compartments
- Bell LaPadua
- BLP Axioms
- Clearance
- MLS File System
- French History
- Covert Channels
- Security Criteria
- ▷ Chinese Wall

Information flow within the system must be considered when enforcing the Chinese Wall policy.

The protection mechanism must ensure that it is not possible for AIB consultant Jones to pass on any bank aib information to BOI consultant Smith, leading to a conflict of interest.

While Smith and Jones can conduct insider trading outside the security perimeter of the system, possible Trojan Horse attack should be considered. For example, a Trojan Horse embedded in software run by Jones will have access to aib information: the protection mechanism must ensure it cannot be passed to Smith.

We would like *assurance* that the Chinese Wall policy is upheld under all circumstances. Simply monitoring email/IM traffic is not sufficient.

Strategy: map the requirements into a MLS policy.

# Enforcing a Chinese Wall using MLS

Trojan Horses  
MAC and DAC  
MLS  
Security Classes  
Compartments  
Bell LaPadua  
BLP Axioms  
Clearance  
MLS File System  
French History  
Covert Channels  
Security Criteria  
▷ Chinese Wall

Let  $ORG$ , the set of all organizations, define the set of multilevel compartments.

The multilevel policy is built from compartments defined by  $ORG$ .

A file/dataset containing organization  $o$  data has security classification  $\{o\}$

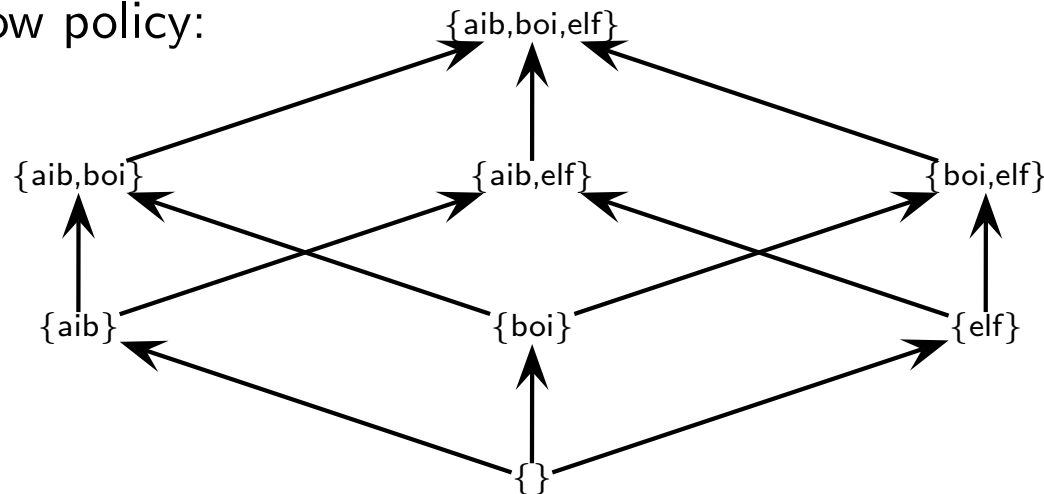
The initial clearance of each consultant  $C$  is  $clear(C) = \{\}$ . A consultant  $C$  wishing to consult for organization  $o$  makes the request  $request(C, o)$ , where:

$$request(C, o) \equiv \begin{cases} \text{if (exists } o' \in clear(C) \text{ such that } o \searrow o') \\ \text{reject: conflict of interest} \\ \text{else} \\ \text{set } clear(C) \text{ to } clear(C) \cup \{o\} \end{cases}$$

A consultant's clearance can only increase and only so long as there is no conflict of interest.

## Example, $ORG = \{\mathbf{aib}, \mathbf{boi}, \mathbf{elf}\}$

Information flow policy:



- ☐ Initially,  $clear(\text{Smith}) = clear(\text{Jones}) = \{\}$
- ☐ Smith asks to consult for aib: accepted:  $clear(\text{Smith}) = \{\mathbf{aib}\}$ .
- ☐ Smith asks to consult for boi: rejected:  $clear(\text{Smith}) = \{\mathbf{aib}\}$ .
- ☐ Jones asks to consult for boi: accepted:  $clear(\text{Jones}) = \{\mathbf{boi}\}$ .
- ☐ Both may ask to consult for elf:  $clear(\text{Smith}) = \{\mathbf{aib}, \mathbf{elf}\}$ ,  
 $clear(\text{Jones}) = \{\mathbf{boi}, \mathbf{elf}\}$ .
- ☐ While both may share elf information, (login at {elf}), no Trojan horse can violate the Chinese Wall between aib and boi.