


Confidentiality Policy

Goals of Confidentiality Policies

- ▶ Confidentiality Policies emphasize the protection of confidentiality.
 - ▶ Confidentiality policy also called **information flow** policy, prevents unauthorized disclosure of information.
 - ▶ Example: Privacy Act requires that certain personal data be kept confidential. E.g., income tax return info only available to IRS and legal authority with court order. It limits the distribution of documents/info.
- 

Discretionary Access Control (DAC)

- ▶ Definition : Mechanism where a user can set access control to allow or deny access to an object
- ▶ Also called Identity-based access control (IBAC) Section 4.4.
- ▶ It is a traditional access control techniques implemented by traditional operating system such as Unix.
 - Based on user identity and ownership
 - Programs run by a user inherits all privileges granted to the user.
 - Programs is free to change access to the user's objects
 - Support only two major categories of users:
 - Completely trusted admins
 - Completely untrusted ordinary users

Problems with DAC

- ▶ Each user has complete discretion over his objects.
 - What is wrong with that?
 - Difficult to enforce a system-wide security policy, e.g.
 - A user can leak classified documents to an unclassified user.
 - Other examples?
- ▶ Only based on user's identity and ownership, ignoring security-relevant info such as
 - User's role
 - Function of the program
 - Trustworthiness of the program
 - Compromised program can change access to the user's objects
 - Compromised program inherits all the permissions granted to the users (especially the root user)
 - Sensitivity of the data
 - Integrity of the data
- ▶ Only support coarse-grained privileges
- ▶ Unbounded privilege escalation
- ▶ Too simple classification of users (How about more than two categories of users?)

Mandatory Access Control (MAC)

- ▶ Definition 4-14: Mechanism where system control access to an object and a user cannot alter that access.
- ▶ Occasionally called rule-based access control?
- ▶ Defined by three major properties:
 - Administratively-defined security policy
 - Control over all subjects (process) and objects (files, sockets, network interfaces)
 - Decisions based on all security-relevant info
- ▶ MAC access decisions are based on labels that contains security-relevant info.

What Can MAC Offer?

- ▶ Supports a wide variety of categories of users in system.
 - For example, Users with labels: (secret, {EUR, US}) (top secret, {NUC, US}).
 - Here security level is specified by the two-tuple: (clearance, category)
- ▶ Strong separation of security domains
- ▶ System, application, and data integrity
- ▶ Ability to limit program privileges
 - Confine the damage caused by flawed or malicious software
- ▶ Processing pipeline guarantees
- ▶ Authorization limits for legitimate users

Mandatory and Discretionary Access Control

- ▶ Bell-LaPadula model combines Mandatory and Discretionary Access Controls.
- ▶ “S has discretionary read (write) access to O”
means that the access control matrix entry for S and O corresponding to the discretionary access control component contains a read (write) right.

| | A | B | C | D | O |
|---|---|---|---|---|---------|
| Q | | | | | |
| S | | | | | read(D) |
| T | | | | | |

- ▶ If the mandatory controls not present, S would be able to read (write) O.

Bell-LaPadula Model

- ▶ Also called the multi-level model,
- ▶ Was proposed by Bell and LaPadula of MITRE for enforcing access control in government and military applications.
- ▶ It corresponds to military-style classifications.
- ▶ In such applications, **subjects and objects are often partitioned into different security levels.**
- ▶ A subject can only access objects at certain levels determined by his security level.
- ▶ For instance, the following are two typical access specifications:
``Unclassified personnel cannot read data at confidential levels" and
``Top-Secret data cannot be written into the files at unclassified levels"

Informal Description

- ▶ Simplest type of confidentiality classification is a set of security clearances arranged in a linear (total) ordering.
- ▶ Clearances represent the security levels.
- ▶ The higher the clearance, the more sensitive the info.
- ▶ Basic confidential classification system:

| | <i>individuals</i> | <i>documents</i> |
|-------------------|--------------------|--------------------|
| Top Secret (TS) | Tamara, Thomas | Personnel Files |
| Secret (S) | Sally, Samuel | Electronic Mails |
| Confidential (C) | Claire, Clarence | Activity Log Files |
| Unclassified (UC) | Ulaley, Ursula | Telephone Lists |

Star Property (Preliminary Version)

- ▶ Let $L(S)=l_s$ be the security clearance of subject S.
- ▶ Let $L(O)=l_o$ be the security classification of object.
- ▶ For all security classification l_i , $i=0, \dots, k-1$, $l_i < l_{i+1}$
- ▶ **Simple Security Condition:**
S can read O if and only if $l_o \leq l_s$ and
S has discretionary read access to O.
- ▶ ***-Property (Star property):**
S can write O if and only if $l_s \leq l_o$ and
S has discretionary write access to O.
- ▶ TS guy can not write documents lower than TS. → Prevent
classified information leak.
- ▶ But how can different groups communicate?

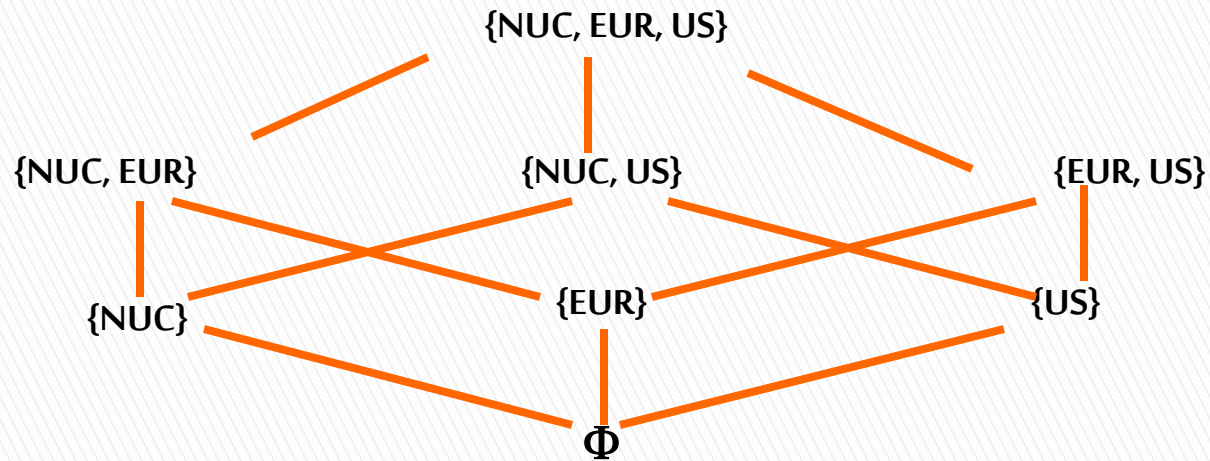
Basic Security Theorem

- ▶ Let Σ be a system with secure initial state σ_0
- ▶ Let T be the set of state transformations.
- ▶ If every element of T preserves the **simple security condition**, preliminary version, and the ***-property**, preliminary version,
Then every state $\sigma_i, i \geq 0$, is secure.

Categories and Need to Know Principle

- ▶ Expand the model by adding a set of categories.
- ▶ Each category describe a kind of information.
- ▶ These category arise from the “need to know” principle → no subject should be able to read objects unless reading them is necessary for that subject to perform its function.
- ▶ Example: three categories: NUC, EUR, US.
- ▶ Each security level and category form a *security compartment*.
- ▶ Subjects *have clearance at* (are cleared into, or are in) a security level.
- ▶ Objects are *at the level of* (or are in) a security level.

Security Lattice



- ▶ William may be cleared into level (SECRET, {EUR})
- ▶ George into level (TS, {NUC, US}).
- ▶ A document may be classified as (C, {EUR})
- ▶ Someone with clearance at (TS, {NUC, US}) will be denied access to document with category EUR.

Dominate (dom) Relation

- ▶ The security level (L, C) dominates the security level (L', C') if and only if $L' \leq L$ and $C' \subseteq C$
- ▶ $\neg \text{Dom} \rightarrow$ dominate relation is false.
- ▶ George is cleared into security level $(S, \{\text{NUC}, \text{EUR}\})$
- ▶ DocA is classified as $(C, \{\text{NUC}\})$
- ▶ DocB is classified as $(S, \{\text{EUR}, \text{US}\})$
- ▶ DocC is classified as $(S, \{\text{EUR}\})$
- ▶ George dom DocA
- ▶ George \neg dom DocB
- ▶ George dom DocC

New Security Condition and *-Property

- ▶ Let $C(S)$ be the category set of subject S .
- ▶ Let $C(O)$ be the category set of object O .
- ▶ **Simple Security Condition** (**not read up**):
 S can read O if and only if $S \text{ dom } O$ and S has discretionary read access to O .
- ▶ ***-Property** (**not write down**):
 S can write to O if and only if $O \text{ dom } S$ and S has discretionary write access to O .
- ▶ **Basic Security Theorem:**
Let Σ be a system with secure initial state σ_0
Let T be the set of state transformations.
If every element of T preserves the simple security condition, preliminary version, and the *-property, preliminary version,
Then every state $\sigma_i, i \geq 0$, is secure.

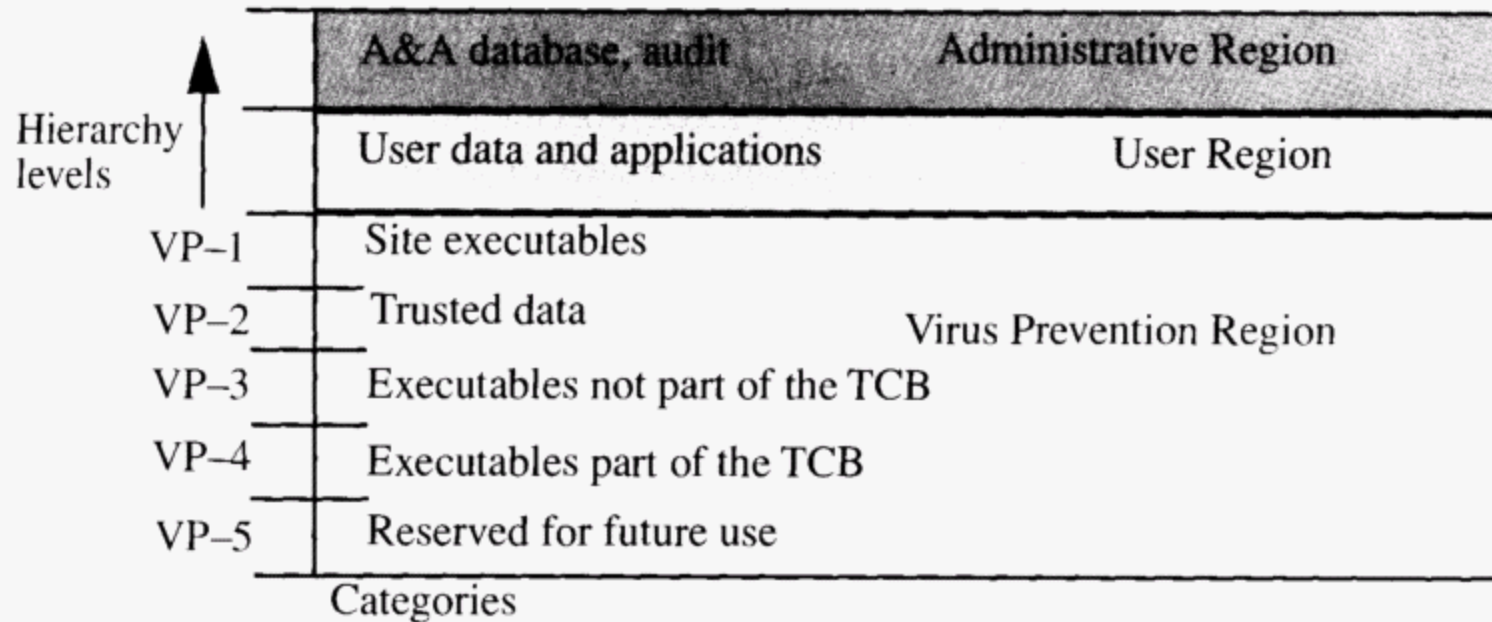
Allow Write Down?

- ▶ Bell-LaPadula allows higher-level subject to write into lower level object that low level subject can read.
- ▶ A subject has a maximum security level and a current security level. maximum security level must dominate current security level.
- ▶ A subject may (effectively) **decrease its security level** from the maximum in order to communicate with entities at lower security levels.
- ▶ Colonel's maximum security level is $(S, \{NUC, EUR\})$. She changes her current security level to $(S, \{EUR\})$. Now she can create document at Major is clearance level $(S, \{EUR\})$.

Data General B2 Unix System

- ▶ Data General B2 Unix (DG/UX) provides mandatory access controls (MAC).
- ▶ The MAC label is a label identifying a particular compartment.
- ▶ The initial label (assigned at login time) is the label assigned to the user in a database called Authorization and Authentication (A&A) Database.
- ▶ When a process begins, it is assigned to MAC label of its parent (whoever creates it).
- ▶ Objects are assigned labels at creation. The labels can be explicit or implicit.
- ▶ The explicit label is stored as parts of the object's attributes.
- ▶ The implicit label derives from the parent directory of the object.
- ▶ IMPL_HI: the least upper bound of all components in DG/UX lattice has IMPL_HI as label.
- ▶ IMPL_LO: the greatest lower bound of all components in DG/UX lattice has IMPL_LO as the label

Three MAC Regions in DG/UX MAC Lattice



Accesses with MAC Labels

- Read up and write up from users to Admin Region not allowed.
- Admin processes sanitize data sent to user processes with MAC Labels in the user region.
- System programs are in the lowest region.
- No user can write to or alter them.
- Only programs with the same label as the directory can create files in that directory.
- The above restriction will prevent
 - compiling (need to access /tmp)
 - mail delivery (need to access mail spool directory)
- Solution → ***multilevel directory***.

Multilevel Directory

- ▶ A directory with a set of subdirectories, one for each label.
- ▶ These hidden directories normally invisible to the user.
- ▶ When a process with label MAC_A creates a file in /tmp, it actually create a file in hidden directory under /tmp with label MAC_A
- ▶ The parent directory of a file in /tmp is the hidden directory.
- ▶ A reference to the parent directory goes to the hidden directory.

Enable Flexible Write in DG/UX

- ▶ Provide a range of labels called MAC tuple.
- ▶ *A range* is a set of labels expressed by *a lower bound* and an *upper bound*. A MAC tuple consists of up to three ranges
- ▶ Example: A system has two security levels. TS and S, the former dominating the latter. The categories are COMP, NUC, and ASIA.
- ▶ Examples of ranges are:
 - ▶ $[(S, \{ \text{COMP} \}), (TS, \{ \text{COMP} \})]$
 - ▶ $[(S, \Phi), (TS, \{ \text{COMP}, \text{NUC}, \text{ASIA} \})]$
 - ▶ $[(S, \{ \text{ASIA} \}), (TS, \{ \text{ASIA}, \text{NUC} \})]$