北京工業大學 软件学院
School of Software Engineering, Beijing University of Technology

Security and Privacy

Prof. Jingsha He
School of Software Engineering
Beijing University of Technology

Project 1 Demo

Place: Software Building 505-506
Time: 8:30-11:30, Friday, Sept. 27
Other times: by appointment

北京工業大學 软件学院
School of Software Engineering, Beijing University of Technology

Security Models and Policies

Reading Material

- Matt Bishop
  - Chapter 4
  - Chapter 5
  - Chapter 6
  - Chapter 7

Protection State

- State
  - Collection of the current values of all the cells of temporary and permanent storages in a system
- Formal description
  - P: all possible states
  - Q: a subset of secure states
  - Security policy
    - Determining the secure states in Q
  - Security mechanism
    - Enforcing the security policy to prevent a system from entering a state outside of Q, i.e., into P-Q

Access Control Matrix Model

- Model components
  - An access control matrix: M
  - A set of subjects: S
    - Active entities: users, processes, threads, etc.
  - A set of objects: O
    - Protected entities: registers, files, devices, processes, etc.
  - Access rights
    - read, write, execute, own
    - send, receive
    - increment, decrement, etc.
- Protection state
  - (S, O, M)

An Example of Access Control Matrix

	File	Device	Register	Process	Mary
John	Read	Control	Read Write	Own	Create
Henry	Write	Send	Read	Execute	
Alice	Execute	Receive	Reset	Stop Resume	Update
Bob	Own	Disable		Hold	Create Destroy

Protection States

- State transition
  - Initial state: $X_0 = (S_0, O_0, M_0)$
  - Operations: $\Pi_1, \Pi_2, \ldots$
  - $X_i \vdash_{\pi_{i+1}} X_{i+1}$
- State transitions
  - $X \vdash^* Y$
- Operations
  - Create subject, create object
  - Enter right, delete right, change right
  - Destroy subject, destroy object
  - ……

System Security

- Security policy
  - A statement that partitions the states of a system into a set of secure states and a set of insecure ones
- Secure system
  - A system that starts with a secure state and NEVER enters into an insecure state
- Violation of security
  - An event in which a system transits from a secure state into an insecure state

Types of Security Policies

- Confidentiality policy
  - A security policy that deals only with confidentiality
- Integrity policy
  - A security policy that deals only with integrity
- Availability policy
  - A security policy that deals only with availability
- In reality
  - Confidentiality policy ↔ military security policy
  - Integrity policy ↔ financial security policy

Policy Enforcement

- Standards
  - Uniform ways of using specific technologies, parameters or procedures
  - Generally very strict
- Guidelines
  - Assistance to the user in complying with a security policy
- Procedures
  - Measures of compliance
  - Very specific steps

Confidentiality Model

- Main concern
  - Unauthorized disclosure of information
- A.k.a information flow policy model
- The Bell-LaPadula Model
  - Modeled after the military-style classification of information and security control
  - Probably the most influential security model ever developed
    - For the development of other models
    - For the development of computer security technologies

Bell-LaPadula Model

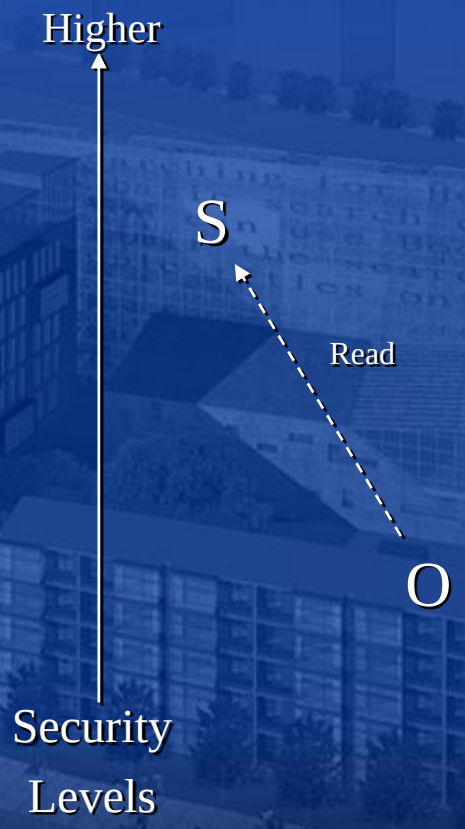
- Access control
  - Mandatory
    - Fixed policy enforced throughout the system
    - Access control policy CANNOT be changed at will
  - Discretionary
    - The access control matrix model
    - Access decisions are based on values in matrix entries
    - Access control policy CAN be changed, usually by the owner of the corresponding object or a super user of the system
- Sequence of policy enforcement
  - Mandatory
  - Discretionary

BLM: Mandatory Policy

- Confidentiality classification system
  - Top secret > secret > confidential > unclassified
- All the subjects and objects are mapped into the classification system and tagged with labels
  - Subject mapping: security clearance
    - John ← top secret
    - Bill ← confidential
  - Object mapping: security classification
    - Personal files ← top secret
    - Phone list files ← unclassified

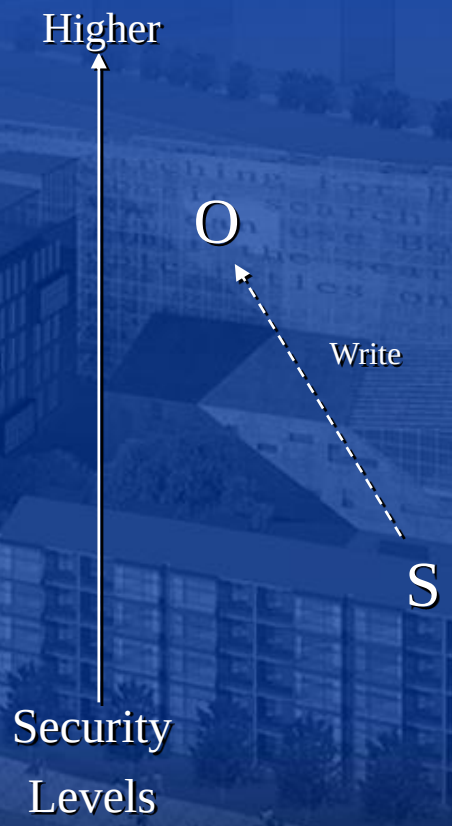
BLM: Properties

- L(S)
  - Security clearance of subject S
- L(O)
  - Security classification of object O
- Simple Security Condition (preliminary version)
  - S can READ (from) O if and only if
    - L(S) ≥ L(O)
    - Subject S has read access right to object O in discretionary access control



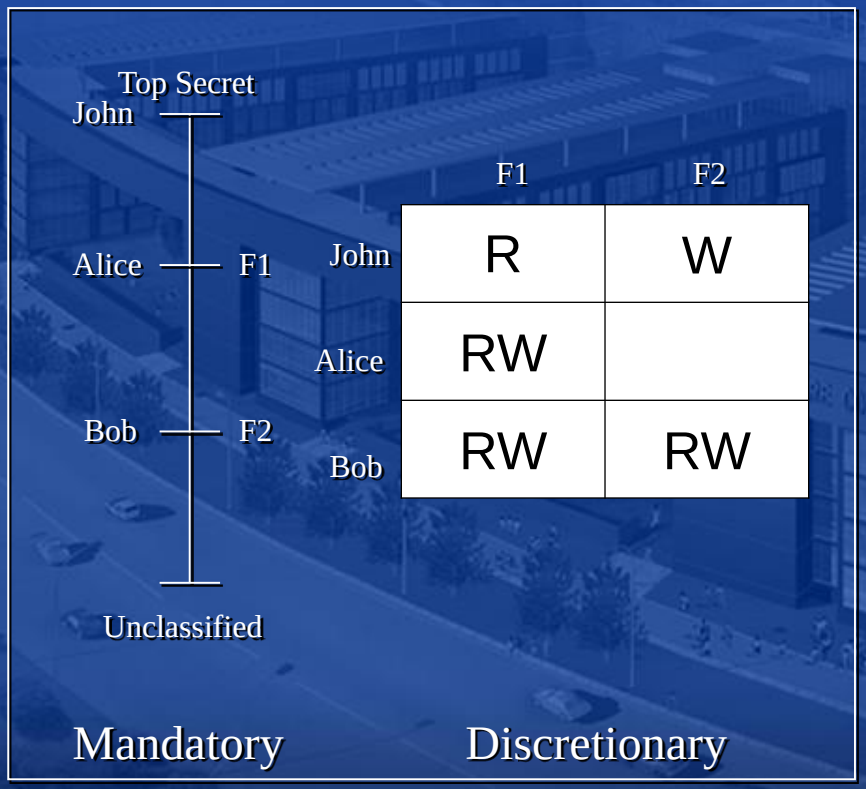
BLM: Properties

- *-Property (Star Property) (preliminary version)
  - S can WRITE (into) O if and only if
    - L(S) ≤ L(O)
    - Subject S has write access right to object O in discretionary access control
- Implication of enforcing the two properties
  - Information can only flow UPWARDS



BLM: Example

Access Control



- John reads from F1
  - SL(John) ≥ SL(F1) ⇒ True
  - R ∈ M[John, F1] ⇒ True
  - Access allowed
- John writes into F2
  - SL(John) ≤ SL(F2) ⇒ False
  - Access denied
- Alice reads from F2
  - SL(Alice) ≥ SL(F2) ⇒ True
  - R ∈ M[Alice, F2] ⇒ False
  - Access denied
- Alice writes into F2
  - SL(Alice) ≤ SL(F2) ⇒ False
  - Access denied
- Bob reads from F1
  - SL(Bob) ≥ SL(F1) ⇒ False
  - Access denied

BLM: Theorem, PV

- Basic security theorem, preliminary version
  - Let Σ be a system with a secure initial state s_0
  - Let T be a set of state transitions
  - If every element of T preserves both the simple security condition (preliminary version) and the *-property (preliminary version)
    - Then every state s_i ($i \geq 0$) is secure
- Proof by contradiction

BLM: Categories

- The “need-to-know” principle
  - No subject should be allowed to access an object unless it is necessary
- Category
  - A set of elements to describe category
  - Example: {Asia, Europe, America, Africa}
- Set of categories
  - A power set of the set of elements
  - Example: set of elements {Asia, Europe, America, Africa}

    Set of categories {},

    {Asia}, {Europe}, {America}, {Africa},

    {Asia, Europe}, {Asia, America}, {Asia, Africa}, {Europe, America},

    {Europe, Africa}, {America, Africa},

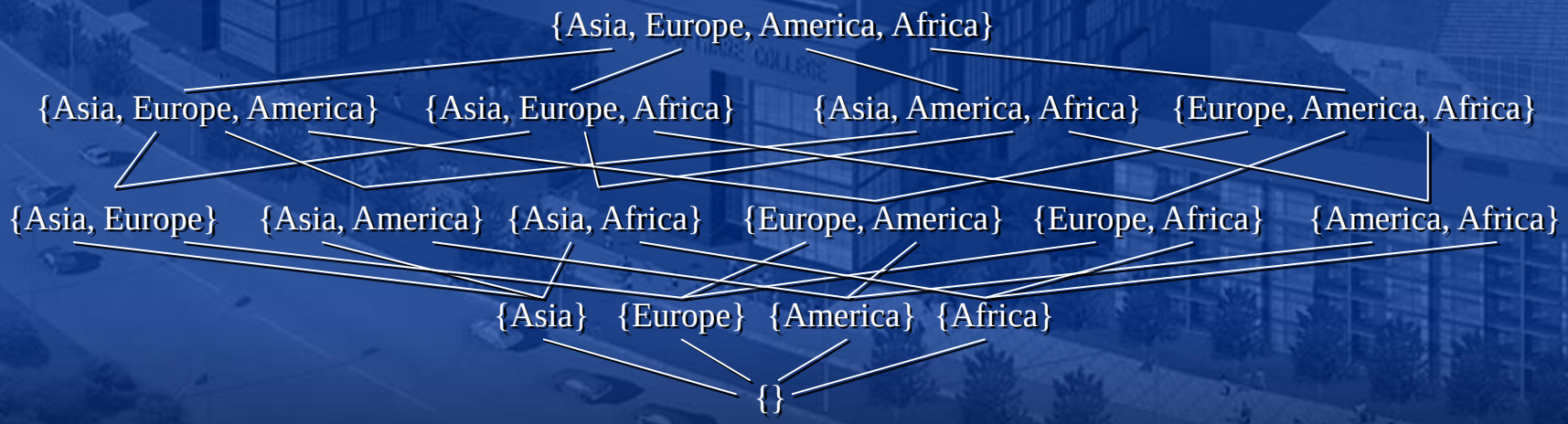
    {Asia, Europe, America}, {Asia, Europe, Africa},

    {Asia, America, Africa}, {Europe, America, Africa},

    {Asia, Europe, America, Africa}

BLM: Lattice

- Lattice
  - Formed for a set of categories under the operation $\subseteq$ (subset of)



BLM: General Model

- Augment the security clearance and security classification with a set of categories
  - Security level
    - For subject: security clearance L(S) + category C
    - For object: security classification L(O) + category C
- Security level SL=(L, C) dominates security level SL'=(L', C') if and only if L'≤L and C'⊆C
  - Denoted as SL dom SL'

BLM: General Properties

- Simple security condition
  - Subject S can READ (from) object O if and only if
    - SL(S) dom SL(O)
    - S has read access right to O in discretionary access control
- *-property
  - Subject S can WRITE (into) object O if and only if
    - SL(O) dom SL(S)
    - S has write access right to O in discretionary access control
- Implication
  - Information can only flow UPWARDS

BLM: Theorem

- Basic security theorem
  - Let Σ be a system with a secure initial state s_0
  - Let T be a set of state transitions
  - If every element of T preserves both the simple security condition and the *-property
  - Then every state s_i ($i \geq 0$) is secure
- Proof by contradiction

BLM: Significance

- First mathematical model for computer security
- Basis for several standards
  - The “Orange Book”
    - Department of Defense Trusted Computer System Evaluation Criteria
- Very successful piece of work
  - However, controversy

Integrity Model

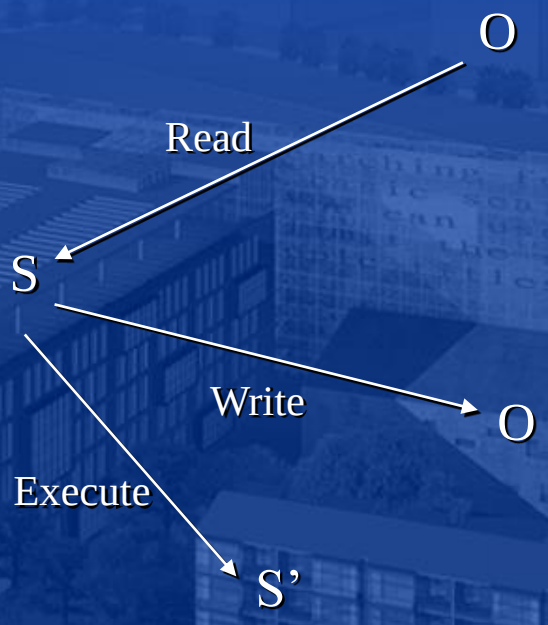
- Main concern
  - Unauthorized modification of information
- The Biba integrity model
  - A mathematical dual to the Bell-LaPadula model
  - Model elements
    - S: a set of subjects
    - O: a set of objects
    - I: a set of integrity levels, totally ordered
  - Intuition
    - The higher the integrity level is, the higher the confidence or trust that one can have on the content of a file (an object) or on the correct execution of a program (a subject)

The Biba Integrity Model

- Low-water-mark policy
  - If $s \in S$ reads from $o \in O$, then $i(s) = \min(i(o), i(s))$
    - To reflect information pollution
  - $s \in S$ can write into $o \in O$ if and only if $i(s) \geq i(o)$
    - To prevent information from being upgraded
  - $s \in S$ can execute $s' \in S$ if and only if $i(s) \geq i(s')$
    - To prevent a less trustworthy process from executing and controlling a more trustworthy one

The Biba Integrity Model

- Strict integrity policy
  - s∈S can read from o∈O if and only if i(s) ≤ i(o)
  - s∈S can write into o∈O if and only if i(s) ≥ i(o)
  - s∈S can execute s'∈S if and only if i(s) ≥ i(s')
- Focus
  - Trustworthiness



Other Models

- Lipner's integrity matrix model
  - Combination of the Bell-LaPadula and the Biba models
  - Modeled more closely to a particular commercial policy
- Clark-Wilson integrity model
  - Radically different from previous models
  - Focus of the model
    - Consistency of data
    - Integrity of transaction

Availability Model

- Model?
  - More difficult
  - Wide range of attacks
    - Numerous ways of making information unavailable
  - Low probability of providing effective protection
- Research directions
  - Intrusion detection
  - Counter-measures to denial of service attacks
  - Prediction models and pro-active methods

Hybrid Policies: The Chinese Wall Model

- Aimed at avoiding conflict of interest
  - Applicable primarily for access to information that belongs to competitors
- Definitions
  - CD: company dataset
  - COI: conflict of interest class
    - Companies that are competitors
  - PR(S): set of objects that subject S has previously read

Hybrid Policies: The Chinese Wall Model

- Control policies
  - CW-Simple Security Condition, PV
    - S can read from O if and only if either of the following conditions holds
      - ∃O' such that S has accessed O' and CD(O')=CD(O)
      - For every O', O'∈PR(S) ⇒ COI(O')≠COI(O)
  - CW-Simple Security Condition
    - S can read from O if and only if any one of the following conditions holds
      - ∃O' such that S has accessed O' and CD(O')=CD(O)
      - For every O', O'∈PR(S) ⇒ COI(O')≠COI(O)
      - O is a sanitized object

Hybrid Policies: The Chinese Wall Model

- Control policies
  - CW-*-Property
    - S can write into O if and only if both of the following conditions hold
      - The CW-Simple Security Condition permits S to read O
      - For all un-sanitized objects O', S can read O' ⇒ CD(O')=CD(O)

Clinical Information Systems Security Policy

- Aimed at providing both confidentiality and integrity
  - Applicable primarily to healthcare services
- Roles and definitions
  - Patient
    - Subject of medical records
  - Medical record
    - Personal health information
  - Clinician
    - Subject who performs access to patient's medical records

Clinical Information Systems Security Policy

- Control policies
  - 4 access principles
  - 1 creation principle
  - 1 deletion principle
  - 1 confinement principle
    - Concatenation of medical records
  - 1 aggregation principle
    - Addition of a subject into the access control list
  - 1 enforcement principle

Originator Controlled Access Control

- Aimed at enabling organizations to control the disclosure of information
- Control policies
  - A subject $s \in S$ marks an object $o \in O$ as ORCON on behalf of an organization
  - The organization would allow o to be disclosed to a subject with the following restrictions
    - Object o cannot be disclosed to any subject without the permission of the organization
    - All copies of o must have the same restrictions on them

Role-Based Access Control

- Aimed at basing access control decisions on one's job functions (or roles) for performing tasks
- Definitions
  - Role: a collection of job functions
  - actr(s): active role that subject s is currently assuming
  - authr(s): set of roles that subject s is authorized to assume
  - canexec(s, t)=true if and only if subject s can execute transaction t at the current time
  - meauth(r): set of roles that subject s cannot assume because r∈authr(s)

Role-Based Access Control

- Control policies
  - Axiom: role assignment rule
    - $(\forall s \in S)(\forall t \in T)\ [canexec(s,t) \rightarrow actr(s) \neq \emptyset]$
  - Axiom: role authorization rule
    - $(\forall s \in S)\ [actr(s) \subseteq authr(s)]$
  - Axiom: transaction authorization rule
    - $(\forall s \in S)(\forall t \in T)\ [canexec(s,t) \rightarrow t \in trans(actr(s))]$
  - Axiom: separation of duty rule
    - $(\forall r_1, r_2 \in R)\ [r_2 \in meauthr(r_1) \rightarrow [(\forall s \in S)\ [r_1 \in authr(s) \rightarrow r_2 \notin authr(s)]]]$

Summary

- General models
  - Access control matrix model
  - Confidentiality: the Bell-LaPadula model
  - Integrity: the Biba integrity model
  - Availability: ?
- Hybrid models
  - The Chinese wall model
  - The clinical information system security model
  - The originator controlled access control model
  - The role based access control model

Q & A