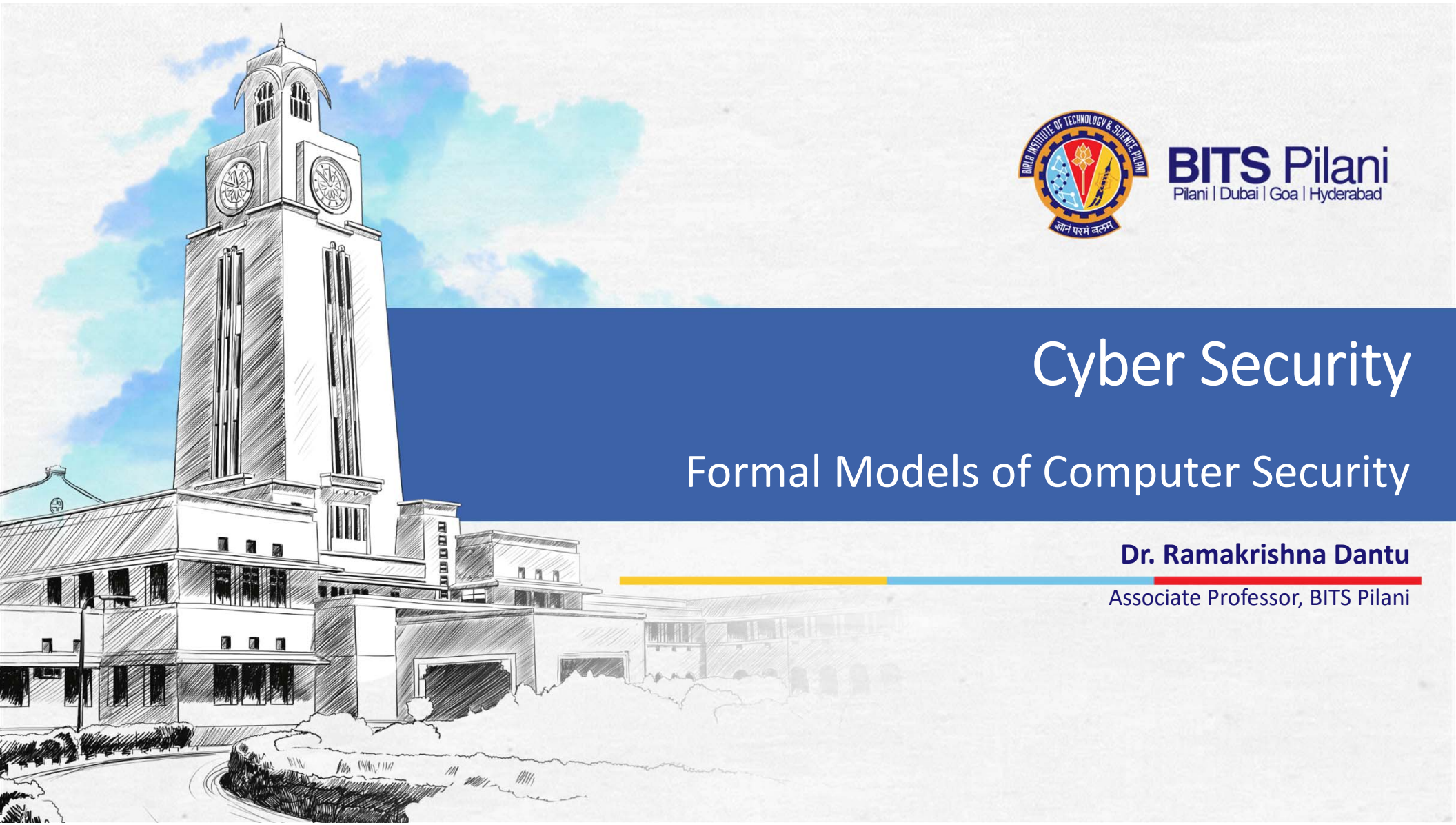


BITS Pilani
Pilani | Dubai | Goa | Hyderabad

Cyber Security

Formal Models of Computer Security

Dr. Ramakrishna Dantu
Associate Professor, BITS Pilani

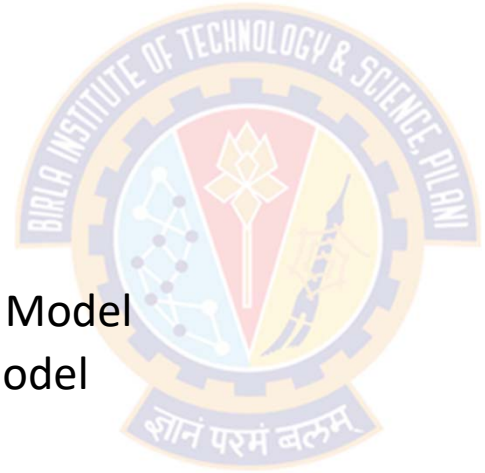
Disclaimer and Acknowledgement

- The content for these slides has been obtained from books and various other source on the Internet
- I here by acknowledge all the contributors for their material and inputs.
- I have provided source information wherever necessary
- I have added and modified the content to suit the requirements of the course

Formal Models of Computer Security

Agenda

- The CIA Classification:
  - Confidentiality Policies:
    - Bell-LaPadula Model
  - Integrity Policies:
    - The Biba Model
    - Lipner's Integrity Matrix Model
    - Clark-Wilson Integrity Model
    - Trust Models
  - Availability Policies:
    - Deadlock
    - Denial of Service Models



Confidentiality Policies

Overview

- A confidentiality policy, also called an information flow policy
- Goal: prevent the unauthorized disclosure of information
  - Deals with the flow of information
  - Unauthorized alteration (integrity) of information is secondary
- Multi-level security models are best-known examples
  - Bell-LaPadula Model basis for many, or most, of these
- Example
  - In the United States, the Privacy Act requires that certain personal data be kept confidential
  - Income tax returns are legally confidential and are available only to the Internal Revenue Service or to legal authorities with a court order
  - Governmental models represent the policies that satisfy these requirements

Bell LaPadula Model

Bell LaPadula Model

Overview

- David Bell and Leonard LaPadula first described the DoD multilevel military security policy in 1973 in abstract, formal mathematical terms
- Each subject and each object is assigned a security class
- Security classes form a strict hierarchy and are referred to as security levels
- Example: The U.S. military classification scheme:
  - top secret > secret > confidential > restricted > unclassified
- Example: Commercial classification scheme
  - strategic > sensitive > confidential > public

Bell LaPadula Model

Overview

- A subject is said to have a security clearance of a given level
- An object is said to have a security classification of a given level
- The security classes control the manner by which a subject may access an object
- The model defined four access modes:
  - read: The subject is allowed only read access to the object
  - append: The subject is allowed only write access to the object
  - write: The subject is allowed both read and write access to the object.
  - execute: The subject is allowed neither read nor write access to the object but may invoke the object for execution
- Authors pointed out that in specific implementation environments, a different set of modes might be used

Bell LaPadula Model

innovate achieve lead

Multilevel Security (MLS)

- When multiple categories or levels of data are defined, the requirement is referred to as multilevel security (MLS)
- Confidentiality-centered multilevel security states that
  - "a subject at a high level may not convey information to a subject at a lower level unless that flow accurately reflects the will of an authorized user as revealed by an authorized declassification"
- A multilevel secure system for confidentiality must enforce the following:
  - No read up: A subject can only read an object of less or equal security level
    - This is referred to as simple security property (ss-property).
  - No write down: A subject can only write into an object of greater or equal security level
    - This is referred to as the *-property (star property)

Bell LaPadula Model

innovate achieve lead

Multilevel Security (MLS) - Reading Information

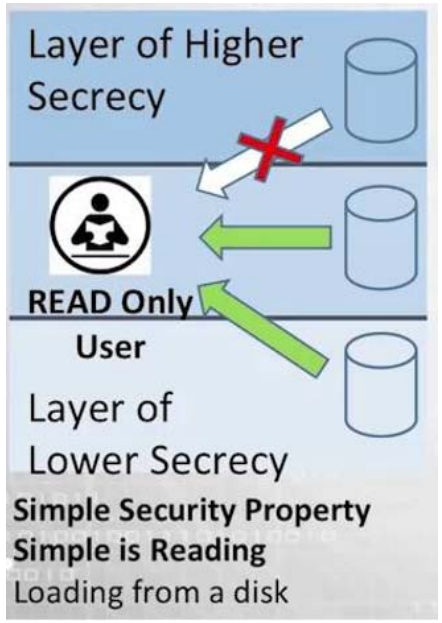
- The Bell-LaPadula security model combines mandatory and discretionary access controls
- Levels consist are:
  - *Security clearance L(s)* for subjects
    - A subject is said to have a security clearance of a given level
  - *Security classification L(o)* for objects
    - An object is said to have a security classification of a given level
- A subject's (E.g., a user) access to an object (E.g., a file) is allowed or disallowed by
  - comparing the object's security classification with the subject's security clearance
- S can read O if and only if L(o) ≤ L(s) and S has discretionary read access to O
  - This is called Simple Security Condition
- BLP model uses mathematical notation and set theory to define the concepts of:
  - a secure state, the modes of access, and the rules for granting access

Bell LaPadula Model

innovate achieve lead

Multilevel Security (MLS) - Reading Information

- Information flows up, not down
  - "Reads up" disallowed, "reads down" allowed
- Simple Security Condition
  - A subject may only read an object if she has a clearance level equal to or greater than the security level of the file
  - Subject s can read object o iff, $L(o) \leq L(s)$ and s has permission to read o
    - Note: combines mandatory control (relationship of security levels) and discretionary control (the required permission)
  - Sometimes called "no reads up" rule

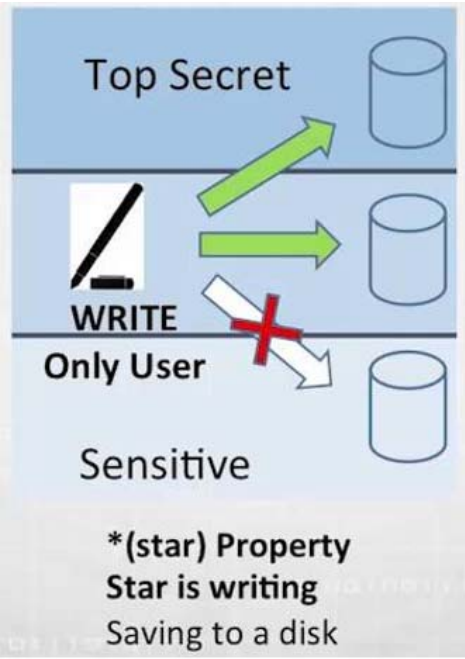


Bell LaPadula Model

innovate achieve lead

Multilevel Security (MLS) - Writing Information

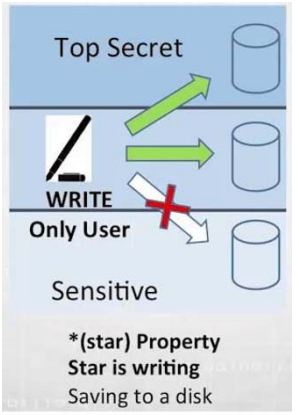
- Information flows up, not down
  - "Writes up" allowed, "writes down" disallowed
- *-Property
  - A subject is allowed write access to an object (a file) only if the security level of the object is greater than or equal to the clearance level of the subject
  - Subject s can write object o iff $L(s) \leq L(o)$ and s has permission to write o
    - Note: combines mandatory control (relationship of security levels) and discretionary control (the required permission)
  - Sometimes called "no writes down" rule

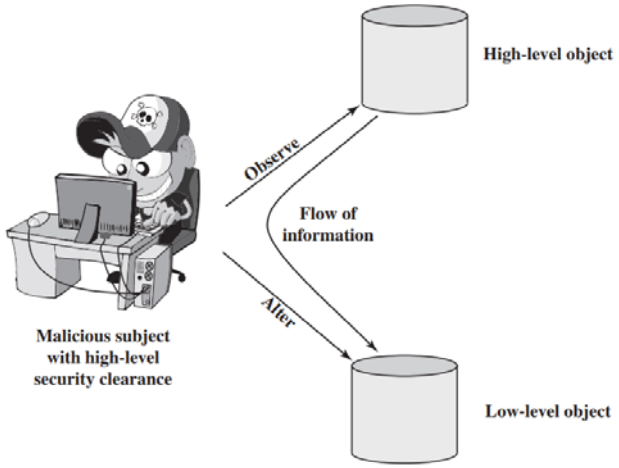


Bell LaPadula Model

What is the need for the *-property?

- Here, a malicious subject passes classified information along by putting it into an information container labeled at a lower security classification than the information itself
- This will allow a subsequent read access to this information by a subject at the lower clearance l





Bell LaPadula Model

innovate achieve lead

Multilevel Security (MLS) - Example

- Confidentiality classification consists of a set of security clearances arranged in a linear ordering
- These clearances represent sensitivity levels
- The higher the security clearance, the more sensitive the information (and the greater the need to keep it confidential)

Security Level	Subject	Object
TOP SECRET (TS)	Tamara, Thomas	Personnel Files
SECRET (S)	Sally, Samuel	Electronic Mail Files
CONFIDENTIAL (C)	Claire, Clarence	Activity Log Files
UNCLASSIFIED (UC)	Ulaley, Ursula	Telephone List Files

- A subject has a security clearance
  - E.g., Claire's security clearance is C (for CONFIDENTIAL), and Thomas's is TS (for TOP SECRET)
- An object has a security classification
  - E.g., the security classification of the electronic mail les is S (for SECRET), and that of the telephone list les is UC (for UNCLASSIFIED)
- Bell-LaPadula security model prevents information flowing from objects at a security classification higher than a subject's clearance to that subject

Bell LaPadula Model

Multilevel Security (MLS) - Example

- Claire and Clarence cannot read personnel files
- Tamara and Sally can read the activity log files
- In fact, Tamara can read any of the files, given her clearance, assuming that the discretionary access controls allow it
- If Tamara does the following, Claire could read the personnel files
  - copy the contents of the personnel files into activity log files and
  - set the discretionary access permissions
- Thus, for all practical purposes, Claire could read the files at a higher level of security
- How can we prevent this?

Security Level	Subject	Object
TOP SECRET (TS)	Tamara, Thomas	Personnel Files
SECRET (S)	Sally, Samuel	Electronic Mail Files
CONFIDENTIAL (C)	Claire, Clarence	Activity Log Files
UNCLASSIFIED (UC)	Ulaley, Ursula	Telephone List Files

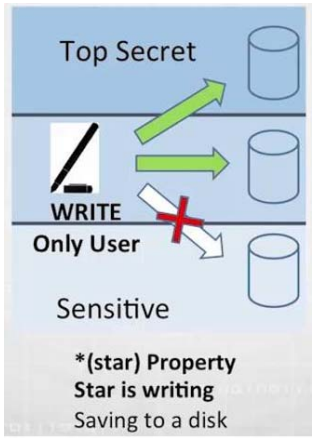
Bell LaPadula Model

innovate achieve lead

Multilevel Security (MLS) - Example

- *-Property (Star Property) can prevent the above situation
- S can write O if and only if L(o) ≥ L(s) and S has discretionary write access to O
- Because the activity log files are classified C and Tamara has a clearance of TS, she cannot write to the activity log files
- If both the simple security condition and the *-property hold, we call the system a secure system
- *Basic Security Theorem:*
  - Let S be a system with a secure initial state s_0, and let T be a set of state transformations
  - If every element of T preserves the simple security condition, and the *-property, then every state s_i, i ≥ 0, is secure

Security Level	Subject	Object
TOP SECRET (TS)	Tamara, Thomas	Personnel Files
SECRET (S)	Sally, Samuel	Electronic Mail Files
CONFIDENTIAL (C)	Claire, Clarence	Activity Log Files
UNCLASSIFIED (UC)	Ulaley, Ursula	Telephone List Files



Bell LaPadula Model

innovate achieve lead

Three Basic Rules

1) The *-property (star property)
2) The simple security condition
3) The tranquility property

- The first two properties provide the confidentiality form of what is known as mandatory access control (MAC)
- Under this MAC, no access is allowed that does not satisfy these two properties
- In addition, the BLP model makes a provision for discretionary access control (DAC)
- An individual (or role) may grant to another individual (or role) access to a document based on the owner's discretion, constrained by the MAC rules
- Thus, a subject can exercise only accesses for which it has the necessary authorization and which satisfy the MAC rules

Bell LaPadula Model

innovate achieve lead

Three Basic Rules

- The *-property (star property)
  - This makes it impossible for data from a highly cleared subject to become available to users with a lower security clearance in an object (file/directory) with a low security level
  - Without this rule, a user with a high security clearance could copy sensitive data into a low security clearance document—thus allowing "confidential" data to be written down, or to flow from a "top secret" to an "unclassified" level

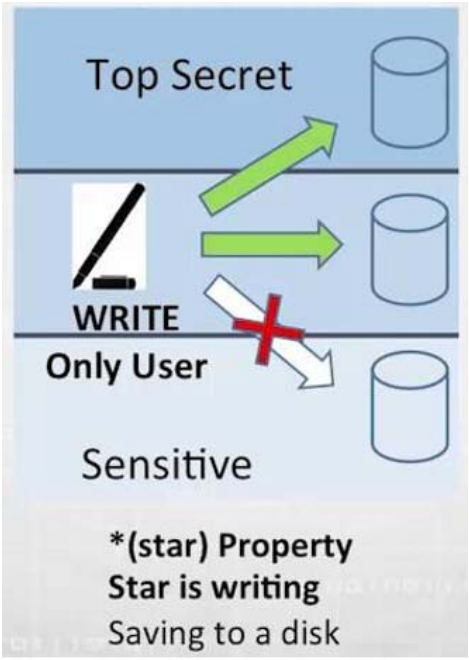


Image Source: Skillset.com

Bell LaPadula Model

innovate achieve lead

Three Basic Rules

- The simple security condition (Step-1)
  - someone with a "secret" security level cannot read a file with a "top secret" security level, but can read a file with a "secret" or "confidential" security level
- The tranquility property
  - It states that the security level of an object cannot be changed while it is being processed by a computer system
  - This keeps a program or attack from modifying the sensitivity of a file while it is open and vulnerable

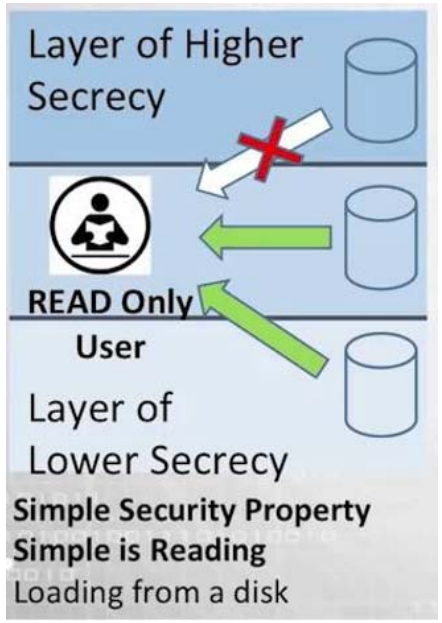


Image Source: Skillset.com

Bell LaPadula Model

innovate achieve lead

Extension

- Why Extension is needed?
  - Since all information is not meant for all people, we need to classify the information also into categories
  - Categories also known as compartments
- Typical military security categories
  - Nuclear Defense (abbreviated: NUC)
  - European Politics (EUR)
  - US Governmental issues (US)
  - army, navy, air force
  - nato, nasa, noforn
- Typical commercial security categories
  - Sales, , R&D, HR
  - Dept A, Dept B, Dept C
- But how these categories can go with security classification levels:
  - Top Secret (TS), Secret (S), Confidential (c) and Unclassified (UC)

Bell LaPadula Model

innovate achieve lead

Attaching Category with i) User and ii) Info. Security Levels

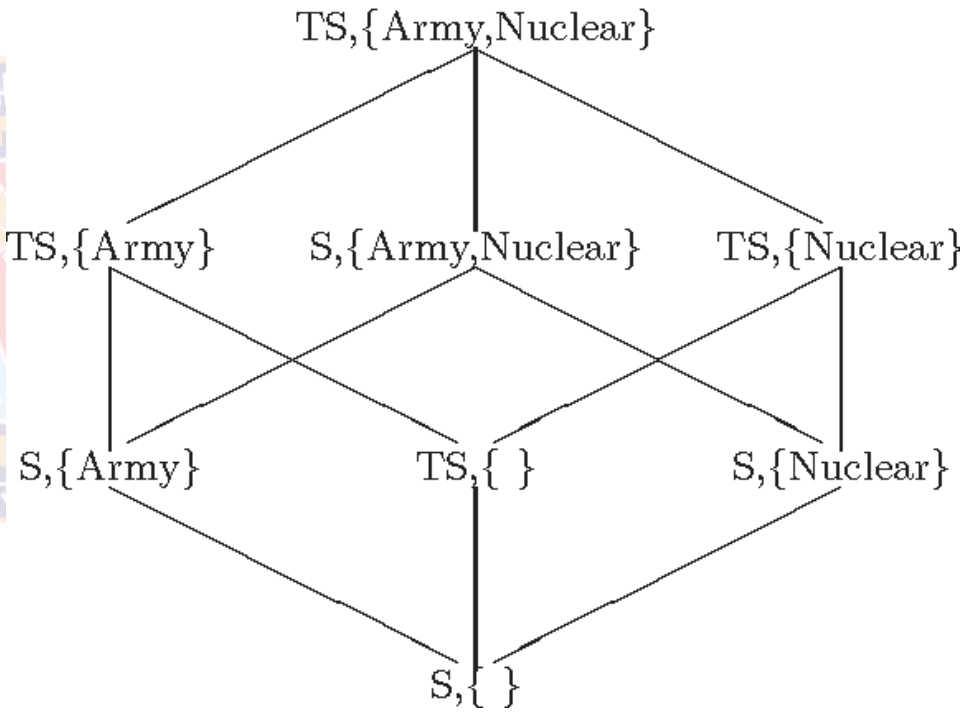
- Expand the model by adding a set of categories to each security classification
- These categories arise from the "need to know" principle:
  - no subject should be able to read objects unless reading them is necessary for that subject to perform its functions
- The sets of categories to which a person may have access is simply the power set of the set of categories
- For example, if the categories are NUC, EUR, and US, someone can have access to any of the following sets of categories:
  - ϕ (none), {NUC}, {EUR}, {US}, {NUC, EUR}, {NUC, US}, {EUR, US}, and {NUC, EUR, US}
- These sets of categories form a lattice under the operation $\subseteq$ (subset of)

Bell LaPadula Model

innovate achieve lead

Lattice of Categories

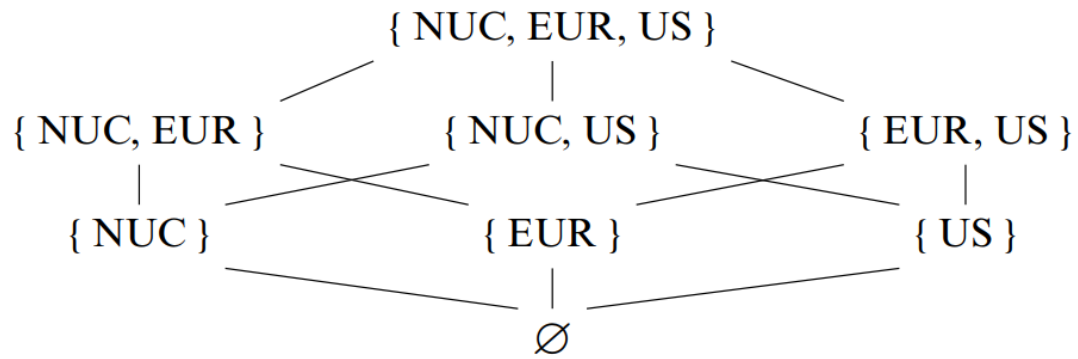
- (TS, {Army, Nuclear}) dominates (S, {Army})
- (TS, {Army, Nuclear}) dominates (TS, {Nuclear})
- (S, {Army, Nuclear}) dominates (S, {Nuclear})
- (S, {Army}) dominates (S, {})



Bell LaPadula Model

Attaching Category with i) User and ii) Info. Security Levels

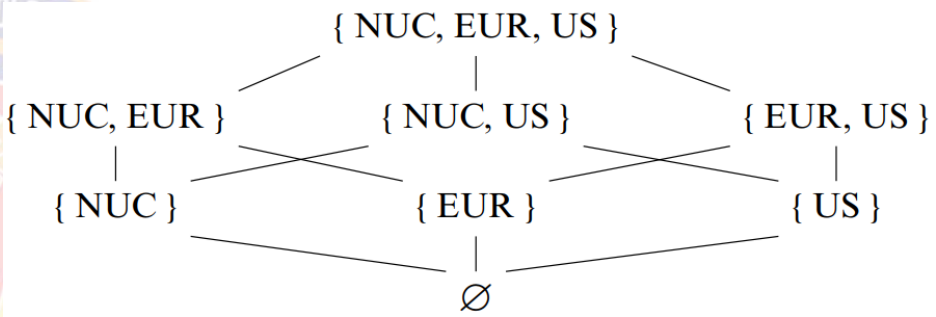
- Each security clearance or classification and category forms a security level
- We say that:
  - subjects have clearance at (or are cleared into, or are in) a security level, and
  - objects are at the level of (or are in) a security level



Bell LaPadula Model

Attaching Category with i) User and ii) Info. Security Levels

- Example:
  - William may be cleared into the level:
    - (SECRET, {EUR}) and
  - George may be cleared into the level
    - (TOP SECRET,{NUC,US})
- A document may be classified as
  - (CONFIDENTIAL, {EUR})



- How can we compare the security levels of user with that of documents?
- This is needed to satisfy the Bell-LaPadula model

Bell LaPadula Model

innovate achieve lead

Attaching Category with i) User and ii) Info. Security Levels

- Security levels (TOP SECRET, SECRET, etc.,.) change access
- Because categories are on a "need to know" basis,
  - a subject with access to the category set {NUC, US} presumably has no need to access items in the category {EUR}
- Hence, read access should be denied, even if
  - the security clearance of the subject (E.g., TOP SECRET) is higher than the security classification of the object (E.g., CONFIDENTIAL)
- However, access should be granted if
  - 1) the desired object is in any security level with category sets ϕ, {NUC}, {US}, or {NUC, US} and
  - 2) the subject's security clearance is no less than the document's security classification

  because the subject is cleared into the same category set as the object

Bell LaPadula Model

Attaching Category with i) User and ii) Info. Security Levels

- Definition
  - The security level (L, C) dominates the security level (L', C'), iff L' ≤ L and C' ⊆ C
  - It is written as written as (L, C) dom(L', C')
- We write (L, C) ¬dom(L', C') when (L, C) dom(L', C') is false

Bell LaPadula Model

innovate achieve lead

Security Categories and Dominance

- Security Level = {Security Classification, {Set of Categories})
  - E.g., (top-secret, {Nuclear, NATO})
- Security level A dominates B if and only if:
  - A's classification level > B's classification level, and
  - A's category set contains B's
- That is,
  - $(SC_1, C_1) \geq (SC_2, C_2)$ iff. $SC_1 \geq SC_2$ and $C_2 \subseteq C_1$
- For instance
  - (top-secret, {Nuclear, NATO}) dominates (secret, {NATO})
- because
  - top-secret > secret, and
  - the set {Nuclear, NATO} contains {NATO}

Bell LaPadula Model

innovate achieve lead

Security Categories and Dominance - Example

- If:
  - George is cleared into security level (SECRET, {NUC, EUR})
  - DocA is classified as (CONFIDENTIAL, {NUC})
  - DocB is classified as (SECRET, {EUR, US})
  - DocC is classified as (SECRET, {EUR})
- Then:
  - George *dom* DocA as SECRET $\geq$ CONFIDENTIAL and {NUC} $\subseteq$ {NUC, EUR}
  - George $\neg$*dom* DocB as {EUR, US} is not $\subseteq$ {NUC, EUR}
  - George *dom* DocC as SECRET $\leq$ SECRET and {EUR} $\subseteq$ {NUC, EUR}

Bell LaPadula Model

innovate achieve lead

Security Categories and Dominance

- Let C(S) be the category set of subject S, and let C(O) be the category set of object O, the simple security condition can be modified as:
- Simple Security Condition:
  - S can read O if and only if S dom O and S has discretionary read access to O
- In the previous example, George can read DocA and DocC but not DocB
  - assuming that the discretionary access controls allow such access
- Paul can read DocB
  - if he is cleared into security level (SECRET, {EUR, US, NUC}) and has discretionary read access to DocB
- George could then read DocB
  - If Paul wishes to copy DocB's contents to DocA and set its access permissions accordingly
- How can we prevent this?

Bell LaPadula Model

Security Categories and Dominance

- *-Property:
  - S can write to O if and only if O dom S and S has discretionary write access to O
- Paul cannot write to DocA because DocA *dom* Paul is false (C(Paul) is not ⊆ C(DocA))
  - C(Paul) = (SECRET, {EUR, US, NUC})
  - C(DocA) = (CONFIDENTIAL, {NUC})
- Remember:
  - The simple security condition is often described as "no reads up" and the *-property as "no writes down"
- A *secure system* is a system in which both the simple security property and the *-property hold

Bell LaPadula Model

Maximum Security Level & Current Security Level

- At times, a subject must communicate with another subject at a lower level
- This requires the higher-level subject to write into a lower-level object that the lower-level subject can read
- Example:
  - A colonel with (SECRET, {NUC, EUR}) clearance needs to send a message to a major with (SECRET, {EUR}) clearance
  - The colonel must write a document that has at most the (SECRET, {EUR}) classification
  - But this violates the *-property, because (SECRET, {NUC, EUR}) *dom* (SECRET, {EUR})


innovate
achieve
lead

BIRLA INSTITUTE OF TECHNOLOGY & SCIENCE, PILANI
ज्ञानं परमं बलम्

Thank You!