UCON Attribute Mutability, UCON Architectures

ISA 767, Secure Electronic Commerce
Xinwen Zhang, xzhang6@gmu.edu
George Mason University

UCON ABC Model Components: 3 Decision Factors & 2 Properties

Continuity Property: Decision can be made during usage for continuous enforcement

Mutability Property: Attributes can be updated as side-effects of subjects' actions

Attributes in Usage Control

Attributes are information or properties associated with subjects or objects
- E.g., ID, Role, Clearance/classification, membership, credit, etc.
- Subject Attributes and Object Attributes are used for authorization decision
- Attributes may have to be updated
  - Immutable Attributes: Attribute updates can be made by administrative actions
  - Mutable Attributes: attributes can be modified as side effects of usage

Attribute Management: Admin-controlled vs. System-controlled

Admin-controlled (Immutable)
- Updates involve administrative decisions and actions
- Admin can be security officer, user (self, non-self)

System-controlled (Mutable)
- Updates are made as side effects of users' usage on objects.
- Our focus is here

Attribute Management Taxonomy

Mutable Attributes

Temporary Attributes (stateless)
- Alive only for a single usage
- Exist only in mutable attributes
- E.g., Usage start time, last active time, etc.

Persistent Attributes (stateful)
- Live for multiple usage decisions
- Exist in both mutable and immutable attributes
- E.g., Total usage hours, user credit balance, etc.
- Utilization of temporary attributes is a design decision and can be eliminated in some cases.
- Temporary subject attributes can be stored as a form of elements of persistent object attributes
Mutability Variations

Mutability for
- Exclusive/Inclusive Attributes
  - History based policies
  - E.g., Dynamic SOD, Chinese Wall policy
- Consumable/creditable Attributes
  - E.g., Limited # of Usage, payment, mileage, etc
- Immediate Revocation
  - To support continuous control throughout usages
- Obligation
  - Attribute update as a result of obligation fulfillment
- Dynamic Confinement
  - E.g., High Watermark in MAC

Mutability for
- Exclusive/Inclusive Attributes
  - History based policies
  - E.g., Dynamic SOD, Chinese Wall policy
- Immediate Revocation
  - To support continuous control throughout usages

Mutability for
- Consumable/Creditable Attributes
  - Mutability for consumable attributes, limited CD burnings

Mutability for
- Obligation
  - License agreements for first time users only

Mutability for
- Dynamic Confinement
  - MAC policies with high watermark property

Mutability for
- Immediate Revocation
  - Long-distance call using Pre-paid phonecard

Mutability for
- Obligation
Discussion

- Mutability variations are not mutually exclusive
  - Multiple mutability variations can be used in a single example.
- Updates can be made on either subject attributes or object attributes
  - In some cases, a policy can be realized by utilizing either subject attributes or object attributes

Conclusions and Future Works

- Consolidated analysis of Attributes and Attribute mutability in a single framework of usage control
  - Temporary and persistent attributes
  - Taxonomy of attribute management
  - Mutable attributes and variations of mutability
  - Mutability with continuity property
- Future research
  - Attribute management for admin-controlled attribute updates (immutable attributes)
  - Further study on attribute mutability

Usage Control Architectures

- We narrow down our focus so we can discuss in detail how UCON can be realized in architecture level
  - Sensitive information protection X CRM
- First systematic study for generalized security architectures for digital information dissemination
- Architectures can be extended to include payment function

Security Architectures for Controlled Digital Information Dissemination

- To develop systematic security architectures for controlling and tracking digital information dissemination and its use.
- We are focusing on Payment-Free Type (PFT).
  - Control dissemination solutions of PFT 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
- Most for confidentiality
  - Controlled information sharing

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

- **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

- **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 recipient 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

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

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)

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/ 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/ 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

<table>
<thead>
<tr>
<th>Characteristics</th>
<th>NC1</th>
<th>NC2</th>
<th>FC1</th>
<th>FC2</th>
<th>EC1</th>
<th>EC2</th>
<th>XC1</th>
<th>XC2</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1 Disseminator can control access and usage of</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>disseminated digital information</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C2 Disseminator can change recipients access rights</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>after dissemination</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C3 Re-disseminated digital information can be</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>protected</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C4 Special client software (virtual machine) is</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>vulnerable to attack</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C5 Tracking re-disseminated digital information is</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>possible</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Functional Characteristics

<table>
<thead>
<tr>
<th>Characteristics</th>
<th>NC1</th>
<th>NC2</th>
<th>FC1</th>
<th>FC2</th>
<th>EC1</th>
<th>EC2</th>
<th>XC1</th>
<th>XC2</th>
</tr>
</thead>
<tbody>
<tr>
<td>C6 Disseminated digital container is reusable for other</td>
<td>Y</td>
<td></td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td></td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>recipients by re-dissemination</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C7 Digital information does not have to be recipient’s</td>
<td></td>
<td></td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td></td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>storage</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C8 Digital information can be accessed from any machine</td>
<td></td>
<td></td>
<td>Y</td>
<td>Y</td>
<td></td>
<td></td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>if it is connected to network</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C9 Recipient should verify digital information to access</td>
<td></td>
<td></td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td></td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>it from multiple machines</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C10 Digital client software (virtual machine) is</td>
<td></td>
<td></td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td></td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>vulnerable to attack</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C11 Special client software (virtual machine) requires</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>significant time to access</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C12 Every access to digital information requires</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>network connection</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C13 The architecture can be supported without network</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>connection</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C14 Special client software (virtual machine) requires</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>significant time to access</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Commercial Solutions

<table>
<thead>
<tr>
<th>Solution</th>
<th>Organization</th>
<th>NC1</th>
<th>NC2</th>
<th>FC1</th>
<th>FC2</th>
<th>EC1</th>
<th>EC2</th>
<th>XC1</th>
<th>XC2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adobe Acrobat</td>
<td>Adobe</td>
<td></td>
<td></td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PDF Merchant</td>
<td>Adobe</td>
<td></td>
<td></td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PostScript</td>
<td>Acrobat</td>
<td></td>
<td></td>
<td>Y</td>
<td>Y</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SafeEBIS</td>
<td>Breaker Technologies</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confidential</td>
<td>Digital Delivery, Inc.</td>
<td></td>
<td></td>
<td>Y</td>
<td>Y</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Courier</td>
<td>InSPACE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIPRESS</td>
<td>Fraunhofer Institute for Computer Graphics &amp;</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mitsubishi Co.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cryptolope</td>
<td>IBM</td>
<td></td>
<td></td>
<td>Y</td>
<td>Y</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>InTether</td>
<td>Infraworks Co.</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>InterTrust</td>
<td>InterTrust Technologies Co.</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RightMarket.com</td>
<td>RightMarket.com Inc.</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>