2110413 Computer Security

Lecture 3
Authorization and Policy

Krerk Piromsopa, Ph.D.
Department of Computer Engineering
Chulalongkorn University

- Definition
- Policy
  - Access Control Models
- Type Enforcement
  - Access Control Matrix (ACLs, Capabilities)
- Security Models
  - Multilevel Security
  - Multilateral Security

Authorization

Honesty is the best policy
Italian Proverb

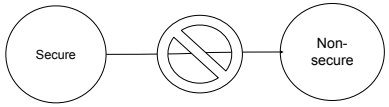
- Application specific
- What to control (Policy)
- How to control (Type Enforcement)

Policy

- "It is a definite course or method of action selected from among alternatives and in light of given conditions to guide and determine present and future decisions" – [Merriam-Webster online Dictionary]
- A security policy is a statement that partitions the states of the system into a set of authorized, or secure, states and a set of unauthorized or insecure, states. – [BISHOP].

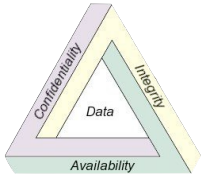
Secure System

- A secure system is a system that starts in an authorized state and cannot enter an unauthorized state. – [BISHOP]



Authorized and Unauthorized

- Commonly partitioned using two properties of data
  - confidentiality
  - integrity
- Availability (e.g. Fault Tolerant)
- Data
  - sensitive information, secrecy, and privacy



Confidentiality and Integrity

- Confidentiality is the obligation to confine or protect data from being access by unauthorized person. In another word, only the right person can access the data. (Who can read the data?)
- Integrity is the condition of being unimpaired. In this context, it simple means that data is not being altered by unauthorized user. (Who can alter the data?)

Access Control Models

- Mandatory Access Control (MAC)
  - Principle: Users are untrustworthy and must be controlled.
- Discretionary Access Control (DAC)
  - Principle: Users are responsible for their own data.
- Role-Based Access Control (RBAC)
  - Principle: least privilege.

MAC

- multilevel systems
- e.g. classified government and military information
- Sensitivity labels (for all subjects and objects)
- Controlling the import of information from other systems and export to other systems

DAC

- File and data ownership
- Access rights and permissions

Role-based

- Access only when needed to perform a certain function.
- Primarily granted permission based on purpose.

Pop Quiz

- Name the access control model behind these systems
  - File permission on UNIX, Windows
  - SELinux, TrustedBSD, Trusted Solaris
  - sudo (superuser do) Unix program

Comparison

- Unix
  - r - read
  - w - write
  - x - execute (program)
  - x - search (directory)
- Windows (NTFS)
  - read
  - write
  - execute
  - delete
  - change permission
  - change ownership

Type Enforcement

Subjects ↓ / Objects →	Print Document	Create Document	Pay Bill	Account Admin	Configure Network
Administrators	✓			✓	✓
Owner	✓	✓			
Remote Users	✓				
Managers	✓		✓	✓	

Unix File permission ?
Windows File permission?

- Access Control Matrix
  - Label subjects
  - Label resources
  - Specify the rules
- Access Control List
- Capabilities

ACL v.s Capability

- ACL
  - Associate with object
  - Object got a list of who can do what with the object.
- Capability
  - Associate with subject
  - Think of capability as a token for key.
  - Granting a permission is passing a key to another person.

Pro and Cons

- ACL
  - Easy to implement
  - Which files do I have access on this system?
- Capabilities
  - ?
  - ?

What do you think?

- A superuser can access every file in a system (including files that he/she does not created). Do you think it is correct?
- Your favorite word processor can open arbitrary files that are accessible by you (including binary files). Thus, your word processor is basically you. Does it sound right?

What to do with it?

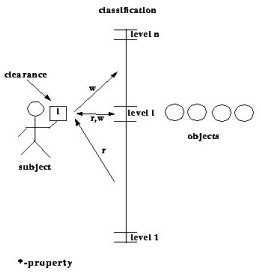
Security Models

- a high-level concept to ease understanding and specifying policy
- a generic framework for dictating a policy system
- Two general frameworks
  - Multilevel Security
  - Multilateral Security

Multilevel Security

- Within an organization
- MAC
- Bell Lapadula
- Biba

Bell-LaPadula



- Principle:
  The system may leak the information.
- classification of military and intelligence data
- High Watermark
- Properties
  - The simple property: no process may read data at a higher level. This is also known as ***no read up*** (NRU).
  - The *-property: no process may write data to a lower level. This is also known as ***no write down*** (NWD).
  - The tranquility property states that the security level of an object cannot be changed while it is being processed by a computer system. (***Declassify***)

Biba

- Principle:
  Information flowing from lower level may be malicious to the system.
- integrity, ignore cofidentiality
- Low Watermark
- Bell-LaPadula upside down
  - ***Never read down or write up***

Multilateral Security

- Between departments
- China Walls model
  - internal rules in a financial firm. The idea is that if a person is recently working for a company in certain sector, this person then cannot work for another company in this sector for a certain period of time.
- Privacy.

More Examples

- Reverse Engineering of Software.
  - Team A studies the software and writes a specification.
  - Team B uses specification to create a new software.

Put it all together

- Analyze a security model (e.g. Bell-Lapadula, Biba, China wall, etc.) of your system.
- Use the model to create a security Model (e.g. MAC, DAC, Role-based)
- Translate it into Access Control Matrix
- Implement a security using the appropriate type enforcement. (e.g. ACL, Capability)

Term Report

Select one for your team

- Kerberos
- RADIUS
- NIS (Sun YP) and NIS+
- LDAP
- MS. Active Directory
- MS. Passport vs. Open ID (and similar tech.)
- SSL/TLS
- TCPA & DRM
- SELinux
- TrustedBSD

What to include in the report?

- 3-4 pages (format will be provide)
- Overviews (General Concepts)
- Protocol/Specification
- Usages
- Does it Secure?
- Possible Attacks or possible workaround.
- Analysis (Pros and Cons) i.e. Will you use it? Why?
- References
- Due last day of class