Usage Control Model (UCON)

MCS 7102 Data Security and Privacy

Lecture 4

3rd September 2024

Introduction

- Origin
  - Since the advent of timesharing system
- Main goal is to selectively determine:
  - who can access services, resources, and digital content
  - what access is exactly provided

Evolvement of AC Models

- Identity-based
  - AC Matrix, DAC, etc
- Label-based
  - MAC
- Function/duty/task/role-based:
  - RBAC, etc
- Attribute-based:
  - UCON
  - DRM
  - Trusted Management

Scenario

- Need for persistent protection of digital information even after dissemination
  - Recent interest is driven by digital rights management (DRM).
  - Access control and trust management have significant relevance to this problem.
  - Develop a conceptual framework called Usage Control (UCON) for this problem that unifies Traditional Access Control, Trust Management and DRM

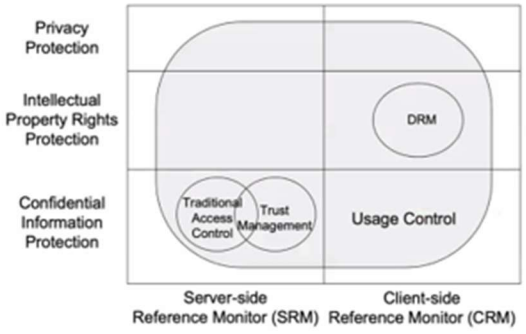
- Traditional Access Control
  - to protect computer/information resources by limiting known users' actions or operations within a closed system.
- Trust Management
  - deals with authorization process in distributed systems environment for the access of unknown users
- Digital Rights Management
  - mainly focus on intellectual property rights protection

Digital Rights Management (DRM)

- Superdistribution
- It's a system, a technology, a service, an application software, and a solution
- No concrete definition.
  - Many interests' groups, many vendors, many solutions, but no standards
- Controlling and tracking access to and usage (including dissemination) of digital information objects
- Securing digital object itself, not the transmission
  - By using cryptographic, and watermarking technologies
- Business perspectives
  - Not just for protections, but new business models
  - Increased revenue

- Problem-specific enhancement to traditional access control
- Enables controls on usage of digital objects at client-side by utilizing Client-side reference monitor
- Mainly focus on intellectual property rights protection.
- Architecture and Mechanism level studies, Functional specification languages –Lack of access control model

UCON Coverage



- Protection Objectives
  - Confidential information protection
  - IPR protection
  - Privacy protection
- Protection Architectures
  - Server-side reference monitor
  - Client-side reference monitor

Control Domain

- Control domain is an area of coverage where rights and usage of rights on digital objects are controlled
- Control Domain usually facilitates a kind of reference monitors;
  - Server-side Reference Monitor (SRM)
  - Client-side Reference Monitor (CRM)
- Server is who provides a digital object and client is who receives/uses the digital object

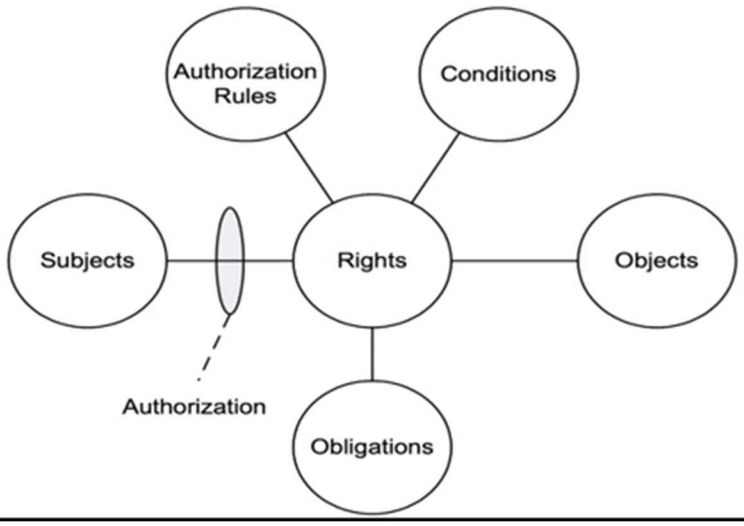
Control Domain w/ Server-side Reference Monitor (SRM)

- Control domain w/ SRM facilitates a central means to control subject's usage on objects of the domain on behalf of a provider subject.
- Subject can be either within same network /organization area or outside the area
- Digital information can be stored either centrally or locally.
  - If DO can be saved at client-side non-volatile storage, it means the changes on the saved DO doesn't have to be controlled (only server-side DO is valid) and freely allowed (bank statements).
  - To be centrally controlled, DO always has to be stored at server-side storage.
- Access control and trust management belong here.

Control Domain w/ Client-side Reference Monitor (CRM)

- No central control authority (SRM) exists.
- Client-side Reference Monitor (CRM) is to verify access on behalf of provider subject (ex., author, dept, company, publisher, re-distributor)
- The control mechanism is likely to be a distributed one
- Disseminated digital information can be stored either centrally or locally
  - If an object is saved at local non-volatile storage, the changes on the object can be controlled (blocked or allowed)
- DRM belongs here

UCON MODEL COMPONENTS



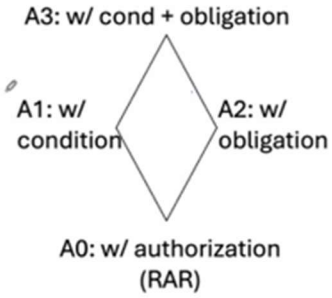
Subjects and Objects

- Subjects
  - Subjects are entities associated with attributes, and hold and exercise certain rights on objects
    - Attributes: identity, role, credit, membership, security level, etc.
    - Subjects : user, process
  - Consumer, Provider, Identifiee subjects
    - Identifiee subjects: identified subjects in digital objects that include their privacy-sensitive information. (patients in health care system).
- Objects
  - Objects are entities that subjects hold usage rights on.
  - associated with attributes, either by themselves or together with rights.
  - Privacy non-sensitive vs. privacy sensitive objects
  - Original vs. derivative objects
    - A derivative object is created in consequence of obtaining or exercising rights on an original object. (usage log, payment information, etc.)

Authorization Rules, Conditions, and Obligations

- Authorization Rules
  - a set of requirements that should be satisfied before allowing access to or use of digital objects
    - Rights-related Authorization Rule (RAR)
    - Obligation-related Authorization Rule (OAR)
- Conditions
  - A set of decision factors that the system should verify at authorization process along with authorization rules before allowing usage of rights on a digital object
    - Dynamic condition (stateful)
    - Static condition (stateless)
- Obligations
  - A list of mandatory requirements that a subject has to do to obtain or exercise rights on an object.

Authorizations in UCON



- A0: Traditional Authorizations (traditional access control, trust management, etc.) belongs here.
- A1: This provides finer-grained authorization.
- A2: This can provide better enforcement on exercising usage rights for both provider and consumer sides.
- A3: DRM's authorization can be here.

A0: w/ Rights-related Authorization Rule

- Subjects (S), objects (O) and objects with rights (O + R) can be associated with certain attributes (At).
- In UCON A0, authorization process can be done in three ways based on the kinds of attributes used in authorization rules (AR).
  - Case 1: R(S,O) = AR(At(S), At(O))
  - Case 2: R(S,O) = AR(At(S), At(O + R))
  - Case 3: R(S,O) = AR(At(S), At(O + R)) + AR(At(S), At(O))
- R(S,O) means a set of authorized rights for S on O.

A1 Examples (w/ Conditions)

- Conditions are used to restrict a location of usage, time period, frequency, etc.
  - In military system, officers can print certain documents to only on-site printer and during office hours.
  - In digital library system, members can download certain e-books, but they are allowed to read the books only on a machine with pre-defined cpu-id.
  - In Video on Demand (VOD) service, children are allowed to watch one movie per day during daytime only.

A2 Examples (w/ Obligations)

- Obligations are what has to be fulfilled for authorizations.
  - In digital library system, users may have to read (click) license agreement or non-disclosure agreements before exercising usage rights
  - Users may have to provide usage log information after exercising usage rights
  - Anyone can download free e-books, but he has to provide his personal information (by filling out a form)

A3 Examples (w/ Conditions & Obligations)

- A consolidated model
  - Certain information can be read during office hours and usage logs have to be reported
- Conditions can be applied for either obligations or authorizations.
  - In military, officers are allowed to read certain documents only on-site, but if it's not office hours, they have to provide usage log information or fill out an access approval code
  - In digital library, anyone can download free e-books, but if it's not on-site they have to pay $2 per download

Conclusion and Future Works

- UCON is a a generalized and unified framework that enables controlling usage of digital information for confidential information protection, intellectual property rights protection, and privacy protection in a systematic manner
- UCON enables finer-grained controls on usage of digital information even after digital information is disseminated regardless of system (computer or network) environments
- The details of the model have to be developed
- Delegation and administration issues have to be studied

Assignment

- Search for articles on Usage control on cloud systems within a 10 year period from this year.
- Read and do a synthesis and write down your summarize your findings based on what the conclusion of authors and future work.
- Submit on MUELE in by 17th September 2024 2359hrs