Usage Control: A Vision for Next Generation Access Control

Infs767, Oct 23, 2003

Ravi Sandhu and Jaehong Park
(www.list.gmu.edu)

Laboratory for Information Security Technology (LIST)
George Mason University

Problem Statement

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

Prior Work

- Problem-specific enhancement to traditional access control
  - Digital Rights Management (DRM)
    - mainly focus on intellectual property rights protection.
    - Architecture and Mechanism level studies, Functional specification languages – Lack of access control model
  - Trust Management
    - Authorization for strangers' access based on credentials

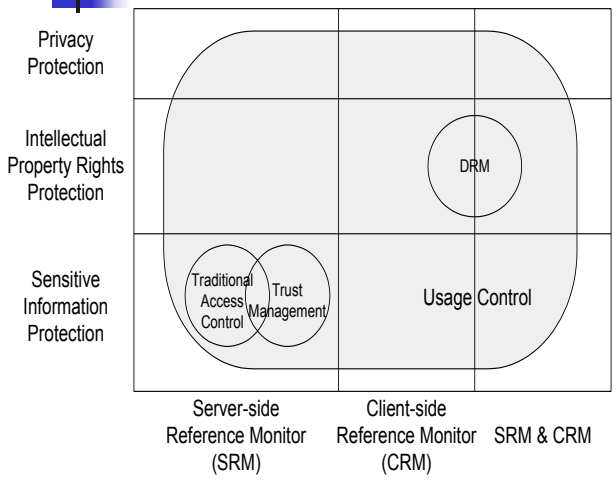
Prior Work

- Incrementally enhanced models
  - Provisional authorization [Kudo & Hada, 2000]
  - EACL [Ryutov & Neuman, 2001]
  - Task-based Access Control [Thomas & Sandhu, 1997]
  - Ponder [Damianou et al., 2001]

Problem Statement

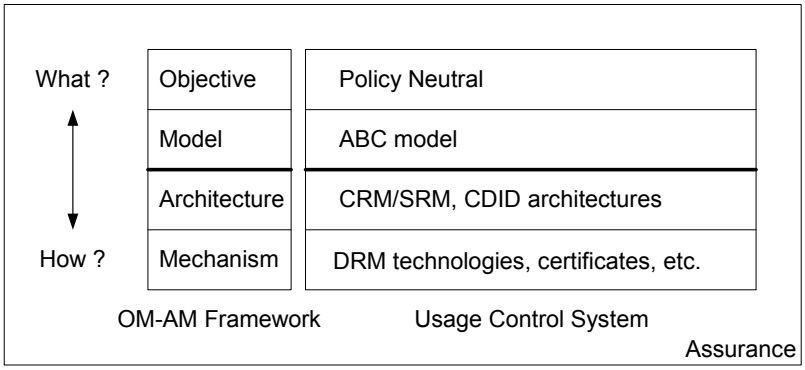
- Traditional access control models are not adequate for today's distributed, network-connected digital environment.
- No access control models available for DRM.
- Recently enhanced models are not comprehensive enough to resolve various shortcomings.
- Need for a unified model that can encompass traditional access control models, DRM and other enhanced access control models from recent literature

Usage Control (UCON) Coverage



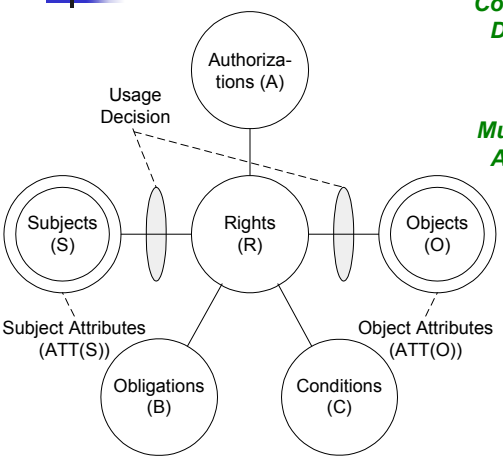
- Protection Objectives
  - Sensitive information protection
  - IPR protection
  - Privacy protection
- Protection Architectures
  - Server-side reference monitor
  - Client-side reference monitor
  - SRM & CRM

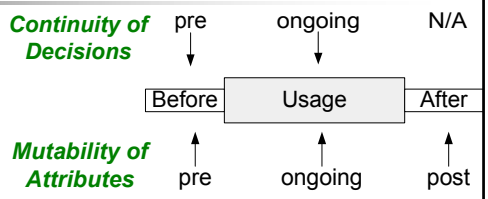
OM-AM layered Approach



- ABC core models for UCON

Building ABC Models





- Continuity
  - Decision can be made during usage for continuous enforcement
- Mutability
  - Attributes can be updated as side-effects of subjects' actions

Examples

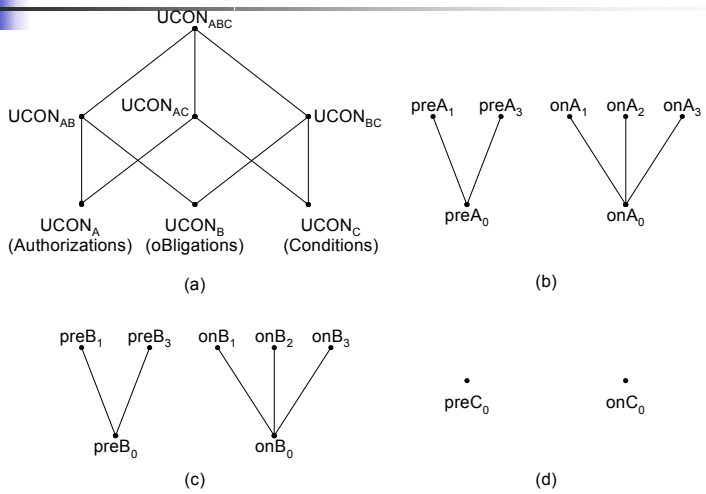
- Long-distance phone (pre-authorization with post-update)
- Pre-paid phone card (ongoing-authorization with ongoing-update)
- Pay-per-view (pre-authorization with pre-updates)
- Click Ad within every 30 minutes (ongoing-obligation with ongoing-updates)
- Business Hour (pre-/ongoing-condition)

ABC Model Space

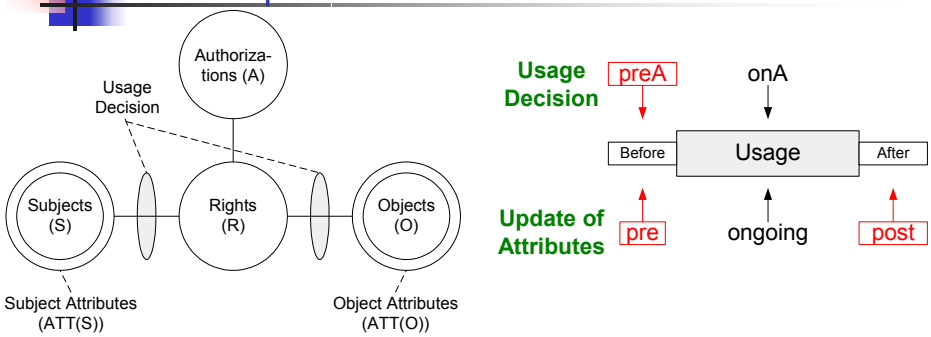
	0(Immutable)	1(pre)	2(ongoing)	3(post)
preA	Y	Y	N	Y
onA	Y	Y	Y	Y
preB	Y	Y	N	Y
onB	Y	Y	Y	Y
preC	Y	N	N	N
onC	Y	N	N	N

N : Not applicable

A Family of ABC Core Models



UCON$_{preA}$



- Online content distribution service
  - Pay-per-view (pre-update)
  - Metered payment (post-update)

$UCON_{preA}$: pre-Authorizations Model

- $UCON_{preA0}$
  - *S, O, R, ATT(S), ATT(O)* and *preA* (subjects, objects, rights, subject attributes, object attributes, and pre-authorizations respectively);
  - *allowed(s,o,r)* $\Rightarrow$ *preA(ATT(s),ATT(o),r)*
- $UCON_{preA1}$
  - *preUpdate(ATT(s)),preUpdate(ATT(o))*
- $UCON_{preA3}$
  - *postUpdate(ATT(s)),postUpdate(ATT(o))*

$UCON_{preA0}$: MAC Example

- *L* is a lattice of security labels with dominance relation $\geq$
- *clearance:* $S \rightarrow L$
- *classification:* $O \rightarrow L$
- *ATT(S) = {clearance}*
- *ATT(O) = {classification}*
- *allowed(s,o,read)* $\Rightarrow$ *clearance(s)* $\geq$ *classification(o)*
- *allowed(s,o,write)* $\Rightarrow$ *clearance(s)* $\leq$ *classification(o)*

DAC in UCON: *with ACL ($UCON_{preA0}$)*

- *N* is a set of identity names
- $id : S \rightarrow N$, one to one mapping
- $ACL : O \rightarrow 2^{N \times R}$, *n* is authorized to do *r* to *o*
- *ATT(S)= {id}*
- *ATT(O)= {ACL}*
- $allowed(s,o,r) \Rightarrow (id(s),r) \in ACL(o)$

RBAC in UCON: *$RBAC_1$ ($UCON_{preA0}$)*

- *P = {(o,r)}*
- *ROLE* is a partially ordered set of roles with dominance relation ≥
- $actRole: S \rightarrow 2^{ROLE}$
- $Prole: P \rightarrow 2^{ROLE}$
- *ATT(S) = {actRole}*
- *ATT(O) = {Prole}*
- $allowed(s,o,r) \Rightarrow \exists role \in actRole(s), \exists role' \in Prole(o,r), role \geq role'$

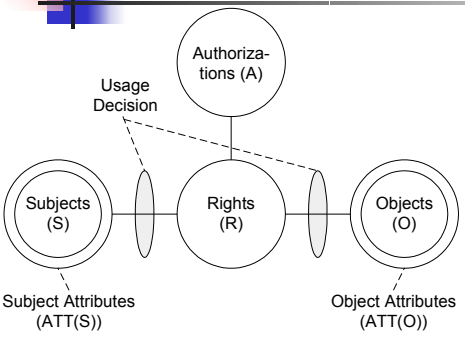
DRM in UCON: *Pay-per-use with a pre-paid credit ($UCON_{preA1}$)*

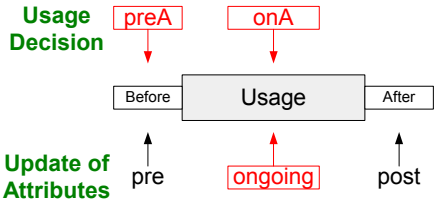
- *M* is a set of money amount
- *credit: S → M*
- *value: O x R → M*
- *ATT(s): {credit}*
- *ATT(o,r): {value}*
- *allowed(s,o,r) ⇒ credit(s) ≥ value(o,r)*
- *preUpdate(credit(s)): credit(s) = credit(s) - value(o,r)*

$UCON_{preA3}$: DRM Example

- Membership-based metered payment
  - *M* is a set of money amount
  - *ID* is a set of membership identification numbers
  - *TIME* is a current usage minute
  - *member: S → ID*
  - *expense: S → M*
  - *usageT: S → TIME*
  - *value: O x R → M* (a cost per minute of r on o)
  - *ATT(s): {member, expense, usageT}*
  - *ATT(o,r): {valuePerMinute}*
  - *allowed(s,o,r) ⇒ member(s) ≠ ∅*
  - *postUpdate(expense(s)): expense(s) = expense(s) + (value(o,r) x usageT(s))*

$UCON_{onA}$



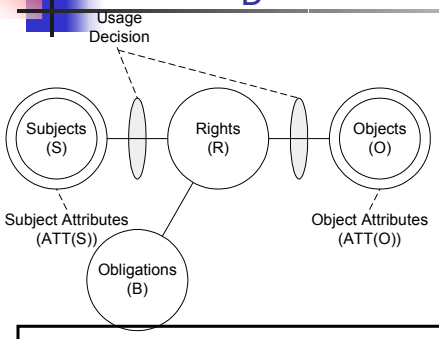


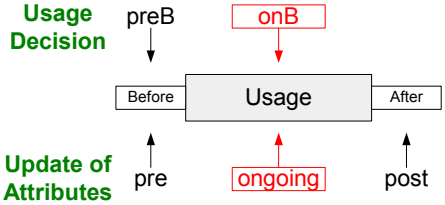
- Pay-per-minutes (pre-paid Phone Card)

$UCON_{onA}$: ongoing-Authorizations Model

- $UCON_{onA0}$
  - *S, O, R, ATT(S), ATT(O)* and *onA*;
  - *allowed(s,o,r)* $\Rightarrow$ *true;*
  - *Stopped(s,o,r)* $\Leftarrow \neg$*onA(ATT(s),ATT(o),r)*
- $UCON_{onA1}$, $UCON_{onA2}$, $UCON_{onA3}$
  - *preUpdate(ATT(s)),preUpdate(ATT(o))*
  - *onUpdate(ATT(s)),onUpdate(ATT(o))*
  - *postUpdate(ATT(s)),postUpdate(ATT(o))*
- Examples
  - Certificate Revocation Lists
  - revocation based on starting time, longest idle time, and total usage time

$UCON_B$





- Free Internet Service Provider
  - Watch Ad window (no update)
  - Click ad within every 30 minutes (ongoing update)

$UCON_{preB0}$: pre-oBligations w/ no update

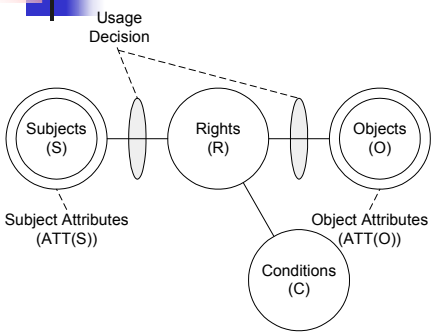
- *S, O, R, ATT(S),* and *ATT(O)*;
- *OBS, OBO* and *OB* (obligation subjects, obligation objects, and obligation actions, respectively);
- *preB* and *preOBL* (pre-obligations predicates and pre-obligation elements, respectively);
- $preOBL \subseteq OBS \times OBO \times OB$;
- $preFulfilled: OBS \times OBO \times OB \rightarrow \{true,false\}$;
- $getPreOBL: S \times O \times R \rightarrow 2^{preOBL}$, a function to select pre-obligations for a requested usage;
- $preB(s,o,r) = \Lambda_{(obs\_i,obo\_i,ob\_i) \in getPreOBL(s,o,r)}\ preFulfilled(obs_i,obo_i,ob_i)$;
- $preB(s,o,r) = true$ by definition if $getPreOBL(s,o,r)=\varnothing$;
- $allowed(s,o,r) \Longrightarrow preB(s,o,r)$.
- Example: License agreement for a whitepaper download

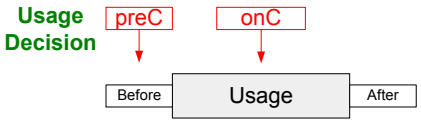
$UCON_{onB0}$: ongoing-oBligations w/ no update

- *S, O, R, ATT(S), ATT(O), OBS, OBO* and *OB*;
- *T*, a set of time or event elements;
- *onB* and on*OBL* (on-obligations predicates and ongoing-obligation elements, respectively);
- $onOBL \subseteq OBS \times OBO \times OB \times T$;
- $onFulfilled: OBS \times OBO \times OB \times T \rightarrow \{true,false\}$;
- $getOnOBL: S \times O \times R \rightarrow 2^{onOBL}$, a function to select ongoing-obligations for a requested usage;
- $onB(s,o,r) = \Lambda_{(obs\_i,obo\_i,ob\_i,\ t\_i) \in\ getOnOBL(s,o,r)}\ onFulfilled(obs_i,obo_i,ob_i,t_i)$;
- $onB(s,o,r) = true$ by definition if $getOnOBL(s,o,r)=\varnothing$;
- $allowed(s,o,r) \Rightarrow true$;
- $Stopped(s,o,r) \Leftarrow \neg\ onB(s,o,r)$.

- Example: Free ISP with mandatory ad window

$UCON_C$





Update of Attributes: **No-Update is possible**

- Location check at the time of access request
- Accessible only during business hours

$UCON_{preC0}$: pre-Condition model

- *S, O, R, ATT(S),* and *ATT(O)*;
- *preCON* (a set of pre-condition elements);
- *preConChecked: preCON* $\rightarrow$ *{true,false}*;
- *getPreCON: S x O x R* $\rightarrow 2^{preCON}$;
- $preC(s,o,r) = \Lambda_{preCon\_i \in getPreCON(s,o,r)}\ preConChecked(preCon_i)$;
- $allowed(s,o,r) \Rightarrow preC(s,o,r)$.

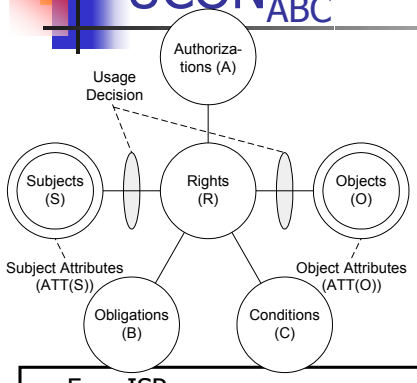
- Example: location checks at the time of access requests

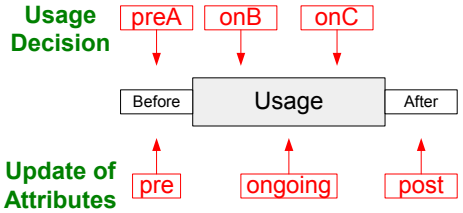
$UCON_{onC0}$: ongoing-Condition model

- *S, O, R, ATT(S),* and *ATT(O)*;
- *onCON* (a set of on-condition elements);
- *onConChecked: onCON* $\rightarrow$ *{true,false}*;
- *getOnCON: S x O x R* $\rightarrow 2^{onCON}$;
- $onC(s,o,r) = \Lambda_{onCon\_i \in getOnCON(s,o,r)}\ onConChecked(onCon_i)$;
- $allowed(s,o,r) \Rightarrow true$;
- $Stopped(s,o,r) \Leftarrow \neg onC(s,o,r)$

- Example: accessible during office hour

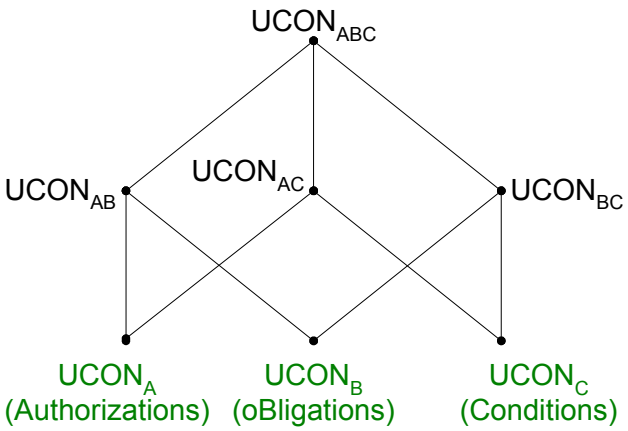
UCON$_{ABC}$



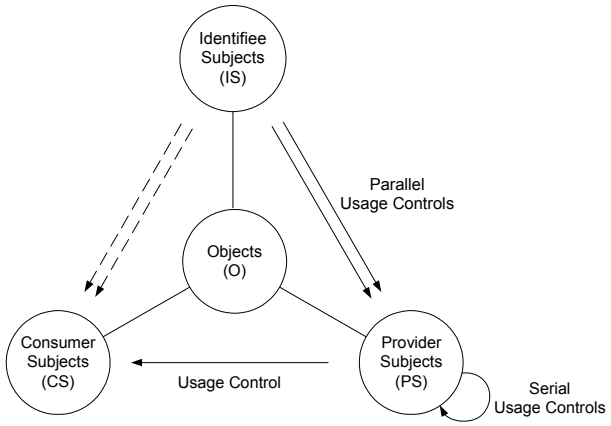


- Free ISP
  - Membership is required (pre-authorization)
  - Have to click Ad periodically while connected (on-obligation, on-update)
  - Free member: no evening connection (on-condition), no more than 50 connections (pre-update) or 100 hours usage per month (post-updates)

ABC Models



Beyond the ABC Core Models



Conclusion

- Developed A family of ABC core models for Usage Control (UCON) to unify *traditional access control models, DRM*, and other modern enhanced models.
- ABC model integrates *authorizations, obligations, conditions*, as well as *continuity* and *mutability* properties.

Future Research

- Enhance the model
  - UCON administration or management
  - Detail of update procedure in ABC model
  - Delegation of usage rights
- Develop Architectures and Mechanisms
  - Payment-based architectures
  - CRM and SRM
  - Architectures for multi-organizations (B2B)
- UCON Engineering
  - Analysis of policy
  - Designing/modeling rules and Attributes

Publications

- Jaehong Park and Ravi Sandhu, "*The ABC Core Model for Usage Control: Integrating Authorizations, oBligations, and Conditions*" to appear on ACM Transactions on Information and System Security (TISSEC), 2004
- Ravi Sandhu and Jaehong Park, "*Usage Control: A vision for Next Generation Access Control*" to appear on The Second International Workshop "Mathematical Methods, Models and Architectures for Computer Networks Security (MMM-ACNS), Sep. 2003.
- Jaehong Park and Ravi Sandhu, "*Towards Usage Control Models: Beyond Traditional Access Control*" In Proceedings of 7th ACM Symposium on Access Control Models and Technologies, Jun. 2002
- Jaehong Park and Ravi Sandhu, "*Originator Control in Usage Control*" In Proceedings of 3rd International Workshop on Policies for Distributed Systems and Networks, pp. 60-66, IEEE, Jun. 2002
- Jaehong Park, Ravi Sandhu, and James Schifalacqua, "*Security Architectures for Controlled Digital information Dissemination*." In Proceedings of Annual Computer Security Applications Conference (ACSAC), pp. 224-233, Dec. 2000