CS431

Computer and Network Security

Access Control

Abhishek Bichhawat

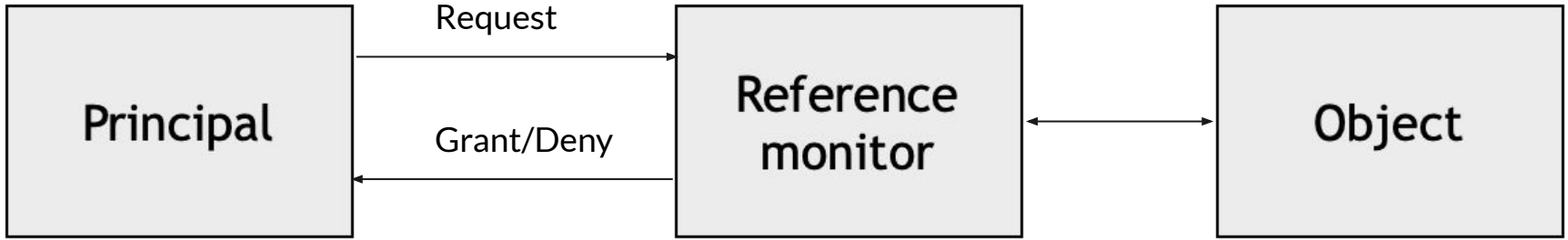
18/01/2024

The Problem

- Resources need to be protected and shared
- Resources:
  - Valuable objects: bike, phone, cash, …
  - Computation resources
    - Communication channels
    - CPU
    - Memory
    - Files …
  - Information
  - Medical records
- How do we regulate access?
  - Saltzer-Schroeder: The Protection of Information in Computer Systems

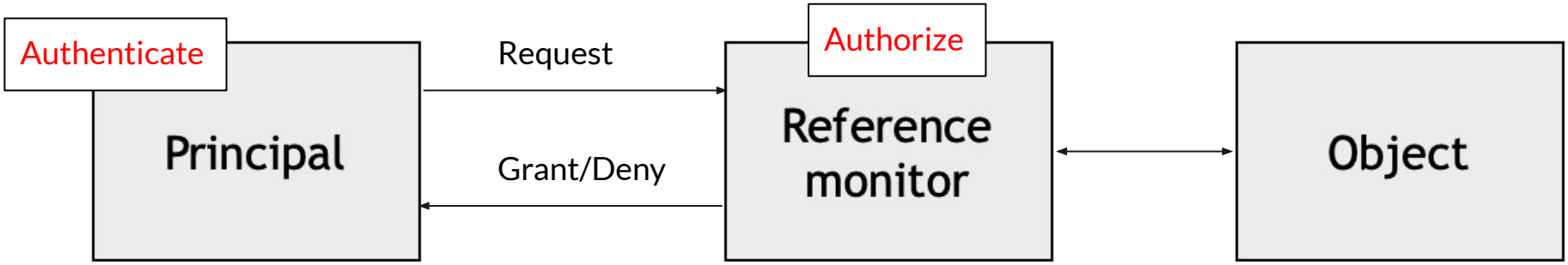
Access Control

- Principal requests some object
- Monitor grants or denies the request



Access Control

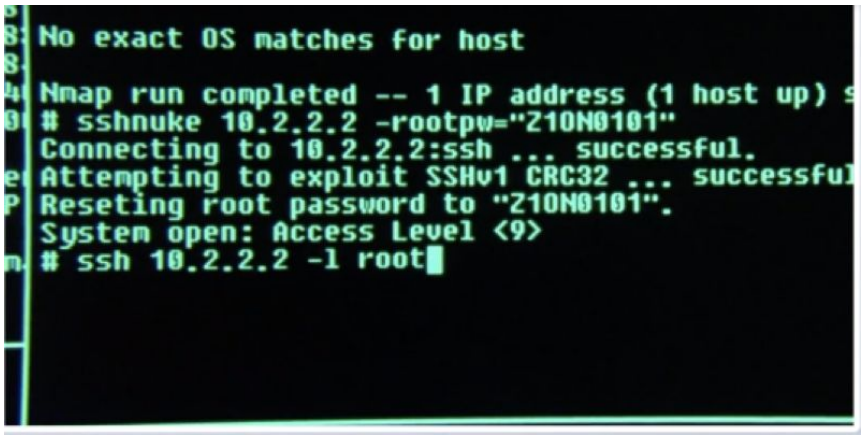
- Principal requests some object
- Monitor grants or denies the request



- Authentication - check that the principal is who they claim to be
- Authorization - which principals are allowed access to the object

Access Control

- Prevents
  - Unauthorized release of (confidential) information
  - Unauthorized modification of (confidential) information
  - Unauthorized denial of use



Policy vs. Mechanism

- Access control policy is a **specification** of who can access what, when, where
  - E.g., Tom should not enter Jerry's home
  - Different approaches to organizing policy are:
    - Discretionary - users can give access
    - Mandatory - central admin sets policy
    - Role-based - all policy specified via roles
- Access control mechanisms make it possible to implement policy
  - E.g., Door to Jerry's home is too small for Tom to enter
  - Access control bits for UNIX files & access control lists
  - Firewalls & firewall rules, physical locks & keys

Challenges with Access Control

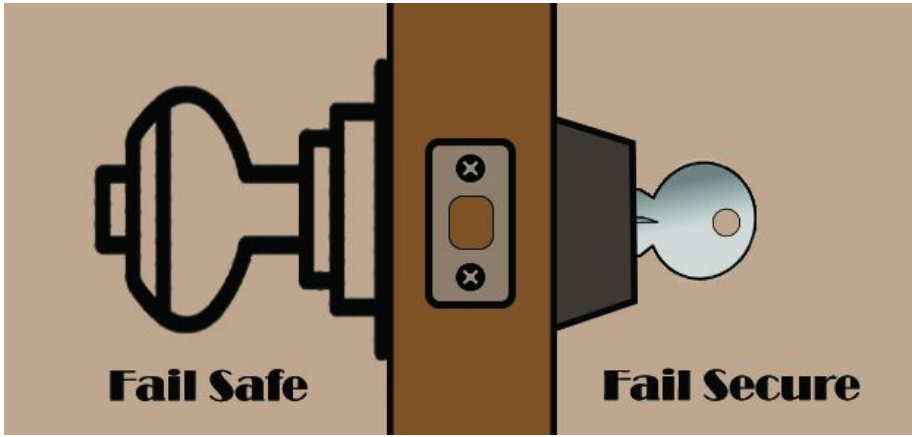
- Suppose Mallory tries to access file CS431!
- Does not have access (Access control policy)
- Mallory tries to change who can access file CS431!
- Cannot change permissions on file (ACP of ACP)
- Mallory tries to change the list of people who can change permissions on files!
- …

Access Control Principles

- Economy of mechanism
- Fail-safe defaults
- Complete mediation
- Open design
- Separation of privilege
- Least privilege
- Least common mechanism
- Psychological acceptability

Access Control Principles

- Economy of mechanism
- Fail-safe defaults
- Complete mediation
- Open design
- Separation of privilege
- Least privilege
- Least common mechanism
- Psychological acceptability

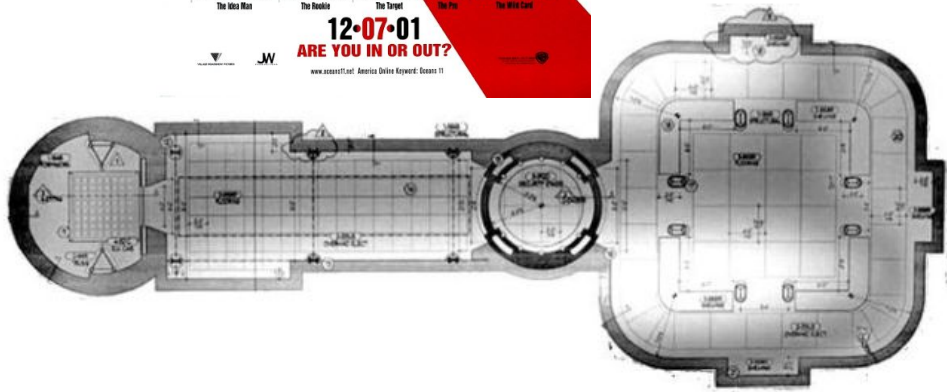


Access Control Principles

- Economy of mechanism
- Fail-safe defaults
- Complete mediation
- Open design
- Separation of privilege
- Least privilege
- Least common mechanism
- Psychological acceptability

Access Control Principles

- Economy of mechanism
- Fail-safe defaults
- Complete mediation
- Open design
- Separation of privilege
- Least privilege
- Least common mechanism
- Psychological acceptability



Access Control Principles

- Economy of mechanism
- Fail-safe defaults
- Complete mediation
- Open design
- Separation of privilege
- Least privilege
- Least common mechanism
- Psychological acceptability

Access Control Principles

- Economy of mechanism
- Fail-safe defaults
- Complete mediation
- Open design
- Separation of privilege
- Least privilege
- Least common mechanism
- Psychological acceptability

Access Control Principles

- Economy of mechanism
- Fail-safe defaults
- Complete mediation
- Open design
- Separation of privilege
- Least privilege
- Least common mechanism
- Psychological acceptability

Access Control Principles

- Economy of mechanism
- Fail-safe defaults
- Complete mediation
- Open design
- Separation of privilege
- Least privilege
- Least common mechanism
- Psychological acceptability

Access Control Policies

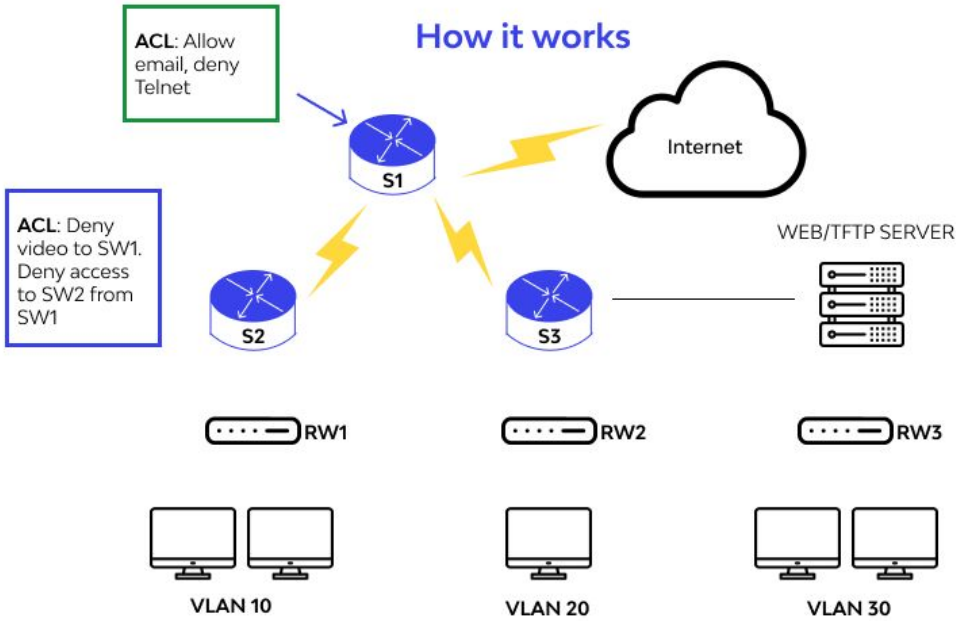
- No access control policy
  - MS-DOS

Access Control Policies

- No access control policy
  - MS-DOS
- Complete isolation
  - Partition the memory - users get own slice of the file system
  - Users are in “sandboxes”, cannot access other users’ files
  - E.g., Virtualization

Access Control Policies

- No access control policy
- Complete isolation
- Controlled sharing
  - Explicitly specify who can access what and under what conditions

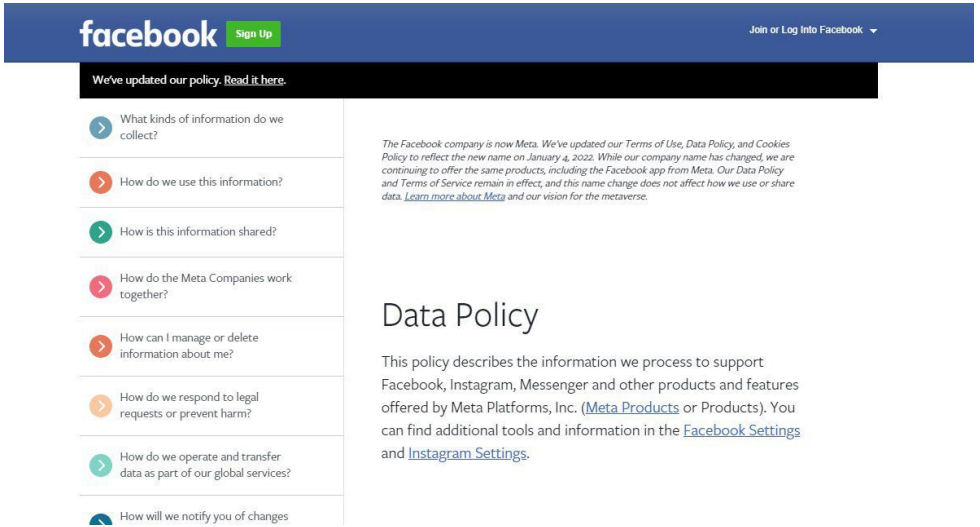


Access Control Policies

- No access control policy
- Complete isolation
- Controlled sharing
- Protected subsystems
  - Collection of programs and data

Access Control Policies

- No access control policy
- Complete isolation
- Controlled sharing
- Protected subsystems
- Access aggregate data
    - Normally associated with privacy

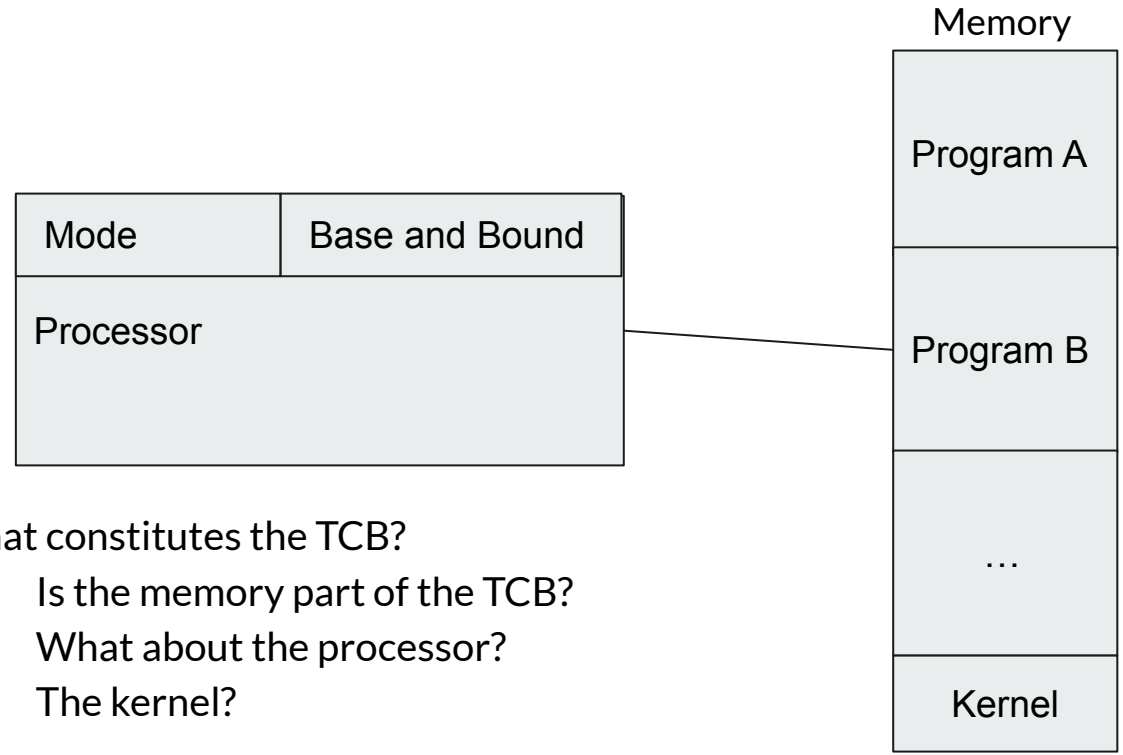


Trusted Computing Base

- The set of components that must function correctly for the system to be secure
- Must be as small as possible!
- Failure of TCB may result in additional access being granted

- Example: AirBnB guest, cat, food in the kitchen
  - Policy: cat cannot access food
  - System 1: lock pantry door
  - System 2: additionally give house guest key to the pantry and ask the house guest to lock the pantry door

Simple Isolation - Operating System



What constitutes the TCB?

- Is the memory part of the TCB?
- What about the processor?
- The kernel?

Access Control Matrix

- A triple : User x Resource x Access-Permission

	OS	Accounts program	Accounting data	Audit trail
Alice (manager)	rx	x	--	--
Bob (auditor)	rx	r	r	r
Charlie (admin)	rwx	rwx	r	r
Accounts program	rw	r	rw	w

Access Control Lists

- Unix contains access control lists (ACLs)
  - A list of all users who can access the resource and how
  - Grouped by accessor types to reduce the length of the list
    - Owner RWX
Group RW
Others R
    - ACL is represented using 9 bits. (RWX for owner, group, others)
    - May contain more bits
      - Is it a directory or symlink…
  - Check chmod to change permissions

Special Permissions in Unix

- suid
  - A file with suid (set user id) always executes as the user
  - -rwsr-xr-x. 1 root root 3354 Jan 22 /usr/bin/passwd
- sgid
  - set group id; if set on a file, allows it to be executed as the group that owns the file
  - drwxrws--- ...

Capabilities

- Each user has a list of programs it can access and how
  - List of access rights; e.g., keychain
- List must be unforgeable
  - User must not be able to modify the list as per their wishes
- Trusted party signs a ticket providing rights to resources
  - User presents this ticket to the reference monitor to get access
  - Resource must have a list of what capabilities can access
- Example : Page tables

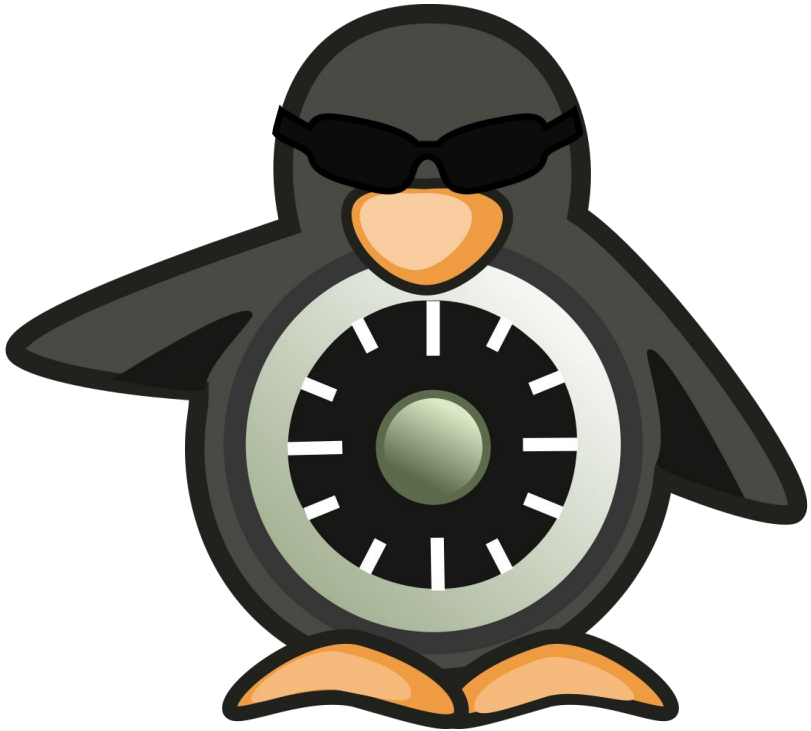
Multilevel Security

Clearance: Level of permission required to view classified information

How do you ensure proper security at each level?

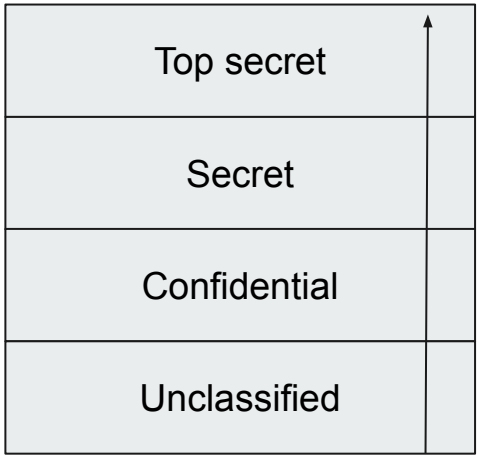
MLS

- Used in SELinux
  - Users, processes, files etc. have a context
  - [username, role, domain]
  - Similar to tags or labels
  - Borrowed from the Bell-LaPadula model



Bell-LaPadula Model

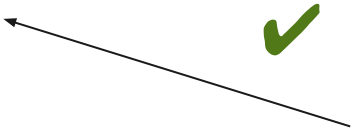
- Describes two security properties
  - Simple security property
    - Subject may not read from higher levels
    - I.e., no read up
  - Star property (*-property)
    - Subject may not write to lower levels
    - I.e. no write down
    - Strong star property prohibits write to upper levels
- Describes the access control mechanism
  - How to secure, not what data to secure



Simple Security Property

- Common sense: someone with no clearance shouldn't be able to read classified information
- On the other hand, nothing prevents someone with a top-secret clearance to read secret or confidential materials

* Property



- Common sense: cannot write classified information to public channels; prevents information leaks
- Hard to implement (e.g., a login password check)

Challenges with BLP

- When data is no longer classified

Home > All India > On Netaji Files, Mamata Banerjee Prods PM Modi Ahead Of Statue Unveiling

On Netaji Files, Mamata Banerjee Prods PM Modi Ahead Of Statue Unveiling

"They (the Centre) had said that when they come to power, they will work on it but nothing happened. In fact, we (state) have released and declassified all files on Netaji Bose," Mamata Banerjee said.

All India | Edited by Anindita Sanyal | Updated: January 23, 2022 5:56 pm IST

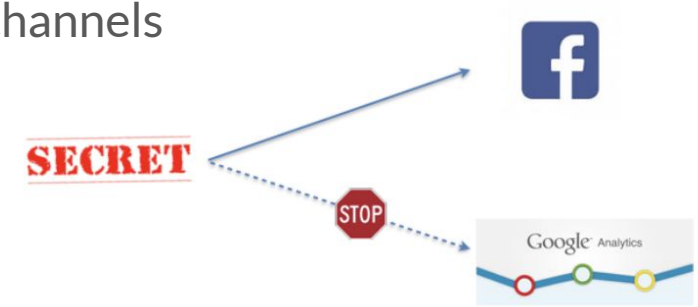
- Change in clearance level
- Does not prevent leaks through covert channels
- Does not mention if other mechanisms can be used

Examples of information flows

```
add(int x, int y) {
    return x+y; }

f(int x, int y) {
    if x>0 return y+y; else return 2*y; }

check_pw(char *s) {
    char *x; return strcmp(x,s); }

g(int x, int y){
    return x*y/x; }
```

Security Properties

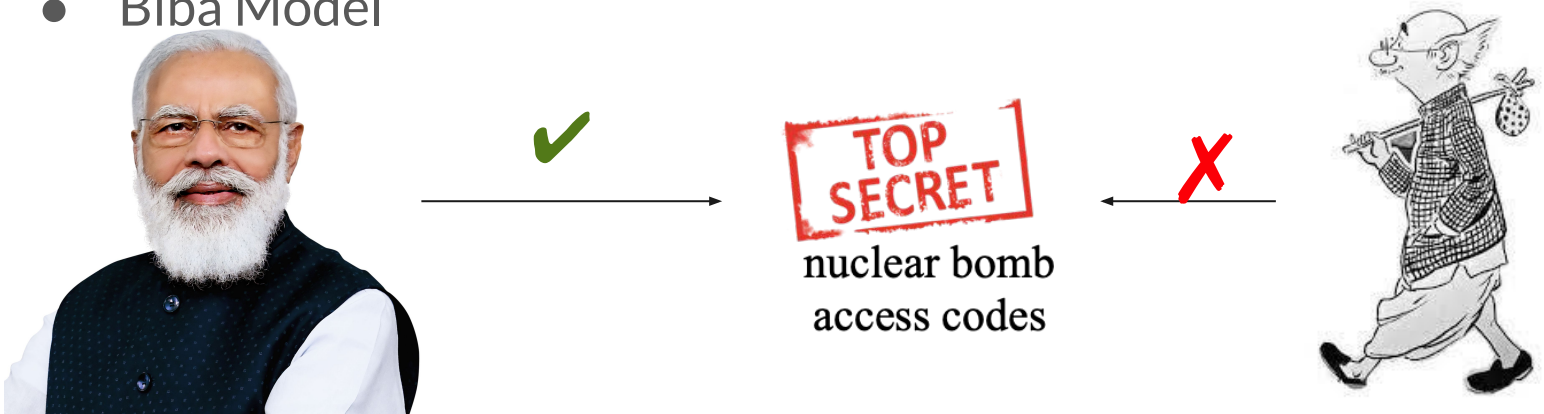
- Noninterference (Denning, Goguen & Meseguer)
  - Secret data should not flow to public channels
  - No matter what the secret input,
    the public output must not change
  - Is too strict in various scenarios



- Nondeducibility (Sutherland)
  - Someone without clearance cannot deduct secret data
    with 100% probability
  - Given possible values of secret inputs and observing the outputs,
    the adversary cannot rule out certain inputs
  - E.g. z = x + y

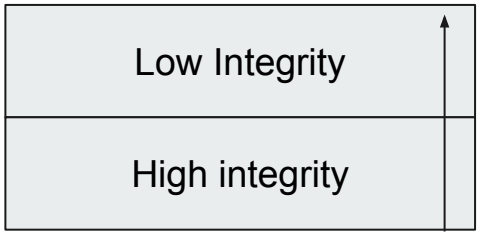
Integrity

- Existing properties and BLP focus on confidentiality of data
- Integrity is important in various systems, too
  - Examples:
    - Integrity constraints in DB
    - Critical data should be modified only by “trusted” principals
- Biba Model



Biba Model of Integrity

- Each subject (process) has an integrity level
- Each object has an integrity level
- Integrity levels are ordered (lattice structure)
- Dual of the confidentiality model
  - High integrity data can affect low integrity data but not vice-versa
- What are examples of data that need high integrity, but no confidentiality?



Chinese Wall Policy

- Used to prevent conflicts of interest
  - Prevent exchange of confidential information (insider trading)
- Suppose
  - S is a subject (e.g., a banker)
  - C is a customer
  - X(C) is C's competitors
  - Y(C) is C's own company
- Simple security property – read policy
  - S can read C if and only if for any C' that S can read, either Y(C') = Y(C) or Y(C') is not in X(C)
- *-property – write policy
  - S can write to C only if S can read C, and
  - Only if S cannot read any C' for which X(C') is not empty and Y(C)≠Y(C')

Chinese Wall Policy

- S = Scrooge is a banker
- Simple security property
  - C = Donald Duck
  - Y(C) = Disney Ducks (C's own company)
    - Daisy Duck is in Y(C)
  - X(C) = All other Disney characters (C's competitors)
  - Scrooge can read Daisy Duck and Bugs Bunny
  - Can Scrooge read Donald Duck?
    - Scrooge can read Donald Duck's account if and only if for any C' that S can read either C' is part of Disney Ducks (e.g., C' = Daisy Duck) or Y(C') is not in X(C), e.g. C' = Bugs Bunny

Chinese Wall Policy

- S = Scrooge is a banker
- C = Donald Duck
- Y(C) = Disney Ducks (C's own company)
  - Daisy Duck in Y(C)
- X(C) = All other Disney characters (C's competitors)
- *-property
  - Can Scrooge write to Bugs Bunny's account? (Y(Bugs Bunny) = Warner Bros.)
    - Scrooge can write to Bugs Bunny's account only if Scrooge can read it,
    - and only if Scrooge cannot read any account C' which has competitors and who is not part of Warner Bros.
  - Star property prevents Scrooge from passing information to Rockerduck about Donald Duck through the Bugs Bunny account, if Rockerduck is in charge of Mickey Mouse's account

Inference Control

- Anonymized data may reveal some information
- Control
  - Restrict the size of query sets
    - E.g. queries that return less than “n” values
  - Reject extreme values in statistical data
    - E.g. If you see that the average height in a particular village is 1m95 and if you see that, for many smaller groups, the average falls to 1m72, you know that some specific tall person lives in the village
  - Cell suppression
    - Conceal data that can be reversed engineered
  - Use random samples to provide statistics
  - Add noise