Usage Based Access Control Model (UCON)

KHT-Applied Information Security Lab (AIS)

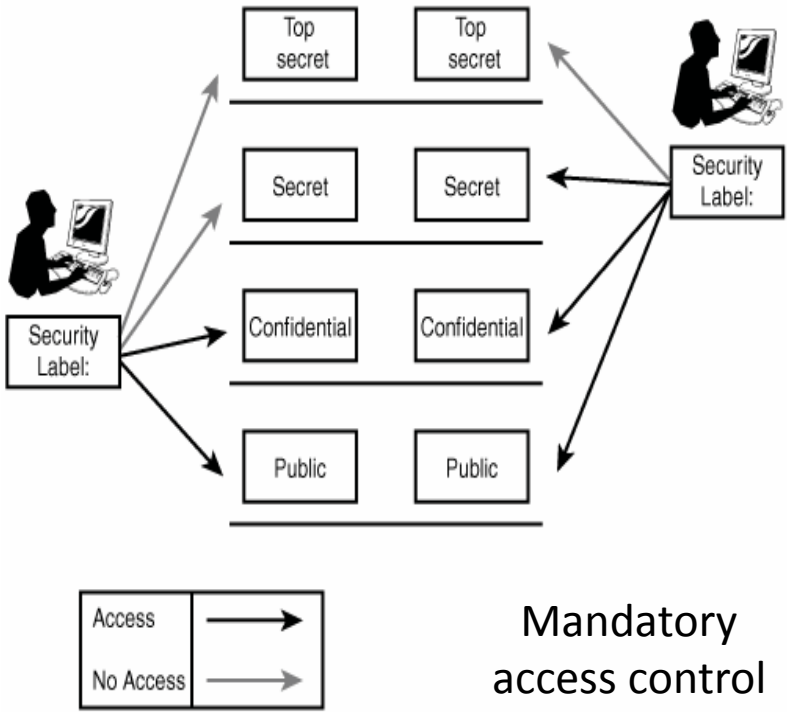
Presented by: Ayesha Kanwal

Agenda

- Traditional Access Control Models
- Motivation for UCON
  - 1- Trust Management
  - 2- Digital Rights Management
- UCON Model Coverage
- UCON Model Components
- UCON-(ABC) Model Space

Traditional Access Control Models

- Based on access control list and capability list
- Protect information against previously known users
- Access Rights are predefined



Mandatory access control

Motivation for Usage Based Access Control Model (UCON)

1- Trust Management

- TM deals with authorization process in distributed systems environment for the access of users who are previously unknown to the system
- Trust management does not utilize identity of a subject for authorization process. Rather, it utilizes capabilities or properties of a subject for authorization decisions.

2- Digital Rights Management (DRM)

- Controlling and tracking access to and usage (including dissemination) of digital information objects.
- Securing digital object itself, not the transmission.

Problems

- Traditional access control models are not adequate for today's distributed, network connected digital environment.
- Authorization only
- Decision is made before access – No ongoing control
- No consumable rights –
- Rights are pre-defined and granted to subjects

Problems (Cont.)

- No access control models available for DRM.
- Recently enhanced models are not comprehensive enough to resolve various shortcomings.
- Need for a unified model that can encompass traditional access control models, DRM and other enhanced access control models.

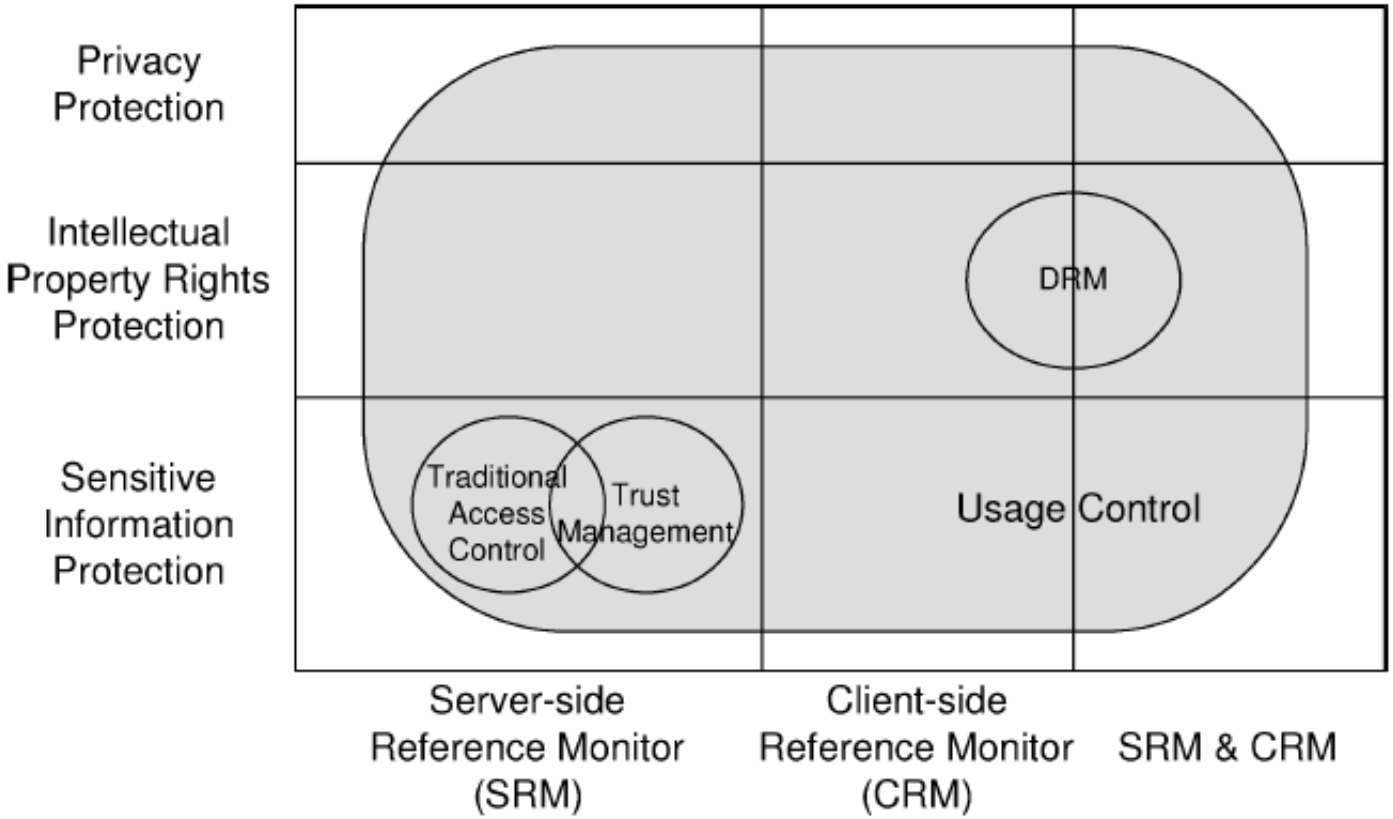
Motivation

- Highly dynamic and distributed computing environments require flexible AC.
- Unknown or partial authenticated users.
- Multi-aspects of access control decisions

  Obligations

  Environmental conditions
- Continually control
- Access is has a duration - usage
- Dynamics of subject and object attributes

Usage Control (UCON) Coverage



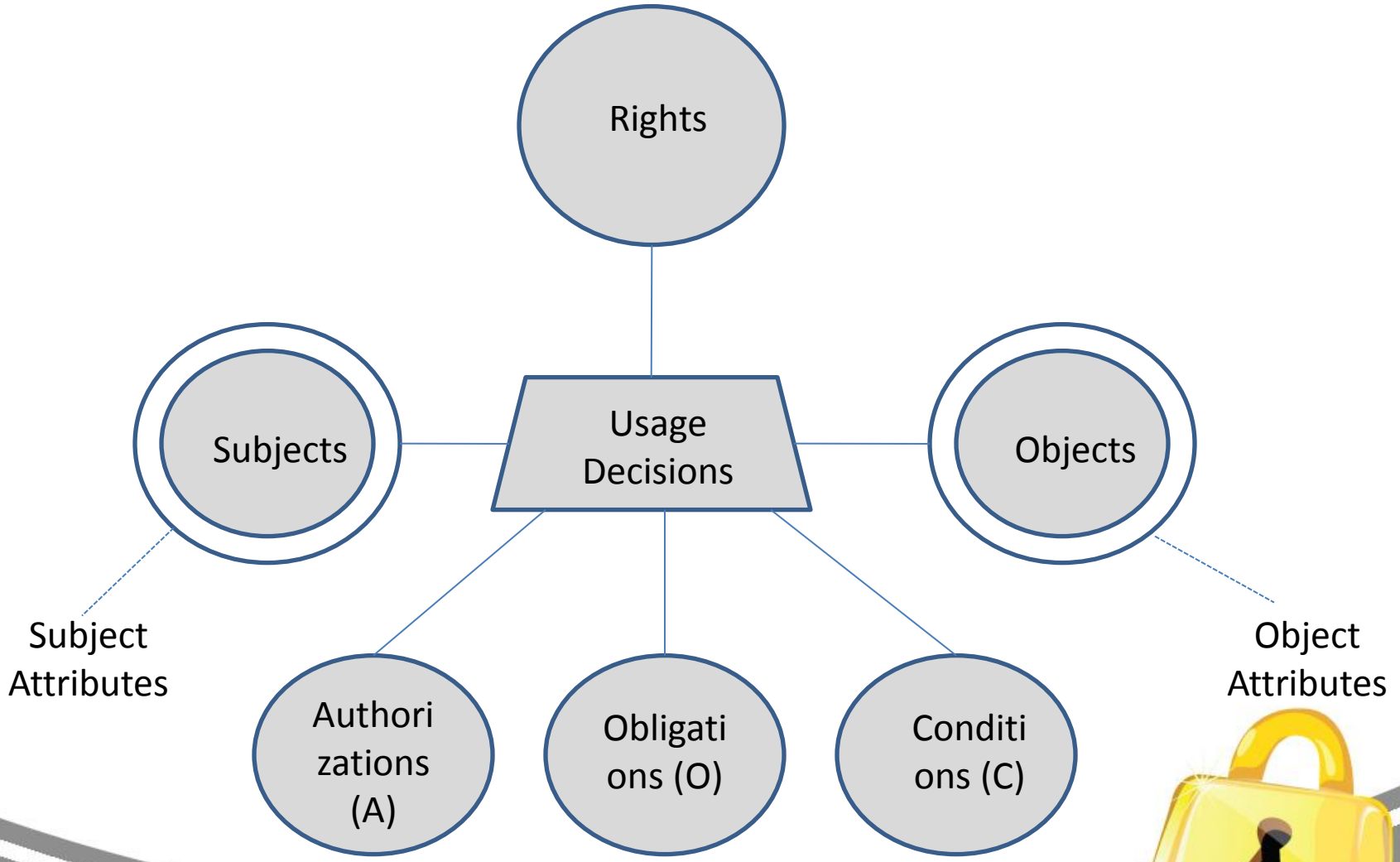
UCON model

- Flexible and comprehensive as access decision is based on multiple factors:
  - ✓ Authorization
  - ✓ Obligations
  - ✓ Conditions

- Decision Continuity- access duration (usage)

- Attributes Mutability -(subjects, objects)

UCON Model Components



Continuity and Attribute mutability

Continuity of Decisions

Pre Decisions | Ongoing Decisions

Before usage | Ongoing usage | After usage

Pre updates | Ongoing Updates | Post Updates

Mutability of Attributes

Subjects (S)

- Entities associated with attributes, and hold and exercise certain rights on objects
- Consumer, Provider, Identifiee subjects

✓ Consumer subjects are entities who exercise the rights to access the objects e-g e-book reader, MP3 music listener.

✓ Provider subjects are entities who provide an object and hold certain rights on it e-g author of an e-book.

✓ Identifiee subjects are entities who are identified in digital objects that include their privacy sensitive information e-g a patient in healthcare system.

Subject Attributes (ATT(S))

- Properties of a subject that can be used for the usage decision process

  identity, role, credit, membership, security level, capability, etc.

- Immutable attributes: can be changed only by administrative action
- Mutable attributes: can be modified as a side effects of subject's access to objects (credit, clearance with high watermark, access time, etc.)

Objects (O)

- Entities that subjects hold rights on.
- Associated with attributes, either by themselves or together with rights.
- Security sensitive objects
- Privacy sensitive objects
- Original vs. derivative objects

Object Attributes (ATT(O))

- Properties of an object that can be used for the usage decision process
- Security classification, role, price, etc.
- Immutable and mutable attributes

Rights (R)

- A subject's privilege on an object
- A set of usage functions that enables a subject's access to objects
- May or may not have a hierarchy
- Existence of right is determined when access is attempted by a subject (not by a predefined access matrix)

Decision Factors and Decision Properties

- 3 Decision Factors
  - ✓ Authorizations (A)
  - ✓ oBligations (B)
  - ✓ Conditions (C)
- A,B, and C are functional predicates used for usage decision making.
- 2 Decision Properties
  - ✓ Mutability
  - ✓ Continuity

Authorizations (A)

- Functional predicates that have to be evaluated for usage decision based on subject and object attributes and the requested specific right
  - ✓ preA: decision is made prior to the access
  - ✓ onA: decision is made during the access
- Updates on Attributes: pre, ongoing, post
  - ✓ preUpdate: High watermark policy
  - ✓ onUpdate: Pre-paid credit for time-based metering
  - ✓ postUpdate: Metered usage payment

oBligations (B)

- Functional predicates that verify mandatory requirements a subject has to perform before or during a usage exercise.
  - ✓ preB utilizes history function to check if certain activities have been fulfilled or not.
  - ✓ onB predicate has to be satisfied continuously during usage. (a user has to watch an ad window while using free Internet services)

    1-Continuously

    2-Periodically

    3-conditionally
- Updates on Attributes: preUpdate, onUpdate, postUpdate

Conditions (C)

- Evaluate current environmental or system status for usage decision
  - ✓ preC: condition is checked before usage
  - ✓ onC: condition has to be satisfied while usage
- Attributes can be used to select which condition requirements has to be satisfied
- No attribute updates
- Time period (Office hour), location (area code, CPUid, IP address), system status (normal, high alert, under attack), etc.

Decision factors in UCON

Authorization

- Pre Authorization
- On Authorization

Obligations

- Pre Obligations
- On Obligations

Updates

- Pre Updates
- On Updates
- Post Updates

Conditions

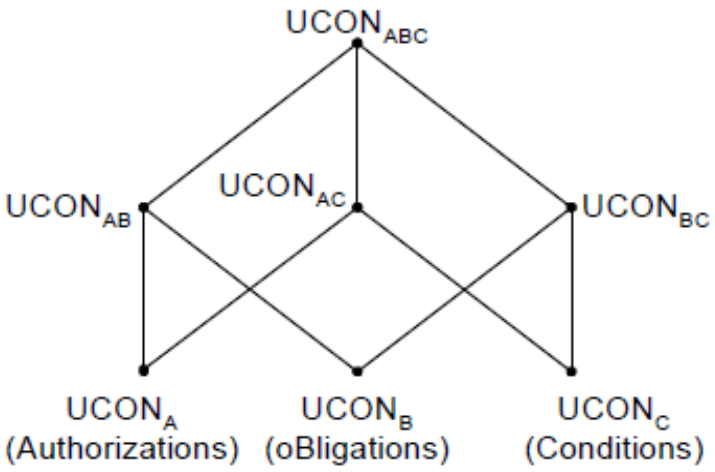
- Pre Condition
- On Condition

16 Basic UCON-(ABC) Models

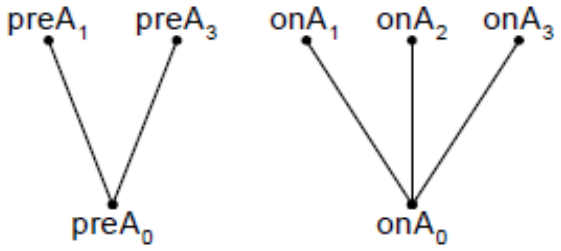
	0(Immutable)	1(pre)	2(ongoing)	3(post)
preA	Y	Y	N	Y
onA	Y	Y	Y	Y
preB	Y	Y	N	Y
onB	Y	Y	Y	Y
preC	Y	N	N	N
onC	Y	N	N	N

N : Not applicable

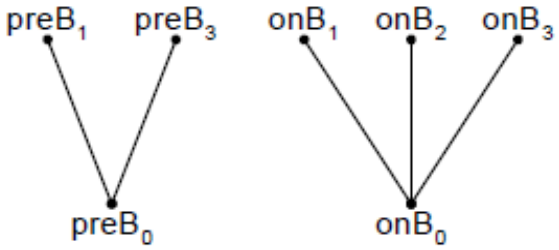
A Family of UCON-(ABC) Core Models



(a)



(b)



(c)

(d)

Examples

- Member of a digital music library. Suppose she has to pay $1/hour of music play (pre-authorization with post-update)
- Pre-paid phone card (ongoing-authorization with ongoing-update)
- Click Ad within every 30 minutes (ongoing obligation with ongoing-updates)
- Business Hour (pre-/ongoing-condition)

Presented by: Ayesha Kanwal