Lecture 1

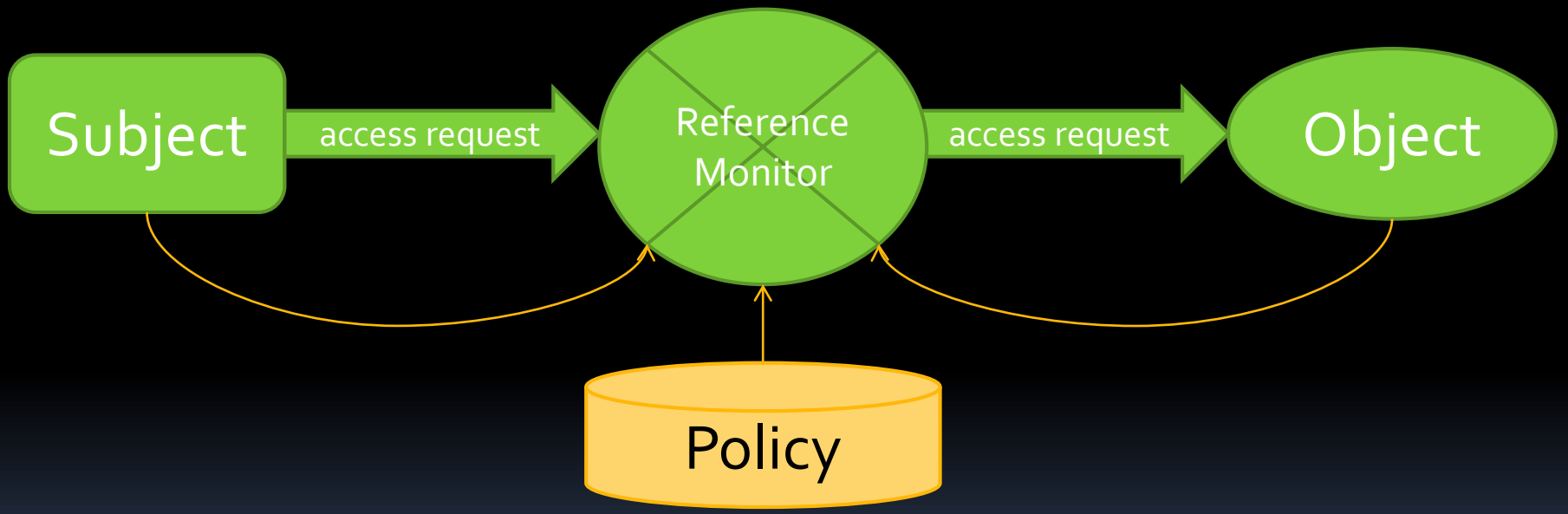
BASICS OF ACCESS CONTROL

You will be learning:

- Basic concepts of access control
- Examples of access control models (DAC, MAC, etc.)

Access control

Access control



Access control matrix

Describes the *protection state* of a system

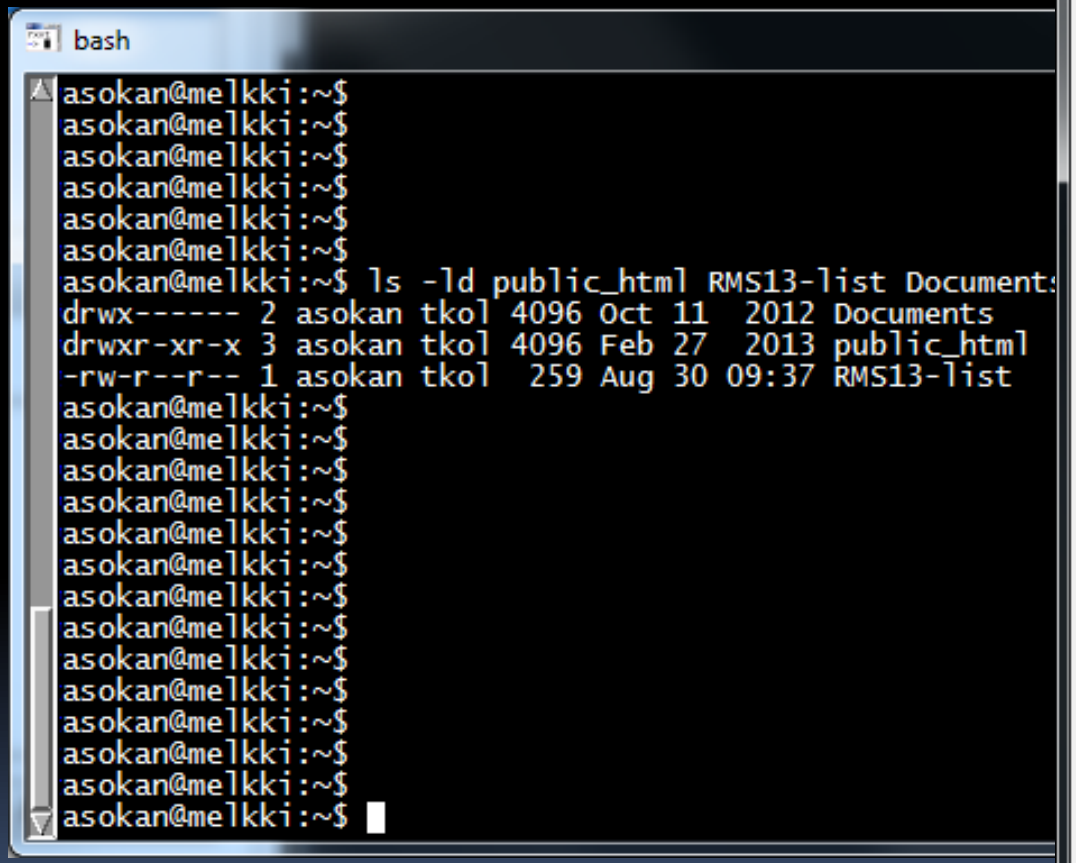
Object / ***Subject***	Documents	RMS13-list
asokan	read, write, enter	read, write
everyone-else	*none*	read

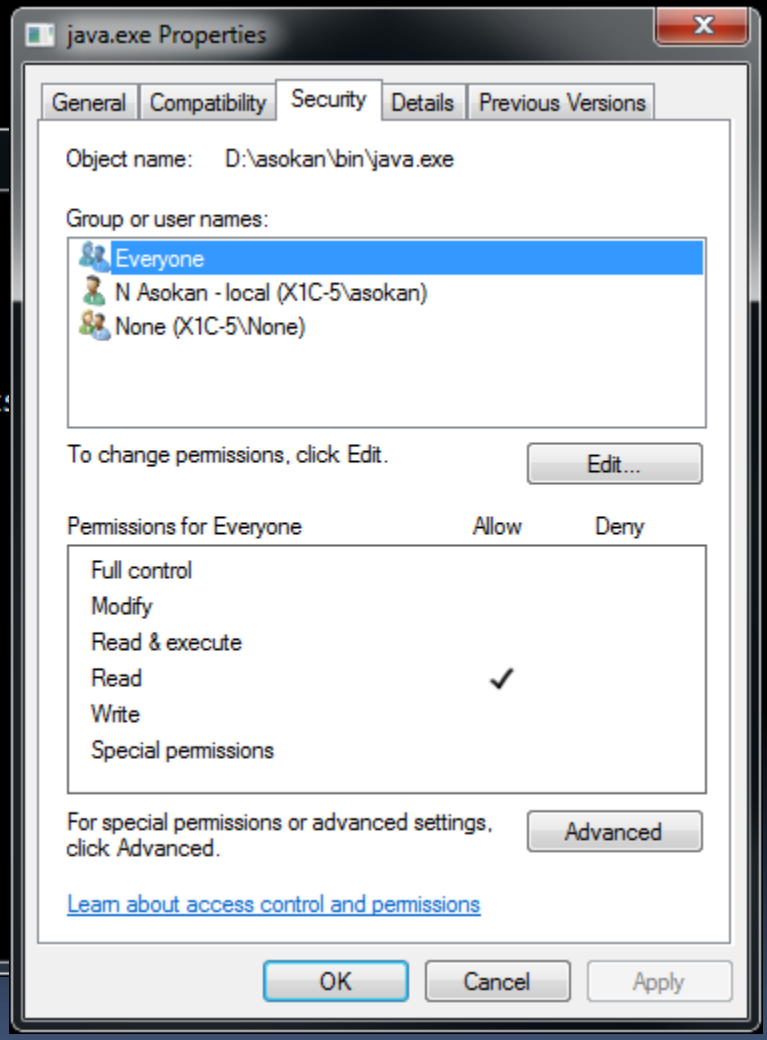
Object / ***Subject***	object1	object2
subject1	allowed ops	allowed ops
subject2	allowed ops	allowed ops

Capability list

Access control list (ACL)

ACL: examples





Access control policy models

Think about access control policies in real world

- Buildings, money, medical records, …
- Who has access? delegatable? who decides?

Access control in real world

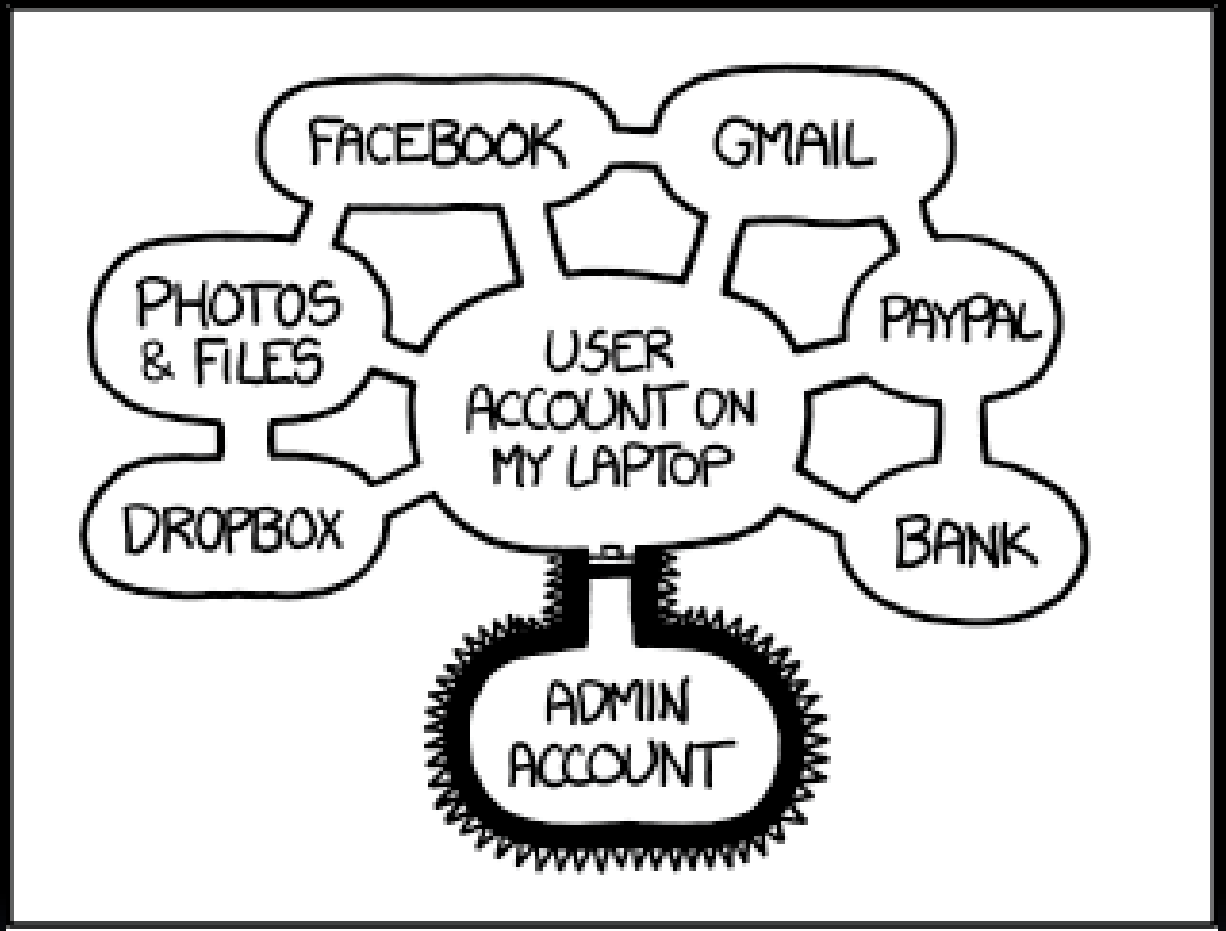
- Apartment in a residential building
  - Who has access (door keys)?
  - Delegatable? Who decides?
- Office door in business premises

Access control policy models

- Discretionary access control (DAC)
  - Subjects can delegate access
    - i.e., change protection state
- Mandatory access control (MAC)
  - Access policy decided centrally

Mandatory Access Control

- Subjects/objects assigned labels
  - labels of a subject ~ its "protection domain"
- Access policy specified in terms of labels
- Rules for relabeling

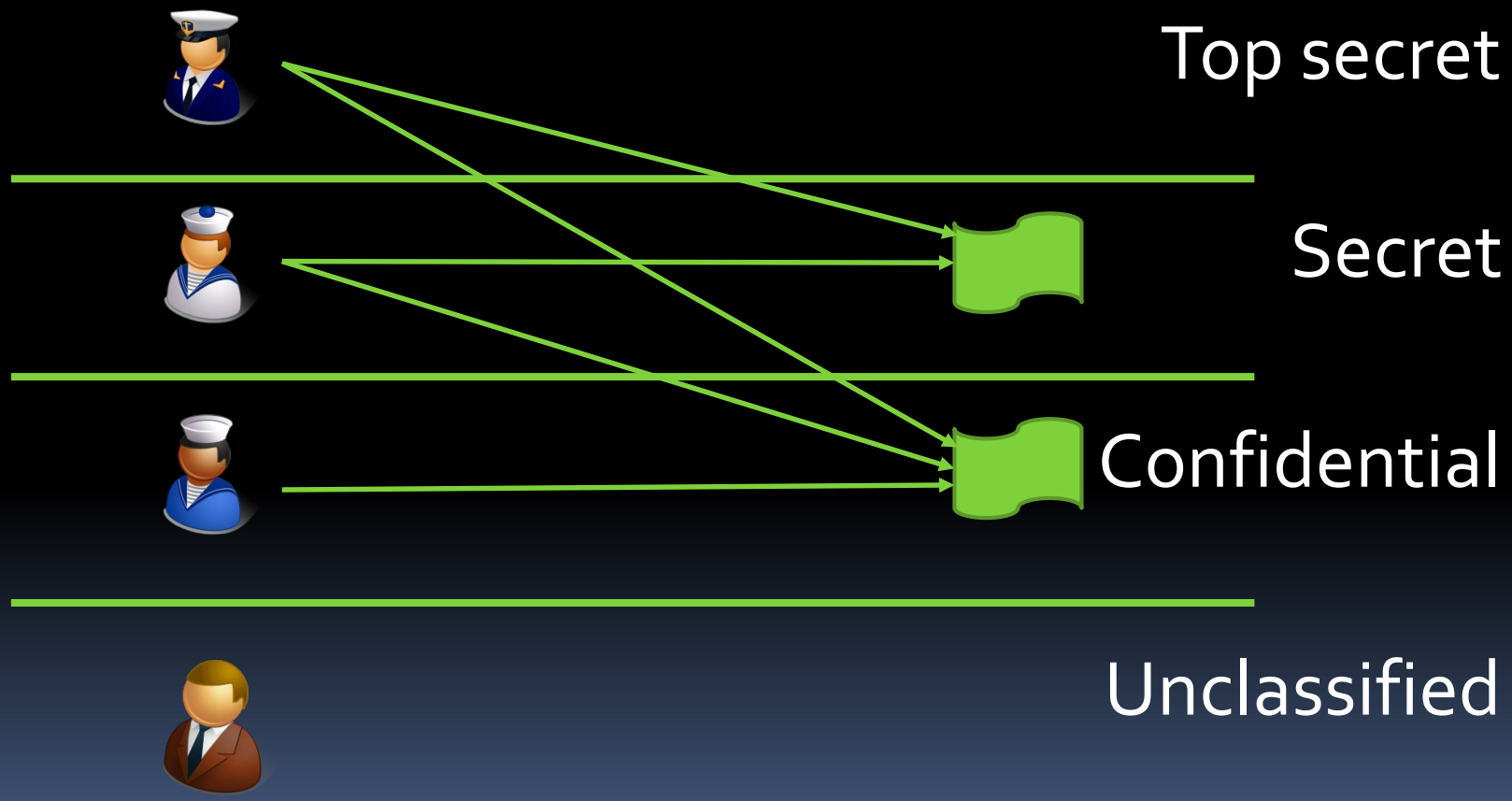


IF SOMEONE STEALS MY LAPTOP WHILE I'M LOGGED IN, THEY CAN READ MY EMAIL, TAKE MY MONEY, AND IMPERSONATE ME TO MY FRIENDS,

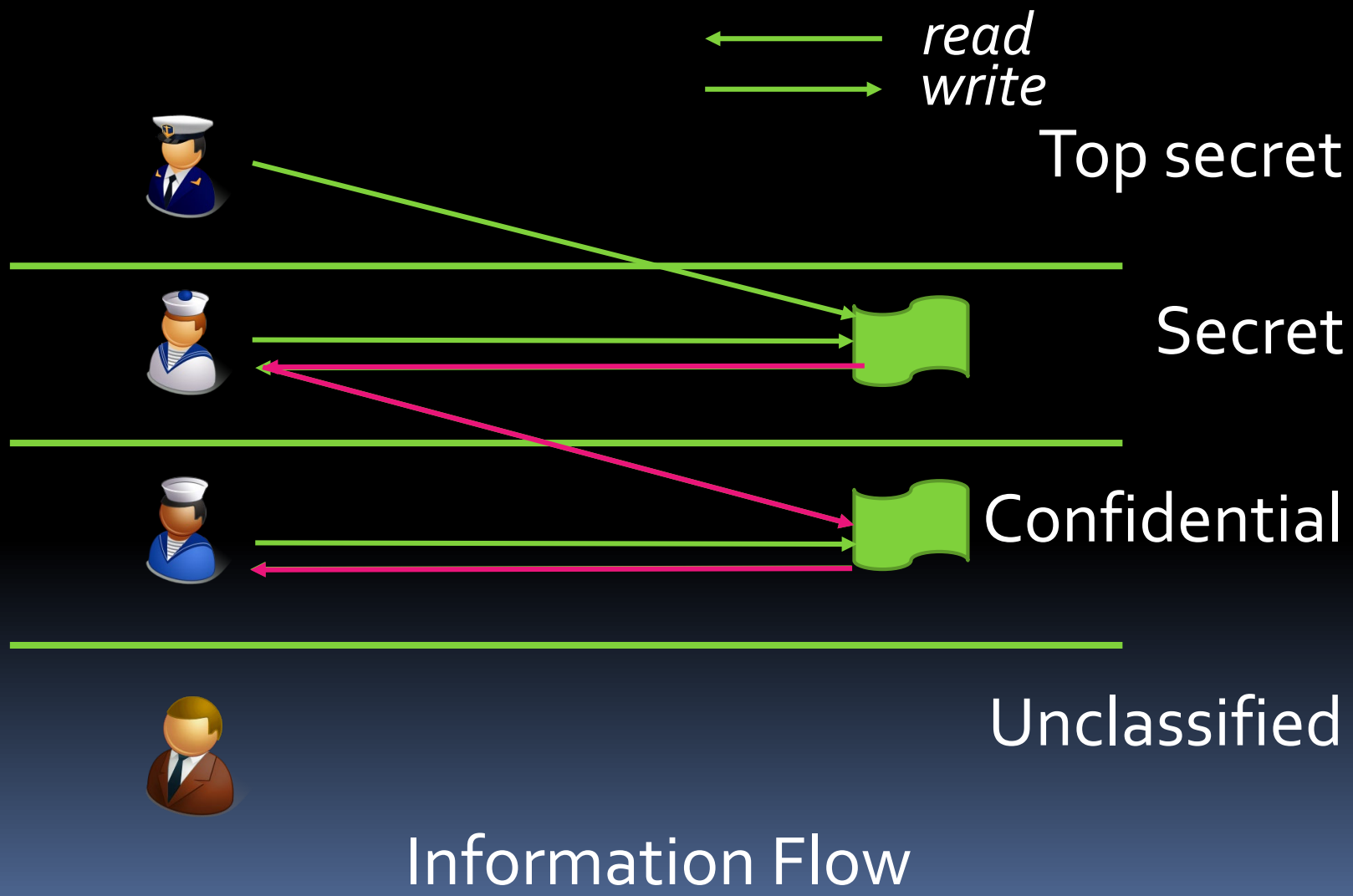
BUT AT LEAST THEY CAN'T INSTALL DRIVERS WITHOUT MY PERMISSION.

http://xkcd.com/1200/

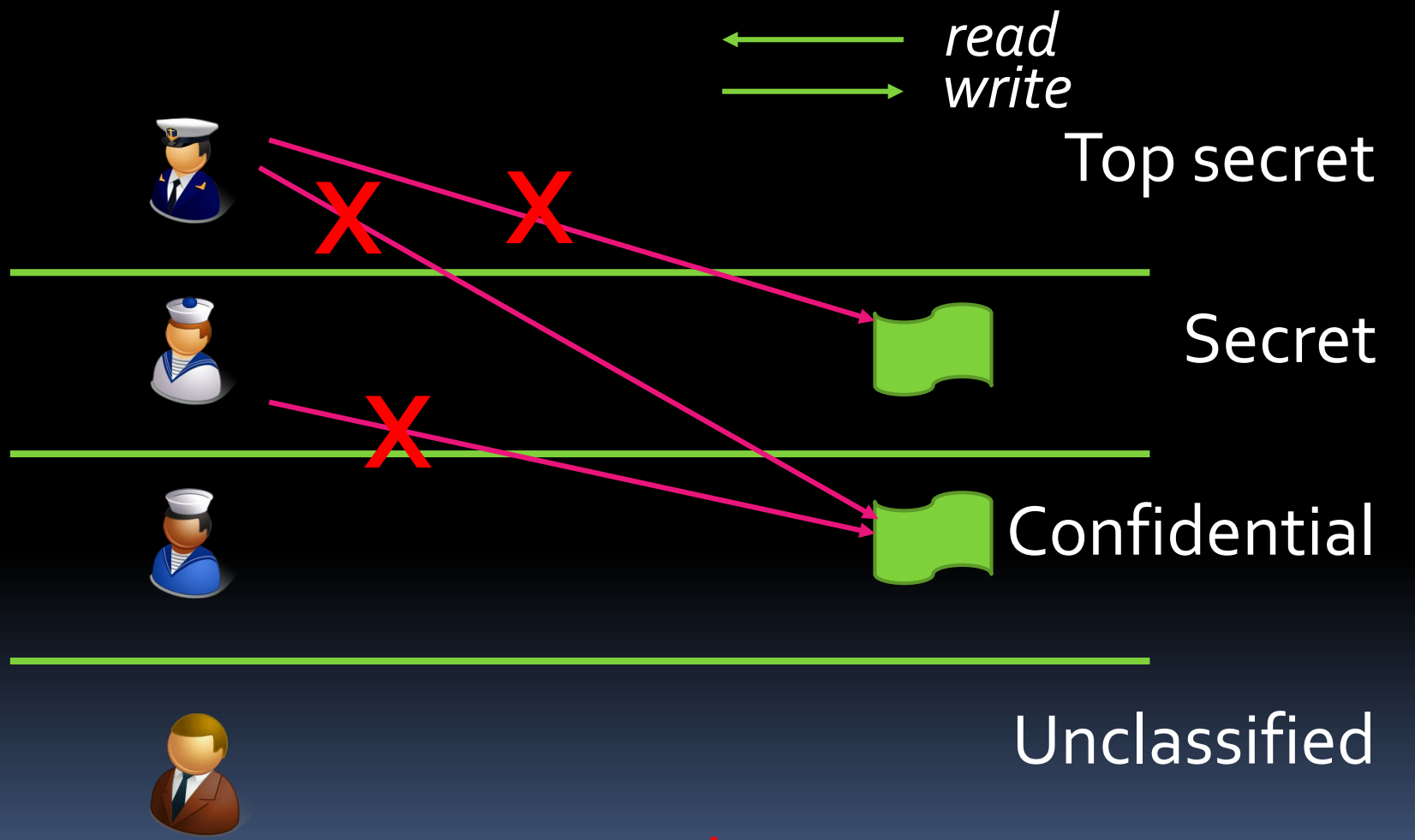
Example: Multi-level security



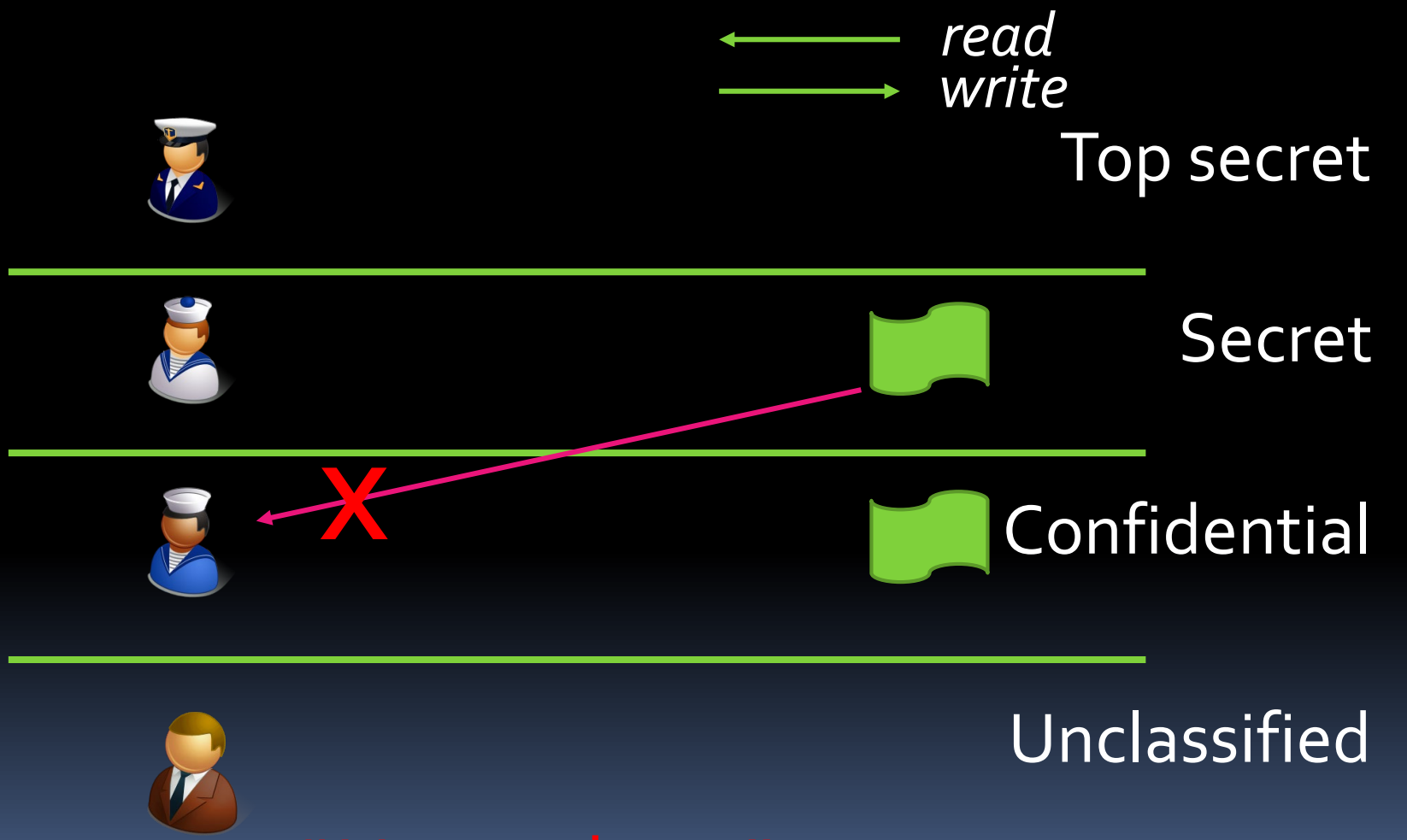
MLS for information systems



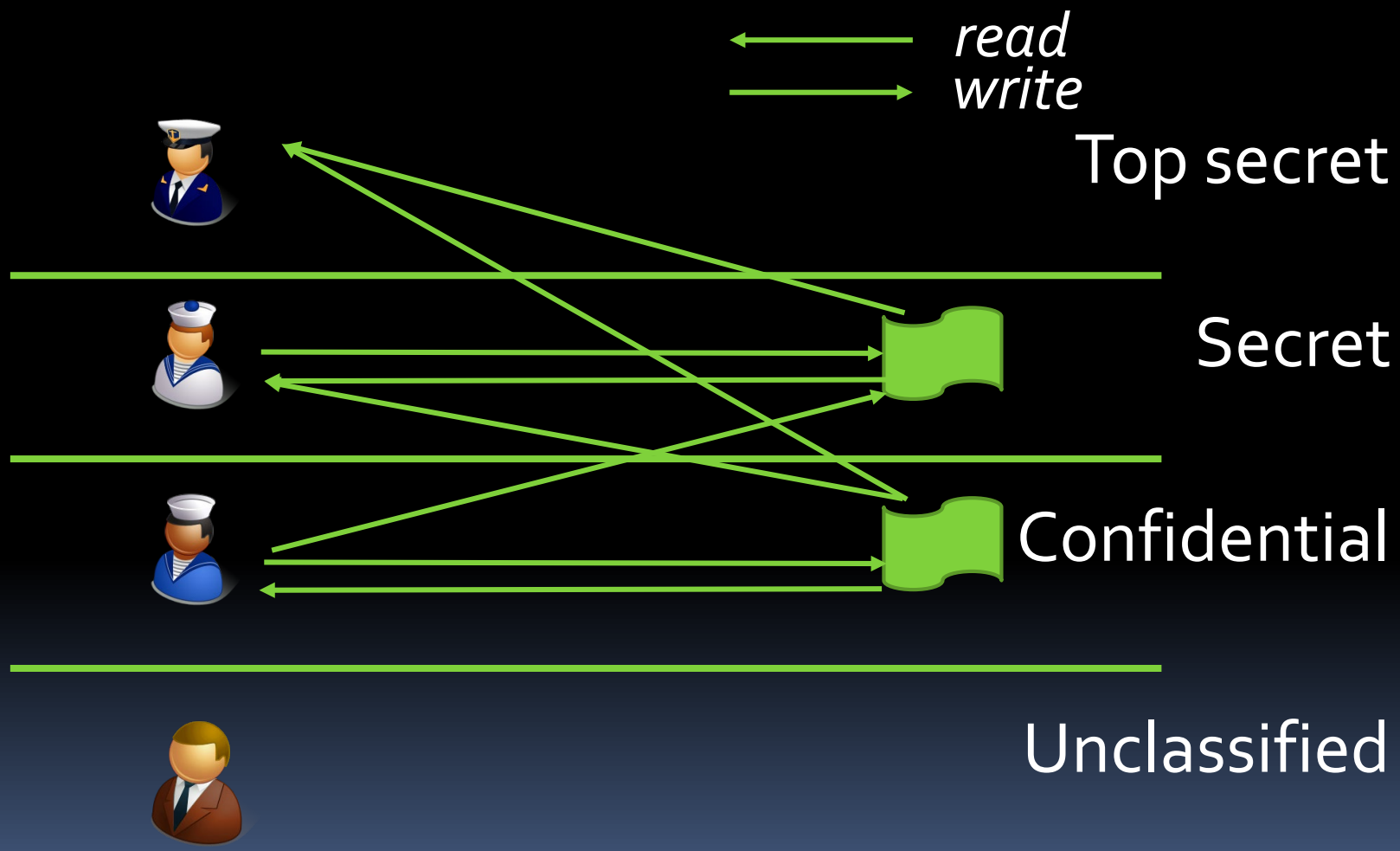
Bell-Lapadula (secrecy)



Bell-Lapadula (secrecy)



Bell-Lapadula (secrecy)



Bell-Lapadula (secrecy)

Simple Security Property:

- S can read from O *iff* L(S) ≥ L(O)
- "No reads up"

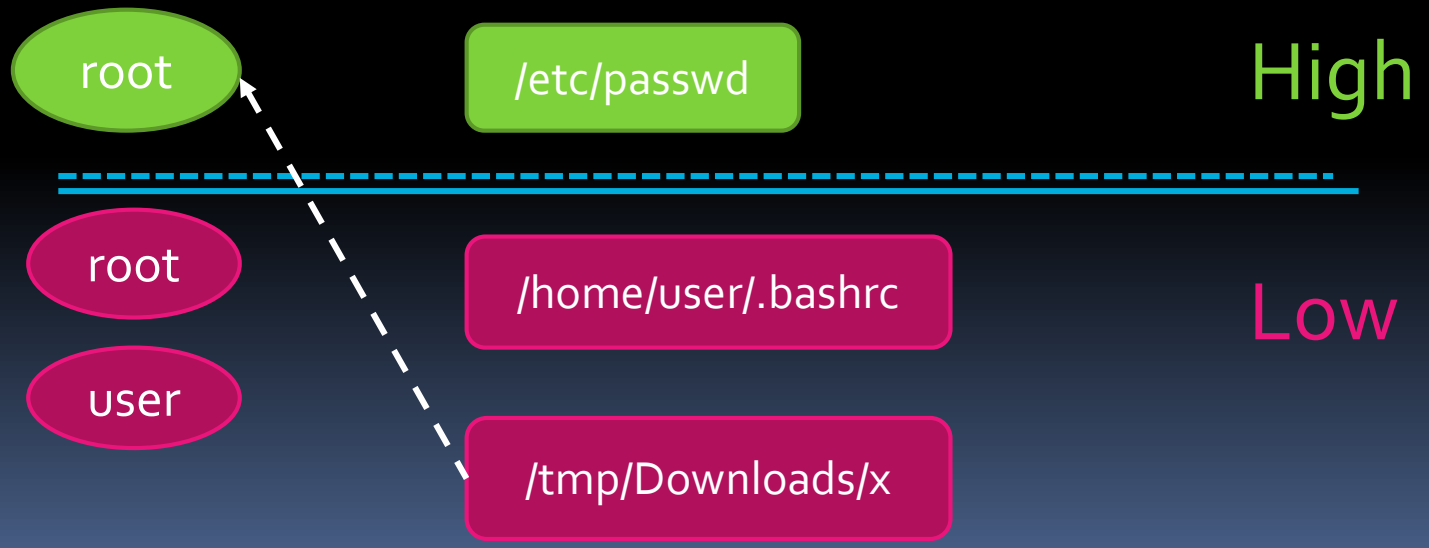
*-Security Property

- S can write to O *iff* L(S) ≤ L(O)
- "No writes down"

- Secrecy: information flows up, not down

Example: LOMAC

- Low-watermark MAC for integrity



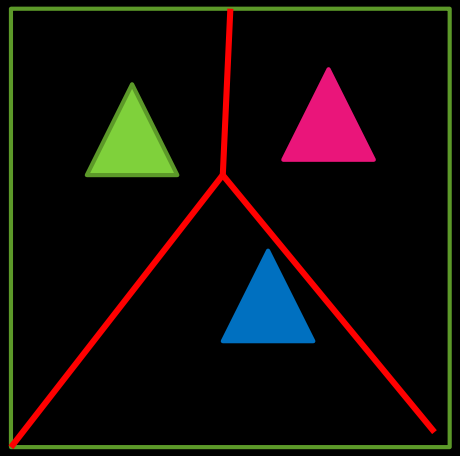
Example: LOMAC

- Low-watermark MAC for integrity
  - Integrity requirement:
    - No "Low" information can leak into "High"
  - Transition rule:
    - if "High" subject reads "Low" object, subject is demoted to "Low" for the rest of the session

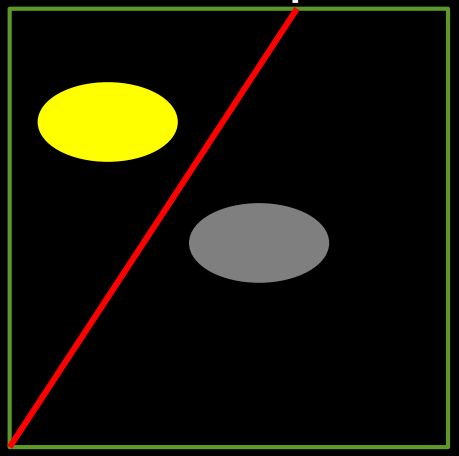
- "LOMAC" for secrecy?

Example: Chinese Wall

Banks

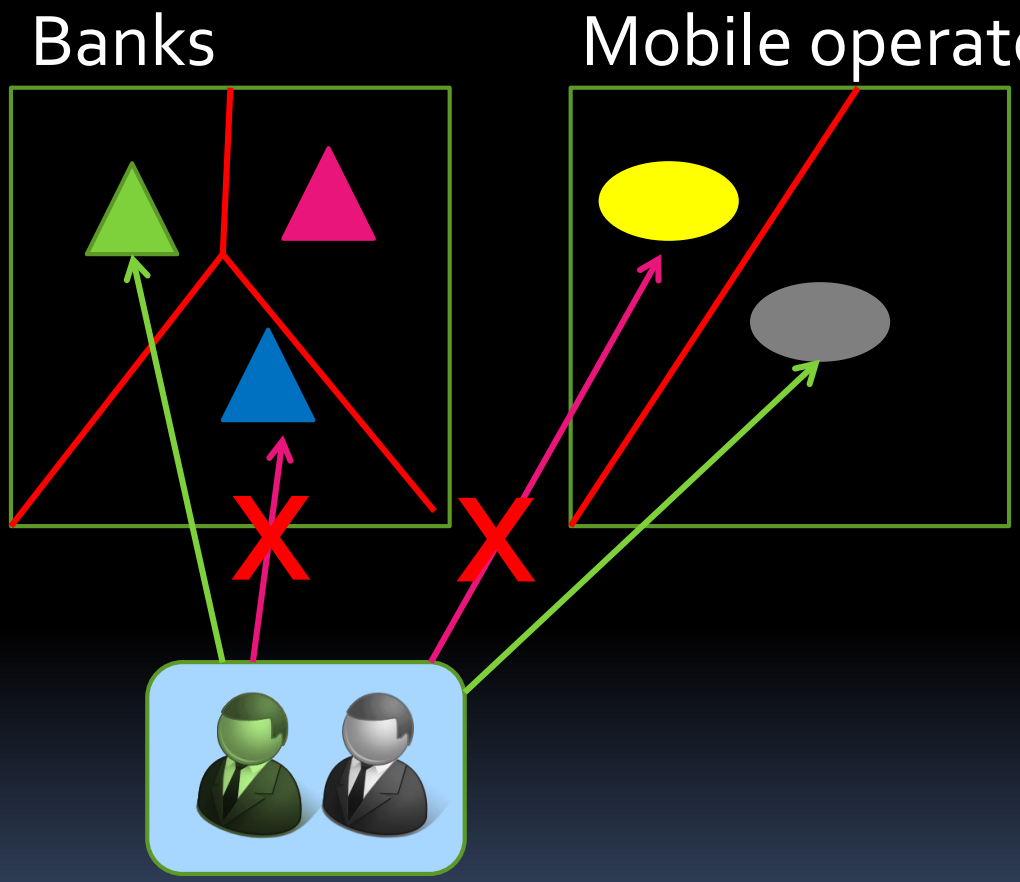


Mobile operators



conflict classes

Example: Chinese Wall



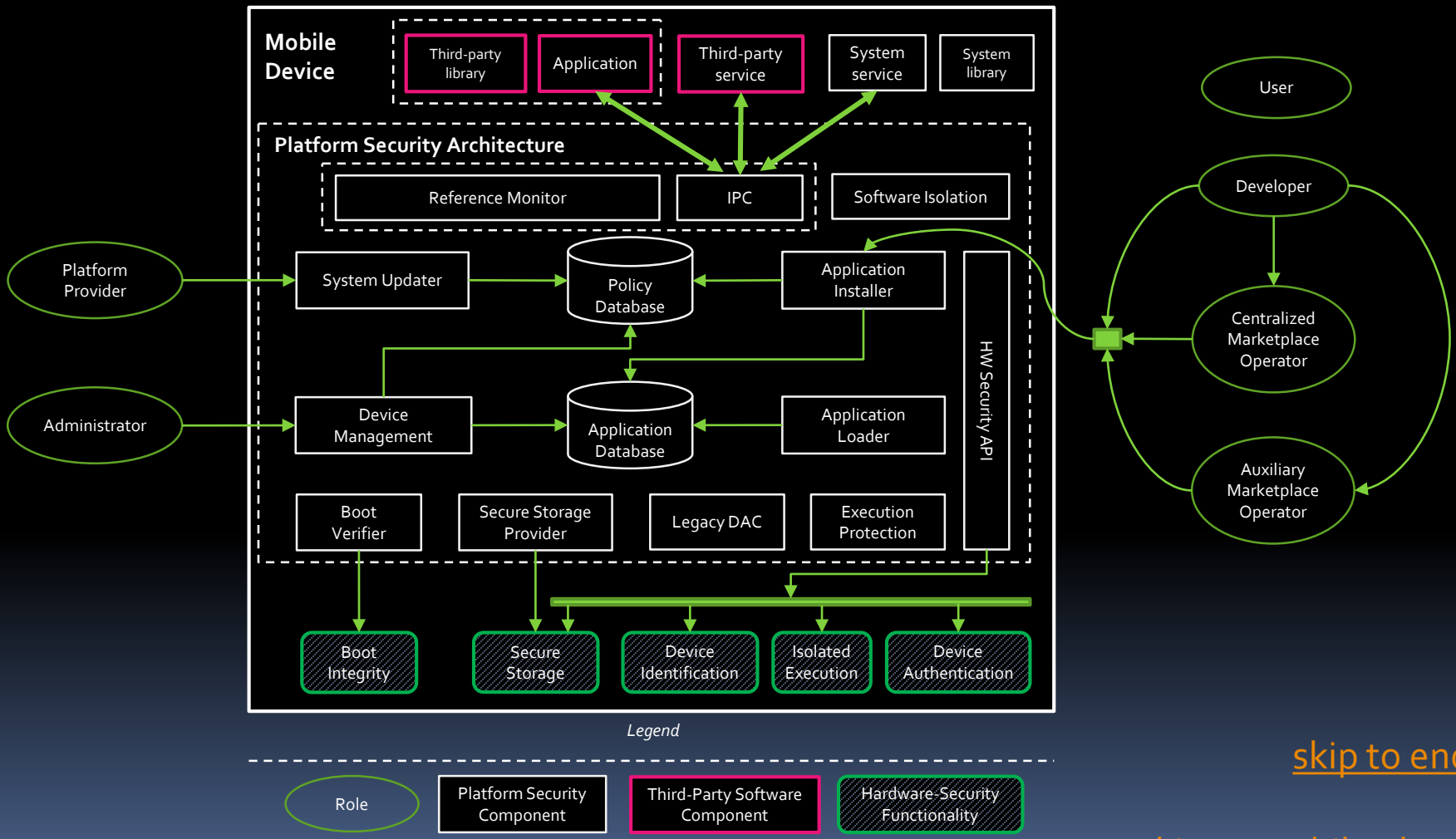
conflict classes

Mobile Platform Security

Some form of MAC required:

- Single user, but apps from many sources
- Sensitive resources (radio network, protected content)
- …

Mobile Software Platform Security



skip to end

skip to mobile platsec

Secure Operating System

Anderson: Computer security technology planning study*: 1972

A reference monitor must be:

1. tamper-proof
2. always involved ("Complete Mediation")
3. small enough to be tested

* until the US government finds a budget, try https://web.mit.edu/Saltzer/www/publications/protection/

Designing a protection system

The Protection of Information in Computer Systems, Saltzer & Schroder: (1975)

1. Simplicity of Design
2. Safe Defaults
3. Complete Mediation
4. Least Privilege

Designing a protection system

The Protection of Information in Computer Systems, Saltzer & Schroder: (1975)

5. Least Common Mechanism
6. Separation of Privilege
7. Open Design
8. Psychological Acceptability
9. [Justifiable Cost]

skip to mobile platsec

Complete Mediation

*"**Every access** to every object must be checked for authority."*

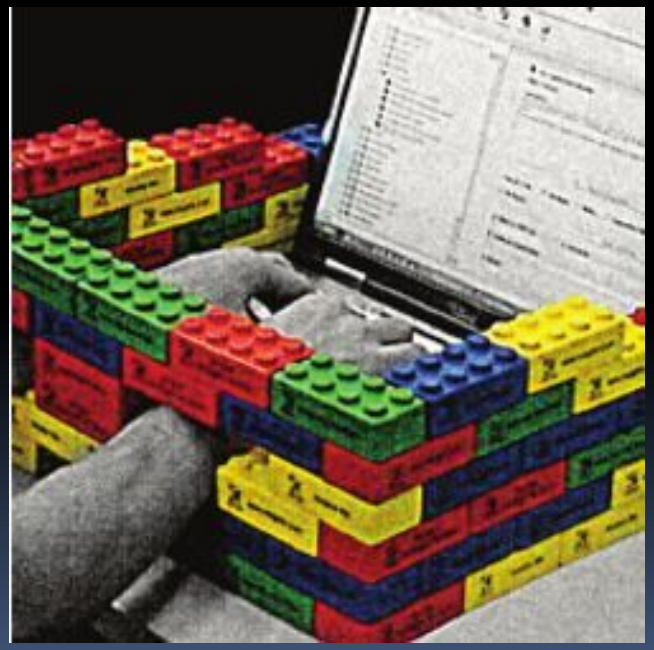
From Leendert van Doorn's Keynote at STC 2007

Least Privilege

*"Every program and every user of the system should operate using the **least set of privileges necessary** to complete the job."*

Psychological Acceptability

"It is essential that the human interface be designed for ease of use, so that ***users routinely and automatically apply the protection mechanisms correctly****."*



skip to end

From "Usable Security: How to Get it", Butler Lampson, CACM 52(11):25-27

Platform security for mobile devices

Mobile network operators;

1. Subsidy locks → immutable ID
2. Copy protection → device authentication, app. separation
3. …

Regulators;

1. RF type approval → secure storage
2. Theft deterrence → immutable ID
3. …

End users;

1. Reliability → app. separation
2. Theft deterrence → immutable ID
3. Privacy → app. separation
4. …

Closed → Open
Different Expectations compared to the PC world

Early adoption of platform security

Both IMSI and IMEI require physical protection.

Physical protection means that manufacturers shall take necessary and sufficient measures to ensure the programming and mechanical security of the IMEI. The manufacturer shall also ensure
(where applicable) remains secu

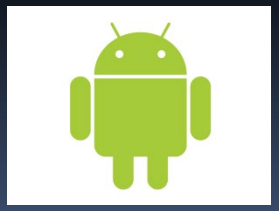
The IMSI is stored securely within the SIM.

The IMEI shall not be changed after the ME's final production process. It shall resist tampering, i.e. manipulation and change, by any means (e.g. physical, electrical and software).

NOTE: This requirement is valid for new GSM Phase 2 and Release 96, 97, 98 and 99 MEs type approved after 1st June 2002.

Different starting points:
widespread use of hardware and software platform security

~2001 ~2002 ~2005 ~2008



Did you learn:

- Basic concepts of access control
- Examples of access control models (DAC, MAC, etc.)

Contributors: N. Asokan

Plan for the course

- Lecture 1: Platform security basics
- Lecture 2: Case study – Android OS Platform Security
- Lecture 3: Mobile platform security
- Lecture 4: Hardware security enablers
- Lecture 5: Usability of platform security
- Lecture 6: Summary and outlook
- Lecture 7: SE Android policies
- Lecture 8: Machine learning and security
- Lecture 8: IoT Security