OS Security

Stockholms universitet

Esmiralda Moradian
2021-12-02

Introduction

- OS goals
- Methods of protection
  - Physical separation
  - Temporal separation
  - Logical separation
  - Cryptographic separation

Memory and address protection

- Fence
- Relocation
- Base register
- Bounds register
- Tagged architecture
- Segmentation

Access control

- Directory
- Access control list
- Access control matrix
- Capability
- Passwords

Security Policies

- Defines what is allowed
- Security policy
  - Considers all relevant aspects of confidentiality, integrity and availability
  - Partitions a system into
    - Set of secure states
    - Set of non-secure state

Security policies (cont.)

Military security policy

Commercial security policy

Security model

- Provides a formal representation of a security policy or set of policies
- Indicate which rules decide who and in which way get an access to the information resources or resources that gives access to the information resources

The Bell-LaPadula Model (BLP)

- Was published in 1973
- Specifies multilevel security
- BLP consists of:
  - Subjects, denoted individually S
  - Objects passive entities, denoted O
  - The modes of access are represented by access attributes *x*
  - Four different access modes are defined in model:
    - e (execute)
    - r (read)
    - a (append)
    - w (write)

The Bell-LaPadula Model (BLP)

- BLP enforces 2 properties
  1. Simple security property (ss-property)(no read-up)
     - S can read O if and only if S dominates O and S has discretionary read access to O
  2. Star property (* property) (no write-down)
     - S can write to O if and only if *O* dominates S and S has discretionary write access to O

Biba model

- defined by Biba in 1977
- The model consists of:
  - A set S of subjects
  - A set O of objects
  - A set I of ordered integrity levels
- Uses a read up, write down approaches

•Clark-Wilson Integrity Model

- Address the security requirements of commercial applications
- Models
  - control of internal and external consistency
  - control of authorised users activities inside the system based on two key concepts:

  1. Well-formed transactions
  2. Separation of duty

Clark-Wilson Integrity Model

The elements of Clark-Wilson model

- Constrained data items (CDIs)
- Unconstrained data items (UDIs)
- Integrity verification procedures (IVPs)
- Transformations procedures (TPs)

•IVPs check that a system starts in a valid state that can only be changed by TPs.

•TPs are certified to preserve the validity of system states

- Enforces four separate, but related security properties, such as Integrity, Access control, Auditability , Accountability

Rule	Description
CR1	IVPs must ensure that CDIs are valid
CR2	TPs on CDIs must result in a valid CDI
ER1	Only certified TPs can operate on TPs
ER2	Users must only access CDIs through TPs for which they are authorised
CR3	Separation of priviledge & least priviledge
ER3	Users must be authenticated
CR4	TPs must be logged
CR5	TPs on UDIs must result in a valid CDI
ER4	Only administrator can specify TP authorisation

Certification rules (CR)
Enforcement rules (ER)

Chinese Wall Security Policy

- The goal of this model is to prevent a conflict of interest
- All corporate information objects are stored in a hierarchically arranged structure
- Three layers of abstraction
  - Objects: objects are items of information related to a company
  - Company group: objects concerning each corporation are grouped together in a company dataset (CD)
  - Conflict classes: datasets whose corporation are in competition, are grouped together in a conflict of interest (COI) class

Chinese Wall Model

- Mandatory rule for restricting read access:
  - Subject S can read object O only if
    1. O is in the same company dataset as an object already accessed by that subject (i.e. O is within the wall), or
    2. O belongs to an entirely different conflict of interest class
- The write rule:

1. S can read O by the read-rule, and
2. No object can be read which is in a different company dataset to the one from which access is requested and contains unsinitized information

The security kernel

- Security Kernel – responsible for enforcing security mechanisms of the entire OS
  - Coverage: ensure that every access is checked
  - Separation: security mechanisms are isolated from the rest of OS and from user space → easier to protect
  - Unity: all security mechanisms are performed by a single set of code → easier to trace problems
  - Modifiability: security mechanism changes are easier to make and test
  - Verifiability: formal methods, all situations are covered

Reference monitor

- Reference monitor: an access control concept that refers to an abstract machine that mediates all accesses to objects by subjects
- Collection of access controls for devices, files, memory and other objects
- Must be single point through which all access requests must pass
- Must be correct

Trusted Computing Base (TCB)

- Trusted Computing Base (TCB) is defined as a totality of hardware and software protection mechanisms responsible for enforcing the security policy of a given system.
- When is TCB monitors four basic interactions:
  - Process activation
  - Domain switching
  - Memory protection
  - I/O operations

Vulnerabilities

- User interaction
- Ambiguity
- Incomplete mediation
- Generality

Assurance methods

- Testing
- Penetration testing
- Formal verification
- Validation
- Evaluation

Thank you!