# Digital Rights Management and Beyond

Nov. 29, 2001

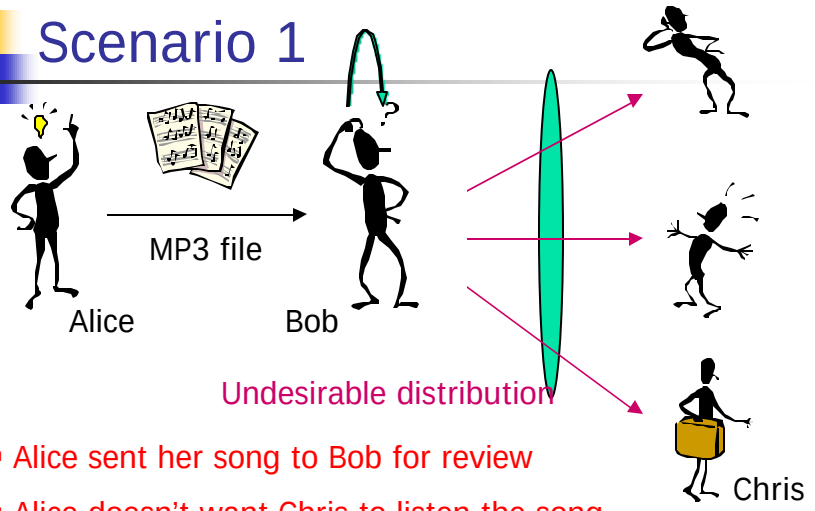
Jaehong Park

Laboratory for Information Security Technology (LIST)
George Mason University
jaehpark@ise.gmu.edu

## Overview

- **DRM Architectures & Mechanisms**
  - ***1. Introduction***
  - 2. Security Architectures
  - 3. Related Mechanisms
  - 4. Commercial Examples
- **Usage Control Models**

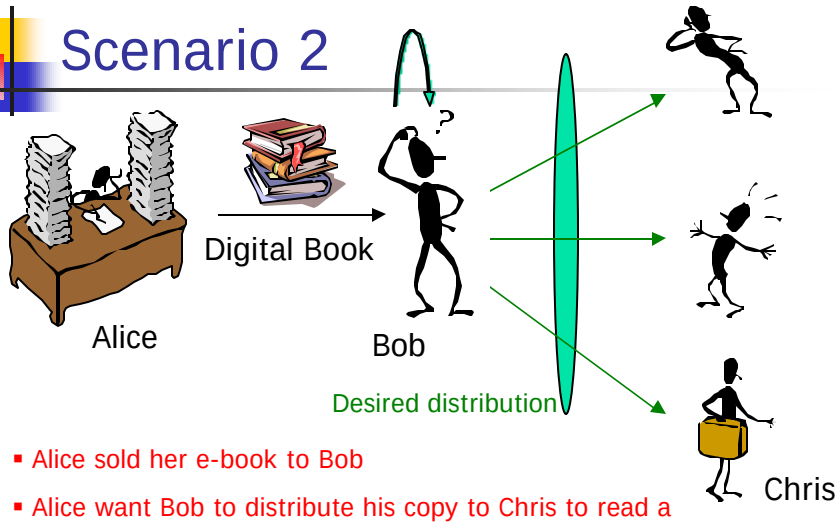
# Scenario 1




- Alice sent her song to Bob for review
- Alice doesn't want Chris to listen the song




# Scenario 2




- Alice sold her e-book to Bob
- Alice want Bob to distribute his copy to Chris to read a part of the book so he can be a potential customer

# Problems

- Unauthorized distribution & Use
  - Reproduction of a digital object does not reduce its quality or value
  - Unauthorized person can access exactly same digital objects as the original copy
  - Commercially, unauthorized dissemination and use of digital object may cause revenue loss
  - Unauthorized dissemination and use of sensitive information causes information leakage (e.x. intelligence community, health care)




# The DRM Origin

- Superdistribution
  - First introduced by Dr. Mori in 1983
  - Digital information is wrapped with digital strings and freely available to everyone
  - No restrictions on copying
  - Copying and distribution is encouraged for marketing purposes
  - Digital information is accessible only where special software is available
  - The usage is controlled by appropriate authorities
  - Well accepted in portions of commercial world

# What is DRM?

- 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




# Dissemination Attributes

- These are some of major factors that should be considered parts of objectives.
  - Dissemination Scale
    - Small, medium, and large scale
  - Dissemination Environment
    - Closed, federated, and open environment
  - Payment-based vs. Payment-free
  - Prevention vs. Detection & Tracking

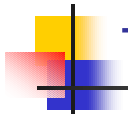
# Dissemination Scale

- Small Scale Dissemination (SSD)
  - 1 item → 1 to 100 recipients
  - Much less tolerance for leakage
  - B2B Business transaction, Intelligence community
- Medium Scale Dissemination (MSD)
  - 1 item → $10^3$ to $10^5$ recipients
  - Textbook publishing, technical journals
- Large Scale Dissemination (LSD)
  - 1 item → $10^6$ to $10^8$ recipients
  - Some leakage is acceptable or even desirable
  - Music, popular books




# Dissemination Environment

- Closed Environment Dissemination (CED)
  - Internal distribution (commercial and Intelligence)
  - Easy to customize client-side systems (both S/W & H/W)
- Federated Environment Dissemination (FED)
  - Limited number of organizations are involved
  - B2B, B2G and G2G dissemination
  - Limited administrative control over recipients
- Open Environment Dissemination (OED)
  - B2B and B2C dissemination
  - Hard to customize client-side system



# Two Types of Dissemination

- Payment-Based Type (PBT)
  - Payment is required in order to access digital content
  - B2C mass distribution e-commerce system
- Payment-Free Type (PFT)
  - Payment is not required
  - Dissemination must be controlled for confidentiality or other security requirements
  - B2B Hub System, Intelligence Community




# Characteristics of PBT & PFT

- PBT
  - A small amount of information leakage is acceptable and even desired
  - The number of legitimate copies of a single digital item is usually greater than that of PFT
  - The objective in PBT is to distribute as many copies as possible and extract payment
- PFT
  - Information leakage is not acceptable
  - The number of legitimate copies of a single digital item is less than that of PBT
  - It is the distribution itself which needs to be limited
  - The security requirements are likely to be more stringent than that of PBT

# Prevention vs. Detection

- Prevention
  - Leakage “cannot” occur
- Detection & Tracking
  - Leakage can occur but can be detected and tracked to re-distributor
- Both solutions can/must coexist




# Commercial Interest

| | Payment | Scale | Environment | Prevent vs. Detect |
|---|---|---|---|---|
| Major Commercial Interest | Yes | Large Medium | Open Federated Closed | Both |
| Less Commercial Interest | No | Medium Small | Open Federated Closed | Both (Prevention emphasis) |

# Overview

- 1. Introduction
- ***2. Security Architectures***
- 3. Related Mechanisms
- 4. Commercial Examples




## Security Architectures for Controlled Digital Information Dissemination (CDID)

- To develop systematic security architectures for controlling and tracking digital information dissemination and its use.
- We are focusing on PFT.
  - Control dissemination solutions of PBT have been developed actively in commercial sector
  - However, no systematic study for more generalized security architectures for controlled digital information dissemination has been done
  - Architectures can be extended to include payment function

# Three Factors of Security Architectures

- Security Architectures have been developed based on the following three factors
- Three factors
  - Virtual Machine (VM)
  - Control Set (CS)
  - Distribution Style




# Three Factors of Security Architectures (continued)

- Virtual Machine (VM)
  - A module that runs on top of vulnerable computing environment and has control functions to provide the means to control and manage access and usage of digital information
  - Foundation of use-control technologies
  - Needs for specialized (trusted) client software/hardware

# Three Factors of Security Architectures (continued)

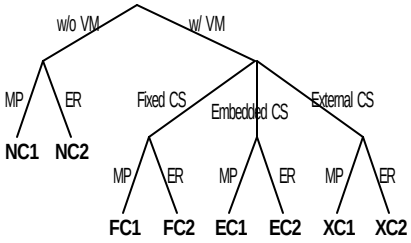
- Control Set (CS)
  - A list of access rights and usage rules that is used by the virtual machine to control a recipient's access to and usage of digital information
    - A *fixed control set* is hardwired into the virtual machine
    - An *embedded control set* is bound to each digital object
    - An *external control set* is separate and independent from the digital object




# Three Factors of Security Architectures (continued)

- Distribution Style
  - Message Push (MP) style
    - Digital information is sent to each recipient
  - External Repository (ER) style
    - Each recipient obtains the digital information from dissemination server on the network

# Architecture Taxonomy

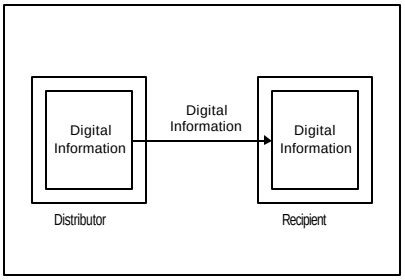



**VM:** Virtual Machine
**CS:** Control Set
**MP:** Message Push
**ER:** External Repository

**NC1:** No control architecture w/ MP
**NC2:** No control architecture w/ ER
**FC1:** Fixed control architecture w/ MP
**FC2:** Fixed control architecture w/ ER
**EC1:** Embedded control architecture w/ MP
**EC2:** Embedded control architecture w/ ER
**XC1:** External control architecture w/ MP
**XC2:** External control architecture w/ ER

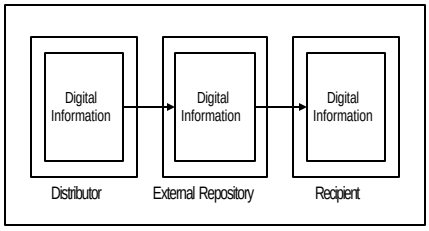



# No Control Architecture w/ Message Push (NC1)




- Distributor directly sends a copy of digital contents to each recipient
- Each recipients stores the copy of digital information at local storage
- After distribution, no direct means to control the distributed digital information
- To access the digital information from multiple system, the recipient needs to transport the information

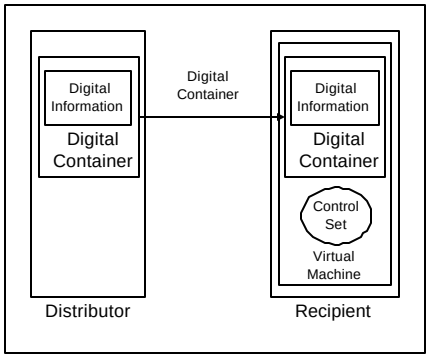
# No Control Architecture w/ External Repository (NC2)




- Digital information is sent to an external repository server for distribution
- A recipient must connect to the external repository to access the digital content
- Once a recipient has received the digital contents, there is no way to control access or usage

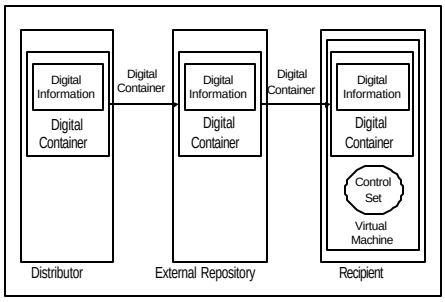



# Fixed Control Architecture w/ Message Push (FC1)




- Digital content is encapsulated in a digital container
- Control set is encoded into virtual machine
- The control set cannot be changed after the distribution of the virtual machine
- Access is controlled based on control set
- Each recipient should keep the received information for further access to it

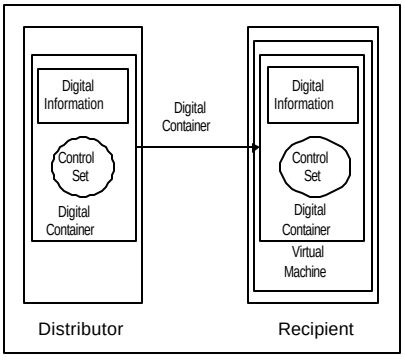
# Fixed Control Architecture w/ External Repository (FC2)




- Similar to FC1, except that digital container is sent to external repository for distribution
- A recipient must connect to the external repository to access or download the digital container
- Accessibility to the content by a single recipient from multiple computers

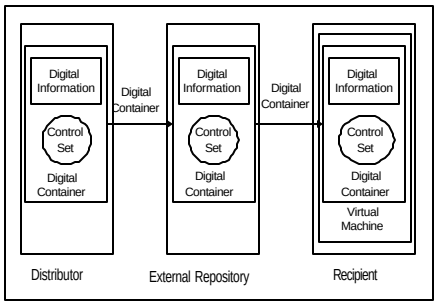



# Embedded Control Architecture w/ Message Push (EC1)




- Control set is embedded in the digital container with digital information
- Distributed content will be controlled based only on the pre-set access rights and usage rules
- After distribution, distributor cannot change the control set of the distributed digital content
- Recipients can access digital content without any network connection
- Only pre-set revocation is available

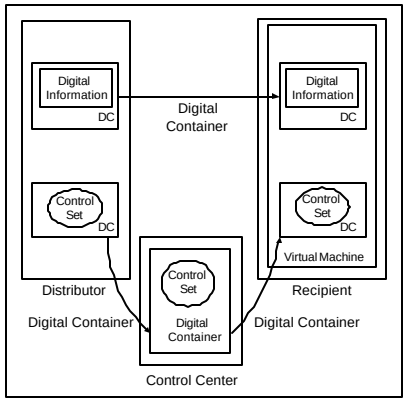
# Embedded Control Architecture w/ External Repository (EC2)




- Digital container is sent to the external repository server for distribution
- If digital container is prohibited from being locally stored, the distributor can revoke a previous granted access by changing control set

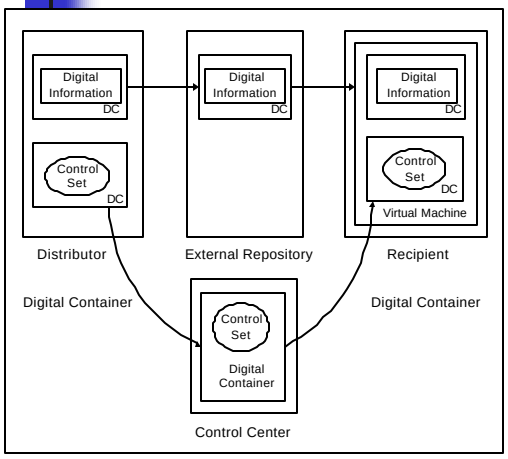



# External Control Architecture w/ Message Push (XC1)




- Control set can be encapsulated independently from digital content
- Two possible options:
  - Network connection is always required
  - Network connection is required from time to time (one time connection is possible)

# External Control Architecture w/ External Repository (XC2)




- Separation of content and access rights
- 4 variations
  - Both encapsulated digital content and encapsulated control set can be stored on recipient's local storage
  - Encapsulated digital content is freely available, but control set cannot be locally stored
  - Only encapsulated control set can be stored
  - Neither can be stored locally




# Security Characteristics

| | Characteristics | NC1 | NC2 | FC1 | FC2 | EC1 | EC2 | XC1 | XC2 |
|---|---|---|---|---|---|---|---|---|---|
| C1 | Disseminator can control access and usage of disseminated digital information | | | Y | Y | Y | Y | Y | Y |
| C2 | Disseminator can change recipients' access rights after dissemination | | | | | | Y | Y | Y |
| C3 | Re-disseminated digital information can be protected | | | Y | Y | Y | Y | Y | Y |
| C4 | Special client software (virtual machine) is vulnerable to attacks | | | Y | Y | Y | Y | Y | Y |
| C5 | Tracking re-disseminated digital information is possible | Y | Y | Y | Y | Y | Y | Y | Y |

# Functional Characteristics

| | Characteristics | NC1 | NC2 | FC1 | FC2 | EC1 | EC2 | XC1 | XC2 |
|---|---|---|---|---|---|---|---|---|---|
| C6 | Disseminated digital container is reusable for other recipients by re-dissemination | | | | | | | Y | Y |
| C7 | Digital information does not have to be on recipient's storage | | Y | | Y | | Y | | Y |
| C8 | Digital information can be accessible from any machine if it is connected to network | | Y | | Y | | Y | | Y |
| C9 | Recipient should carry digital information to access it from multiple machines | Y | | Y | | Y | | Y | |
| C10 | Special client software (virtual machine) is required | | | Y | Y | Y | Y | Y | Y |
| C11 | In case of large digital information, download time can be significantly costly | | Y | | Y | | Y | | Y |
| C12 | Every access to digital information requires network connection. | | | | | | | | |
| C13 | The architecture can be supported without network connection | Y | | Y | | Y | | | |
| C14 | Control center trusted by both distributors and recipients is mandatory | | | | | | | Y | Y |




# Commercial Solutions

| Solution | Organization | NC1 | NC2 | FC1 | FC2 | EC1 | EC2 | XC1 | XC2 |
|---|---|---|---|---|---|---|---|---|---|
| Adobe Acrobat | Adobe | | | | | X | | | |
| PDF Merchant & WebBuy | Adobe | | | | | | | | X |
| PageVault | Authentica | | | | | | | X | |
| SoftSEAL | Breaker Technologies | | | | | | | | X |
| Confidential Courier | Digital Delivery, Inc. | | | | | X | | | |
| docSPACE | DocSPACE Co. | | X | | | | | | |
| CIPRESS | Fraunhofer Institute for Computer Graphics & Mitsubishi Co. | | | | | | | | X |
| Cryptolope | IBM | | | | | | | X | |
| InTether | Infraworks Co. | | | | | X | | | |
| InterTrust | InterTrust Technologies Co. | | | | | | | X | |
| RightMarket | RightMarket.com Inc. | | | | | | | X | |

# Overview

- 1. Introduction
- 2. Security Architectures
- ***3. Related Mechanisms***
- 4. Commercial Examples




# Metadata Languages

- Metadata
  - A  data of data
  - Includes semantics of the data
- Metadata Languages
  - A language specification used to present metadata
  - A Key mechanism for DRM standards
- Examples
  - XrML
  - ODRL

# Access Control

- Payment based access control
  - Authorization is based on payment
  - Most of commercial solutions
- Non-payment based access control
  - Little studies on this for DRM
  - MAC, DAC, RBAC, ORCON
  - Non-commercial (I.e., intelligence community, health care)




# Digital Watermarking

- Digital Watermark
  - Digital watermark is used to mark the identity of the objects with information such as author's name, date, or usage right
  - Can provide tracking capability to illicit distribution
  - Can be implemented all of our security architectures
  - Watermarking technologies are dependent on the type of digital information (e.g., text, image, audio and etc.)
  - Minimum size of object is required
  - Difficulty of embedding different watermark (fingerprint) in each copy of original objects in case of mass distribution

# Digital Watermarking

- Visible Watermarking
  - Watermark is visible (e.g.background logo)
  - Can be used for sample digital objects to reduce commercial value on them
- Invisible Watermarking
  - Most of Watermarking belongs here
  - Digital Watermark can be detected by special software




# Digital watermarking

- Public Watermarking
  - Watermark information w/ publicly known key (w/o any secret key)
  - Everyone can read watermarked information
  - In commercial sector, customer can find copyright owner's information
- Private Watermarking
  - Only authorized users can detect the watermarks
  - Good for tracking purpose

# Digital Watermarking

- Watermark retrieval
  - Reference-required watermark
    - The original object or embedded watermark information is required for comparison
  - Reference-free watermark
    - Watermark can be retrieved without the original document or added information
    - The mechanism detects specific properties and patterns from documents




# Digital Watermarking

- Different format, different watermarking
  - text, image, audio, and video
- Text Watermarking (Brassil, et al.)
  - Line-shift coding
    - Text lines are shifted imperceptibly up and down
  - Word-shift coding
    - Words are shifted horizontally
    - Original un-watermarked documents are required for extracting watermarked information
  - Feature coding
    - Characters are altered (vertical or horizontal)
    - Least discernible, larger information embedded

# Overview

- 1. Introduction
- 2. Security Architectures
- 3. Related Mechanisms
- ***4. Commercial Examples***




# Commercial Efforts for Open-standard (XrML)

XrML: Extensible Rights Markup Language

- What is XrML?
  - "A language in XML for describing specifications of rights, fees and conditions for using digital contents, together with message integrity and entity authentication within these specifications" (www.xrml.org)
  - An extension of the Xerox "Digital Property Rights Language version 2.0 (DPRL)"
  - ContentGuard™ has developed XrML as an open specification licenced on a royalty-free basis
- Why XrML?
  - In CDID Architecture, XrML can be viewed as one of potential mechanisms for Control Set (CS) implementation.
  - XrML is extensible, open specification

# Top-Level Structure

```
<XrML>
    <BODY>
        (TIME)?                    time interval in which this spec is valid
        (ISSUED)?                  time moment at which this spec is issued
        (DESCRIPTOR)?              description or meta data of this spec
        (ISSUER)?                  principal who issues this spec
        (ISSUEDPRINCIPALS)?        list of principals this spec is issued to
          (PRINCIPAL)+
        (WORK)?                    work and rights this spec specifies
        (AUTHENTICATEDDATA)?       data that provided to application
    </BODY>
    (SIGNATURE)?
</XrML>
```

"?" denotes zero or one occurrence; "+" denotes one or more occurrences; and "*" denotes zero or more occurrences




# Digital Works & Usage Rights

```
<WORK>
    OBJECT              object used to identify the work
    DESCRIPTION         description of the work
    CREATOR             creator of the work
    OWNER               owner of the work
    METADATA            additional metadata of the work
    DIGEST              digest value of the work
    PARTS               parts of the work, each of which is a work itself
    CONTENTS            indicator of where content of the work is
    COPIES              number of copies of the work that are specified
    COMMENT             Comment
    SKU                 Stock Keeping Unit, for extensibility to allow people to
                        identify this work in their own stock.
    FORMAT              Digital or physical manifestation of the work
    (RIGHTSGROUP | REFERENCEDRIGHTSGROUP )+    rights group associated
                        with the work | reference rights group of the work
</WORK>
```

## Rights in RIGHTSGROUP Element

- Digital property rights
- Specifying times, fees and incentives
- Specifying access controls (licenses/certificates, security levels)
- Specifying territory information
- Specifying tracking information
- Specifying watermark information
- Bundle specifications (time limits, fees, access, and watermark info inside bundle)




## Usage Control (UCON) Models

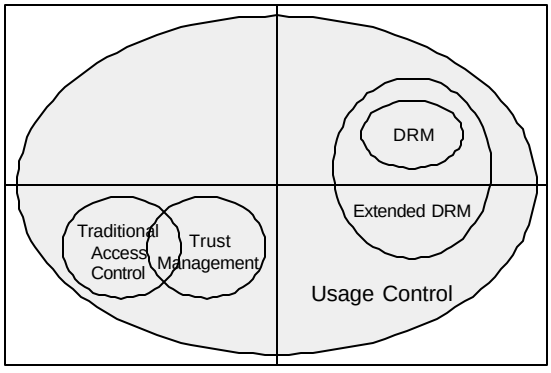
Oct. 29, 2001

# UCON in Information Security

- UCON is a comprehensive engineering framework that includes all aspects (policies, models, architectures, and mechanisms) for controlling and tracking access to and usage of digital objects
- UCON unifies access control, trust management, and digital rights management and goes beyond in its definition and area of interests
- UCON enables finer-grained control over usage of digital objects than that of traditional access control policies and models
- UCON covers both centrally controlled environment and an environment where central control authority is not available.
- UCON also deals with privacy issues.
- Watermarking can exist in all areas for Detection (tracking) purpose though it's not shown in the diagram.




# UCON in Information Security



## Our Focus in UCON

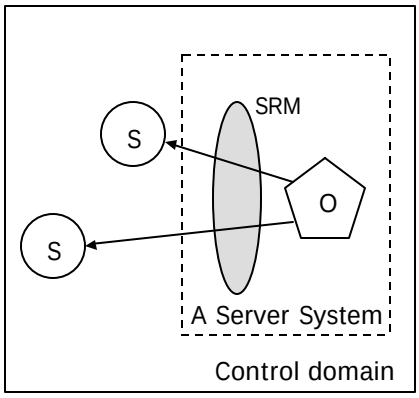
- We are trying to cover at least a consolidated models of these three areas by unifying them.




## 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)



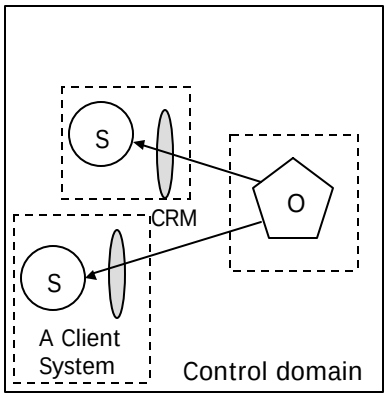

- Control domain w/ SRM facilitates a central means (SRM) to control access and usage of a subject to any digital information objects of the domain on behalf of a provider subject.
- Subject (S) can be either within same organization/network area or outside the area




# Control Domain w/ SRM (cont)

- 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.
- CED can be utilized in this environment
- OED also can be used but no control on client-side DO
- 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 DO is saved at local non-volatile storage, the changes on DO can be controlled (blocked or allowed)
- CED, OED, and FED belong here.
- DRM belongs here.




# Payment-Based vs. Payment-Free

- Been there.

# Digital Rights Management (DRM)

- DRM mainly focus on payment-based disseminations though underlying technologies can also be used for payment-free dissemination environment.
- DRM enables client-side controls in a control domain without using SRM.
- Lack of well-defined policies and models for controlling and managing rights and usages of rights.




# Access Control

- Access control enables controls only in a control domain where server-side reference monitor exists and mainly focus on payment-free environment. Both conventional mainframe or client-server systems can be used.
- Access control primarily deals with access of users who are previously known to the system (no control on strangers) though capability based approaches may be an exception.

# Trust Management

- TM deals with authorization process for the access of users who are previously unknown to the system
- TM focus only on a control domain where server-side reference monitor is available.




# UCON issues

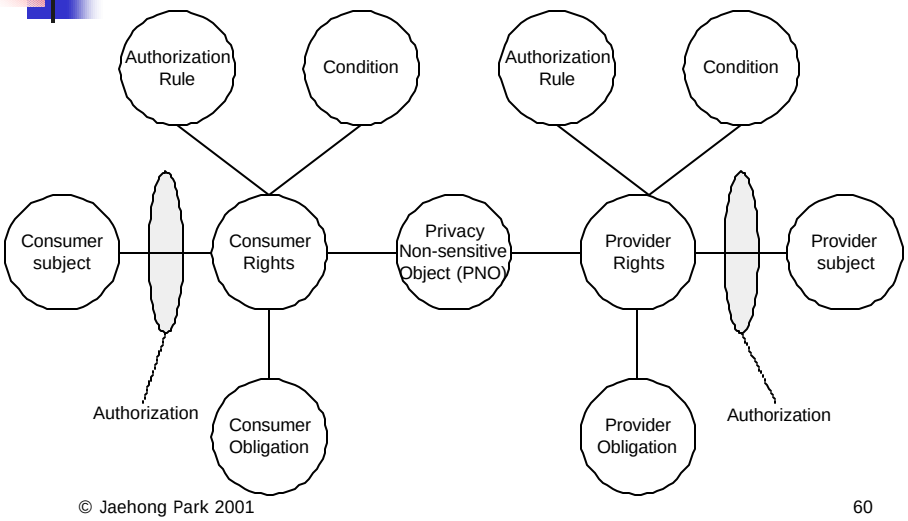
- Privacy based UCON (PUCON) vs. Non-privacy based UCON (NUCON)
- Family of UCON models
  - UCON Authorization Models
  - UCON Rights Models
    - UCON Usage Rights Models
    - UCON Delegation Rights Models (?)
  - UCON Administration Models (?)
- Reverse UCON

# Base components of UCON Models

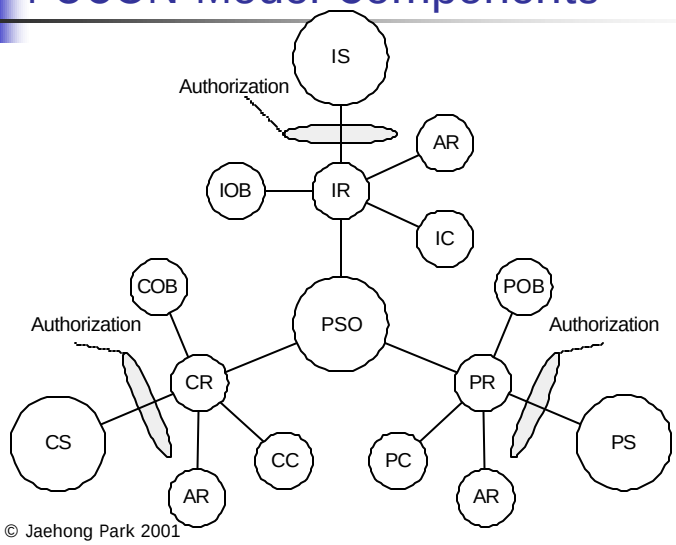
- Subject
  - An entity that exercise certain rights on objects
  - Consumer (CS), Provider (PO), Identified individual subject (IS)
- Object
  - A digital information resource that a subject holds rights on
  - Privacy non-sensitive (PNO) vs. privacy sensitive (PSO)
  - Original vs. derivative
- Rights
  - A subject's privilege on a object
  - Legal vs. procurable
  - Inverse vs. reverse
  - Consumer (CR) vs. provider (PR) vs. Identified individual (IR)
  - Functional classifications (read, play, print, copy, etc.)




# NUCON Model Components



## PUCON Model Components







## NUCON vs. PUCON (examples)

- PCASSO ('97) by UCSD, SAIC, and NIH.
- The Privacy Rule ('01): "Standards for Privacy of Individually Identifiable Health Information" by Dept. of Health and Human Services.

# 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)
- authorization rules are a set of decision factors used to check whether a subject is qualified for the use of certain rights on an object, whereas condition is used to check whether existing limitations and conditions of usage rights on an object are valid, and has to be checked upon the use if updates are necessary or not




# Condition

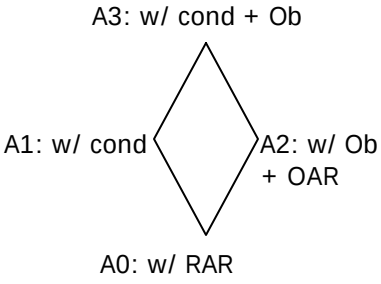
- A set of decision factors that the system should verify at authorization process along with authorization rules before allowing usage of rights on a digital object
- *Dynamic condition* (stateful)
  - The number of usage times (e.g., can read 5 times, can print 2 times), usage log (e.g., already read portion cannot be accessed again), and whatever has to be checked at each time of usages for updates.
- *Static condition (*stateless)
  - Accessible time period (e.g., office hour), accessible location (e.g., workplace), allowed printer name, and those that do not have to be checked at each time of usages for updates.

# Obligation

- A list of mandatory requirements that a subject has to do after the exercise of rights on an object.
- Obligation is likely to be fulfilled after the use of rights, though in its real world implementation, this may have to be done before the exercise of rights (obligation-related authorization rule).
  - Consumer subject may have to accept metered payment agreements for the usage on certain digital information or should report usage log information to provider subject.
  - Another example is that the consumer subject must agree on a payment (deducting the amount of charge from her account) upon access to a digital information object




# UCON Authorization Models




- UCON A0: w/ RAR
- UCON A1: w/ condition
- UCON A2: w/ obligation & OAR
- UCON A3: w/ condition + obligation

- UCON Authorization models can cover both CD w/ SRM and CRM
- Authorization Models cover both PUCON & NUCON

## UCON A0: w/ Authorization Rules (RAR)

- Traditional authorization processes are under this model
- Traditional access control and trust management utilize this model as an authorization mechanism




## UCON A1: w/ Condition

- In addition to authorization rule, there exist condition as a part of authorization process.
- This provides finer-grained authorization

## UCON A2: w/ Obligation + OAR

- In addition to authorization rule, there exist obligation as a part of authorization process.
- This can provide better enforcement on exercising usage rights for both provider and consumer sides.




## UCON A3: w/ Condition & Obligation

- In addition to authorization rule, there exist condition and obligation as parts of authorization process.
- DRM solutions are utilizing both condition and obligation though they may not explicitly define conditions and obligations.

# UCON Usage Rights Models

- Two major usage rights UR = {V, M} where
  - V: view
  - M: modification
  - Modification includes all other usages that change original digital objects such as derivative works (i.e., cut & paste pictures), etc.
- Control is denoted as C and C = {0, 1, α} where
  - 0 : Closed to public, no one can access it,
  - 1 : Open to public, everyone can access it,
  - α : selective (controlled) to public, access approval is selective, and
  - 0 < α < 1 : openness of control, availability of DO
- V = {v| v ∈ C}, M = {m| m ∈ C}

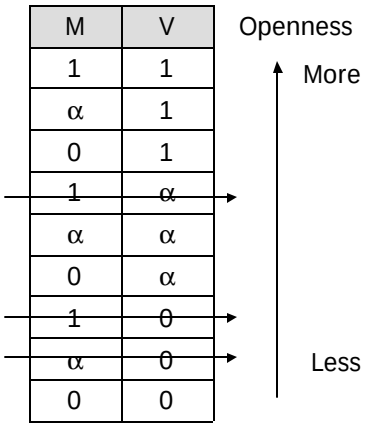



# UCON UR Models (cont.)

| M | V |
|---|---|
| 1 | 1 |
| α | 1 |
| 0 | 1 |
| 1 | α |
| α | α |
| 0 | α |
| 1 | 0 |
| α | 0 |
| 0 | 0 |

- $C_{mv}$ = {(m,v)| m ∈ M, v ∈ V}
  - $C_{mv}$ is a set of controls in terms of M and V
  - This gives us 9 different combinations of control sets.

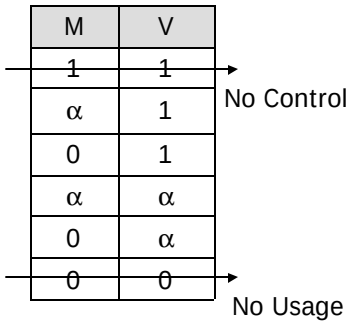
# UCON UR Models (cont.)




- $C_{mv}$ = {(m,v)| m ∈ M, v ∈ V, m <= v}
  - Since we can consider subject cannot modify an object without viewing it, M cannot be more accessible than V ($C_{mv}$ = {(m,v)| m <= v}).
  - This rules out 3 of 9 combinations.

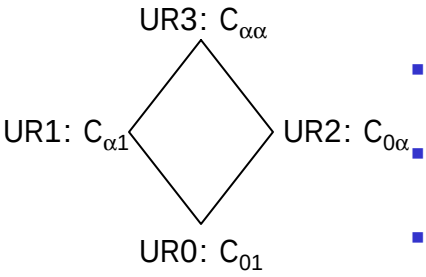



# UCON UR Models (cont.)




- $C_{mv}$ = {(m,v)| m ∈ M, v ∈ V, m <= v, (1,1) ∉ (m,v), (0,0) ∉ (m,v)}
  - Since, $C_{11}$ means no control and $C_{00}$ means no usage, we discard these two cases from our UCON usage rights models.
- $C_{mv}$ = {(0, 1), (α, 1), (0, α), (α, α)}
  - Therefore, there are four cases to be considered as above.

# UCON UR Models (cont.)




- α (controlled) is most complicated to implement and 1 (open) will be easiest one.
- The sequence of $C_{\alpha 1}$ and $C_{0\alpha}$ is subjective
- Each model may have different interests groups
- Each can be combined with different authorization models




# UCON UR0

- {(0,1)}
- View only, modification is blocked
- Public websites

## UCON UR1

- {(0,1), (1,1)}
- View is open to public
- Modification is allowed selectively




## UCON UR2

- {(0,0), (0,1)}
- Modification is not allowed
- View is allowed selectively
- e-book/MP3 distribution, digital library for member only

# UCON UR3

- {(0,0), (0,1), (1,1)}
- Both modification and view are selective
- (a,b) is not possible
- Hospital patients information system (only authorized doctors can see or update certain patients data)




# Reverse/derivative UCON

- Exercising usage rights on a digital object may create another digital information object (derivative DO) that also needs controls for the access to and usage on it (payment info, usage log).
- The usage control on this derivative DO is reverse in its control direction (provider and consumer subjects are changed) and called reverse UCON and the rights called reverse rights.
- Furthermore, exercising reverse rights on this derivative DO may also creates another derivative DO and reverse rights on it.
- Controls and protections on rights and usage of rights on these derivative DOs have been hardly recognized/discussed in literature.
- This is where privacy issues are raised. Adequate controls on derivative DOs require for better privacy treatment.
- Example: MP3 distribution

# Reverse/derivative UCON (cont)

- UCON systems are likely to be implemented and managed by either provider subject (PS) side or CS. This means it's hard to guarantee availability of adequate control mechanisms implemented for the other side of subjects on the rights and usage of rights.
- There can be also a third party who develop/manage UCON system on behalf of both of PS and CS sides
- To make reverse UCON available, there should be either a voluntary commitment from development/ management group or a legal enforcement.




# Reverse/derivative UCON (cont)

- UCON models can be used for both ordinary/inverse and reverse UCON.
- UCON system may have to include following mechanisms for reverse UCON.
  - To provide ability to refuse creation of derivative DO (consumer may have to give up exercising original rights).
  - To provide ability to restrict reverse usage by blocking certain part of derivative DO (ex. identity) or by allowing only aggregated information of individual DOs.
  - To provide ability to monitor reverse usage on derivative DO (this cause another round of reverse UCON).

## Reverse/derivative UCON (cont)

- In UCON model, there are two kinds of rights: legal rights and procurable rights.
- Definition of Legal rights: ?
- By law, legal rights have to be included within the system.
- If legal rights are not defined by law, it still can be implemented voluntarily.




## Conclusion

- Layered approach: security objectives, models, security architectures, and mechanisms
- The first systematic study on security architectures and models which are not previously defined in this manner
- UCON defines a new area of security issues encompassing access control, trust management, and DRM
- Our work provides basis for future researches and development for controlling and tracking dissemination of digital contents