

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

© 2003 GMU LIST

2

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

© 2003 GMU LIST

3

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]

© 2003 GMU LIST

4

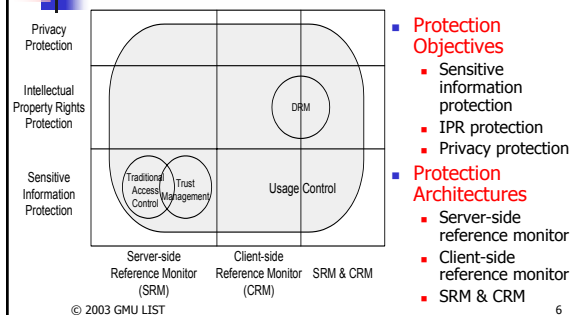
Problem Statement

- 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

© 2003 GMU LIST

5

Usage Control (UCON) Coverage



© 2003 GMU LIST

6

OM-AM layered Approach

What ?	Objective	Policy Neutral
	Model	ABC model
How ?	Architecture	CRM/SRM, CDID architectures
	Mechanism	DRM technologies, certificates, etc.

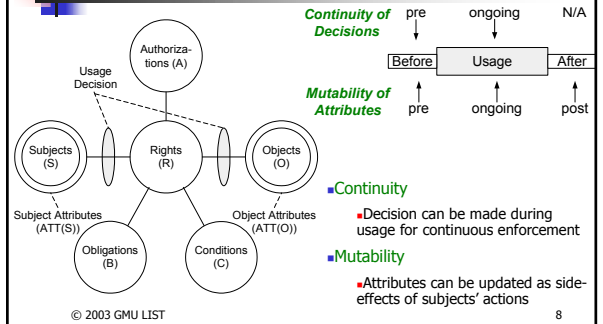
OM-AM Framework Usage Control System Assurance

- ABC core models for UCON

© 2003 GMU LIST

7

Building ABC Models



8

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)

© 2003 GMU LIST

9

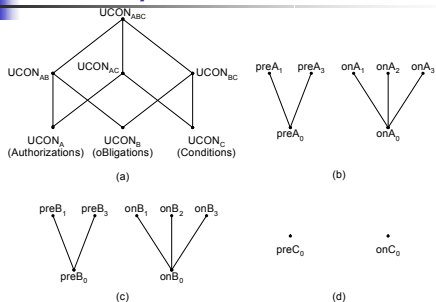
ABC Model Space

	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
© 2003 GMU LIST

10

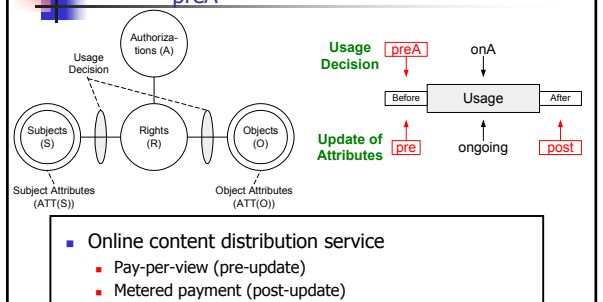
A Family of ABC Core Models



© 2003 GMU LIST

11

UCON_{preA}



12

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: *RBAC₁* (UCON_{preA0})

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

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

- M is a set of money amount
- $credit: S \rightarrow M$
- $value: O \times R \rightarrow M$
- $ATT(s): \{credit\}$
- $ATT(o,r): \{value\}$
- $allowed(s,o,r) \Rightarrow credit(s) \geq value(o,r)$
- $preUpdate(credit(s)): credit(s) = credit(s) - value(o,r)$

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
 - $member: S \rightarrow ID$
 - $expense: S \rightarrow M$
 - $usageT: S \rightarrow TIME$
 - $value: O \times R \rightarrow M$ (a cost per minute of r on o)
 - $ATT(s): \{member, expense, usageT\}$
 - $ATT(o,r): \{valuePerMinute\}$
 - $allowed(s,o,r) \Rightarrow member(s) \neq \emptyset$
 - $postUpdate(expense(s)): expense(s) = expense(s) + (value(o,r) \times usageT(s))$

UCON_{onA}

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

© 2003 GMU LIST 19

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_{onA1r}, UCON_{onA2r}, 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

© 2003 GMU LIST 20

UCON_B

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

© 2003 GMU LIST 21

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;
- $preB(s,o,r) = \bigwedge_{(obs_i, obo_i, ob_i) \in getPreOBL(s,o,r)} preFulfilled(obs_i, obo_i, ob_i)$;
- $preB(s,o,r) = true$ by definition if $getPreOBL(s,o,r) = \emptyset$;
- $allowed(s,o,r) \Rightarrow preB(s,o,r)$.

- Example: License agreement for a whitepaper download

© 2003 GMU LIST 22

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 $onOBL$ (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;
- $onB(s,o,r) = \bigwedge_{(obs_i, obo_i, ob_i, t_i) \in getOnOBL(s,o,r)} onFulfilled(obs_i, obo_i, ob_i, t_i)$;
- $onB(s,o,r) = true$ by definition if $getOnOBL(s,o,r) = \emptyset$;
- $allowed(s,o,r) \Rightarrow true$;
- $Stopped(s,o,r) \Leftarrow \neg onB(s,o,r)$.

- Example: Free ISP with mandatory ad window

© 2003 GMU LIST 23

UCON_C

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

© 2003 GMU LIST 24

UCON_{preC0}: pre-Condition model

- $S, O, R, ATT(S)$, and $ATT(O)$;
 - $preCON$ (a set of pre-condition elements);
 - $preConChecked: preCON \rightarrow \{true, false\}$;
 - $getPreCON: S \times O \times R \rightarrow 2^{preCON}$;
 - $preC(s,o,r) = \bigwedge_{preCon_i \in getPreCON(s,o,r)} preConChecked(preCon_i)$;
 - $allowed(s,o,r) \Rightarrow preC(s,o,r)$.
- Example: location checks at the time of access requests

© 2003 GMU LIST

25

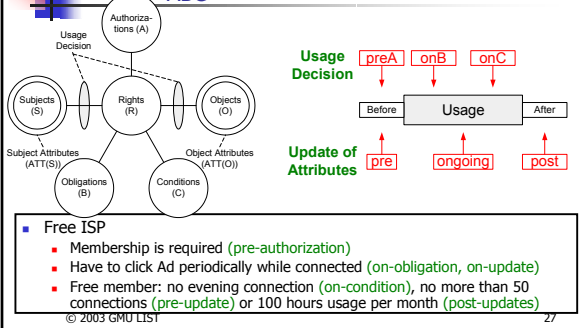
UCON_{onC0}: ongoing-Condition model

- $S, O, R, ATT(S)$, and $ATT(O)$;
 - $onCON$ (a set of on-condition elements);
 - $onConChecked: onCON \rightarrow \{true, false\}$;
 - $getOnCON: S \times O \times R \rightarrow 2^{onCON}$;
 - $onC(s,o,r) = \bigwedge_{onCon_i \in getOnCON(s,o,r)} onConChecked(onCon_i)$;
 - $allowed(s,o,r) \Rightarrow true$;
 - $Stopped(s,o,r) \Leftarrow \neg onC(s,o,r)$
- Example: accessible during office hour

© 2003 GMU LIST

26

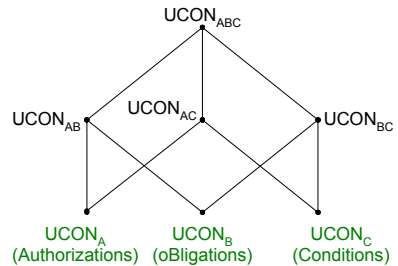
UCON_{ABC}



© 2003 GMU LIST

27

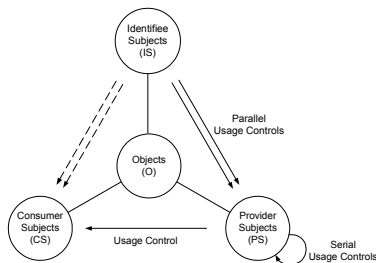
ABC Models



© 2003 GMU LIST

28

Beyond the ABC Core Models



© 2003 GMU LIST

29

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.

© 2003 GMU LIST

30



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