2550 Intro to cybersecurity

L17: Authorization

abhi shelat

Thanks Christo for slides!

Authentication:

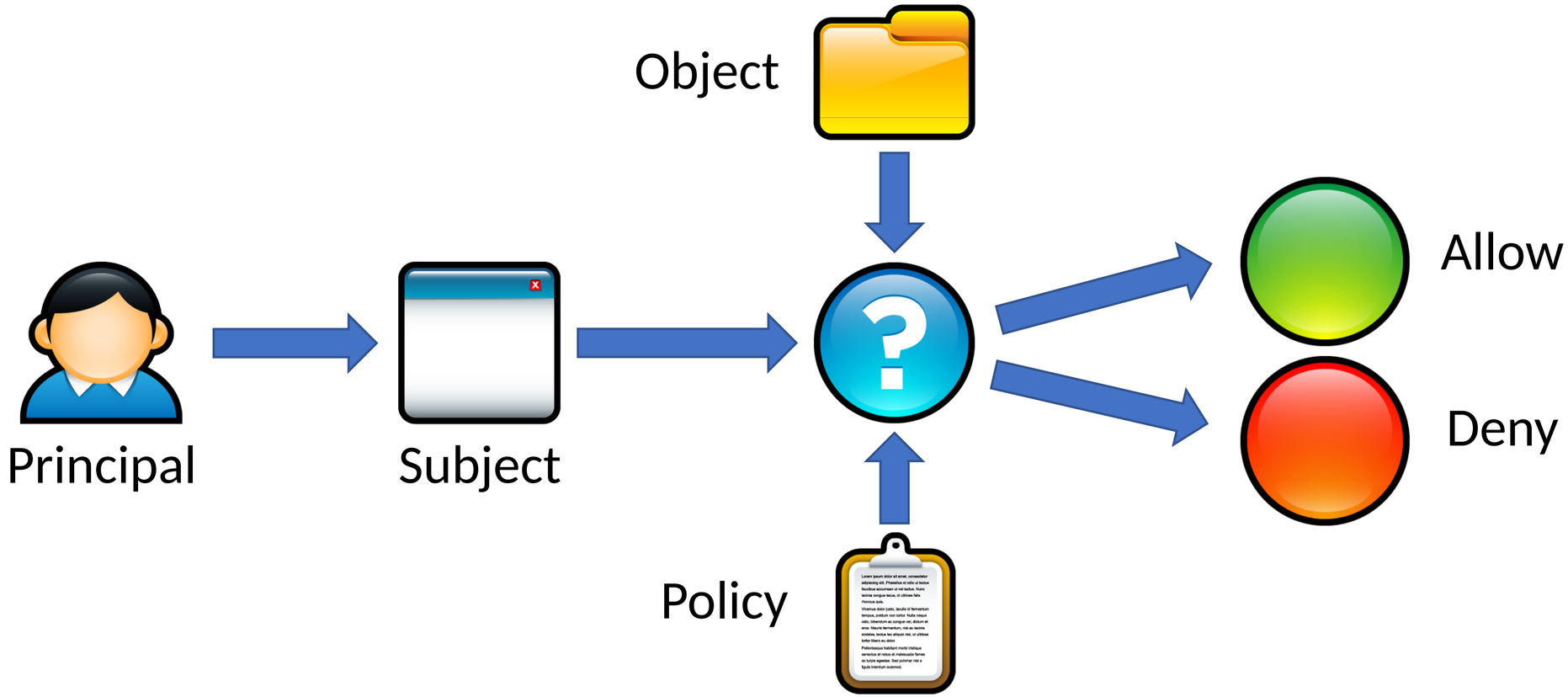
Authorization

After Authenticating a subject, what next?

Principle-Subject-Object

Access Control Check

- Given an access request from a subject, on behalf of a principal, for an object, return an access control decision based on the policy



Two main types of access control

Discretionary access control

ACL

	o_1	o_2	o_3
s_1	RW	RX	
s_2	R	RWX	RW
s_3		RWX	

Capability-based systems

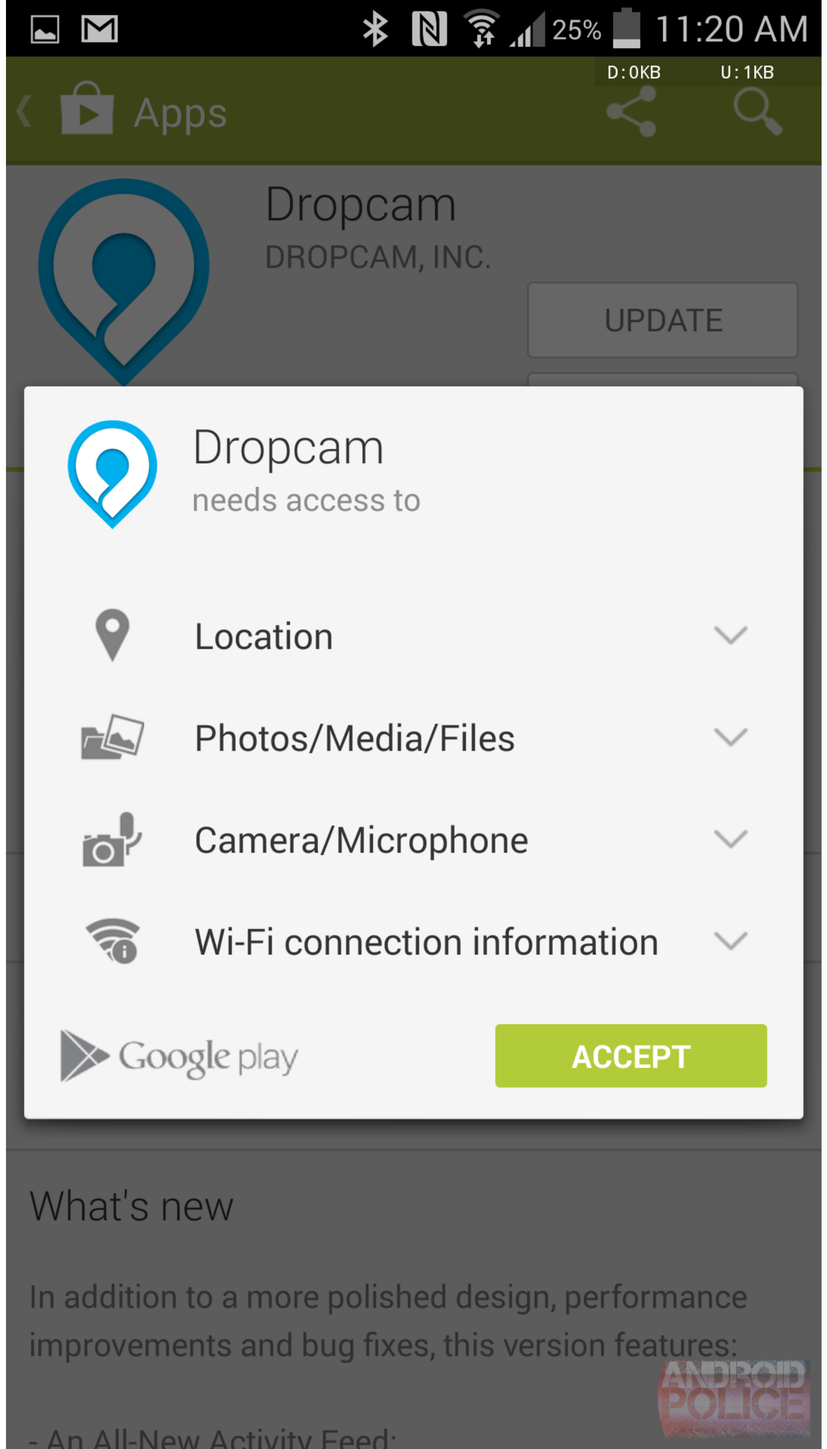
	o_1	o_2	o_3
s_1	RW	RX	
s_2	R	RWX	RW
s_3		RWX	

Capability-based Access Control

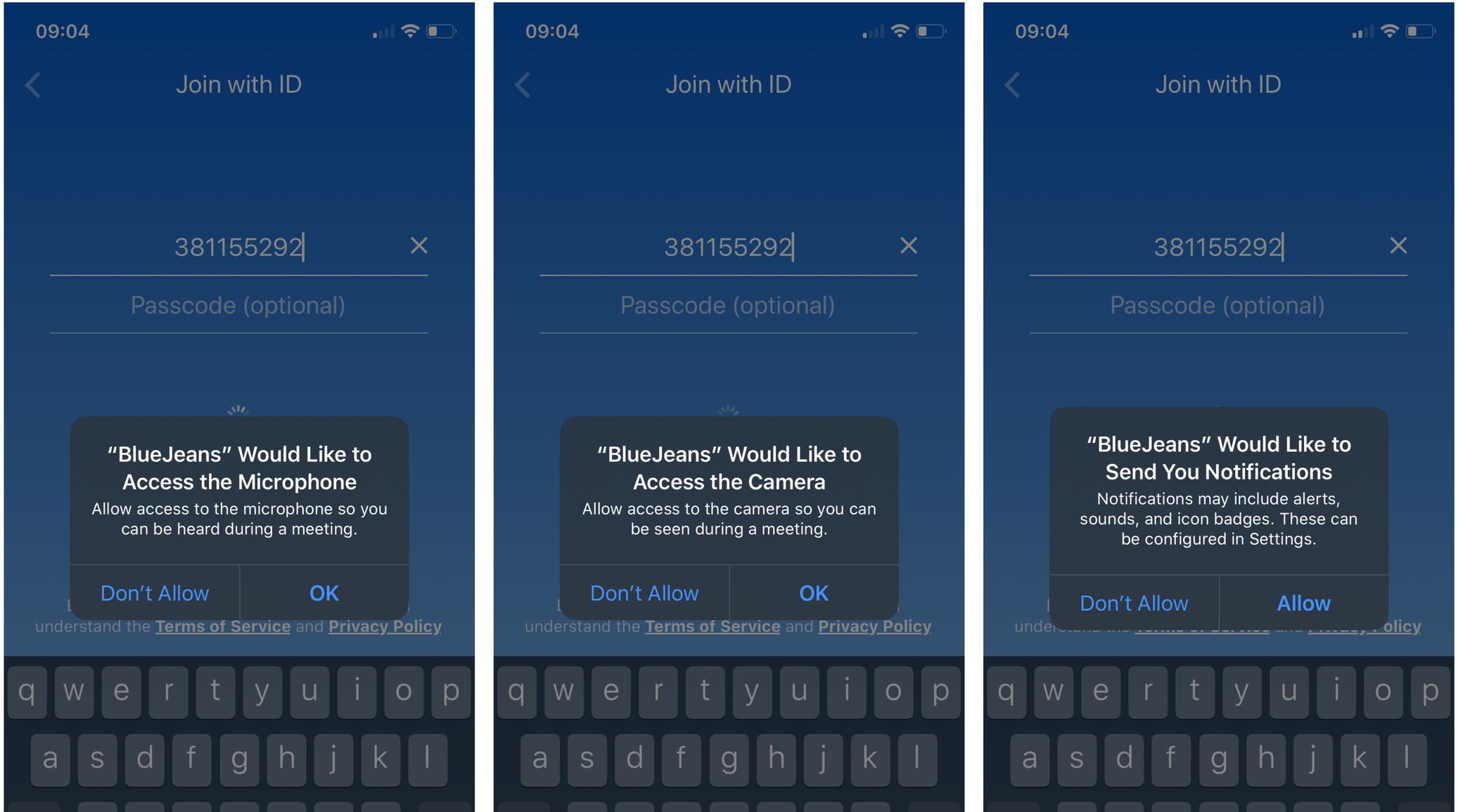
- Principals and subjects have capabilities which:
  - Give them access to objects
    - Files, keys, devices, etc.
  - Are transferable and unforgeable tokens of authority
    - Can be passed from principal to subject, and subject to subject
    - Similar to file descriptors
- Why do capabilities solve the confused deputy problem?
  - When attempting to access an object, a capability must be selected
  - Selecting a capability inherently also selects a master

Android/iOS Capabilities

- Android and iOS support (relatively) fine grained capabilities for apps
  - User must grant permissions to apps at install time
  - May only access sensitive APIs with user consent
- Apps can “borrow” capabilities from each other by exporting *intents*
  - Example: an app without camera access can ask the camera app to return a photo



Android/IOS just-in-time capability



Per-event capability

Failure of DAC

- DAC cannot prevent the leaking of secrets

User A

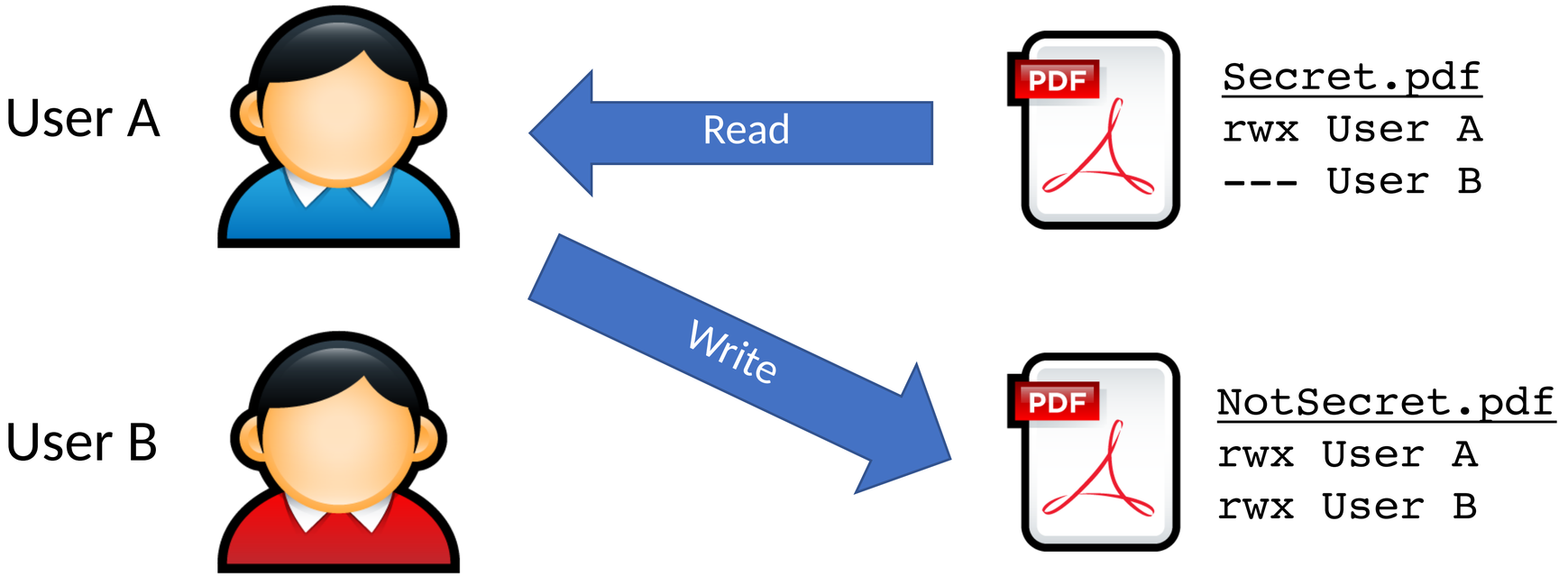
User B

Secret.pdf
rwx User A
--- User B

NotSecret.pdf
rwx User A
rwx User B

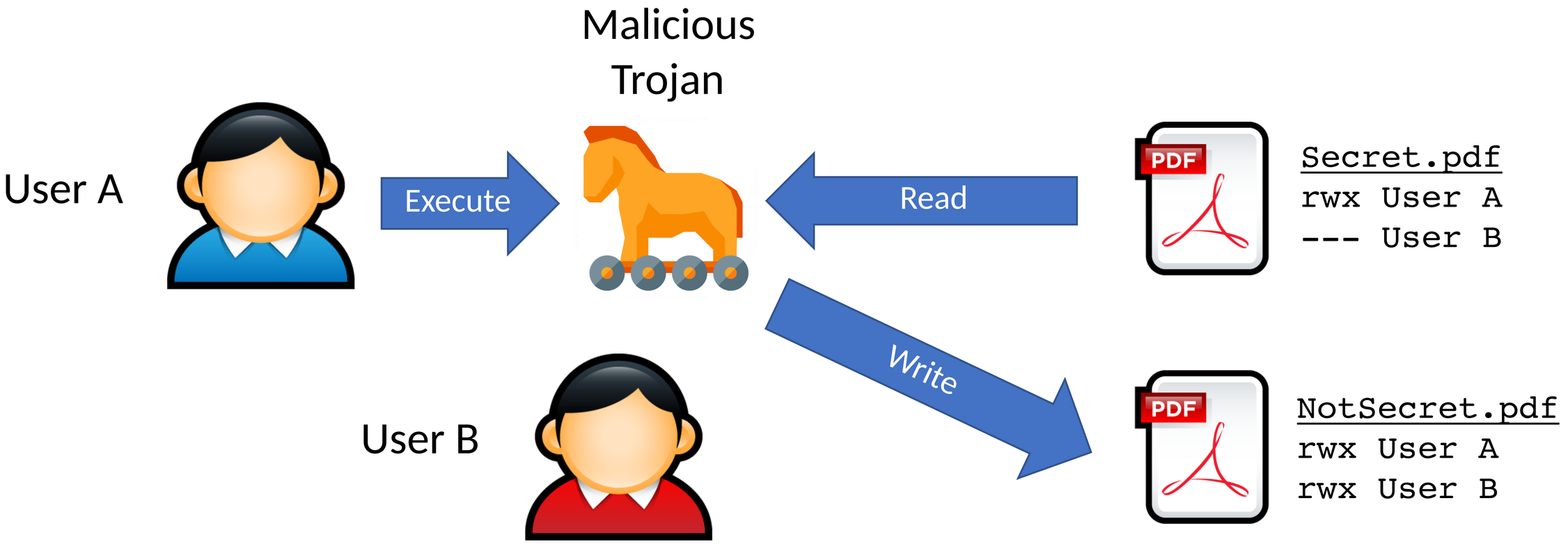
Failure of DAC

- DAC cannot prevent the leaking of secrets



Failure of DAC

- DAC cannot prevent the leaking of secrets



Mandatory Access Control

Mandatory Access Control Goals

- Restrict the access of subjects to objects based on a system-wide policy

Bell-Lapadula (1973)

“No read , no write ”

System Model:

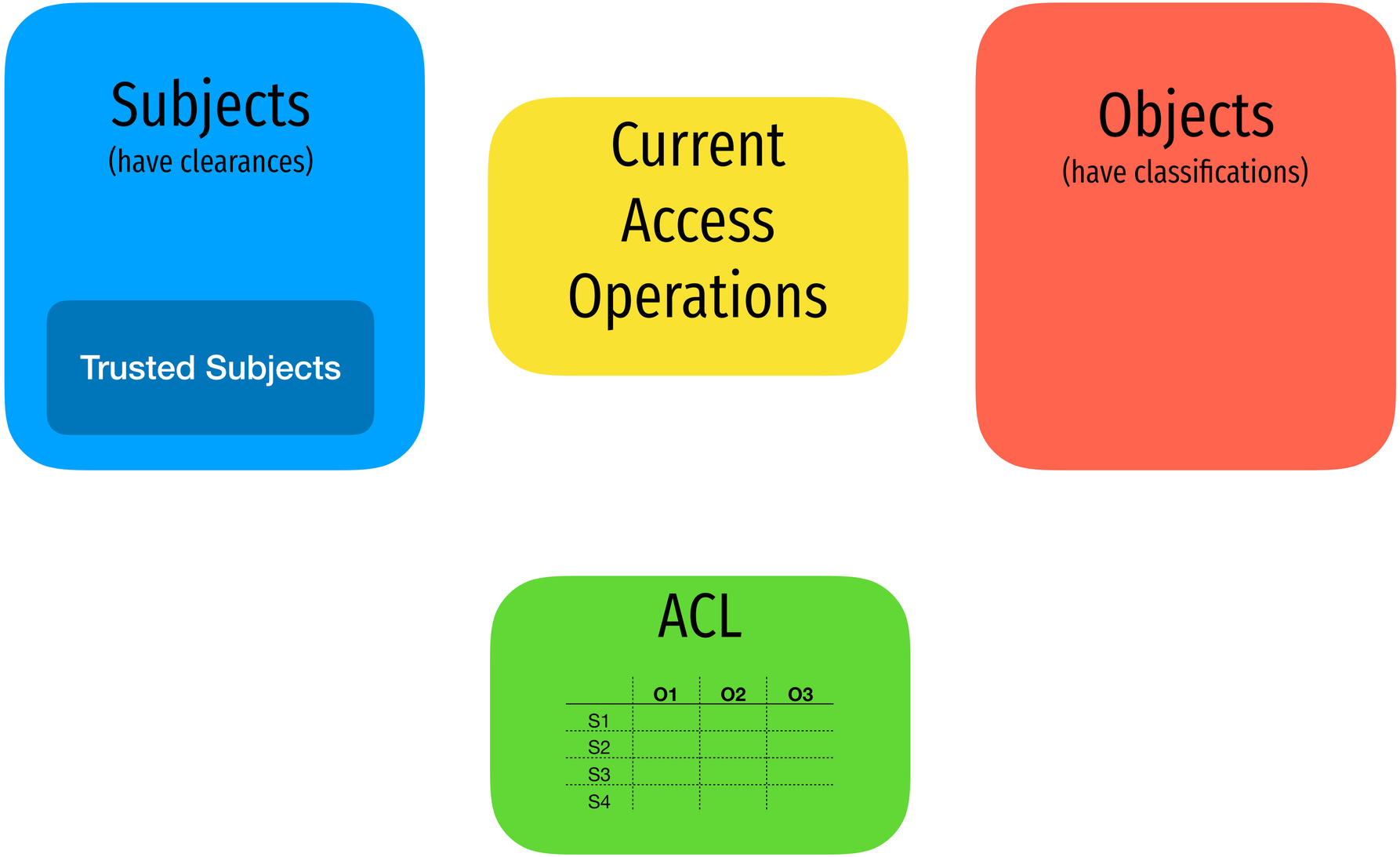
Security Policy:

BLP System Model

Clearances:

Classifications:

BLP System State



BLP Idea

A computer system is in a state, and undergoes state transitions whenever an operation occurs..

System is secure if all transitions satisfy 3 properties:

Simple:

Star:

Discretionary:

BLP Idea

A computer system is in a state, and undergoes state transitions whenever an operation occurs..

System is secure if all transitions satisfy 3 properties:

Simple: S can read O if S has higher clearance

Star: S can write O if S has lower clearance.

Discretionary: Every access allowed by ACL.

Users are trusted

Subjects are not trusted. (Malware)

Not Enough

TopSecret.pdf
rwx User A
--- User B

NotSecret.pdf
rwx User A
rwx User B

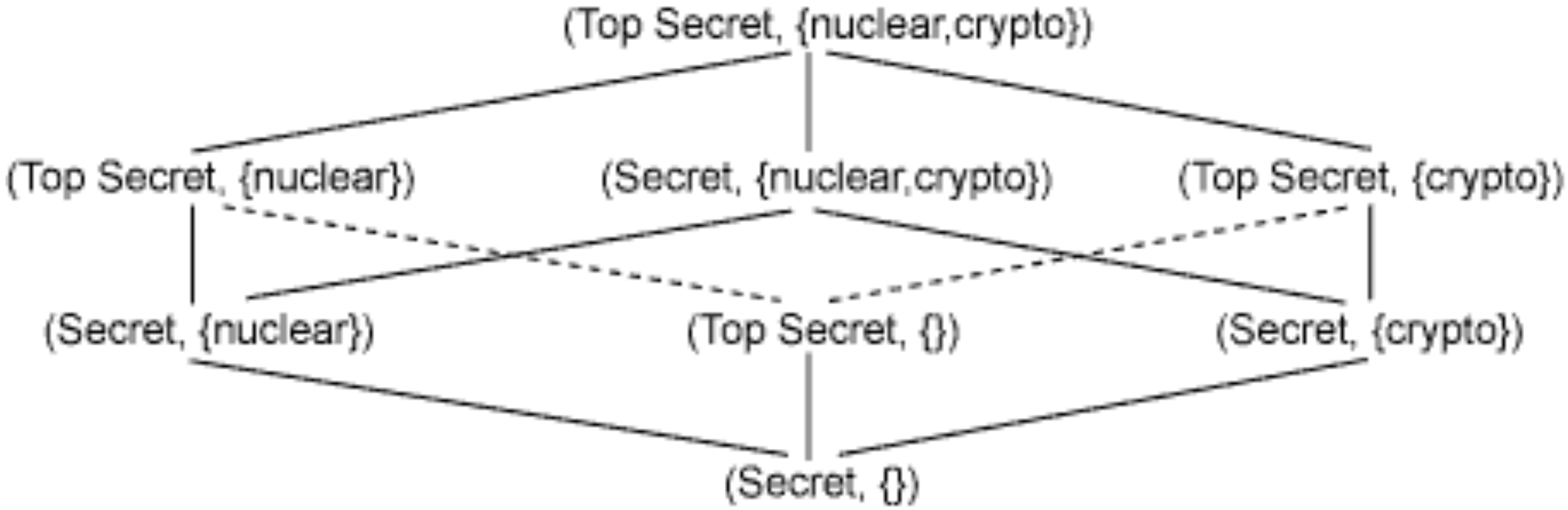
Not Enough: Covert channels

Security Lattice

Compartments:

Ordering between (Level, Compartment)

Lattice


(Top Secret, {nuclear,crypto})
(Top Secret, {nuclear})
(Secret, {nuclear,crypto})
(Top Secret, {crypto})
(Secret, {nuclear})
(Top Secret, {})
(Secret, {crypto})
(Secret, {})

Need-to-Know policy

Hybrid

SELinux, TrustedBSD: MAC + DAC system

Confidentiality? What else?

Biba Integrity Policy

Comparison

BPL

- Offers confidentiality
- “Read down, write up”
- Focuses on controlling reads
- Theoretically, no requirement that subjects be trusted
  - Even malicious programs can’t leak secrets they don’t know

Biba

Comparison

BPL

- Offers confidentiality
- “Read down, write up”
- Focuses on controlling reads
- Theoretically, no requirement that subjects be trusted
  - Even malicious programs can’t leak secrets they don’t know

Biba

- Offers integrity

Comparison

BPL

- Offers confidentiality
- “Read down, write up”
- Focuses on controlling reads
- Theoretically, no requirement that subjects be trusted
  - Even malicious programs can’t leak secrets they don’t know

Biba

- Offers integrity
- “Read up, write down”

Comparison

BPL

- Offers confidentiality
- “Read down, write up”
- Focuses on controlling reads
- Theoretically, no requirement that subjects be trusted
  - Even malicious programs can’t leak secrets they don’t know

Biba

- Offers integrity
- “Read up, write down”
- Focuses on controlling writes

Comparison

BPL

- Offers confidentiality
- “Read down, write up”
- Focuses on controlling reads
- Theoretically, no requirement that subjects be trusted
  - Even malicious programs can’t leak secrets they don’t know

Biba

- Offers integrity
- “Read up, write down”
- Focuses on controlling writes
- Subjects must be trusted
  - A malicious program can write bad information

Failures of Operation

Social engineering

Baiting

Very simple physical attack

1. Preload USB keys with malware
2. Drop the keys in public, near victims
3. Wait for victims to pick up and plug in
4. Victim executes malware
   - Either by accident due to curiosity
   - Or autorun by the OS (e.g. Windows)

Baiting

Very simple physical attack

1. Preload USB keys with malware
2. Drop the keys in public, near victims
3. Wait for victims to pick up and plug in
4. Victim executes malware
   - Either by accident due to curiosity
   - Or autorun by the OS (e.g. Windows)

Tailgating

Technique used by penetration testers

Goal: break in to a secure facility

- Security guards at the main entrance
- All doors have keycard access control

Idea:

1. Wait for an unsuspecting employee to open a door
2. Follow them inside
3. Leverages courtesy bias and ingroup bias