ECE458/ECE750T27: Computer Security

Information Flow Control

Dr. Kami Vaniea
Electrical and Computer Engineering
kami.vaniea@uwaterloo.ca

UNIVERSITY OF WATERLOO | FACULTY OF ENGINEERING

First, the news...

- First 5 minutes we talk about something interesting and recent
- You will not be tested on the news part of lecture
- You may use news as an example on tests
- Why do this?
    1. Some students show up late for various good reasons
    2. Reward students who show up on time
    3. Important to see real world examples

ACCESS CONTROL

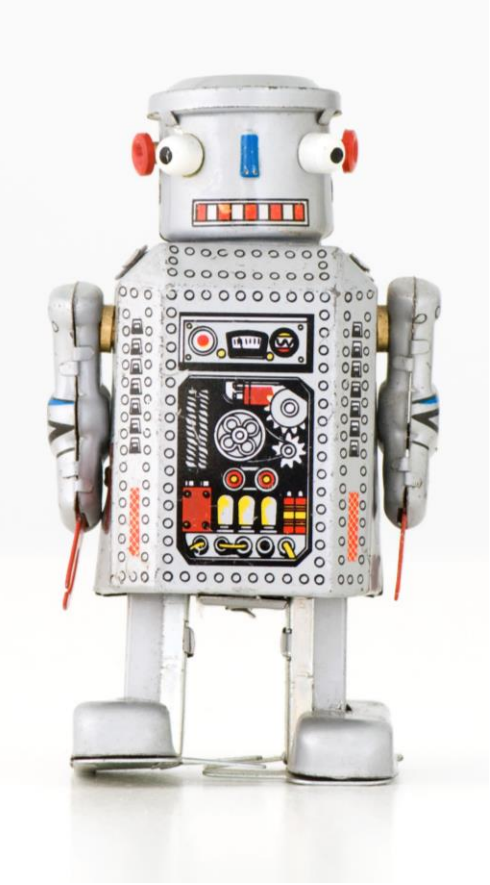
Access Control

- Ensure that certain users can use a resource in one way (i.e. read-only), others in a different way (i.e. write), and still others not at all.
- **Subjects** – human users who are often represented by surrogate programs running on behalf of the users.
- **Objects** – things on which an action can be performed. Such as files, database tables, programs, memory objects, hardware, network connections, and processors. User accounts can also be objects since they can be added to the system, removed, and modified.
- **Access modes** – any controllable actions of subjects on objects, including read, write, modify, delete, execute, create, destroy, copy export, and import.

Reference Monitor

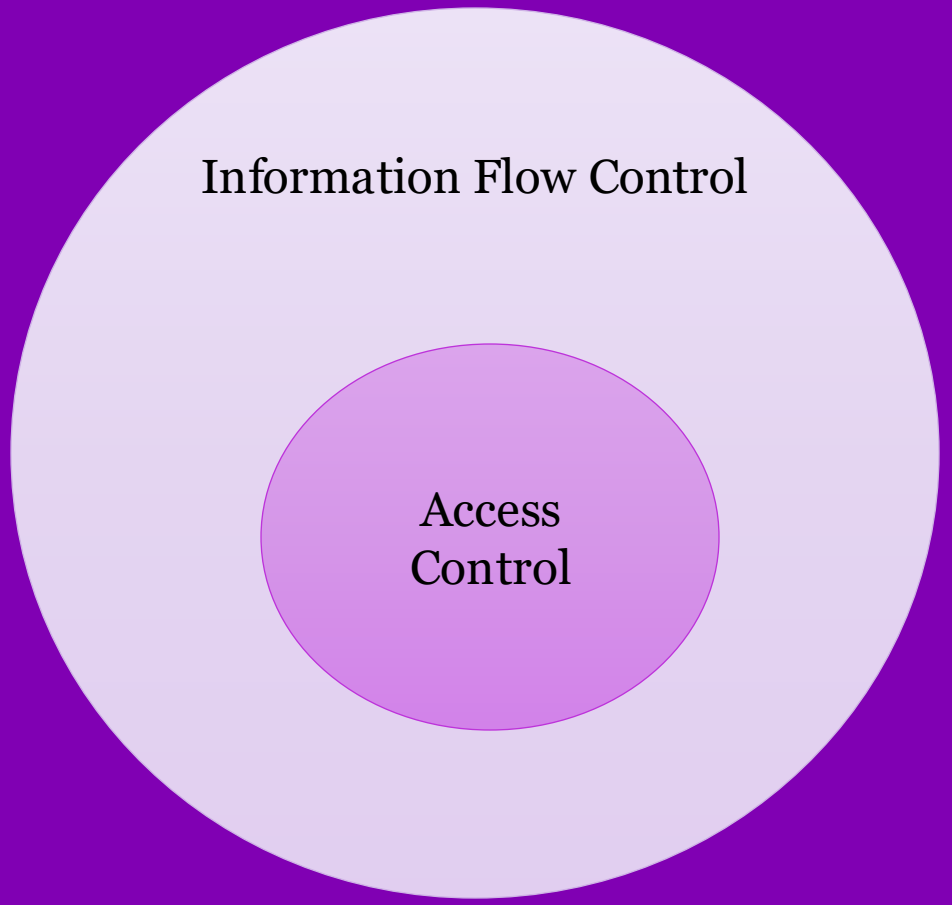
Theoretical construct that manages what objects subjects can access and what actions they can perform on those objects.

1. Always invoked; so that it validates every access attempt
2. Immune from tampering
3. Assuredly correct



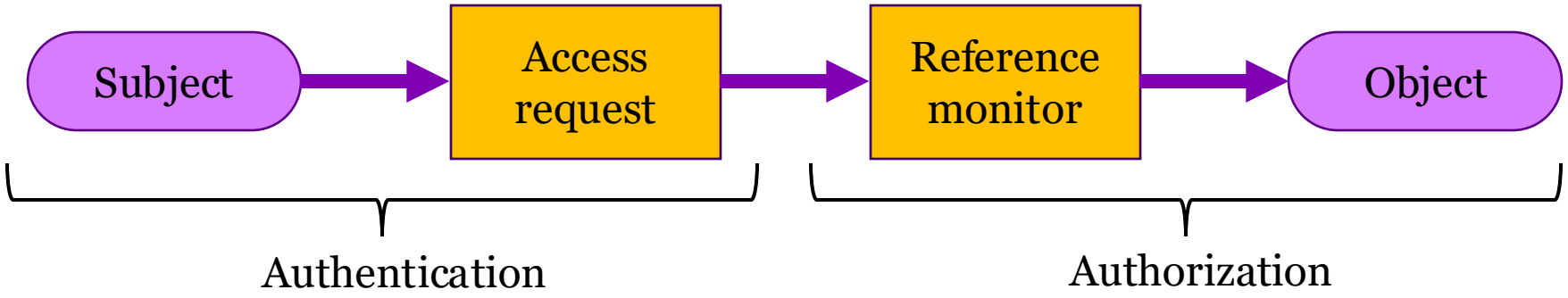
There are several ways to implement an access monitor

INFORMATION FLOW CONTROL



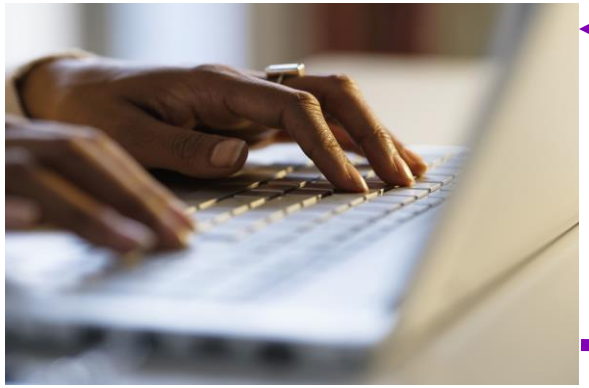
Access control

A guard controls whether a principal (the subject) is allowed access to a resource (the object).



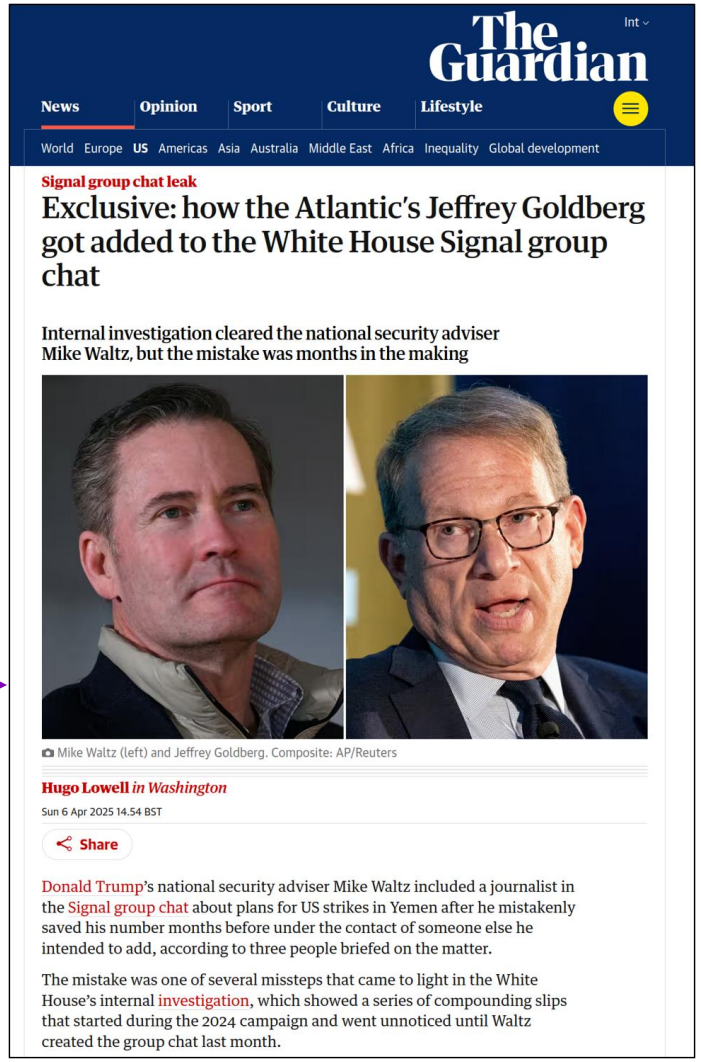
Access Control

User



Read file on hard drive

Email Journalist



The Guardian

Int

News | Opinion | Sport | Culture | Lifestyle

World Europe US Americas Asia Australia Middle East Africa Inequality Global development

Signal group chat leak

Exclusive: how the Atlantic's Jeffrey Goldberg got added to the White House Signal group chat

Internal investigation cleared the national security adviser Mike Waltz, but the mistake was months in the making

Mike Waltz (left) and Jeffrey Goldberg. Composite: AP/Reuters

Hugo Lowell *in Washington*

Sun 6 Apr 2025 14.54 BST

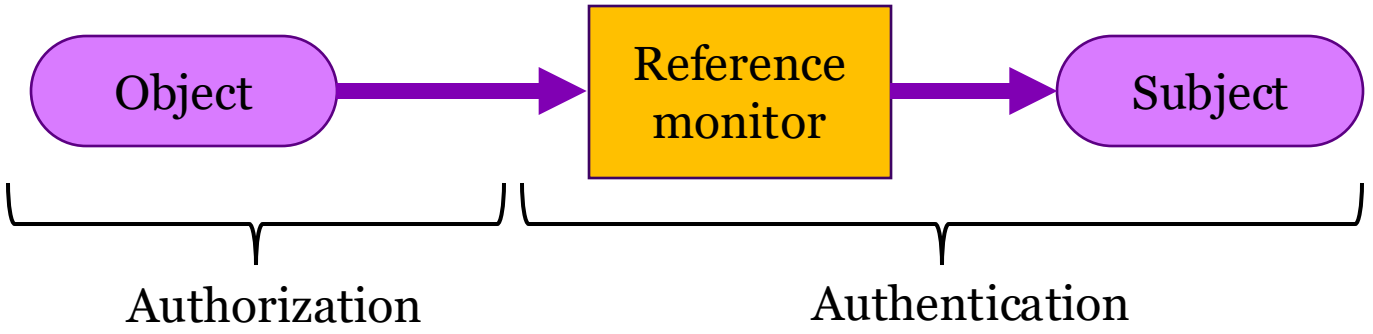
Share

Donald Trump's national security adviser Mike Waltz included a journalist in the Signal group chat about plans for US strikes in Yemen after he mistakenly saved his number months before under the contact of someone else he intended to add, according to three people briefed on the matter.

The mistake was one of several missteps that came to light in the White House's internal investigation, which showed a series of compounding slips that started during the 2024 campaign and went unnoticed until Waltz created the group chat last month.

Information flow control

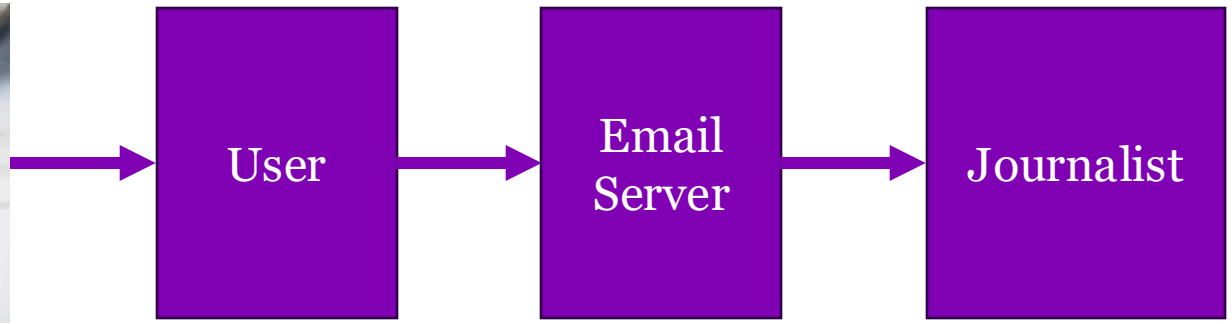
A guard controls whether a principal (the subject) is allowed access to a resource (the object).



This is the dual notion, sometimes used when confidentiality is the primary concern.

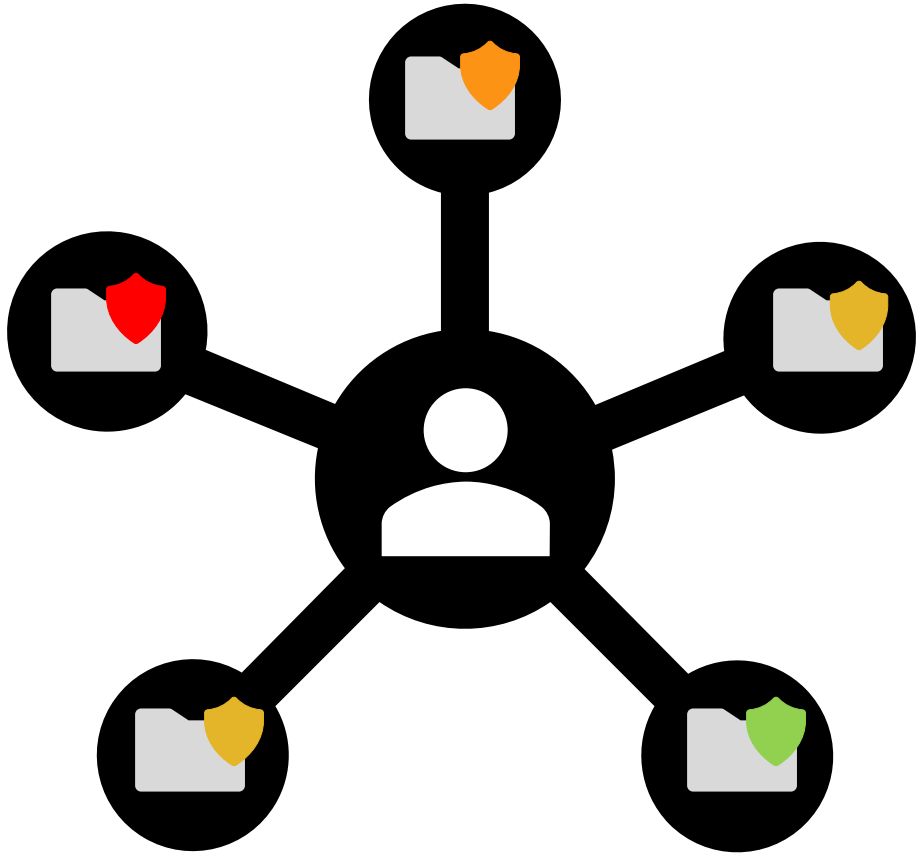
Information flow control

Document with top secret data



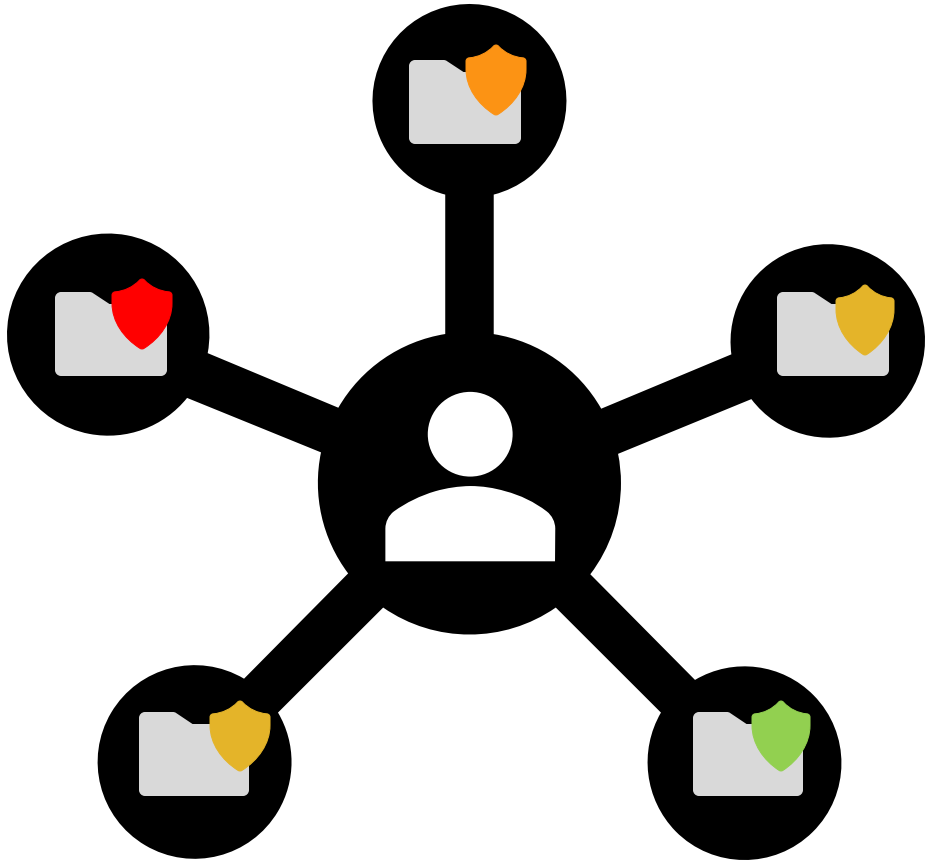
Accident prevention

- Users have access to a mix of confidentiality documents
- User meant to send fileA (confidential) but instead sent fileB (highly restricted)
- User thought a document was only confidential but actually it contains personal information (restricted)
- Goal is to identify (potentially) incorrect file transfer and either stop it or alert user



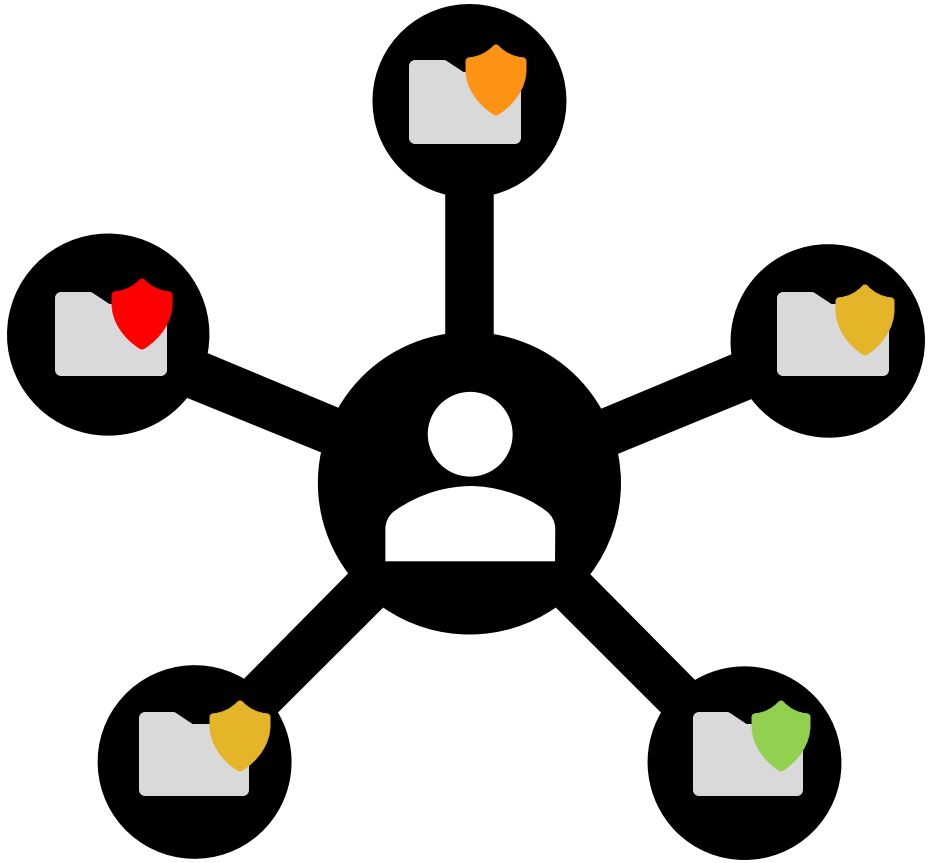
Insider attack

- User intentionally trying to send high security documents to low security external user/location.
- User intentionally trying to overwrite high security document.
  - Example, modify the list of people who will get a raise.
- Completely stop any transfer between high and low security.



Information poisoning

- Files are being created or modified
- Need to ensure that only appropriate information used
- AI model building: models should be built on “high quality” data
- Legal case construction: references need to be of a certain form



SCIF: Sensitive Compartmented Information Facility

https://scifglobal.com/scif-definition-what-is-a-scif/

MULTILEVEL SECURITY MODELS

Multi-level security

- **Multi-level security** (MLS) systems originated in the military. A **security level** is a label for subjects and objects to describe a policy.
- These are models or ways of thinking about the problem of access control logically and are not implementations
- Security levels are ordered

  Unclassified ≤ Confidential ≤ Secret ≤ Top Secret
- Ordering is important since it can express policies like “no write down” to prevent a subject with high-level clearance from writing secrets into a low-level document

Ways of thinking

- Philosophy about how to best control how information flows “correctly”
- Maybe used in security-intensive situations
- Helpful to learn this way of thinking
- Two models
  - Bell-LaPadula
  - Biba

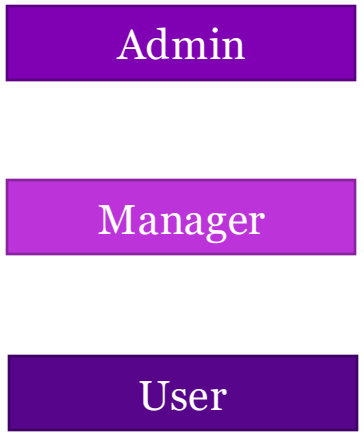
Think-pair-share

- Imagine a class context:
  - Students, TAs, Instructor, University Admin
- What types of data or files might need this type of protection?
- What is an example of needing to write “up” but not be able to read?
- What is an example of needing to read “down” but not write?

Running Example

Classifications (H)

- Admin
- Manager
- User

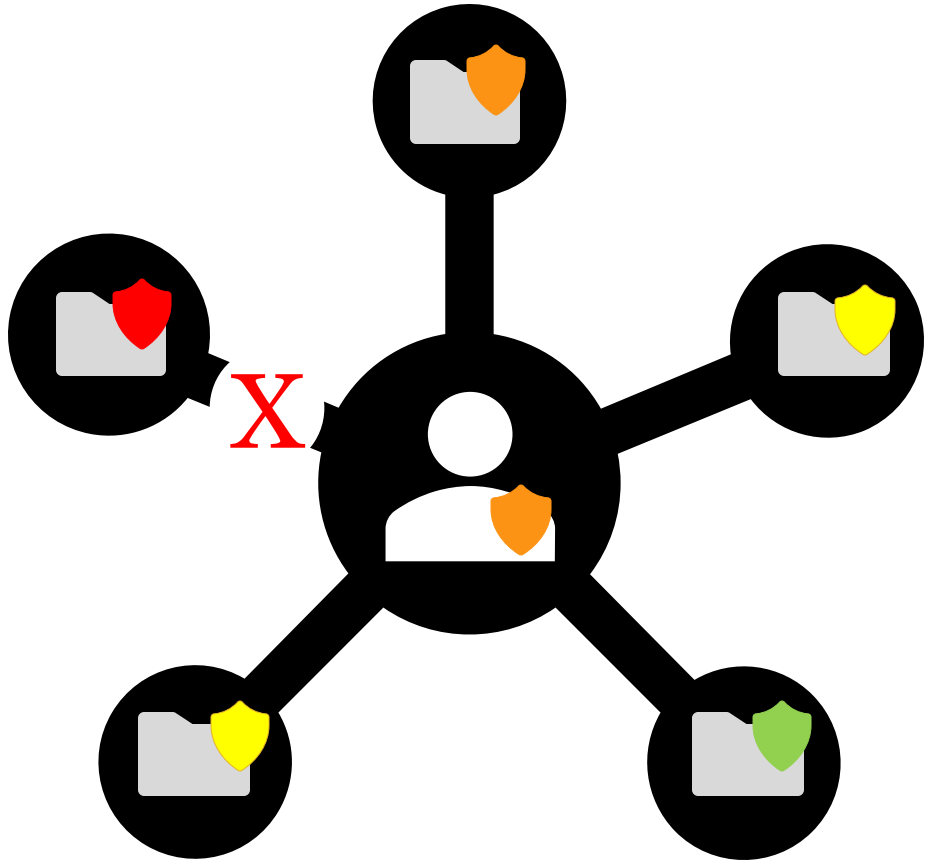


Bell-LaPadula

- Simple model of MLS designed to promote academic thought
  - **Simple Security Condition** – Subject S can read object O if and only if $L(O) \leq L(S)$
  - ***-Property (star property)** - Subject S can write object O if and only if $L(S) \leq L(O)$
- In other words:
  - No read up
  - No write down

Bell-LaPadula: Simple security (read)

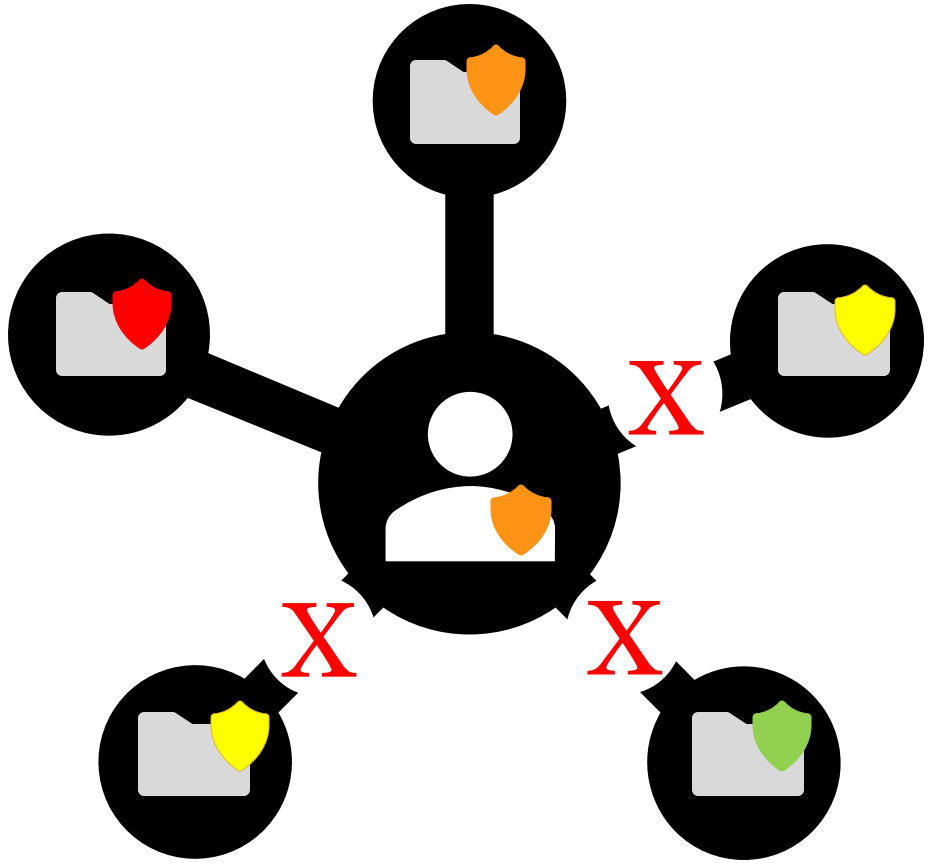
- Simple model of MLS designed to promote academic thought
  - **Simple Security Condition** – Subject S can read object O if and only if $L(O) \leq L(S)$
  - ***-Property (star property)** - Subject S can write object O if and only if $L(S) \leq L(O)$
- In other words:
  - No read up
  - No write down



Simple Security Condition (read)

Bell-LaPadula: *-Property (write)

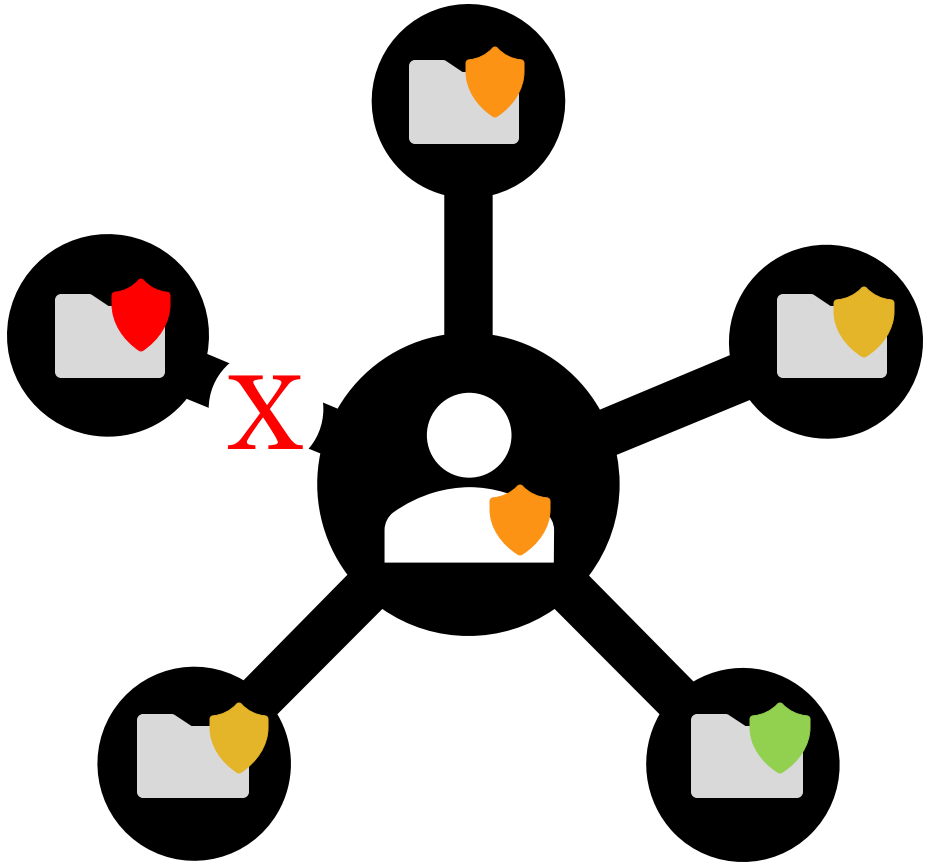
- Simple model of MLS designed to promote academic thought
  - **Simple Security Condition** – Subject S can read object O if and only if $L(O) \leq L(S)$
  - ***-Property (star property)** - Subject S can write object O if and only if $L(S) \leq L(O)$
- In other words:
  - No read up
  - No write down



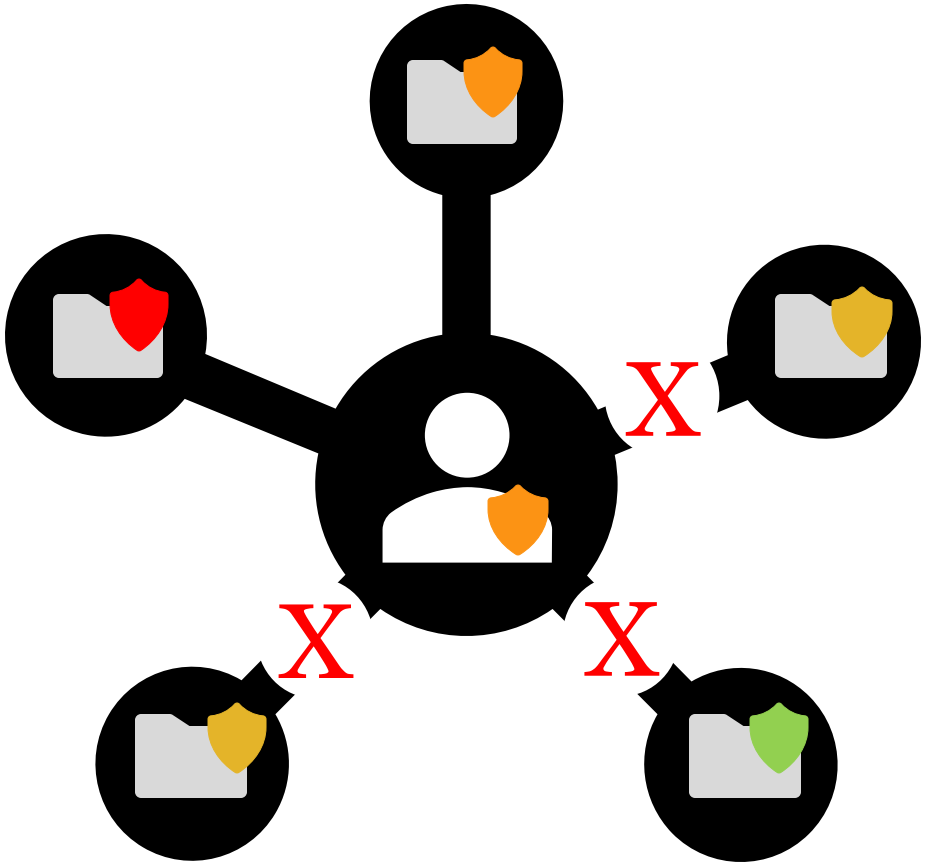
*-property (write)

Bell-LaPadula

Simple Security Condition (read)



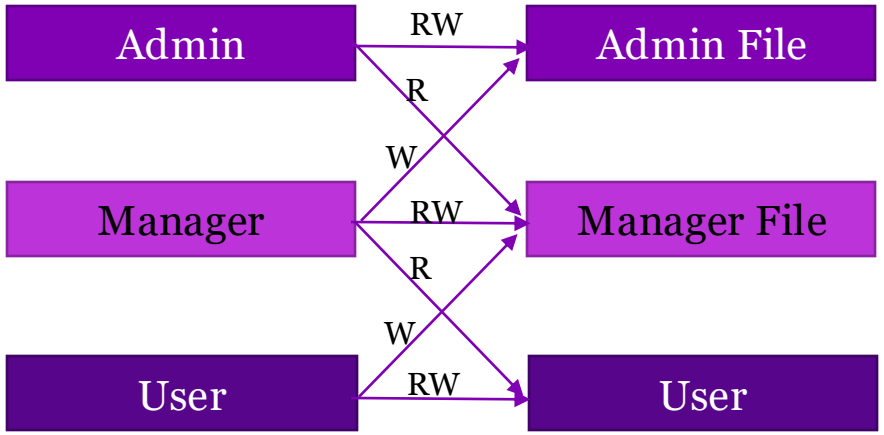
*-Property (write)



Running Example

Classifications (H)

- Admin
- Manager
- User



Think-pair-share

- Imagine a class context:
  - Students, TAs, Instructor, University Admin
- What types of data or files might need this type of protection?
- What is an example of needing to write "up" but not be able to read?
- What is an example of needing to read "down" but not write?

Bell-LaPadula

- Simple model of MLS designed to promote academic thought
  - **Simple Security Condition** – Subject S can read object O if and only if $L(O) \leq L(S)$
  - ***-Property (star property)** - Subject S can write object O if and only if $L(S) \leq L(O)$
- In other words:
  - No read up
  - No write down

Problem: most real systems don't fit neatly into clearence levels. It is rare that someone with a Top Security clearance really needs access to all Top Security files.

Solution: categories

Security lattice

- A lattice is a set L equipped with a partial ordering $\leq$ such every two elements a, b $\in$ L has a least upper bound a $\vee$ b and a greatest lower bound a $\wedge$ b. A finite lattice must have top and bottom elements.
- take a set of classifications H and linear ordering $\leq_H$
- take a set C of categories; compartments are subsets of C
- security levels are pairs (h, c) with h $\in$ H and c $\subseteq$ C
- ordering (h1, c1) $\leq$ (h2, c2) $\Longleftrightarrow$ h1 $\leq$ h2, c1 $\subseteq$ c2 gives a lattice.

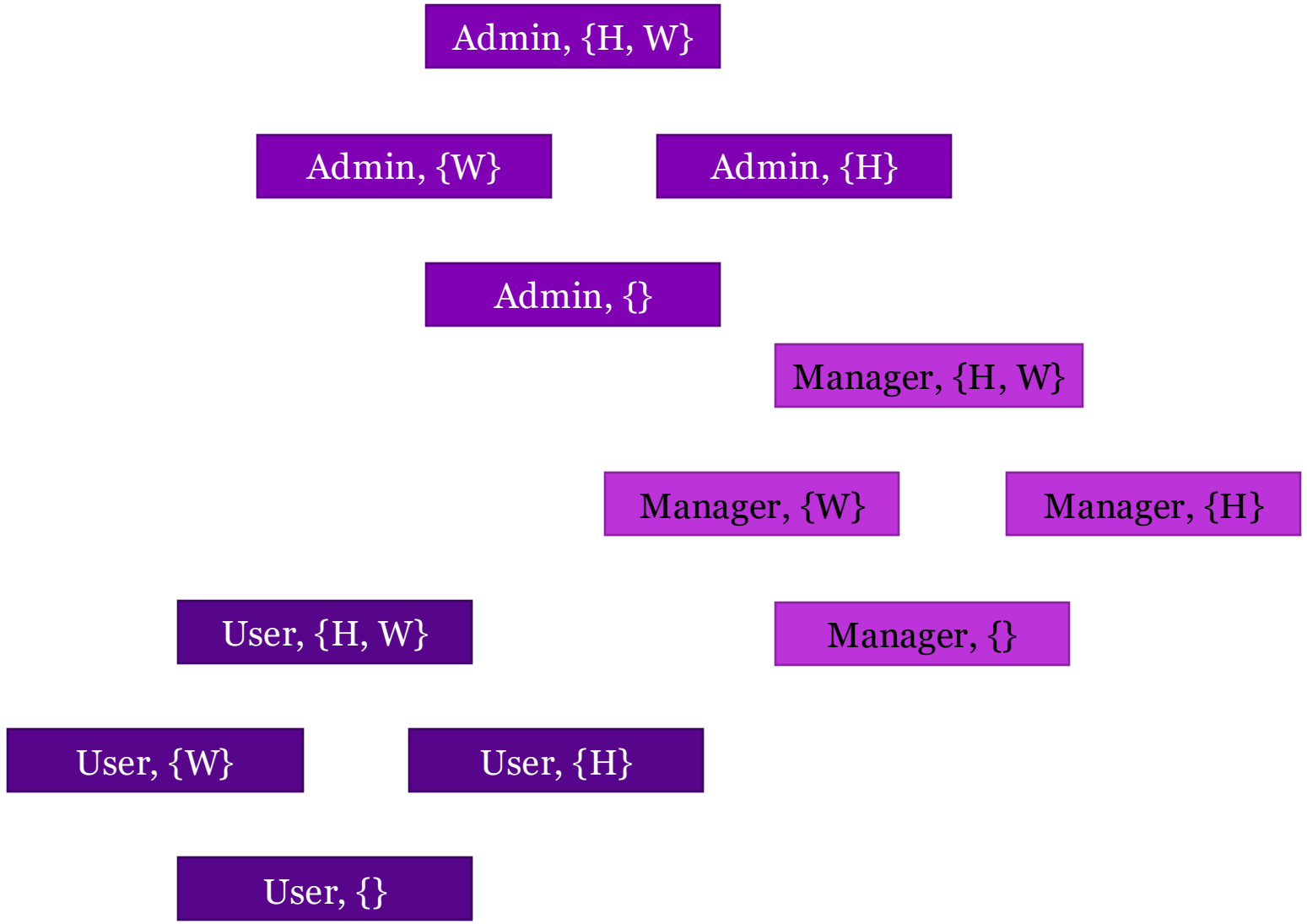
Running Example

Classifications (H)

- Admin
- Manager
- User

Categories (C)

- H (Hippo project)
- W (Walrus project)



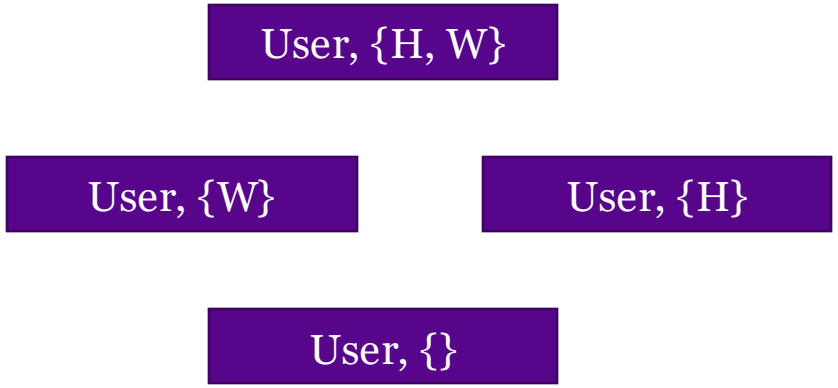
Running Example

Classifications (H)

- Admin
- Manager
- User

Categories (C)

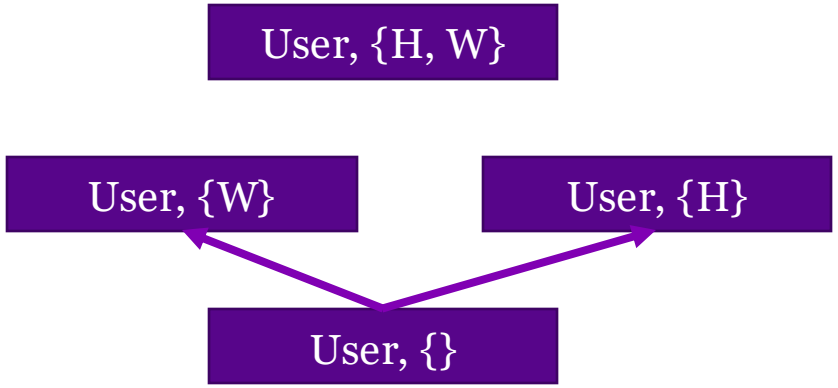
- H (Hippo project)
- W (Walrus project)



Orderings:

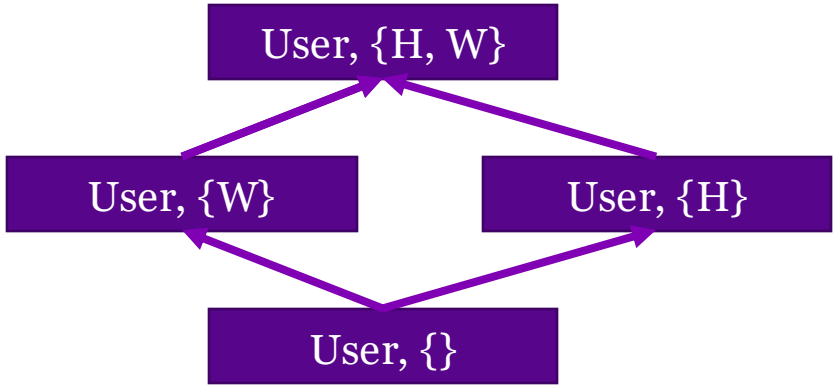
(User,{}) ≤ (User, {W})

(User,{}) ≤ (User, {H})



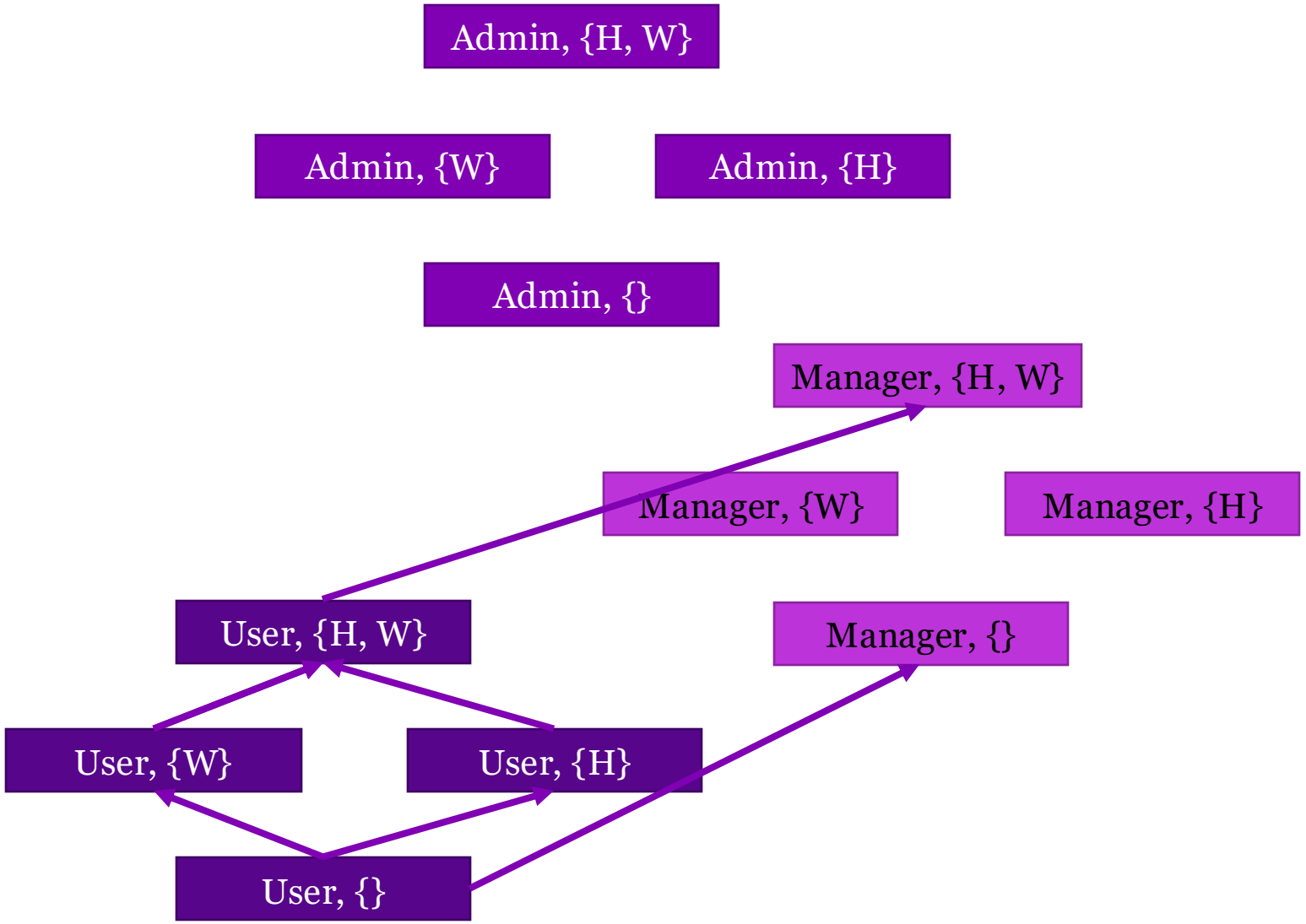
Orderings:

(User,{}) ≤ (User, {W})
(User,{}) ≤ (User, {H})
(User,{W}) ≤ (User, {H, W})
(User,{H}) ≤ (User, {H, W})



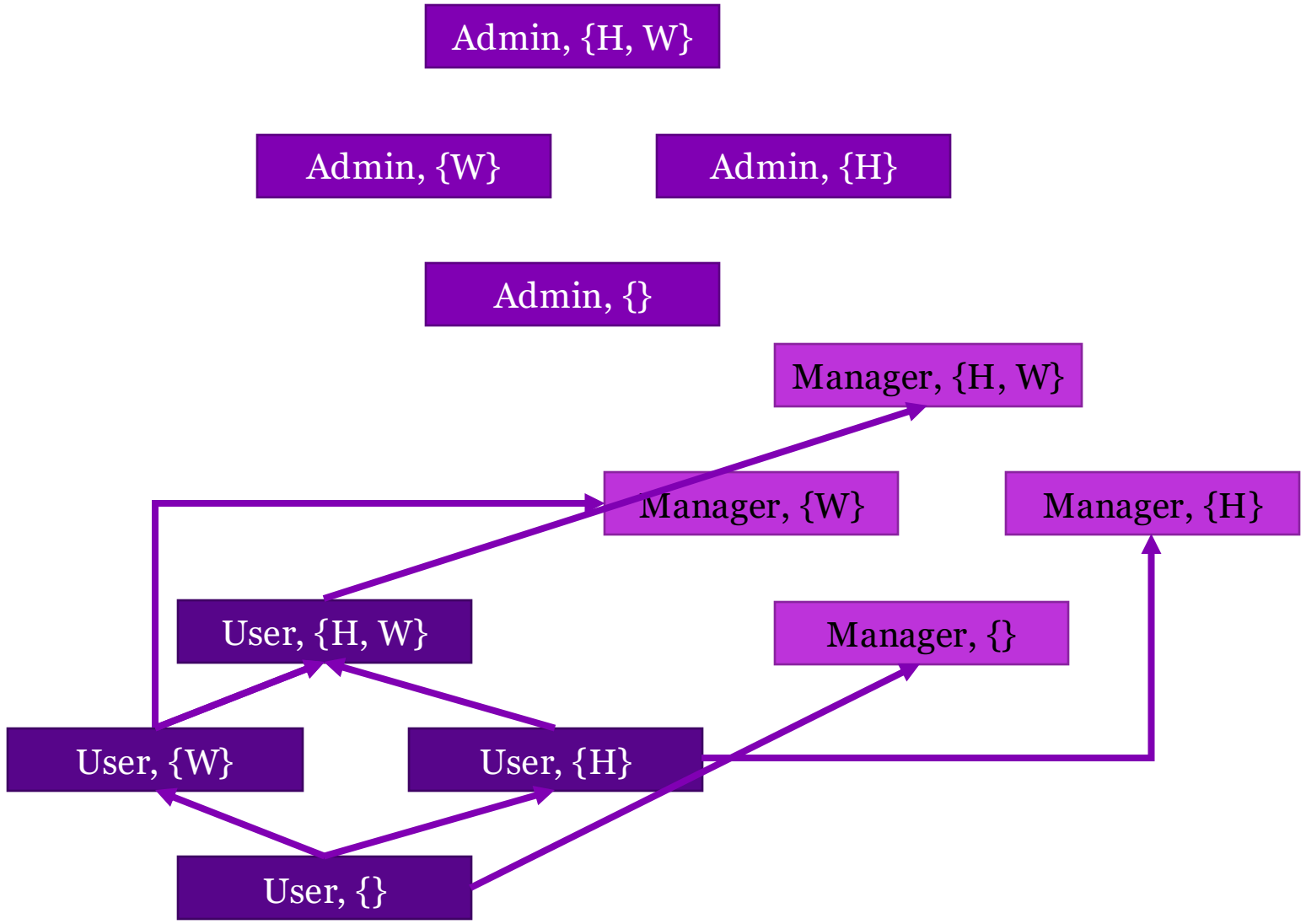
Orderings:

(User,{}) ≤ (User, {W})
(User,{}) ≤ (User, {H})
(User,{W}) ≤ (User, {H, W})
(User,{H}) ≤ (User, {H, W})
(User,{}) ≤ (Manager,{})
(User,{H,W})≤(Manager,{H,W})



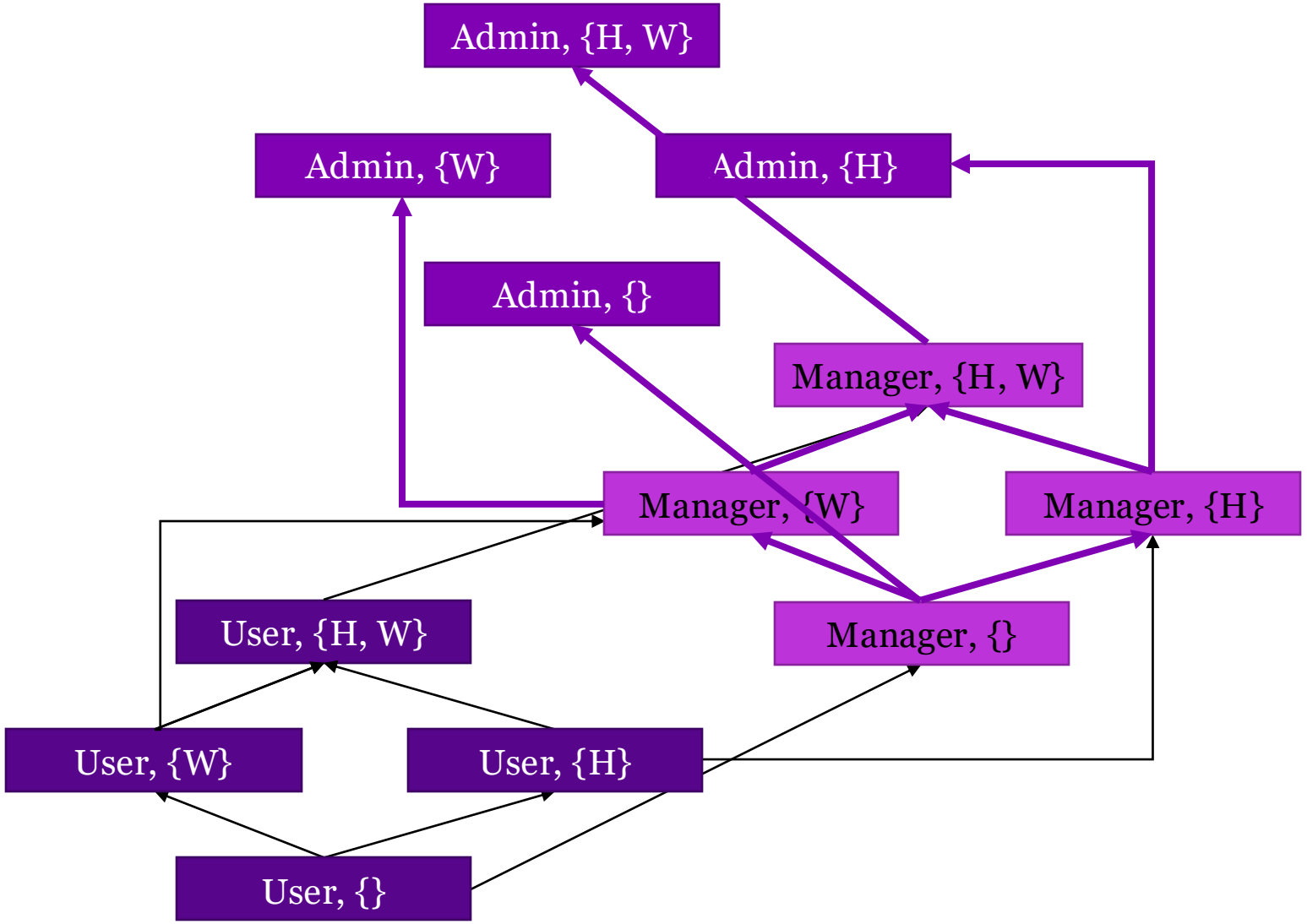
Orderings:

(User,{}) ≤ (User, {W})
(User,{}) ≤ (User, {H})
(User,{W}) ≤ (User, {H, W})
(User,{H}) ≤ (User, {H, W})
(User,{}) ≤ (Manager,{})
(User,{H,W})≤(Manager,{H,W})
(User,{W}) ≤ (Manager,{W})
(User,{H}) ≤ (Manager,{H})



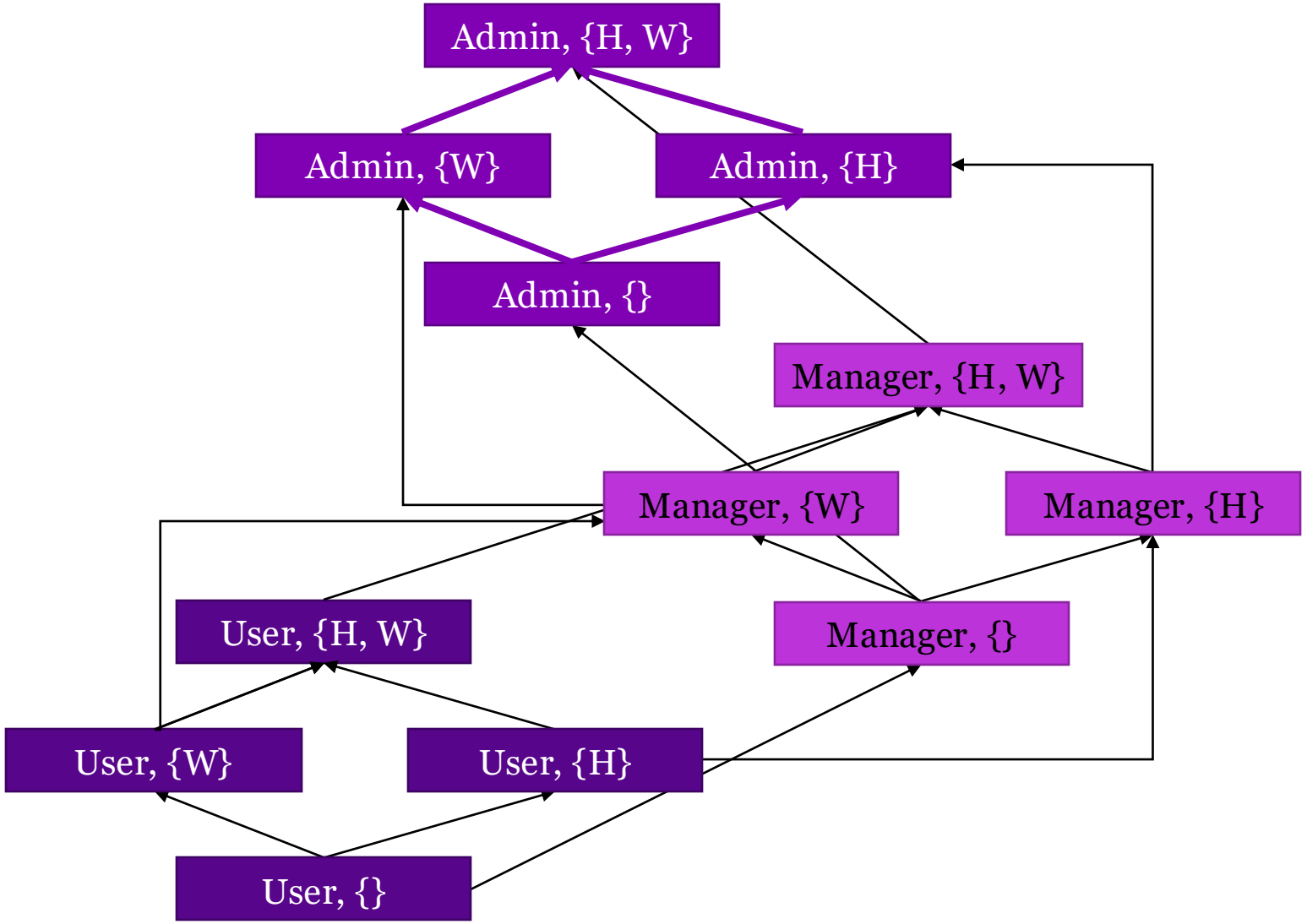
Orderings:

(Manager,{}) ≤ (Manager, {W})
(Manager,{}) ≤ (Manager, {H})
(Manager,{W}) ≤ (Manager, {H, W})
(Manager,{H}) ≤ (Manager, {H, W})
(Manager,{}) ≤ (Admin,{})
(Manager,{H,W})≤(Admin,{H,W})
(Manager,{W}) ≤ (Admin,{W})
(Manager,{H}) ≤ (Admin,{H})



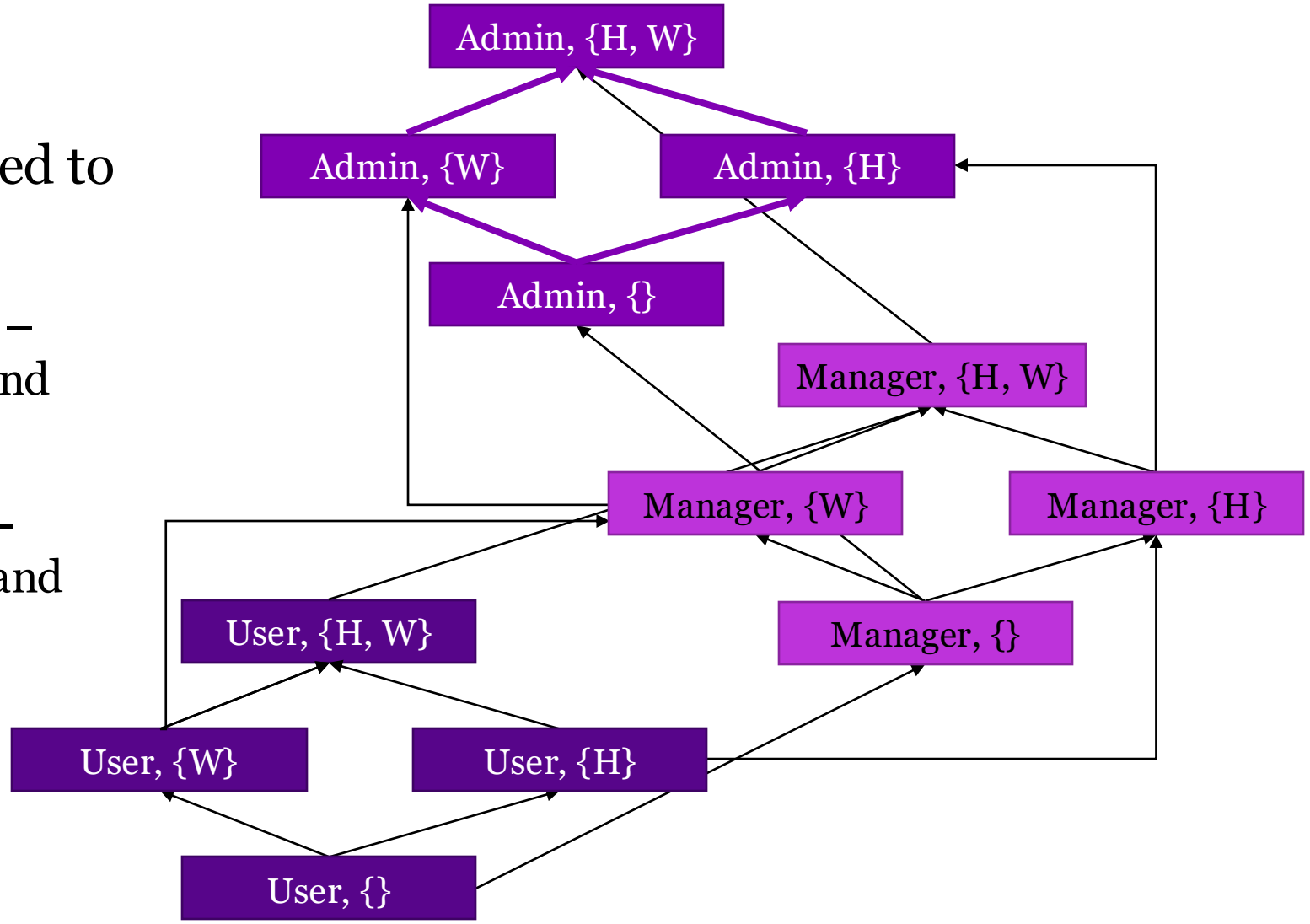
Orderings:

(Admin,{}) ≤ (Admin, {W})
(Admin,{}) ≤ (Admin, {H})
(Admin,{W}) ≤ (Admin, {H, W})
(Admin,{H}) ≤ (Admin, {H, W})



Bell-LaPadula

- Simple model of MLS designed to promote academic thought
  - **Simple Security Condition** – Subject S can read object O if and only if $L(O) \leq L(S)$
  - ***-Property (star property)** - Subject S can write object O if and only if $L(S) \leq L(O)$
- In other words:
  - No read up
  - No write down

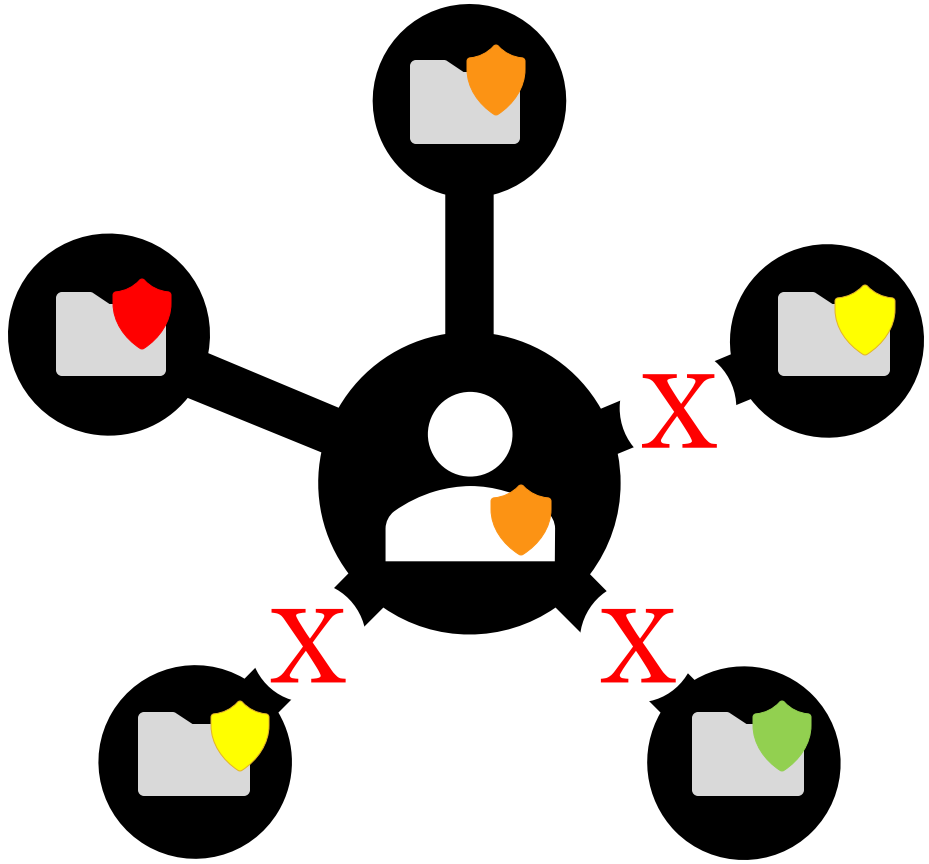


Biba Integrity Model

- Focus on the integrity of the data rather than the confidentiality
- Subjects S and Objects O have Integrity values
- **Simple Integrity Property** – subjects at a given level of integrity must not read data at a lower integrity level (no read down)
- * **Integrity Property** – subjects at a given level of integrity must not write to data at a higher level of integrity (no write up)
- **Invocation Property** – processes from below cannot request higher access; only with subjects at an equal or lower level

Biba: Simple Integrity Property (read)

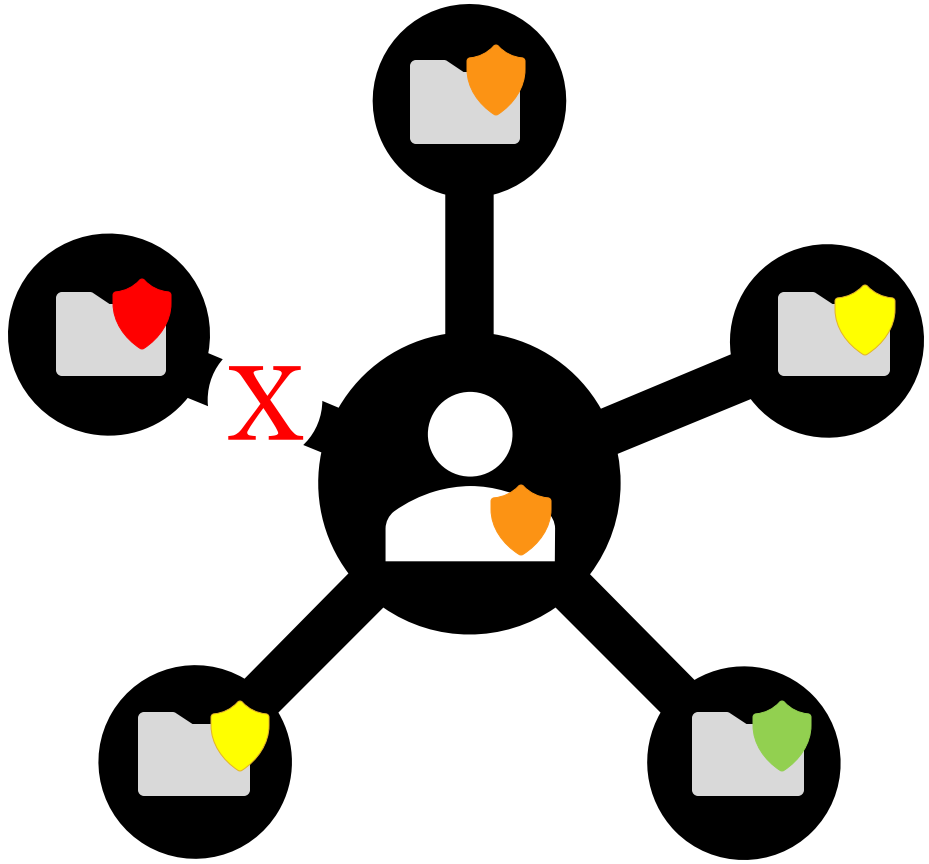
- Subjects S and Objects O have Integrity values
- **Simple Integrity Property** – subjects at a given level of integrity must not read data at a lower integrity level (no read down)
- * **Integrity Property** – subjects at a given level of integrity must not write to data at a higher level of integrity (no write up)
- **Invocation Property** – processes from below cannot request higher access; only with subjects at an equal or lower level
- In other words
  - No read down
  - No write up



Simple Integrity Property (read)

Biba: * Integrity Property (write)

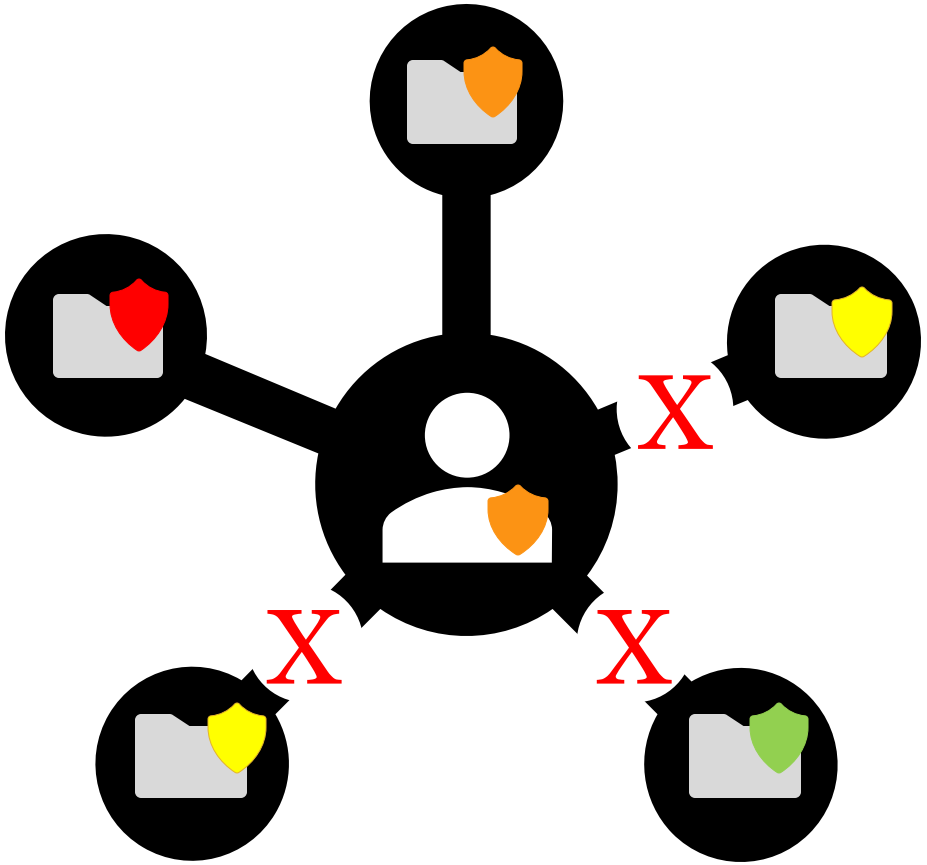
- Subjects S and Objects O have Integrity values
- **Simple Integrity Property** – subjects at a given level of integrity must not read data at a lower integrity level (no read down)
- * **Integrity Property** – subjects at a given level of integrity must not write to data at a higher level of integrity (no write up)
- **Invocation Property** – processes from below cannot request higher access; only with subjects at an equal or lower level
- In other words
  - No read down
  - No write up



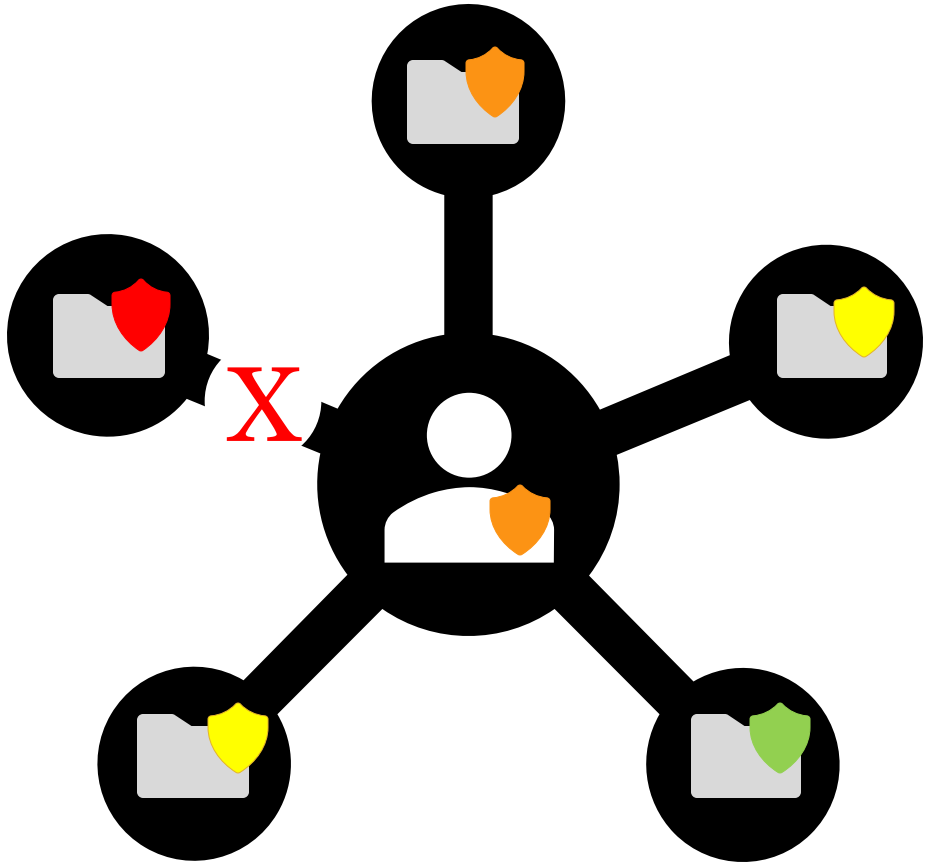
*** Integrity Property (write)**

Biba

Simple Integrity Property (read)



*** Integrity Property (write)**



Think-pair-share

- Imagine a class context:
  - Students, TAs, Instructor, University Admin
- What types of data or files might need this type of protection?
- What is an example of needing to read “up” but not be able to write?
- What is an example of needing to write “down” but not read?

Biba

- Subjects S and Objects O have Integrity values
- **Simple Integrity Property** – subjects at a given level of integrity must not read data at a lower integrity level (no read down)
- * **Integrity Property** – subjects at a given level of integrity must not write to data at a higher level of integrity (no write up)
- **Invocation Property** – processes from below cannot request higher access; only with subjects at an equal or lower level
- In other words
  - No read down
  - No write up

Covert channels

- Leaning information through indirect means.
- Sending information through indirect means

Example:

- An employee wants to know if they will be fired after a review.
- They cannot read their manager's files. But they can see if a file name exists (touch).
- They list the files in their manager's directory and see an "alice-performance-poor.txt" file.

QUESTIONS