Lecture 3

Tuesday, 13 September 2022 10:38

today: Mandatory access control

recap: discretionary access control
→ permissions at discretion of resource owner
→ state transitions in access matrix based on commands
→ problem: DAC can leak rights due to e.g. Trojan horses
i.e. sensitive to privilege escalation

multi-level security
- Bell-LaPadula model → access should not flow to lower level security classes
- Biba model

multilateral security
- Chinese wall model

security classes consist of a
- security level
- category

this introduces a partial order on security classes, called dominance
→ this introduces a lattice with
- reflexivity
- transitivity
- antisymmetry
- least upper bound
- greatest lower bound

security classes are assigned to
- subject (level of clearance)
- object (sensitivity)

Bell-LaPadula (BLP) model: data should not flow to lower (or incomparable) security classes
→ can read on own level and below, write on own level and above

for subjects, we distinguish between current and maximum security classes (is lower bound)

a state is secure if, where:
- no read up
- *-property: no write down
- every access is allowed by the access matrix

Exercise: make an 'access matrix' for three classes: $TS \geq S \geq C$

Objects / Subjects	TS	S	C
TS	rw	r	r
S	w	rw	r
C	w	w	rw

problem: oftentimes, communication between subjects of different is not possible
→ Solution: allow users access system as low-classed subject (for a given session)
downside: assume user (e.g. admin) is trusted not to leak information

limitations: only focuses on confidentiality, not integrity
- assumes fixed rights
- vulnerable to covert channels

suppose that transitions can change security level of subjects & objects
assume that when a subject requests access, object + subjects are downgraded to lowest class

Secure in theory, not in practice

strong tranquility: subject + object do not change class during lifetime
weak tranquility: 'Subjects and objects do not change labels in a way that violates the "spirit" of the security policy'

BLP assumes strong tranquility property

another issue: low-level subjects can destroy high-level information
→ Biba model → prevent information flow to higher classes

similar to BLP-model, but with 'inverted' permissions (on integral levels)

rules: no read down
no write up

assumes strong tranquility

can be relaxed:
- either: low watermark for subjects → allow read down → but drops integrity level of subject → e.g. machine no longer safe after reading infected email
- or: low watermark for objects → allow write up → but drops integrity level of object → e.g. files written by viruses are considered unsafe and quarantined

---

combine models: needs independent secrecy and integrity levels
otherwise, could only read & write to own level

Objects / Subjects	$S_L I_L$	$S_L I_H$	$S_H I_L$	$S_H I_H$
$S_L I_L$	rw	r	w	—
$S_L I_H$	w	rw	w	w
$S_H I_L$	r	r	rw	r
$S_H I_H$	—	r	w	rw

---

multilateral security: goal → protect information from leaking between compartments at the same level

Chinese wall model: aims to prevent information flows that cause conflicts of interest

organize information in:
- basic objects
- company datasets
- conflict of interest classes

S can read O only if
- O is in a company dataset that S has already accessed
- or O belongs to a different conflict of interest class

problem: data from one COI class can be leaked via another

S can write only if
- access is permitted by the simple property
- no object can be read by S which is in a different company dataset to those for which write access is requested (optionally: and which contains unsanitized information)
→ to sanitize is to remove/anonymize corporate/identifying information, so that identity of company cannot be discovered

covert channel: channel which can be used to transmit information, although it is not intended for that

- timing (how long did a computation take?)
- power consumption
- resource consumption/exhausting/locking