Security (CS4028)

Lecture 12. Security Models

Chunyan Mu

chunyan.mu@abdn.ac.uk

The School of Natural and Computing Sciences

Schedule

	Week	Lecture 1	Lecture 2	Tutorial
	1	Intro to course & security	Intro to Crypto	-
	2	Symmetric Crypto	Hash	Math for crypto
	3	Asymmetric Crypto-1	Asymmetric Crypto-2	Symmetric Crypto
	4	Signatures	Zero Knowledge Proof	Asymmetric Crypto
	5	Certificates	Authentication	Signature & certificates
⇒	6	Access Control	Security models	Authentication
	7	Information flow	Information flow	Access control
	8	Management	Protocols	Concepts & management
	9	Network security	Network security	Protocols
	10	Advanced topic	Advanced topic	Network
	11	Revision		

Outline

Recap: key definition in security model

Information flow policy

Formal security models
- BLP
- Biba
- Chinese wall

Summary

Outline

Security models

- Security policy: a statement that partitions the states of the system into a set of *secure* states and a set of *non-secure* states.
- Security mechanism: a method, tool, or procedure that enforces some part of the security policy.
- Security model: a model that represents a particular policy or set of policies.

Security Models

- How do we design policies?
  - describe the entities governed by the policy
  - state the rules
- How well is this done?
  - incompleteness and ambiguity are common
  - formal models help to address the dependability of policy and protocol design

Outline

Information flow policy

Information flow

Accessing a computer resource can be regarded as initiating an information flow:

- Read access causes information to flow from an object to a subject;
- Write access causes information to flow from a subject to an object.

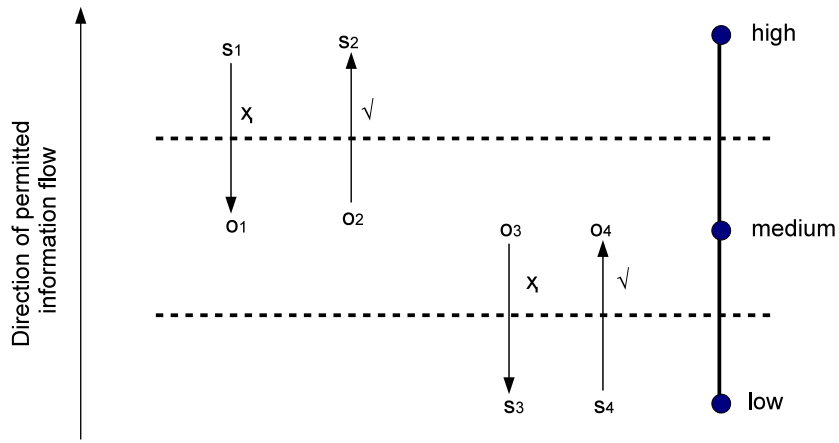
An information flow policy

- The notion of information flows can be used to construct an access control model.
- The following policy enforces confidentiality requirements:
  - Every object and subject has a security level (security label)
  - The set of security labels is a (partially) ordered set;
  - Information flows must respect the partial ordering, in that information can only flow from entity a to entity b if $a \leq b$ (where $\leq$ is the partial ordering)

An information flow policy

Example

- Assume subjects s_1 and s_2 have high security clearance; objects o_1, o_2, o_3 and o_4 have medium security sensitivity; subjects s_3 and s_4 have low security clearance. Then:
  - s_2 can read o_2;s_4 can write to o_4;
  - s_1 cannot write to o_1; s_3 cannot read o_3
- This policy enables "read down" and "write up".



An information flow policy

What does this policy prevent?

- Information leaks due to inappropriate read actions:
  - Prevents unclassified user reading classified information
- Information leaks due to inappropriate write actions:
  - Prevents classified information being printed to an unclassified printer;

Outline

The Bell-LaPadula Model (1973)

Overview

- David Bell and Len Lapadula, 1973
- Most famous and influential security model
- Purposes:
  - Simple security mechanisms enabling verification
  - Confidentiality of information

The Bell-LaPadula Model (1973)

Basic idea

- Implements an information flow policy for confidentiality:
  - a state machine model capturing confidentiality aspects of access control
- Employs a security lattice (a partially ordered set of security labels)
- Employs a protection matrix, where this matrix refines the information flow policy
- Keep track of current security levels of subjects, current set of accesses
- Gives a set of properties, which, if they hold, guarantee that all states of the system will be secure

The Bell-LaPadula Model (1973)

State-machine models

- State: represents the condition of a system at a point in time.
- Transitions to the next states reachable from the current one in a single step
- State Transition Function: defines the next state, given the current state and some input.

The Bell-LaPadula Model (1973)

Multi-level Security System (MLS)

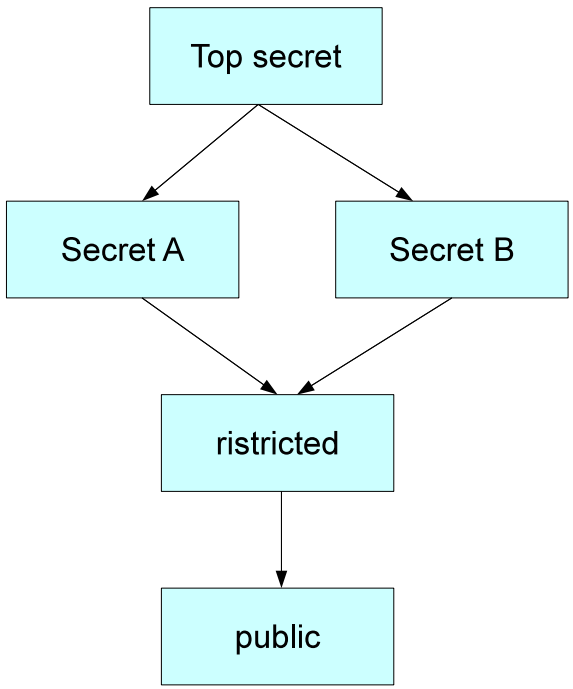
- Formal policy model for madatory access control in a military multilevel security (MLS) environment
- Four confidentiality levels:

  unclassified $<$ confidential $<$ secret $<$ top secret
- All subjects and data objects are labelled with one confidentiality level
- The system policy automatically prevents the flow of information from high-level objects to lower levels
  - A process that reads top secret data becomes tagged as top secret, as will be all files it writes afterwards
  - Each user has a maximum allowed confidentiality level specified and cannot receive data beyond that level

The Bell LaPadula Models (1973)

Definitions

- Fixed sets of subjects S and objects O
- lattice of security levels L, with a partial ordering $\leq$:
  - for each two security levels there are greatest lower bound (glb) and least upper bound (lub)
- Assign security levels to subjects and objects
- Access matrix $M : S \times O \rightarrow 2^R$ mirror the access rights



The Bell-LaPadula Model (1973)

Security labels

Security label has two parts H and C, where H is a security classification and C is a subset of security categories:

- Security level classifications, $\leq_H$, e.g.:
  - unclassified $<$ classified $<$ secret $<$ top secret
- Set of security ("needs-to-know") categories, e.g.:
  - $\{$army, navy, air force, marines$\}$
  - $\{$support, administrator, tutor, researcher$\}$

The Bell-LaPadula Model (1973)

Partial ordering of security labels

- A partial ordering $\leq$ is defined in the set of security labels, such that: $(h_1, c_1) \leq (h_2, c_2)$ iff $h_1 \leq h_2$ and $c_1 \subseteq c_2$
- For example,
  - $(u, \emptyset) \leq (u, \{army\})$
  - $(u, \emptyset) \leq (c, \emptyset)$
  - $(c, \{army\}) \leq (t, \{army, navy, marines\})$

  where u stands for unclassified, c for classified, s for secret, and t for top secret.

The Bell-LaPadula Model (1973)

States

- A state (M, B, λ) is a "snapshot" of the system, given by three components:
  - M is a protection matrix: rows corresponding to the subjects, and columns corresponding to objects
  - the security function λ associates each object and each subject with a security label
  - B is the set of active triples, i.e., $(s, o, a) \in B$ implies that subject s currently has access to object o using access right a
- if a user s has requested read access r to a file o and it has been granted: the file has been loaded into primary memory, then $(s, o, r) \in B$

The Bell-LaPadula Model (1973)

The security properties: overview

The BLP model requires three security properties to hold:

- the simple security property
- the *-property
- the discretionary property

The Bell-LaPadula Model (1973)

The simple security property

- Covers read accesses: only can read down
- Requires that, for all $(s, o, a) \in B$, if a is a read access mode, then

$$\lambda(s) \geq \lambda(o)$$

- In other words, if subject s has been granted read-type access to object o, then s must have a security label that is at least as high as that of o.
- This is implied by the information flow policy.

The Bell-LaPadula Model (1973)

Example: the simple security property

- As an example, suppose that
  - $\lambda(o) = (c, \{army\})$
  - $\lambda(s_1) = (u, \{army, navy\})$
  - $\lambda(s_2) = (s, \{army, marines\})$
- The simple security property would:
  - prevent $(s_1, o, read)$ from entering B;
  - allow $(s_2, o, read)$ to enter B;

The Bell-LaPadula Model (1973)

The *-property

- Addresses write access: only can write up
- Requires that, for all $(s, o, w) \in B$, if w is a write access mode, then

$$\lambda(s) \leq \lambda(o)$$

- In other words, if subject s has been granted write-type access to object o, then s must have a security label that is no higher than that of o

The Bell-LaPadula Model (1973)

The discretionary property

- Addresses discretionary access control, requires that, for all $(s, o, a) \in B$, $(s, o, a) \in M$
- In other words, access is only granted if authorised by the protection matrix
- The protection matrix can be used to refine the information flow policy (enforced by the simple security property and *-property).

The Bell-LaPadula Model (1973)

Example

- One subject s, and three objects o_1, o_2, o_3:

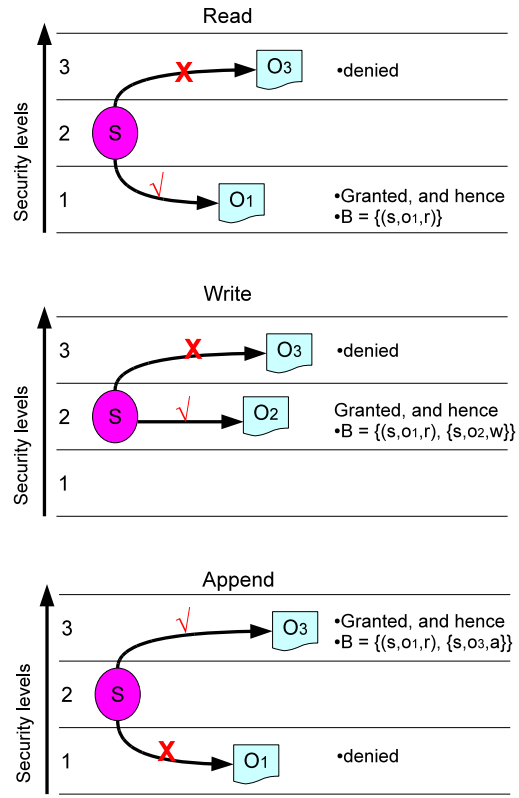
$$\lambda(s) = 2, \lambda(o_1) = 1, \lambda(o_2) = 2, \lambda(o_3) = 3$$

- $B = \emptyset$
- Three access rights: read(r), append(a), and write(w):
  - Append is write only access mode
  - Write is a read and write access mode: this means $\lambda(s) \geq \lambda(o)$ and $\lambda(s) \geq \lambda(o)$ and thus $\lambda(s) = \lambda(o)$
- M contains every access right in each entry: every request is authorised

The Bell-LaPadula Model (1973)

Example: the security properties

- s read access to o_3: denied
- s read access to o_1: granted; $B = \{(s, o_1, r)\}$
- s append access to o_1: denied
- s write access to o_2: granted; $B = \{(s, o_2, w)\}$
- s write access to o_3: denied
- Suppose the access (s, o_2) ends, and hence: $B = \{(s, o_1, r)\}$
- s append access to o_3: granted, $B = \{(s, o_1, r), (s, o_3, a)\}$



The BLP model

BLP disadvantages

- Lacks relevance to commercial systems
- Most seriously, the model only covers data confidentiality (no integrity)
- It was designed for government/military applications
- It lacks flexibility

The Biba model (1977)

- Aspect of security: integrity
- Classification according to levels of integrity
- Requirements
  - Dual simple security property (no read down):

$$\forall s \in S. \forall o \in O : (s, o, r) \Rightarrow \lambda(s) \leq \lambda(o)$$

  - Dual *-property (no write up):

$$\forall s \in S. \forall o \in O : (s, o, r) \Rightarrow \lambda(s) \leq \lambda(o)$$

- Biba is directly opposed to BLP

The Chinese wall model (1989)

Overview

- In a commercial context, it is necessary to establish "Chinese Walls" to handle potential conflicts of interest.
- Suppose a consultancy company has contracts with competing companies A and B.
- Consultant who acquires access to information regarding company A should immediately be excluded for access to information about company B, and vice versa.
- There must be no information flow that causes a conflict of interest.
- Note: dynamic nature of allocation of rights to roles.

The Chinese wall model (1989)

Motivation

- Introduced by Brewer and Nash in 1989
- The motivation for this work was to avoid that sensitive information concerning a company be disclosed to competitor companies through the work of financial consultants
- It dynamically establishes the access rights of a user based on what the user has already accessed

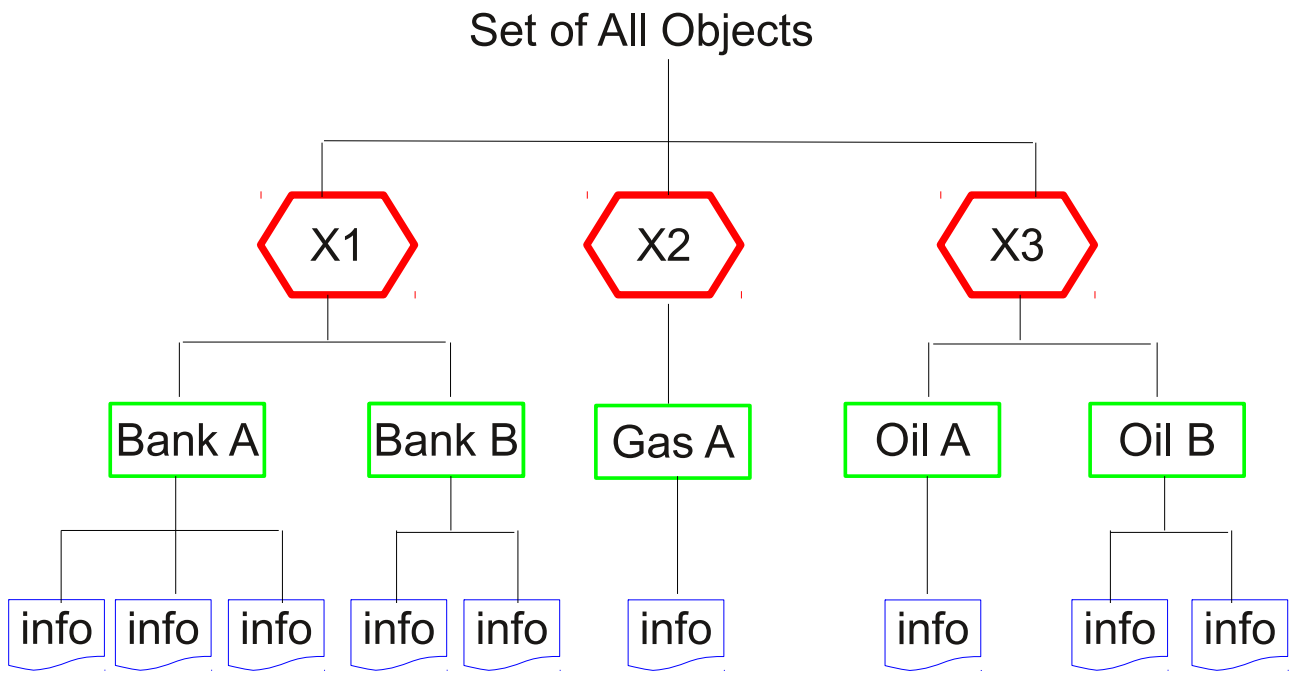
The Chinese wall model (1989)

Policy

- Subjects: Active entities accessing protected objects
- Objects: Data organised according to 3 levels
  - information
  - dataset
  - conflict-of-interest classes denoted by X
- Access rules:
  - read rule
  - write rule

The Chinese wall model (1989)

Data classification [from Bertino]

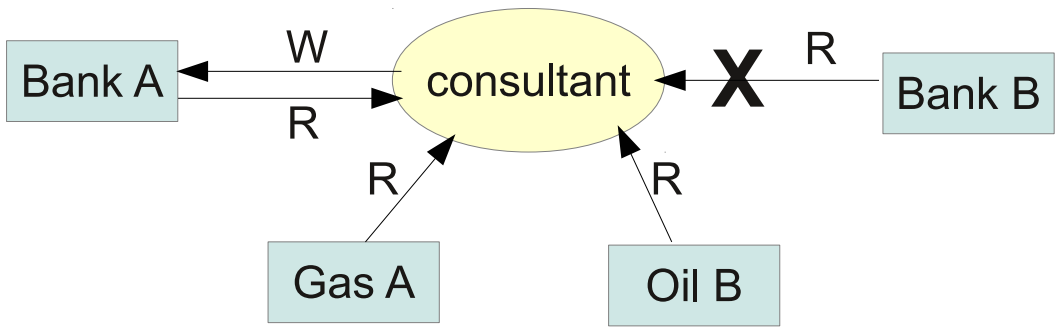


The Chinese wall model (1989)

Read rule

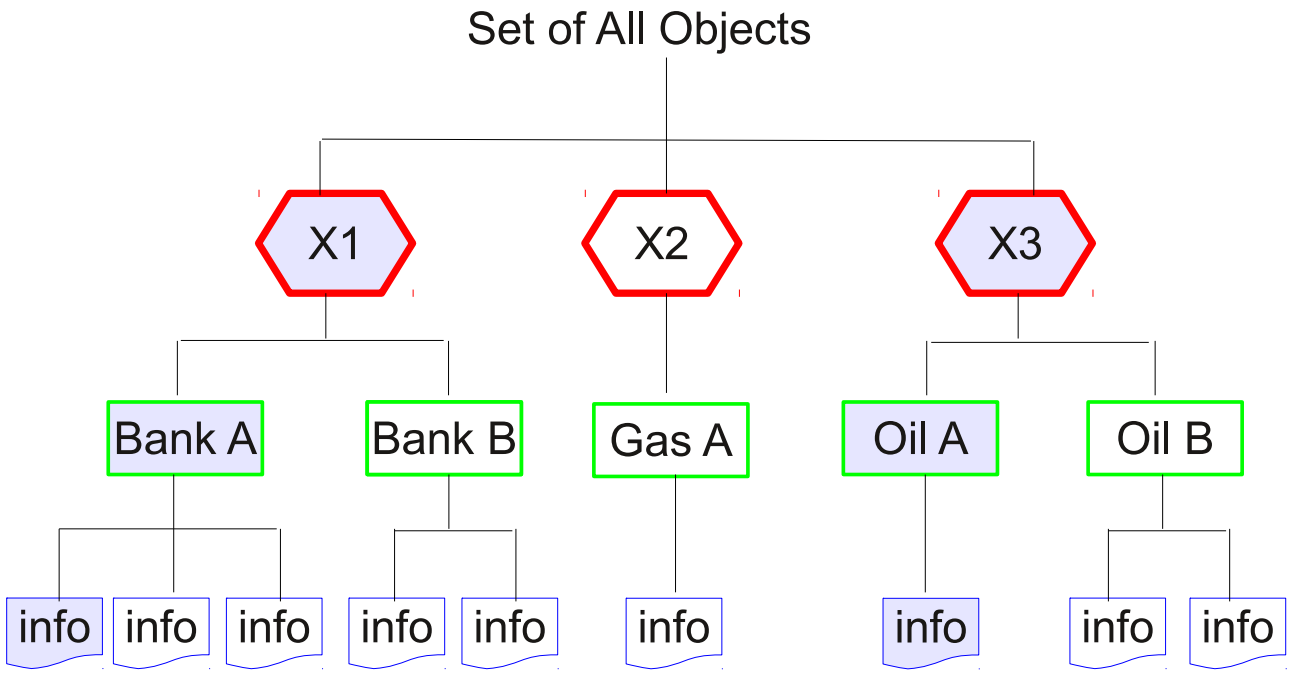
A subject s can read an object o if:

- o is in the same dateset as an object already access by s OR
- o belongs to a conflict-of-interest from which s has not yet accessed any information



The Chinese wall model (1989)

Read rule: S_1



The Chinese wall model (1989)

Remark

- The Chinese Wall Policy is a combination of free choice and mandatory control
- Initially a subject is free to access any object it wishes
- Once the initial choice is made, a Chinese Wall is created for that user around the dataset to which the object belongs

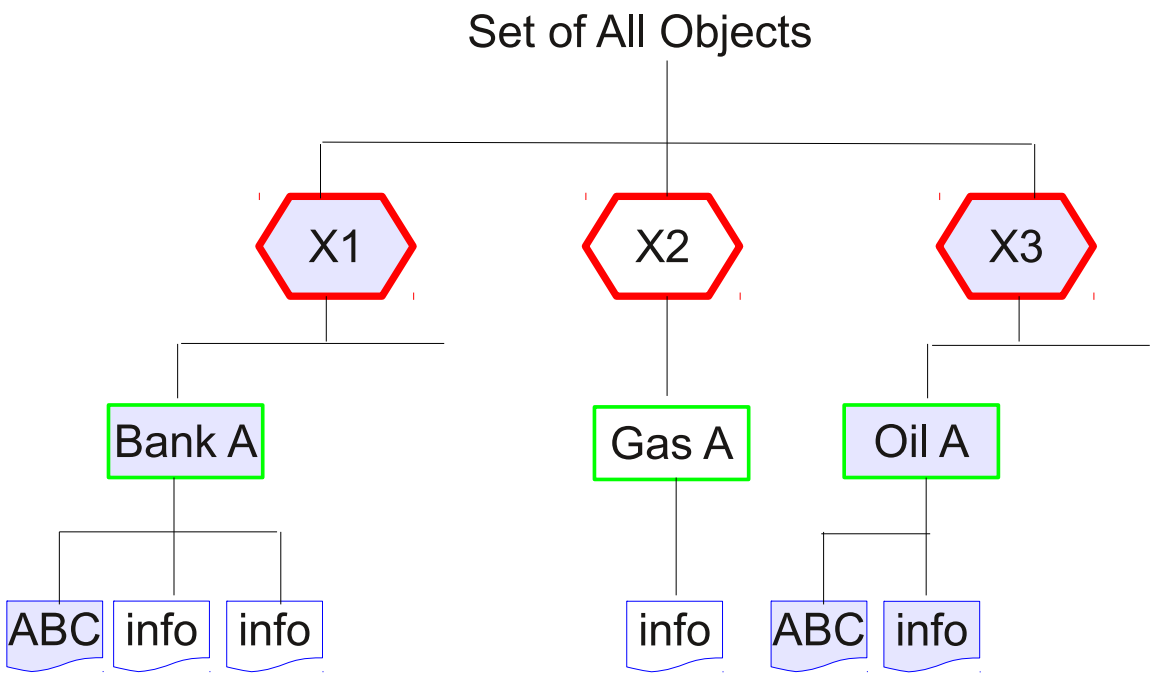
The Chinese wall model (1989)

Write rule

- The read rule does not prevent indirect flow of information
- Consider the following case:
  - S_1 has access to Bank A and Oil A
  - S_2 has access to Bank B and Oil A
- If S_1 is allowed to read Bank A and write into Oil A, it may transfer information about Bank A that can then be read by S_2

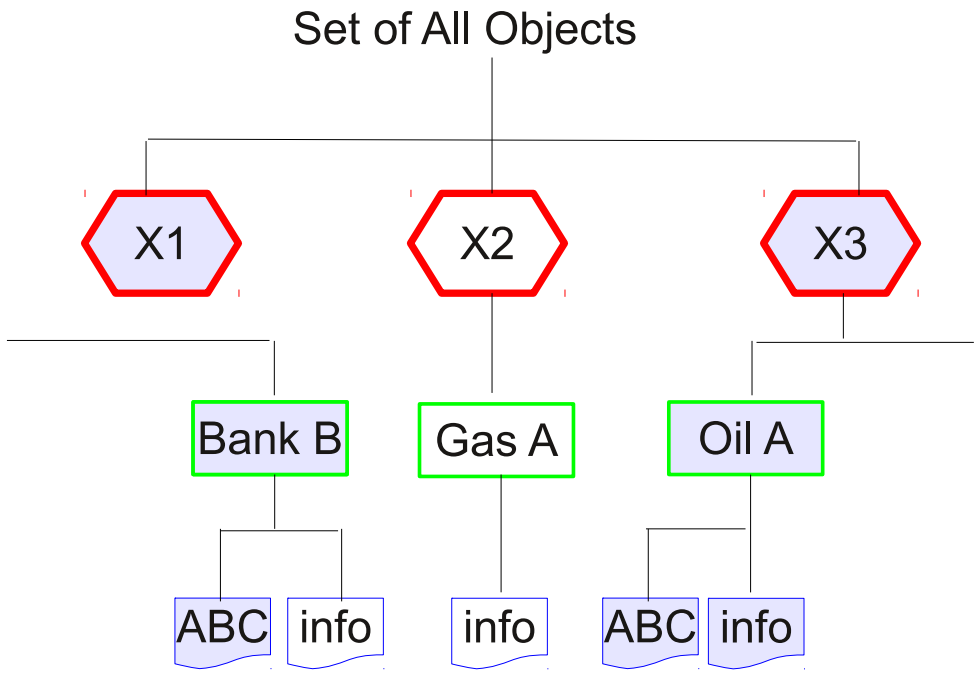
The Chinese wall model (1989)

Write rule: S_1



The Chinese wall model (1989)

Write rule: S_2

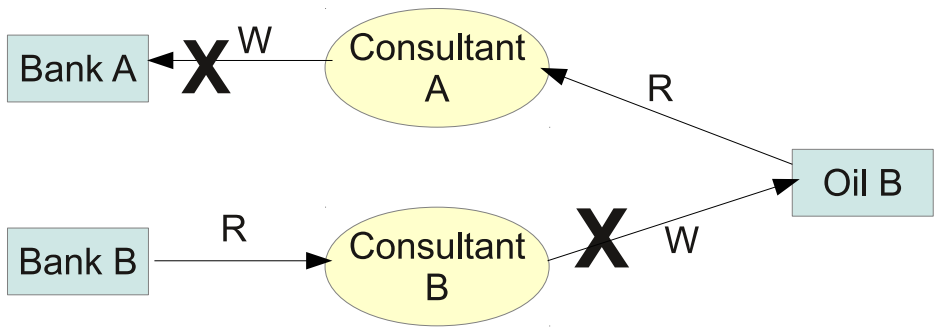


The Chinese wall model (1989)

Write rule

A subject s can write an object o if:

- s can read o according to the read rule AND
- No object has been read by s which is in a different company dataset to the one on which write is performed



The Chinese wall model (1989)

Remarks

- According to the write rule: the flow of information is confined to its own company dataset.
- The write rule is very restrictive:
  - a user that has read objects from more than one dataset is not able to write any object
  - the user can only read and write objects from a single dataset

Outline

Summary

This lecture: security models

- Multi-level security
- Information flow policies
- Formal security models: BLP, Biba, Chinese wall

Next week

- Security management