Semantics-Enabled Web Policies for Privacy Protection: Current Status and Future Trend

Prof. Dr. Yuh-Jong Hu

Emerging Network Technology(ENT) Lab.
Department of Computer Science
National Chengchi University, Taipei, Taiwan

Dec.-15th-2010

IM.NUU Seminar

Part I

Research Goals

Short Term Research Goals

Semantics-Enabled privacy protection policies

- A formal semantic policy model of P3P and EPAL
- Data sharing and protection on the Web
- Data integration and protection in the cloud

Current Status[16]

- Semantics-enabled of privacy protection policies
- Policies alignment between semantics-enabled P3P and EPAL
- A semantic privacy-preserving model for data sharing and integration

Short Term Research Goals

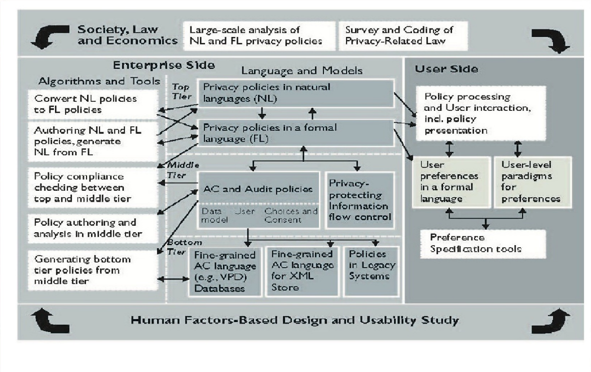
Semantics-Enabled privacy protection policies

- A formal semantic policy model of P3P and EPAL
- Data sharing and protection on the Web
- Data integration and protection in the cloud

Current Status[16]

- Semantics-enabled of privacy protection policies
- Policies alignment between semantics-enabled P3P and EPAL
- A semantic privacy-preserving model for data sharing and integration

The Framework for an Online Privacy Policy Management



–Annie I. Ant'on et al., CACM, 50(7), July 2007.

Long Term Research Goals

SemPIF Framework: PIF + Meta-PIF

- Policy Interchange Format (PIF)
- Meta-PIF for policy management services

Legalized Computer-Enabled Policy

- Semantics-enabled privacy protection policies and systems
- Enforcing privacy policies across multiple domains
- Legalized privacy protection policies

Long Term Research Goals

SemPIF Framework: PIF + Meta-PIF

- Policy Interchange Format (PIF)
- Meta-PIF for policy management services

Legalized Computer-Enabled Policy

- Semantics-enabled privacy protection policies and systems
- Enforcing privacy policies across multiple domains
- Legalized privacy protection policies

Part II

Semantics-Enabled Web Policies

Policy Representation

Natural Language

- Pros: human readable and understandable
- Cons: machine unfriendly, no formal semantics

Pure FOL

- Pros: formal and clear syntax and semantics
- Cons: machine unfriendly, possibly undecidable computation; policy writer (or reader) needs to be a logician

Policy Representation

Natural Language

- Pros: human readable and understandable
- Cons: machine unfriendly, no formal semantics

Pure FOL

- Pros: formal and clear syntax and semantics
- Cons: machine unfriendly, possibly undecidable computation; policy writer (or reader) needs to be a logician

Policy Representation (conti.)

Rights Expression Languages

- Pros: machine processing of its XML-based documents
- Cons: no formal semantics for the machine

Ontology+Rule with XML Presentation Syntax

- Pros: automatic machine processing and understanding
- Cons: limited expressing power under some conditions

Policy Representation (conti.)

Rights Expression Languages

- Pros: machine processing of its XML-based documents
- Cons: no formal semantics for the machine

Ontology+Rule with XML Presentation Syntax

- Pros: automatic machine processing and understanding
- Cons: limited expressing power under some conditions

What Do You Mean Computer-Based Policies?

Definition (Computer-Based Policies)

- Declared as knowledge bases, i.e., ontologies and rules
- Reducing program coding to a minimum level
- Framework supports policy interoperability
- Low deployment and maintenance cost
- Machine understandable on context of policies

Policy Specification, Enforcement, and Integration, WG I2, REWERSE FP6

What Do You Mean Meta-Policies?

Definition (Meta-Policy)

- A policy about policies
- Enforcing policy management services for adding/changing/coordination
- Allowing to set up policy priority to enforce, negotiate, and resolve conflicts of multi-policies

Hosmer, H. H., Metapolicies I, ACM SIGSAC Review, 1992

XML-Based Policy Lacks Semantics

XML-based Policy Languages

- XrML [18] ⇐ digital rights expression language
- ODRL [17] ⇐ digital rights expression language
- P3P [6] ⇐ privacy rights expression language
- EP3P (EPAL) [2] ⇐ privacy rights expression language
- XACML [2] ⇐ general policy language and framework

Pure FOL-Based Policies Are Not Web-Enabled

Formal semantics of policies in DL or LP

- Semantic ODRL [27] $\Leftarrow$ FOL semantics
- Semantic XrML [11] $\Leftarrow$ FOL semantics
- Semantic P3P [34] $\Leftarrow$ relational semantics
- FAF [19] $\Leftarrow$ LP semantics
- Semantic E-P3P (or EPAL) [2] $\Leftarrow$ FAF semantics
- Rein, KAoS [32] $\Leftarrow$ DL-based FOL semantics
- Protune [4] $\Leftarrow$ LP semantics
- AIR [1] $\Leftarrow$ RDF semantics

Pure FOL-Based Policies Are Not Web-Enabled

Formal semantics of policies in DL or LP

- Semantic ODRL [27] $\Leftarrow$ FOL semantics
- Semantic XrML [11] $\Leftarrow$ FOL semantics
- Semantic P3P [34] $\Leftarrow$ relational semantics
- FAF [19] $\Leftarrow$ LP semantics
- Semantic E-P3P (or EPAL) [2] $\Leftarrow$ FAF semantics
- Rein, KAoS [32] $\Leftarrow$ DL-based FOL semantics
- Protune [4] $\Leftarrow$ LP semantics
- AIR [1] $\Leftarrow$ RDF semantics

Semantics-Enabled Web Policies

Policies in semantic web languages

- Ontology Languages: RDF(S), OWL-DL, OWL2
- Rules Languages: N3, RuleML, RIF
- Ontology+Rule Language: SWRL, OWL2-RL

Semantics-Enabled Web Policies (conti.)

Why use ontology+rule?

- Exploiting two semantic web core technologies
- Automatic machine processing of policies
- Major knowledge representations on the Web
- Allowing policy interchange, interoperation, and integration

Why not use ontologies or rules alone?

- Policies might be in DL or in LP semantics
- Power enhancement from ontologies and rules
- Options to use ontologies, rules alone or both

Semantics-Enabled Web Policies (conti.)

Why use ontology+rule?

- Exploiting two semantic web core technologies
- Automatic machine processing of policies
- Major knowledge representations on the Web
- Allowing policy interchange, interoperation, and integration

Why not use ontologies or rules alone?

- Policies might be in DL or in LP semantics
- Power enhancement from ontologies and rules
- Options to use ontologies, rules alone or both

Semantics-Enabled Web Policies (conti.)

Which ontology+rule combination for Policies?

- Issues to consider:
  1. Decidability of computation
  2. Expressive power of ontology+rule
  3. Semantics differences between DL and LP
  4. Uni-(or bi-)directional of knowledge flow
  5. Homogeneous of ontology+rule
  6. Heterogeneous of ontology+rule

Semantics-Enabled Web Policy (conti.)

Homogeneous of Ontology+Rule [30]

- CARIN [21]
- Description Logic Program (DLP) [9]
- Semantic Web Rule Language (SWRL) [13]
- OWL2-RL

Part III

Privacy Protection Policies

Privacy Protection on the Web

Privacy Protection on the Web 1.0

- Policy representation through natural language
- Profile and digital traces
- Policies and mechanisms are embedded together
- Whether policies comply with the laws? Unknown!

Privacy Protection on the Web 2.0

- Information disclosure's opt-in/opt-out
- Digital traces protection is an issue
- Policy compliance? Still unknown!

Privacy Protection on the Web 1.0

- Policy representation through natural language
- Profile and digital traces
- Policies and mechanisms are embedded together
- Whether policies comply with the laws? Unknown!

Privacy Protection on the Web 2.0

- Information disclosure's opt-in/opt-out
- Digital traces protection is an issue
- Policy compliance? Still unknown!

Privacy Protection on the Web 3.0

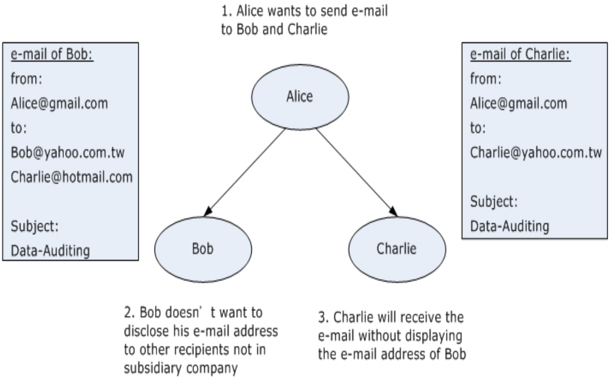
- Decoupling policies and mechanisms
- Semantics-enabled of profile and digital traces format
- Machine automatic enforcement of policies
- Machine auditing and verifying the compliance of policies

Natural Language for Mail Sending Policies

Example (Policies as Natural Language)

Under company *SD* internal regulation, anyone sends an email through a mailing list with multiple recipients, where email recipients $\in SD$ cannot be disclosed his/her email address to those people not $\in SD$ domain under any purposes. Therefore, the email recipient $Charlie \in CP$ cannot explicitly see the email address of the recipient $Bob \in SD$ in his receiving email address header.

Non-disclosure of a recipient's email address



Ontology Module

Example (Axiom in an Ontology Module)

- $COMPANY \sqsubseteq PRIVATE$
- $PRIVATE \sqsubseteq ORGANIZATION$
- $OWNER \sqsubseteq PERSON$
- $COMPANY \xleftarrow{domain} HAS\_COOPERATIVE \xrightarrow{range} COMPANY$
- $COMPANY \xleftarrow{domain} HAS\_SUBSIDIARY \xrightarrow{range} COMPANY$
- $HAS\_COOPERATIVE \equiv HAS\_COOPERATIVE^{-}$
- $PERSON \xleftarrow{domain} IS\_STAFF\_OF \xrightarrow{range} ORGANIZATION$
- $MAIL\_TRACE \xleftarrow{domain} HAS\_MAIL\_TRACE \xrightarrow{range} EMAIL$
- $EMAIL \sqsubseteq \exists\ HAS\_MAIL\_TRACE\_ONLINE^{-}.O\_EMAIL\_SENDER$
- $EMAIL \sqsubseteq \forall\ HAS\_MAIL\_TRACE\_ONLINE.O\_EMAIL\_RECEIVER$
- $DATA\_AUDIT\_ANNOUN. \sqsubseteq AUDIT\_ANNOUN.$

Ontology Module

EXAMPLE (AXIOM IN AN ONTOLOGY MODULE)

- $COMPANY \sqsubseteq PRIVATE$
- $PRIVATE \sqsubseteq ORGANIZATION$
- $OWNER \sqsubseteq PERSON$
- $COMPANY \xleftarrow{domain} HAS\_COOPERATIVE \xrightarrow{range} COMPANY$
- $COMPANY \xleftarrow{domain} HAS\_SUBSIDIARY \xrightarrow{range} COMPANY$
- $HAS\_COOPERATIVE \equiv HAS\_COOPERATIVE^{-}$
- $PERSON \xleftarrow{domain} IS\_STAFF\_OF \xrightarrow{range} ORGANIZATION$
- $MAIL\_TRACE \xleftarrow{domain} HAS\_MAIL\_TRACE \xrightarrow{range} EMAIL$
- $EMAIL \sqsubseteq \exists\, HAS\_MAIL\_TRACE\_ONLINE^{-}.O\_EMAIL\_SENDER$
- $EMAIL \sqsubseteq \forall\, HAS\_MAIL\_TRACE\_ONLINE.O\_EMAIL\_RECEIVER$
- $DATA\_AUDIT\_ANNOUN. \sqsubseteq AUDIT\_ANNOUN.$

Ontology Module

Example (Facts in an Ontology Module)

- *ORGANIZATION(G)*
- *HAS_SUBSIDIARY(G, J-Corp.)*
- *HAS_COOPERATIVE(G, Q-Corp.)*
- *IS_STAFF_OF(Alice, J-Corp.)*
- *IS_STAFF_OF(Bob, J-Corp.)*
- *IS_STAFF_OF(Charlie, Q-Corp.)*
- *HAS_EMAIL_ADDRESS (Charlie,Charlie@hotmail.com)*
- *O_EMAIL_RECEIVER(Bob@yahoo.com.tw)*
- *HAS_EMAIL_ADDRESS (Alice,Alice@gmail.com)*
- *HAS_EMAIL_ADDRESS (Bob,Bob@yahoo.com.tw)*
- *O_EMAIL_SENDER(Alice@gmail.com),*
- *O_EMAIL_RECEIVER (Charlie@hotmail.com)*
- *HAS_MAIL_TRACE_ONLINE (Alice@gmail.com,Bob@yahoo.com.tw)*
- *HAS_MAIL_TRACE_ONLINE (Alice@gmail.com,Charlie@hotmail.com)*

Ontology Module

Example (Facts in an Ontology Module)

- *ORGANIZATION(G)*
- *HAS_SUBSIDIARY(G, J-Corp.)*
- *HAS_COOPERATIVE(G, Q-Corp.)*
- *IS_STAFF_OF(Alice, J-Corp.)*
- *IS_STAFF_OF(Bob, J-Corp.)*
- *IS_STAFF_OF(Charlie, Q-Corp.)*
- *HAS_EMAIL_ADDRESS (Charlie,Charlie@hotmail.com)*
- *O_EMAIL_RECEIVER(Bob@yahoo.com.tw)*
- *HAS_EMAIL_ADDRESS (Alice,Alice@gmail.com)*
- *HAS_EMAIL_ADDRESS (Bob,Bob@yahoo.com.tw)*
- *O_EMAIL_SENDER(Alice@gmail.com),*
- *O_EMAIL_RECEIVER (Charlie@hotmail.com)*
- *HAS_MAIL_TRACE_ONLINE (Alice@gmail.com,Bob@yahoo.com.tw)*
- *HAS_MAIL_TRACE_ONLINE (Alice@gmail.com,Charlie@hotmail.com)*

Rule Module

Example (Rules in a Rule Module)

- **cando**(*?c,?b-email, display)*
  $\Longleftarrow$ *opt-in(?b,?b-email,?p)), data-user(?c), data-owner(?b), HAS_EMAIL_ADDRESS(?b,?b-email).* $\leftarrow$ *(a1)*
- **cando**(*?c,?b-email, nill)*
  $\Longleftarrow$ *opt-out(?b,?b-email,?p)), data-user(?c), data-owner(?b), HAS_EMAIL_ADDRESS(?b, ?b-email).* $\leftarrow$ *(a2)*
- *opt-in(?b,?b-email,?p)*
  $\Longleftarrow$ *data-owner(?b), data-user(?c), purpose(?p), data-type(?b-email), IS_STAFF_OF(?b,?c1), IS_STAFF_OF(?c, ?c2), HAS_SUBSIDIARY(?c1,?c2), HAS_MAIL_TRACE_ONLINE(?a-email,?c-email), O_EMAIL_SENDER(?a-email), O_EMAIL_RECEIVER(?c-email).* $\leftarrow$ *(a3)*
- *opt-out(?b,?b-email,?p)*
  $\Longleftarrow$ *data-owner(?b), data-user(?c), purpose(?p), data-type(?b-email), IS_STAFF_OF(?b,?c1), IS_STAFF_OF(?c, ?c2), HAS_COOPERATIVE(?c1,?c2), HAS_MAIL_TRACE_ONLINE(?a-email,?c-email), O_EMAIL_SENDER(?a-email), O_EMAIL_RECEIVER(?c-email).* $\leftarrow$ *(a4)*

Rule Module

Example (Rules in a Rule Module)

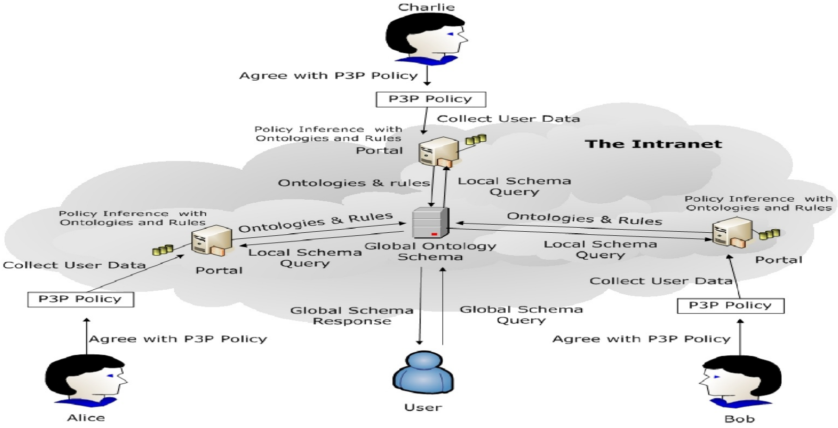
- **cando***(?c,?b-email, display)*
  $\Longleftarrow$ *opt-in(?b,?b-email,?p)), data-user(?c), data-owner(?b),*
  HAS_EMAIL_ADDRESS(?b,?b-email). $\leftarrow$ *(a1)*
- **cando***(?c,?b-email, nill)*
  $\Longleftarrow$ *opt-out(?b,?b-email,?p)), data-user(?c), data-owner(?b),*
  HAS_EMAIL_ADDRESS(?b, ?b-email). $\leftarrow$ *(a2)*
- *opt-in(?b,?b-email,?p)*
  $\Longleftarrow$ *data-owner(?b), data-user(?c), purpose(?p), data-type(?b-email),*
  IS_STAFF_OF(?b,?c1), IS_STAFF_OF(?c, ?c2), HAS_SUBSIDIARY(?c1,?c2),
  HAS_MAIL_TRACE_ONLINE(?a-email,?c-email),
  O_EMAIL_SENDER(?a-email), O_EMAIL_RECEIVER(?c-email). $\leftarrow$ *(a3)*
- *opt-out(?b,?b-email,?p)*
  $\Longleftarrow$ *data-owner(?b), data-user(?c), purpose(?p), data-type(?b-email),*
  IS_STAFF_OF(?b,?c1), IS_STAFF_OF(?c, ?c2), HAS_COOPERATIVE(?c1,?c2),
  HAS_MAIL_TRACE_ONLINE(?a-email,?c-email),
  O_EMAIL_SENDER(?a-email), O_EMAIL_RECEIVER(?c-email). $\leftarrow$ *(a4)*

Rule Module

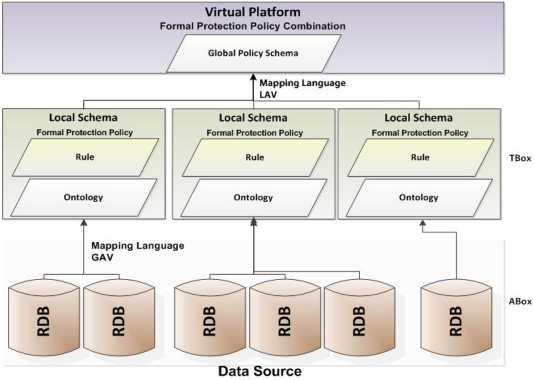
Example (Facts in a Rule Module)

- *data-user(Bob), data-owner(Bob),*
- *data-user(Charlie), data-owner(Charlie),*
- *purpose(data-auditing),*
- *data-type(Bob@yahoo.com.tw),*
- *data-type(Charlie@hotmail.com),*
- *opt-in(c,Charlie@yahoo.com, data-auditing),*
- *cando(Bob,Charlie@yahoo.com,display),*
- *cando(Charlie,Bob@yahoo.com.tw,nill),*
- *opt-out(b,Bob@yahoo.com.tw, data-auditing)*

Semantics-Enabled of P3P and EPAL



A Semantic Privacy Protection Model



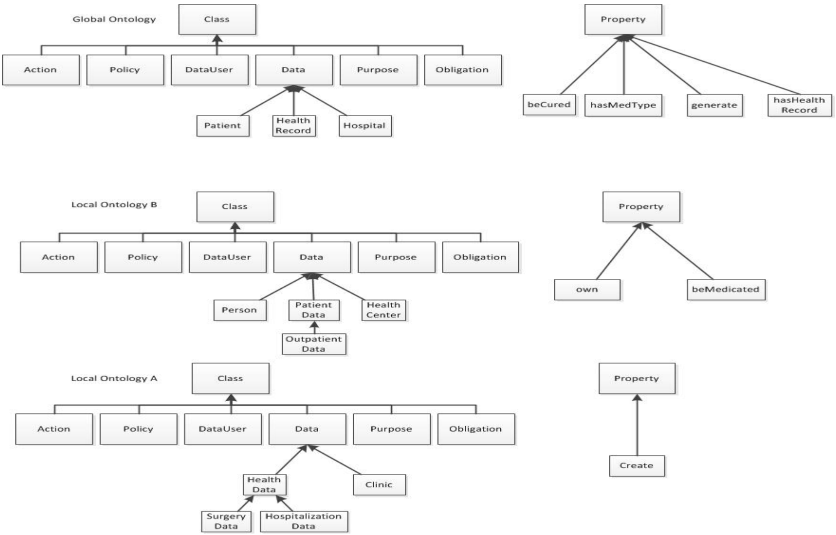
EHR Usage Policies

Example (Policies as Natural Language)

Under the data protection law, two hospitals, `A` and `B`, have allowed to share their patients' Electronic Health Records (EHRs) after patients give their consents for various medication purposes.

A patient was hospitalized in hospital `A` for a surgery. After that, this patient went to hospital `B` for an outpatient medication. A physician in the hospital `B` was authorized to query this patient's shareable EHR at the $\mathcal{VP}$ collected from hospital `A` and hospital `B`'s RDB data sources.

A Partial Ontology for EHR Sharing and Protection



Vocabularies for the Hospital LS_A and LS_B

Partial ontology of LS_A vocabularies

Class:
SurgeryData $\sqsubseteq$ Clinic, HospitalizationData $\sqsubseteq$ HealthData

Property:
T $\sqsubseteq \forall$ create.Hospital, T $\sqsubseteq \forall$ create$^-$.HealthData

Partial ontology of LS_B vocabularies

Class:
Person, HealthCenter, OutPatientData $\sqsubseteq$ PatientData

Property:
T $\sqsubseteq \forall$ own.Person, T $\sqsubseteq \forall$ own$^-$.PatientData.

T $\sqsubseteq \forall$ beMedicated.Person, T $\sqsubseteq \forall$ beMedicated$^-$.HealthCenter.

Vocabularies for the Hospital LS_A and LS_B

Partial ontology of LS_A vocabularies

Class:
SurgeryData $\sqsubseteq$ Clinic, HospitalizationData $\sqsubseteq$ HealthData

Property:
$T \sqsubseteq \forall$ create.Hospital, $T \sqsubseteq \forall$ create$^-$.HealthData

Partial ontology of LS_B vocabularies

Class:
Person, HealthCenter, OutPatientData $\sqsubseteq$ PatientData

Property:
$T \sqsubseteq \forall$ own.Person, $T \sqsubseteq \forall$ own$^-$.PatientData.

$T \sqsubseteq \forall$ beMedicated.Person, $T \sqsubseteq \forall$ beMedicated$^-$.HealthCenter.

Views Use at the $\mathcal{VP}$

Views Created from LS_A

$\texttt{def}(\texttt{V1}_{\texttt{Clinic}}) = \texttt{Hospital}$
$\texttt{def}(\texttt{V2}_{\texttt{HealthData}}) = \texttt{HealthRecord}$
$\texttt{def}(\texttt{V3}_{\texttt{SuregeryData}}) = \texttt{HealthRecord} \wedge \forall \texttt{hasMedType.Surgery}$
$\texttt{def}(\texttt{V4}_{\texttt{HospitalizationData}}) = \texttt{HealthRecord} \wedge \forall\ \texttt{hasMedType.Hospitalization}$

$\texttt{def}(\texttt{V5}_{\texttt{create}}) = \texttt{generate}$

Views Created from LS_B

$\texttt{def}(\texttt{V6}_{\texttt{Person}}) = \texttt{Patient}$
$\texttt{def}(\texttt{V7}_{\texttt{HealthCenter}}) = \texttt{Hospital}$
$\texttt{def}(\texttt{V8}_{\texttt{PatientData}}) = \texttt{HealthRecord}$
$\texttt{def}(\texttt{V9}_{\texttt{OutPatientData}}) = \texttt{HealthRecord} \wedge \forall\ \texttt{hasMedType.OutPatient}$
$\texttt{def}(\texttt{V10}_{\texttt{beMedicated}}) = \texttt{beCured}$

$\texttt{def}(\texttt{V11}_{\texttt{own}}) = \texttt{hasHealthRecrod}$

Views Use at the $\mathcal{VP}$

Views Created from LS_A

$\texttt{def}(\texttt{V1}_{\texttt{Clinic}}) = \texttt{Hospital}$
$\texttt{def}(\texttt{V2}_{\texttt{HealthData}}) = \texttt{HealthRecord}$
$\texttt{def}(\texttt{V3}_{\texttt{SuregeryData}}) = \texttt{HealthRecord} \wedge \forall \texttt{hasMedType.Surgery}$
$\texttt{def}(\texttt{V4}_{\texttt{HospitalizationData}}) = \texttt{HealthRecord} \wedge \forall \texttt{hasMedType.Hospitalization}$

$\texttt{def}(\texttt{V5}_{\texttt{create}}) = \texttt{generate}$

Views Created from LS_B

$\texttt{def}(\texttt{V6}_{\texttt{Person}}) = \texttt{Patient}$
$\texttt{def}(\texttt{V7}_{\texttt{HealthCenter}}) = \texttt{Hospital}$
$\texttt{def}(\texttt{V8}_{\texttt{PatientData}}) = \texttt{HealthRecord}$
$\texttt{def}(\texttt{V9}_{\texttt{OutPatientData}}) = \texttt{HealthRecord} \wedge \forall \texttt{hasMedType.OutPatient}$
$\texttt{def}(\texttt{V10}_{\texttt{beMedicated}}) = \texttt{beCured}$

$\texttt{def}(\texttt{V11}_{\texttt{own}}) = \texttt{hasHealthRecrod}$

A Physician Queries at the $\mathcal{VP}$

Original Query

$\texttt{Patient}(?x) \wedge \texttt{beCured}(?x, ?y) \wedge \texttt{hasHealthRecrod}(?x, ?r) \wedge \texttt{HealthRecord}(?r) \wedge \texttt{hasMedType}(?r, \texttt{Surgery}) \wedge \texttt{generate}(?y, ?r) \longrightarrow \texttt{sqwrl} : \texttt{select}(?x, ?r)$

Rewriting Queries One

$\texttt{V6}_{\texttt{Person}} \wedge \texttt{V10}_{\texttt{beMedicated}} \wedge \texttt{V11}_{\texttt{own}} \wedge \texttt{V9}_{\texttt{OutPatientData}} \wedge \texttt{V5}_{\texttt{create}} \longrightarrow \texttt{sqwrl} : \texttt{select}(?x, ?r)$

$\texttt{B} : \texttt{Person}(?p) \wedge \texttt{B} : \texttt{beMedicated}(?p, ?c) \wedge \texttt{B} : \texttt{own}(?p, ?d) \wedge \texttt{B} : \texttt{OutPatientData}(?od) \wedge \texttt{A} : \texttt{create}(?h, ?hd) \longrightarrow \texttt{sqwrl} : \texttt{select}(?p, ?od)$

Rewriting Queries Two

$\texttt{V6}_{\texttt{Person}} \wedge \texttt{V10}_{\texttt{beMedicated}} \wedge \texttt{V11}_{\texttt{own}} \wedge \texttt{V3}_{\texttt{SuregeryData}} \wedge \texttt{V5}_{\texttt{create}} \longrightarrow \texttt{sqwrl} : \texttt{select}(?x, ?r)$

$\texttt{B} : \texttt{Person}(?p) \wedge \texttt{B} : \texttt{beMedicated}(?p, ?c) \wedge \texttt{B} : \texttt{own}(?p, ?d) \wedge \texttt{A} : \texttt{SuregeryData}(?sd) \wedge \texttt{A} : \texttt{create}(?h, ?hd) \longrightarrow \texttt{sqwrl} : \texttt{select}(?p, ?sd)$

A Physician Queries at the $\mathcal{VP}$

Original Query

$\mathtt{Patient}(?x) \wedge \mathtt{beCured}(?x, ?y) \wedge \mathtt{hasHealthRecrod}(?x, ?r) \wedge \mathtt{HealthRecord}(?r) \wedge \mathtt{hasMedType}(?r, \mathtt{Surgery}) \wedge \mathtt{generate}(?y, ?r) \longrightarrow \mathtt{sqwrl} : \mathtt{select}(?x, ?r)$

Rewriting Queries One

$\mathtt{V6}_{\mathtt{Person}} \wedge \mathtt{V10}_{\mathtt{beMedicated}} \wedge \mathtt{V11}_{\mathtt{own}} \wedge \mathtt{V9}_{\mathtt{OutPatientData}} \wedge \mathtt{V5}_{\mathtt{create}} \longrightarrow \mathtt{sqwrl} : \mathtt{select}(?x, ?r)$

$\mathtt{B} : \mathtt{Person}(?p) \wedge \mathtt{B} : \mathtt{beMedicated}(?p, ?c) \wedge \mathtt{B} : \mathtt{own}(?p, ?d) \wedge \mathtt{B} : \mathtt{OutPatientData}(?od) \wedge \mathtt{A} : \mathtt{create}(?h, ?hd) \longrightarrow \mathtt{sqwrl} : \mathtt{select}(?p, ?od)$

Rewriting Queries Two

$\mathtt{V6}_{\mathtt{Person}} \wedge \mathtt{V10}_{\mathtt{beMedicated}} \wedge \mathtt{V11}_{\mathtt{own}} \wedge \mathtt{V3}_{\mathtt{SuregeryData}} \wedge \mathtt{V5}_{\mathtt{create}} \longrightarrow \mathtt{sqwrl} : \mathtt{select}(?x, ?r)$

$\mathtt{B} : \mathtt{Person}(?p) \wedge \mathtt{B} : \mathtt{beMedicated}(?p, ?c) \wedge \mathtt{B} : \mathtt{own}(?p, ?d) \wedge \mathtt{A} : \mathtt{SuregeryData}(?sd) \wedge \mathtt{A} : \mathtt{create}(?h, ?hd) \longrightarrow \mathtt{sqwrl} : \mathtt{select}(?p, ?sd)$

A Physician Queries at the $\mathcal{VP}$

Original Query

$\texttt{Patient}(?x) \wedge \texttt{beCured}(?x, ?y) \wedge \texttt{hasHealthRecrod}(?x, ?r) \wedge \texttt{HealthRecord}(?r) \wedge \texttt{hasMedType}(?r, \texttt{Surgery}) \wedge \texttt{generate}(?y, ?r) \longrightarrow \texttt{sqwrl} : \texttt{select}(?x, ?r)$

Rewriting Queries One

$\texttt{V6}_{\texttt{Person}} \wedge \texttt{V10}_{\texttt{beMedicated}} \wedge \texttt{V11}_{\texttt{own}} \wedge \texttt{V9}_{\texttt{OutPatientData}} \wedge \texttt{V5}_{\texttt{create}} \longrightarrow \texttt{sqwrl} : \texttt{select}(?x, ?r)$

$\texttt{B} : \texttt{Person}(?p) \wedge \texttt{B} : \texttt{beMedicated}(?p, ?c) \wedge \texttt{B} : \texttt{own}(?p, ?d) \wedge \texttt{B} : \texttt{OutPatientData}(?od) \wedge \texttt{A} : \texttt{create}(?h, ?hd) \longrightarrow \texttt{sqwrl} : \texttt{select}(?p, ?od)$

Rewriting Queries Two

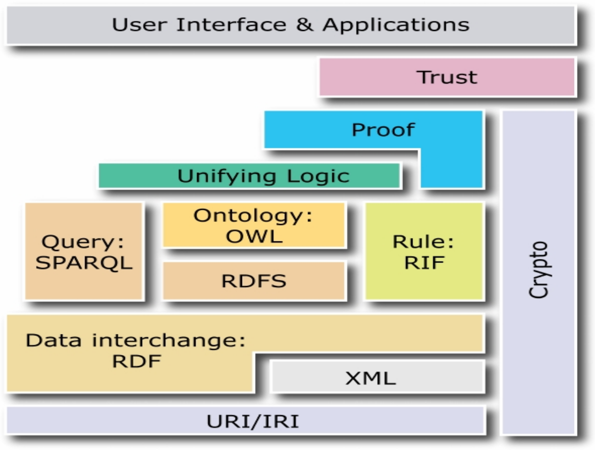
$\texttt{V6}_{\texttt{Person}} \wedge \texttt{V10}_{\texttt{beMedicated}} \wedge \texttt{V11}_{\texttt{own}} \wedge \texttt{V3}_{\texttt{SuregeryData}} \wedge \texttt{V5}_{\texttt{create}} \longrightarrow \texttt{sqwrl} : \texttt{select}(?x, ?r)$

$\texttt{B} : \texttt{Person}(?p) \wedge \texttt{B} : \texttt{beMedicated}(?p, ?c) \wedge \texttt{B} : \texttt{own}(?p, ?d) \wedge \texttt{A} : \texttt{SuregeryData}(?sd) \wedge \texttt{A} : \texttt{create}(?h, ?hd) \longrightarrow \texttt{sqwrl} : \texttt{select}(?p, ?sd)$

Part IV

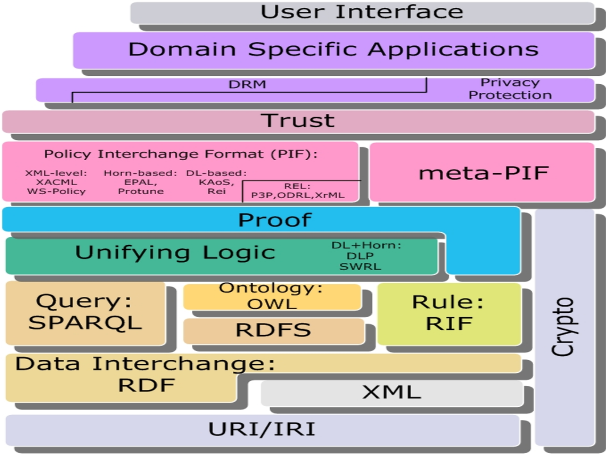
SemPIF (Cooperation with IIT NRC, Canada)

Well-Known Semantic Web Layer Cake (2007 Version)



–http://www.w3.org/2007/03/layerCake.svg

SemPIF Extends Semantic Web Architecture



SemPIF's Related Work

Where Are Current Available Policy Frameworks?

- W3C PLING
- OMG SBVR
- MIT DIG Rein
- FP6 REWERSE Protune
- W3C Policy Working Group Privacy Rulesets

What Are the Features of SemPIF

- Extends from the Semantic Web architecture
- Explicitly decoupling meta-PIF from PIF
- A combination of ontology+rule

SemPIF's Related Work

Where Are Current Available Policy Frameworks?

- W3C PLING
- OMG SBVR
- MIT DIG Rein
- FP6 REWERSE Protune
- W3C Policy Working Group Privacy Rulesets

What Are the Features of SemPIF

- Extends from the Semantic Web architecture
- Explicitly decoupling meta-PIF from PIF
- A combination of ontology+rule

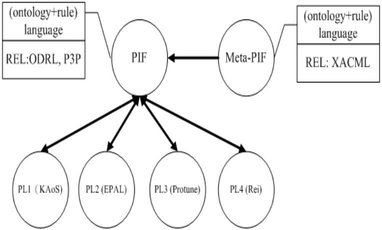
Research Issues in SemPIF

Could be more than the following!

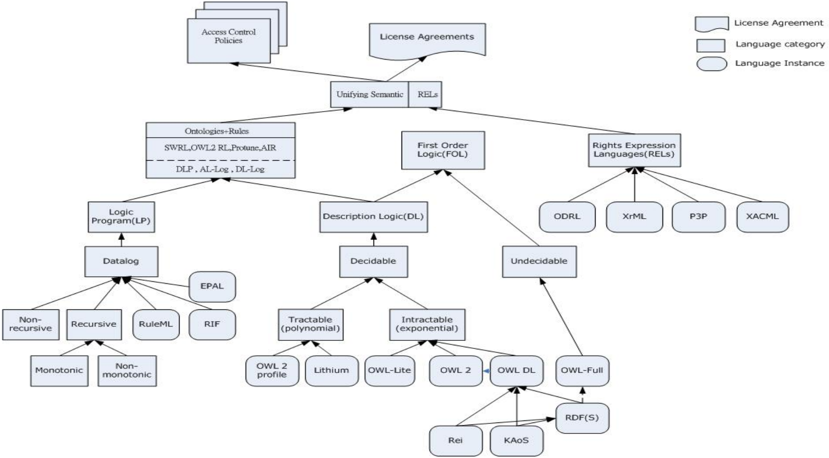
- Policy representation and enforcement
- Policy interoperability and management services
- Policy negotiation and conflict resolution
- Trust establishment on the Web

Policy Management Services in Meta-Policies

- Policies are formulated as knowledge bases, i.e., ontology+rule.
- Meta-policies are also formulated as ontology+rule, which provides a set of rules to enforce policy management services, such as naming/adding/deleting/updating/integration, and conflict resolution, etc.



Taxonomy of Semantic Rights Expression Language for Policies



A Scenario of Digital Library Subscription

Server side's policy description as natural language

- The NCCU university library has subscribed to IEEE, ACM, and Springer digital library services, which provide a set of eJournal article access rights for authorized students and staff.
- There are two types of policy for an IEEE Web server: one is for DRM and the other one is for privacy statement declaration.

Client side's policy description as natural language

- A student, as a Web client, has privacy protection policies to address how and what of his personal data can (or cannot) be collected, retained, or disclosed in a Web server.

A Scenario of Digital Library Subscription

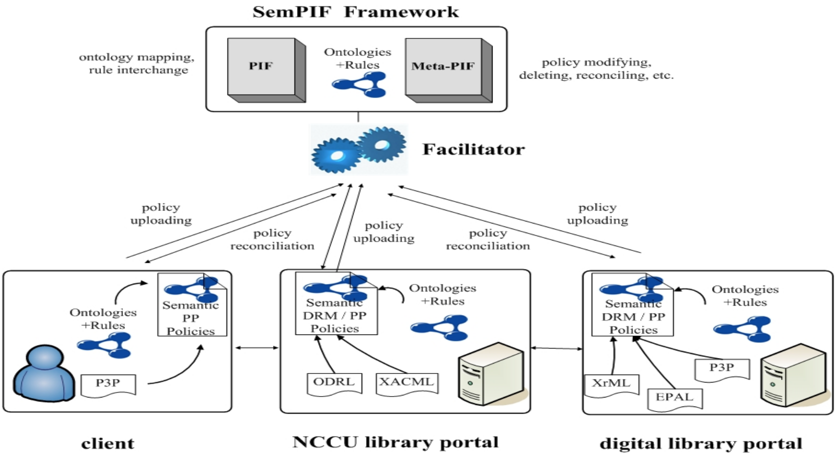
Server side's policy description as natural language

- The NCCU university library has subscribed to IEEE, ACM, and Springer digital library services, which provide a set of eJournal article access rights for authorized students and staff.
- There are two types of policy for an IEEE Web server: one is for DRM and the other one is for privacy statement declaration.

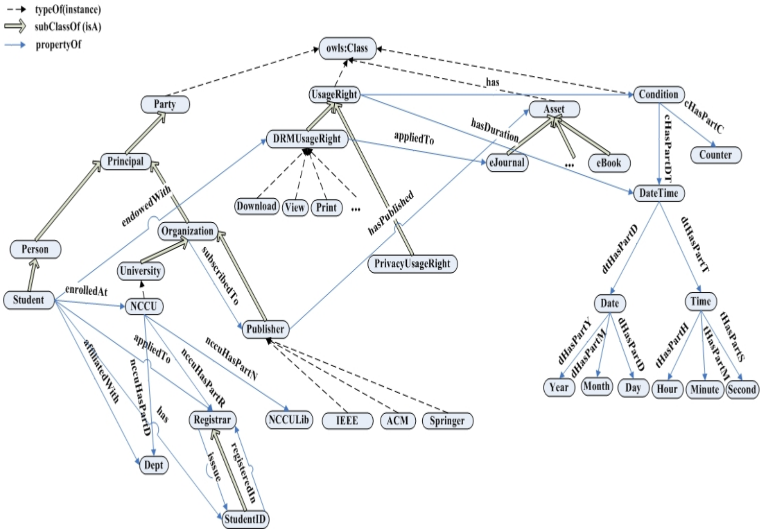
Client side's policy description as natural language

- A student, as a Web client, has privacy protection policies to address how and what of his personal data can (or cannot) be collected, retained, or disclosed in a Web server.

Agents in the Facilitator for Policy Integration Services



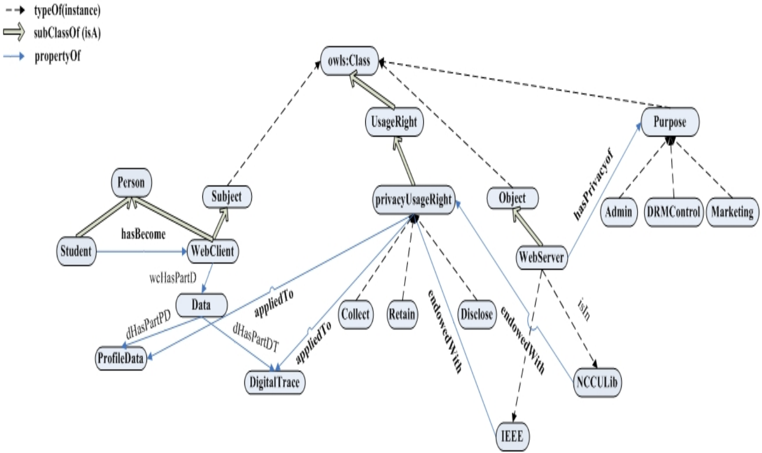
A PIF-based Ontology for a DRM Policy



A PIF-based Rule for a Server's DRM Policy

$$
\begin{aligned}
&\texttt{?st\#Student}\wedge\texttt{?id\#StudentID}\wedge\texttt{?st[own}\rightarrow\texttt{?id]}\\
&\wedge\texttt{?uni[nccuHasPartR}\rightarrow\texttt{?rg]}\wedge\texttt{?st[enrolledAt}\rightarrow\texttt{?uni]}\\
&\wedge\texttt{?rg[issue}\rightarrow\texttt{?id]}\wedge\texttt{?uni[nccuhasPartN}\rightarrow\texttt{?lib]}\\
&\wedge\texttt{?lib[subscribedTo}\rightarrow\texttt{IEEE]}\wedge\texttt{IEEE[hasPublished}\rightarrow\texttt{?ejr]}\\
&\wedge\texttt{IEEE[endowedWith}\rightarrow\texttt{?rgt]}\wedge\texttt{?rgt[appliedTo}\rightarrow\texttt{?ejr]}\\
&\wedge\texttt{IEEE[delegate}\rightarrow\texttt{?st]}\\
\Longrightarrow&\texttt{?st[endowedWith}\rightarrow\texttt{?d]}\wedge\texttt{?st[endowedWith}\rightarrow\texttt{?v]}\\
&\wedge\texttt{?st[endowedWith}\rightarrow\texttt{?p]}\wedge\texttt{?d\#Download}\wedge\texttt{?d[appliedTo}\rightarrow\texttt{?ejr]}\\
&\wedge\texttt{?v\#View}\wedge\texttt{?v[appliedTo}\rightarrow\texttt{?ejr]}\wedge\texttt{?p\#Print}\wedge\texttt{?p[appliedTo}\rightarrow\texttt{?ejr]}.
\end{aligned}
$$

A PIF-based Ontology for a Privacy Protection Policy



A PIF-based Rule for a Client's Privacy Protection Policy

$$
\begin{aligned}
&\texttt{?per[endowedWith} \rightarrow \texttt{?drmr]} \wedge \texttt{?drmr[appliedTo} \rightarrow \texttt{?ejr]}\\
&\wedge \texttt{IEEE[hasPublished} \rightarrow \texttt{?ejr]} \wedge \texttt{IEEE[hasPrivacyOf} \rightarrow \texttt{DRMControl]}\\
&\wedge \texttt{?per[dHasPartPD} \rightarrow \texttt{?prf]} \wedge \texttt{?per[dHasPartDT} \rightarrow \texttt{?dif]}\\
&\wedge \texttt{?per[endowedWith} \rightarrow \texttt{?ppr]} \wedge \texttt{?per[delegate} \rightarrow \texttt{IEEE]}\\
&\wedge \texttt{Retain[hasDuration} \rightarrow = \mathsf{2Month}]\\
&\wedge \texttt{?sdtime[dHasPartD} \rightarrow \texttt{?dtime]} \wedge \texttt{?edtime[dHasPartD} \rightarrow \texttt{?dtime]}\\
&\wedge \mathsf{subtract\text{-}dateTimes}(\texttt{?edtime}, \texttt{?sdtime}) \leq \texttt{Retain}\\
\Longrightarrow\ &\texttt{IEEE[endowedWith} \rightarrow \texttt{?ppr]} \wedge \texttt{?ppr[appliedTo} \rightarrow \texttt{?prf]}\\
&\wedge \texttt{?ppr[appliedTo} \rightarrow \texttt{?dif]}.
\end{aligned}
$$

Conclusion and Future Work

Conclusion

1. Semantics-enabled of privacy protection policies are shown as the SWRL with P3P/APPEL rights expression languages.
2. SemPIF, including PIF and meta-PIF, extends the W3C's Semantic Web architecture.
3. Several use case scenarios demonstrate the applicability of our concepts.

Further Study

- The specification of PIF grammar has not yet been completed. In fact, this is a big challenge.
- Another challenge is to verify the meta-PIF concepts for policy management services on the Web.

Conclusion and Future Work

Conclusion

1. Semantics-enabled of privacy protection policies are shown as the SWRL with P3P/APPEL rights expression languages.
2. SemPIF, including PIF and meta-PIF, extends the W3C's Semantic Web architecture.
3. Several use case scenarios demonstrate the applicability of our concepts.

Further Study

- The specification of PIF grammar has not yet been completed. In fact, this is a big challenge.
- Another challenge is to verify the meta-PIF concepts for policy management services on the Web.

AIR Policy Language http://dig.csail.mit.edu/2009/AIR/.

A. H. Anderson.
A comparison of two privacy policy languages: EPAL and XACML.
In *Proceedings of the 3rd ACM Workshop on Secure Web Services (SWS'06)*, pages 53–60. ACM, 2006.

M. Blaze, J. Figenebaum, and M. Strauss.
Compliance checking in the policymaker trust management system.
In *Proc. of the Financial Cryptography*, LNCS 1465, pages 254–274. Springer, 1998.

Bonatti, P. and D. Olmedilla.
Policy language specification, enforcement, and integration
Project Deliverable D2, Working Group I2,REWERSE, 2005

A. Borgida.
On the relative expressiveness of description logic and predicate logics.
Artificial Intelligence, 82:353–367, 1996.

L. Cranor et al.
The platform for privacy preferences (p3p) 1.0 (p3p 1.0) specification, 2002.
http://www.w3.org/P3P/.

M. F. Donini et al.
AL-log: Integrating Datalog and description logics.
Journal of Intelligent Information Systems, 10(3):227–252, 1998.

R. Garcia, I. Gallego, and J. Delgado.
Formalising ODRL semantics using web ontologies.
In *2nd International ODRL Workshop*, Lisbon, Portugal, July 2005. The Open Digital Rights Language (ODRL) Initiative.
http://odrl.net/workshop2005/.

N. B. Grosof et al.
Description logic programs: Combining logic programs with description logic.
In *World Wide Web 2003*, pages 48–65, Budapest, Hungary, 2003.

S. Guth, G. Neumann, and M. Strembeck.
Experiences with the enforcement of access rights extracted from ODRL-based digital contracts.
In *Digital Rights Management (DRM) Workshop 2003*, Washington, DC, USA, 2003. ACM.

Joseph Y. Halpern and Vicky Weissman.
A formal foundation for XrML.
Journal of the ACM, 55(1):1–42, 2008.

Y. J. Halpern and V. Weissman.
Using first-order logic to reason about policies.
In *Proc. of 16th IEEE Computer Security Foundations Workshop (CSFW'03)*, pages 187–201, July 2003.

I. Horrocks et al.
SWRL: A semantic web rule language combing owl and RuleML, 2004.
http://www.w3.org/Submission/SWRL/.

Ian Horrocks et al.
OWL rules: A proposal and prototype implementation.
J. of Web Semantics, 3(1):23–40, 2005.

Y. J. Hu.
Semantic-driven enforcement of rights delegation policies via the combination of rules and ontologies.
In *Workshop on Privacy Enforcement and Accountability with Semantics in conjunction with ISWC+ASWC 2007*, 2007.

Y. J. Hu, H. Y. Guo, and G. D. Lin.
Semantic enforcement of privacy protection policies via the combination of ontologies and rules.
In *IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC 2008)*, Taichung, Taiwan, June 2008.

R. Iannella.
Open digital rights language (ODRL), version 1.1.
W3c note 19, The ODRL Initiative, September 2002.
http://www.w3.org/TR/odrl/.

ContentGuard Inc.
eXtensible rights Markup Language (XrML), ver. 2.0.
Technical report, ContentGuard Inc., 2002.
`http://www.xrml.org/index.asp`.

S. Jajodia et al.
Flexible support for multiple access control policies.
ACM Trans. on Database Systems, 26(2):214–260, June 2001.

A. B. LaMacchia.
Key challenges in DRM: An industry perspective.
In *Digital Rights Management (DRM) Workshop 2002*, LNCS 2696. Springer, 2003.

Y. Alon Levy and M.-C. Rousset.
CARIN: A representation language combining horn rules and description logics.
In *Proc. of the 12th Eur. Conf. on Artificial Intelligence (ECAI'96)*, pages 323–327, 1996.

N. Li, B. N. Grosof, and J. Feigenbaum.
Delegation logic: A logic-based approach to distributed authorization.
ACM Trans. Information and System Security, 6(1):128–171, 2003.

B. Motik et al.
Can OWL and logic programming live together happily ever after?
In *5th International Semantic Web Conference (ISWC) 2006*, LNCS 4273, Athens, GA, USA, Nov. 2006.

B. Motik, U. Sattler, and R. Studer.
Query answering for OWL-DL with rules.
In *3rd International Semantic Web Conference (ISWC) 2004*, LNCS 3298, pages 549–563. Springer, 2004.

J. Pan and I. Horrocks.
Web ontology reasoning with datatype groups.
In *ISWC 2003*, LNCS2870, pages 47–63. Springer, 2003.

J. Park and R. T. Sandhu.
The UCON_{ABC} usage control model.
ACM Trans. on Information and System Security, 7(1):128–174, 2004.

R. Pucella and V. Weissman.
A formal foundation for ODRL.
In *Workshop on Issues in the Theory of Security (WITS)*, 2004.

R. Rosati.
On the decidability and complexity of integrating ontologies and rules.
Web Semantics: Science, Services and Agents on the World Wide Web 3, pages 61–73, 2005.

R. Rosati.
DL+log: Tight integration of description logics and disjunctive Datalog.
In *Proc. of the 10th International Conference on Principles of Knowledge Representation and Reasoning (KR)*, 2006.

R. Rosati.
Integrating ontologies and rules: Semantic and computational issues.
In *Reasoning Web 2006*, LNCS 4126, pages 128–151, 2006.

M. Stefik.
Letting loose the light: Igniting commerce in electronic publication.
In *Internet Dreams: Archetypes, Myths, and Metaphors*. MIT Press, 1996.

G. Tonti et al.
Semantic web languages for policy representation and reasoning: A comparison of KAoS, Rein, and Ponder.
In *2nd International Semantic Web Conference (ISWC) 2003*, LNCS 2870, pages 419–437. Springer, 2003.

D. J. Weitzner et al.

Creating a policy-aware web: Discretionary, rule-based access for the world wide web.

In E. Ferrari and B. Thuraisingham, editors, *Web and Information Security*, pages 1–31. Idea Group Inc., 2006.

T. Yu, A. N. Li, and I. Antón.

A formal semantics for p3p.

In *ACM Workshop on Secure Web Services*, Fairfax, VA, USA, Oct. 2004.

http://citeseer.ist.psu.edu/750176.html.