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
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
**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
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
- 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] ⇐ FOL semantics
- Semantic P3P [34] ⇐ relational semantics
- FAF [19] ⇐ LP semantics
- Semantic E-P3P (or EPAL) [2] ⇐ FAF semantics
- Protune [4] ⇐ LP semantics
- AIR [1] ⇐ RDF semantics
Pure FOL-Based Policies Are Not Web-Enabled

**Formal semantics of policies in DL or LP**

- Semantic ODRL [27] ⇐ FOL semantics
- Semantic P3P [34] ⇐ relational semantics
- FAF [19] ⇐ LP semantics
- Semantic E-P3P (or EPAL) [2] ⇐ FAF semantics
- Rein, KAoS [32] ⇐ DL-based FOL semantics
- Protune [4] ⇐ LP semantics
- AIR [1] ⇐ RDF semantics
Policies in semantic web languages

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

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
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

1. Alice wants to send e-mail to Bob and Charlie

- **e-mail of Bob:**
  - from: Alice@gmail.com
  - to: Bob@yahoo.com.tw Charlie@hotmail.com
  - Subject: Data-Auditing

2. Bob doesn’t want to disclose his e-mail address to other recipients not in subsidiary company

3. Charlie will receive the e-mail without displaying the e-mail address of Bob

- **e-mail of Charlie:**
  - from: Alice@gmail.com
  - to: Charlie@yahoo.com.tw
  - Subject: Data-Auditing
Ontology Module

Example (Axiom in an Ontology Module)

- $\text{COMPANY} \subseteq \text{PRIVATE}$
- $\text{PRIVATE} \subseteq \text{ORGANIZATION}$
- $\text{OWNER} \subseteq \text{PERSON}$
- $\text{COMPANY} \xrightarrow{\text{domain}} \text{HAS}\_\text{COOPERATIVE} \xrightarrow{\text{range}} \text{COMPANY}$
- $\text{COMPANY} \xrightarrow{\text{domain}} \text{HAS}\_\text{SUBSIDIARY} \xrightarrow{\text{range}} \text{COMPANY}$
- $\text{HAS}\_\text{COOPERATIVE} \equiv \text{HAS}\_\text{COOPERATIVE}^-$
- $\text{PERSON} \xrightarrow{\text{domain}} \text{IS}\_\text{STAFF}\_\text{OF} \xrightarrow{\text{range}} \text{ORGANIZATION}$
- $\text{MAIL}\_\text{TRACE} \xrightarrow{\text{domain}} \text{HAS}\_\text{MAIL}\_\text{TRACE} \xrightarrow{\text{range}} \text{EMAIL}$
- $\text{EMAIL} \sqsubseteq \exists \text{HAS}\_\text{MAIL}\_\text{TRACE}\_\text{ONLINE}^- \cdot \text{O}\_\text{EMAIL}\_\text{SENDER}$
- $\text{EMAIL} \sqsubseteq \forall \text{HAS}\_\text{MAIL}\_\text{TRACE}\_\text{ONLINE}. \text{O}\_\text{EMAIL}\_\text{RECEIVER}$
- $\text{DATA}\_\text{AUDIT}\_\text{ANNOUN.} \subseteq \text{AUDIT}\_\text{ANNOUN.}$
**Example** (Axiom in an Ontology Module)

- \( \text{COMPANY} \sqsubseteq \text{PRIVATE} \)
- \( \text{PRIVATE} \sqsubseteq \text{ORGANIZATION} \)
- \( \text{OWNER} \sqsubseteq \text{PERSON} \)
- \( \text{COMPANY} \xleftarrow{\text{domain}} \text{HAS\_COOPERATIVE} \xrightarrow{\text{range}} \text{COMPANY} \)
- \( \text{COMPANY} \xleftarrow{\text{domain}} \text{HAS\_SUBSIDIARY} \xrightarrow{\text{range}} \text{COMPANY} \)
- \( \text{HAS\_COOPERATIVE} \equiv \text{HAS\_COOPERATIVE}^- \)
- \( \text{PERSON} \xleftarrow{\text{domain}} \text{IS\_STAFF\_OF} \xrightarrow{\text{range}} \text{ORGANIZATION} \)
- \( \text{MAIL\_TRACE} \xleftarrow{\text{domain}} \text{HAS\_MAIL\_TRACE} \xrightarrow{\text{range}} \text{EMAIL} \)
- \( \text{EMAIL} \sqsubseteq \exists \text{HAS\_MAIL\_TRACE\_ONLINE}^- \cdot \text{O\_EMAIL\_SENDER} \)
- \( \text{EMAIL} \sqsubseteq \forall \text{HAS\_MAIL\_TRACE\_ONLINE} \cdot \text{O\_EMAIL\_RECEIVER} \)
- \( \text{DATA\_AUDIT\_ANNOUN.} \sqsubseteq \text{AUDIT\_ANNOUN.} \)
**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, Charlie@hotmail.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_SENDER(Alice@gmail.com),**
- **O_EMAIL_RECEIVER(Charlie@hotmail.com)**
- **HAS_EMAIL_ADDRESS** (Alice, Alice@gmail.com)
- **HAS_EMAIL_ADDRESS** (Bob, Bob@yahoo.com.tw)
- **HAS_EMAIL_ADDRESS** (Charlie, Charlie@hotmail.com)
- **HAS_EMAIL_ADDRESS** (Alice, Alice@gmail.com)
- **HAS_EMAIL_ADDRESS** (Bob, Bob@yahoo.com.tw)
- **HAS_MAIL_TRACE_ONLINE** (Alice@gmail.com, Charlie@hotmail.com)
- **HAS_MAIL_TRACE_ONLINE** (Alice@gmail.com, Bob@yahoo.com.tw)
**Example (Rules in a Rule Module)**

- **cando(?c, ?b-email, display)**
  \[\text{\textless= opt-in(?b, ?b-email, ?p)), data-user(?c), data-owner(?b),}
  \text{HAS.EMAIL_ADDRESS(?b, ?b-email).} \leftarrow (a1)\]

- **cando(?c, ?b-email, null)**
  \[\text{\textless= opt-out(?b, ?b-email, ?p)), data-user(?c), data-owner(?b),}
  \text{HAS.EMAIL_ADDRESS(?b, ?b-email).} \leftarrow (a2)\]

- **opt-in(?b, ?b-email, ?p)**
  \[\text{\textless= data-owner(?b), data-user(?c), purpose(?p), data-type(?b-email),}
  \text{IS.STAFF.OF(?b, ?c1), IS.STAFF.OF(?c, ?c2), HAS.SUBSIDIARY(?c1, ?c2),}
  \text{HAS_MAIL_TRACE_ONLINE(?a-email, ?c-email),}
  \text{O.EMAIL_SENDER(?a-email), O.EMAIL_RECEIVER(?c-email).} \leftarrow (a3)\]

- **opt-out(?b, ?b-email, ?p)**
  \[\text{\textless= data-owner(?b), data-user(?c), purpose(?p), data-type(?b-email),}
  \text{IS.STAFF.OF(?b, ?c1), IS.STAFF.OF(?c, ?c2), HAS.COOPERATIVE(?c1, ?c2),}
  \text{HAS_MAIL_TRACE_ONLINE(?a-email, ?c-email),}
  \text{O.EMAIL_SENDER(?a-email), O.EMAIL_RECEIVER(?c-email).} \leftarrow (a4)\]
**EXAMPLE ( Rules in a Rule Module)**

- **cando**(?c, ?b-email, display)
  \[ \leftarrow \text{opt-in}(?b, ?b-email, ?p), \text{data-user}(?c), \text{data-owner}(?b), \text{HAS_EMAIL_ADDRESS}(?b, ?b-email). \leftarrow (a1) \]

- **cando**(?c, ?b-email, null)
  \[ \leftarrow \text{opt-out}(?b, ?b-email, ?p), \text{data-user}(?c), \text{data-owner}(?b), \text{HAS_EMAIL_ADDRESS}(?b, ?b-email). \leftarrow (a2) \]

- **opt-in**(?b, ?b-email, ?p)
  \[ \leftarrow \text{data-owner}(?b), \text{data-user}(?c), \text{purpose}(?p), \text{data-type}(?b-email), \text{IS_STAFF_OF}(?b, ?c1), \text{IS_STAFF_OF}(?c, ?c2), \text{HAS_SUBSIDIARY}(?c1, ?c2), \text{HAS_MAIL_TRACE_ONLINE}(?a-email, ?c-email), \text{O_EMAIL_SENDER}(?a-email), \text{O_EMAIL_RECEIVER}(?c-email). \leftarrow (a3) \]

- **opt-out**(?b, ?b-email, ?p)
  \[ \leftarrow \text{data-owner}(?b), \text{data-user}(?c), \text{purpose}(?p), \text{data-type}(?b-email), \text{IS_STAFF_OF}(?b, ?c1), \text{IS_STAFF_OF}(?c, ?c2), \text{HAS_COOPERATIVE}(?c1, ?c2), \text{HAS_MAIL_TRACE_ONLINE}(?a-email, ?c-email), \text{O_EMAIL_SENDER}(?a-email), \text{O_EMAIL_RECEIVER}(?c-email). \leftarrow (a4) \]
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

The Intranet

P3P Policy

Agree with P3P Policy

Collect User Data

Policy Inference with Ontologies and Rules

Portal

Ontologies & Rules

Local Schema
Query

Global Ontology
Query

Collect User Data

Policy Inference with Ontologies and Rules

Portal

Ontologies & Rules

Local Schema
Query

Global Schema
Query

Global Schema
Response

Agree with P3P Policy

Alice

User

Bob
A Semantic Privacy Protection Model

Virtual Platform
Formal Protection Policy Combination

Global Policy Schema

Mapping Language
LAV

Local Schema
Formal Protection Policy
Rule
Ontology

Local Schema
Formal Protection Policy
Rule
Ontology

Local Schema
Formal Protection Policy
Rule
Ontology

TBox

Mapping Language
GAV

RDB
RDB
RDB
RDB
RDB

Data Source

ABox
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 $VP$ 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 ⊑ Clinic, HospitalizationData ⊑ HealthData

Property:
T ⊑ ∀ create.Hospital, T ⊑ ∀ create⁻.HealthData

**PARTIAL ONTOLOGY OF $LS_B$ VOCABULARIES**

Class:
Person, HealthCenter, OutPatientData ⊑ PatientData

Property:
T ⊑ ∀ beMedicated.Person, T ⊑ ∀ beMedicated⁻.HealthCenter.
Vocabularies for the Hospital $LS_A$ and $LS_B$

**Partial ontology of $LS_A$ vocabularies**

Class:
SurgeryData ⊑ Clinic, HospitalizationData ⊑ HealthData

Property:
$T ⊑ \forall \text{create.Hospital}$, $T ⊑ \forall \text{create^{-}.HealthData}$

**Partial ontology of $LS_B$ vocabularies**

Class:
Person, HealthCenter, OutPatientData ⊑ PatientData

Property:
$T ⊑ \forall \text{own.Person}$, $T ⊑ \forall \text{own^{-}.PatientData}$.

$T ⊑ \forall \text{beMedicated.Person}$, $T ⊑ \forall \text{beMedicated^{-}.HealthCenter}$. 
**Views Use at the $\mathcal{VP}$**

**Views Created from $\mathcal{LS}_A$**

\[
\begin{align*}
def(V_{1\text{Clinic}}) &= \text{Hospital} \\
def(V_{2\text{HealthData}}) &= \text{HealthRecord} \\
def(V_{3\text{SurgeryData}}) &= \text{HealthRecord} \land \forall \text{hasMedType.Surgery} \\
def(V_{4\text{HospitalizationData}}) &= \text{HealthRecord} \land \forall \text{hasMedType.Hospitalization} \\
def(V_{5\text{create}}) &= \text{generate}
\end{align*}
\]

**Views Created from $\mathcal{LS}_B$**

\[
\begin{align*}
def(V_{6\text{Person}}) &= \text{Patient} \\
def(V_{7\text{HealthCenter}}) &= \text{Hospital} \\
def(V_{8\text{PatientData}}) &= \text{HealthRecord} \\
def(V_{9\text{OutPatientData}}) &= \text{HealthRecord} \land \forall \text{hasMedType.OutPatient} \\
def(V_{10\text{beMedicated}}) &= \text{beCured} \\
def(V_{11\text{own}}) &= \text{hasHealthRecord}
\end{align*}
\]
Views Use at the $\mathcal{VP}$

**Views Created from $LS_A$**

\[
\begin{align*}
\text{def}(V_{1\text{Clinic}}) &= \text{Hospital} \\
\text{def}(V_{2\text{HealthData}}) &= \text{HealthRecord} \\
\text{def}(V_{3\text{SurgeryData}}) &= \text{HealthRecord} \land \forall \text{hasMedType}.\text{Surgery} \\
\text{def}(V_{4\text{HospitalizationData}}) &= \text{HealthRecord} \land \forall \text{hasMedType}.\text{Hospitalization} \\
\text{def}(V_{5\text{create}}) &= \text{generate}
\end{align*}
\]

**Views Created from $LS_B$**

\[
\begin{align*}
\text{def}(V_{6\text{Person}}) &= \text{Patient} \\
\text{def}(V_{7\text{HealthCenter}}) &= \text{Hospital} \\
\text{def}(V_{8\text{PatientData}}) &= \text{HealthRecord} \\
\text{def}(V_{9\text{OutPatientData}}) &= \text{HealthRecord} \land \forall \text{hasMedType}.\text{OutPatient} \\
\text{def}(V_{10\text{beMedicated}}) &= \text{beCured} \\
\text{def}(V_{11\text{own}}) &= \text{hasHealthRecord}
\end{align*}
\]
A Scenario of Privacy Protection for EHR

**A Physician Queries at the VP**

**Original Query**

\[
\text{Patient}(?x) \land \text{beCured}(?x, ?y) \land \text{hasHealthRecord}(?x, ?r) \land \text{HealthRecord}(?r) \land \\
\text{hasMedType}(?r, \text{Surgery}) \land \text{generate}(?y, ?r) \rightarrow \text{sqwr1 : select}(?x, ?r)
\]

**Rewriting Queries One**

\[
\text{V6Person} \land \text{V10beMedicated} \land \text{V11own} \land \text{V9OutPatientData} \land \text{V5create} \rightarrow \text{sqwr1 : select}(?x, ?r)
\]

\[
\text{B : Person}(?p) \land \text{B : beMedicated}(?p, ?c) \land \text{B : own}(?p, ?d) \land \text{B : OutPatientData}(?od) \land \\
\text{A : create}(?h, ?hd) \rightarrow \text{sqwr1 : select}(?p, ?od)
\]

**Rewriting Queries Two**

\[
\text{V6Person} \land \text{V10beMedicated} \land \text{V11own} \land \text{V3SurgeryData} \land \text{V5create} \rightarrow \text{sqwr1 : select}(?x, ?r)
\]

\[
\text{B : Person}(?p) \land \text{B : beMedicated}(?p, ?c) \land \text{B : own}(?p, ?d) \land \text{A : SurgeryData}(?sd) \land \\
\text{A : create}(?h, ?hd) \rightarrow \text{sqwr1 : select}(?p, ?sd)
\]
A Scenario of Privacy Protection for EHR

A Physician Queries at the VP

**Original Query**

\[
\text{Patient}(\text{x}) \land \text{beCured}(\text{x}, \text{y}) \land \text{hasHealthRecord}(\text{x}, \text{r}) \land \text{HealthRecord}(\text{r}) \land \text{hasMedType}(\text{r}, \text{Surgery}) \land \text{generate}(\text{y}, \text{r}) \rightarrow \text{sqwrl} : \text{select}(\text{x}, \text{r})
\]

**Rewriting Queries One**

\[
\text{V6Person} \land \text{V10beMedicated} \land \text{V11own} \land \text{V9OutPatientData} \land \text{V5create} \rightarrow \text{sqwrl} : \text{select}(\text{x}, \text{r})
\]

\[
\text{B} : \text{Person}(\text{p}) \land \text{B} : \text{beMedicated}(\text{p}, \text{c}) \land \text{B} : \text{own}(\text{p}, \text{d}) \land \text{B} : \text{OutPatientData}(\text{od}) \land \text{A} : \text{create}(\text{h}, \text{hd}) \rightarrow \text{sqwrl} : \text{select}(\text{p}, \text{od})
\]

**Rewriting Queries Two**

\[
\text{V6Person} \land \text{V10beMedicated} \land \text{V11own} \land \text{V3SurgeryData} \land \text{V5create} \rightarrow \text{sqwrl} : \text{select}(\text{x}, \text{r})
\]

\[
\text{B} : \text{Person}(\text{p}) \land \text{B} : \text{beMedicated}(\text{p}, \text{c}) \land \text{B} : \text{own}(\text{p}, \text{d}) \land \text{A} : \text{SurgeryData}(\text{sd}) \land \text{A} : \text{create}(\text{h}, \text{hd}) \rightarrow \text{sqwrl} : \text{select}(\text{p}, \text{sd})
\]
A Scenario of Privacy Protection for EHR

A Physician Queries at the \( \mathcal{VP} \)

**Original Query**

\[
\text{Patient}(?x) \land \text{beCured}(?x, ?y) \land \text{hasHealthRecord}(?x, ?r) \land \\
\text{hasMedType}(?r, \text{Surgery}) \land \text{generate}(?y, ?r) \rightarrow \text{sqwrl} : \text{select}(?x, ?r)
\]

**Rewriting Queries One**

\[
\text{V6Person} \land \text{V10beMedicated} \land \text{V11own} \land \text{V9OutPatientData} \land \text{V5create} \rightarrow \text{sqwrl} : \text{select}(?x, ?r)
\]

\[
\begin{align*}
\text{B : Person}(?p) & \land \text{B : beMedicated}(?p, ?c) \land \text{B : own}(?p, ?d) \land \text{B : OutPatientData}(?od) \land \\
\text{A : create}(?h, ?hd) & \rightarrow \text{sqwrl} : \text{select}(?p, ?od)
\end{align*}
\]

**Rewriting Queries Two**

\[
\text{V6Person} \land \text{V10beMedicated} \land \text{V11own} \land \text{V3SurgeryData} \land \text{V5create} \rightarrow \text{sqwrl} : \text{select}(?x, ?r)
\]

\[
\begin{align*}
\text{B : Person}(?p) & \land \text{B : beMedicated}(?p, ?c) \land \text{B : own}(?p, ?d) \land \text{A : SurgeryData}(?sd) \land \\
\text{A : create}(?h, ?hd) & \rightarrow \text{sqwrl} : \text{select}(?p, ?sd)
\end{align*}
\]
Part IV

SEMPIF (Cooperation with IIT NRC, Canada)
Well-Known Semantic Web Layer Cake (2007 Version)

User Interface & Applications

Trust

Proof

Unifying Logic

Query: SPARQL

Ontology: OWL

Rule: RIF

RDFS

Data interchange:

RDF

XML

URI/IRI

Crypto

- http://www.w3.org/2007/03/layerCake.svg
SemPIF Extends Semantic Web Architecture

User Interface

Domain Specific Applications

DRM

Privacy Protection

Trust

Policy Interchange Format (PIF):
- XML-level: XACML, WS-Policy
- Horn-based: EPAL, Protune
- DL-based: KAoS, Rel
- REL: P3P, ODRL, XrML

meta-PIF

Proof

Unifying Logic
- DL+Horn: DLP, SWRL

Query: SPARQL

Ontology: OWL

Rule: RIF

RDFS

Data Interchange:
- RDF
- XML

URI/IRI

Crypto
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
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

- **Access Control Policies**
  - **License Agreements**
    - Unifying Semantic REls
      - Ontologies-Rules
        - SWRL, OWL2 EL, Protégé, AIR
        - DLP, AL-Log, DL-Log
      - Logic Program (LP)
        - Datalog
          - EPAL
            - Non-recursive
              - Monotonic
              - Non-monotonic
            - Recursive
            - RuleML
            - RIF
        - Decidable
          - Tractable (polynomial)
            - OWL 2 profile
            - Lithium
          - Intricable (exponential)
            - OWL 2
            - OWL DL
            - OWL-Full
            - RDF(S)
            - Rei
            - KAoS
      - Description Logic (DL)
        - ODRL
        - XrML
        - P3P
        - XACML
      - Undecidable
**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

SemPIF Framework

ontology mapping, rule interchange

PIF

Ontologies +Rules

Meta-PIF

policy modifying, deleting, reconciling, etc.

Facilitator

policy uploading

policy reconciliation

policy uploading

policy uploading

policy uploading

client

NCCU library portal

digital library portal
A PIF-based Ontology for a DRM Policy
A PIF-based Rule for a Server’s DRM Policy

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

∧ IEEE[hasPublished → ?ejr] ∧ IEEE[hasPrivacyOf → DRMControl]
∧ Retain[hasDuration → = 2 Month]
∧ subtract-dateTimes(?edtime, ?sdtime) ≤ Retain

∧ ?ppr[appliedTo → ?dif].
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.

A. H. Anderson.
A comparison of two privacy policy languages: EPAL and XACML.

M. Blaze, J. Figenebaum, and M. Strauss.
Compliance checking in the policymaker trust management system.

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.

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.


Formalising ODRL semantics using web ontologies.


http://odrl.net/workshop2005/.

N. B. Grosof et al.

Description logic programs: Combining logic programs with description logic.


S. Guth, G. Neumann, and M. Strembeck.

Experiences with the enforcement of access rights extracted from ODRL-based digital contracts.

Joseph Y. Halpern and Vicky Weissman.
A formal foundation for XrML.

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),

I. Horrocks et al.
http://www.w3.org/Submission/SWRL/.

Ian Horrocks et al.
OWL rules: A proposal and prototype implementation.
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.

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.
http://www.w3.org/TR/odrl/.

ContentGuard Inc.
eXtensible rights Markup Language (XrML), ver. 2.0.
http://www.xrml.org/index.asp.
S. Jajodia et al.
Flexible support for multiple access control policies.

A. B. LaMacchia.
Key challenges in DRM: An industry perspective.

Y. Alon Levy and M.-C. Rousset.
CARIN: A representation language combining horn rules and description logics.

N. Li, B. N. Grosof, and J. Feigenbaum.
Delegation logic: A logic-based approach to distributed authorization.

B. Motik et al.
Can OWL and logic programming live together happily ever after?
B. Motik, U. Sattler, and R. Studer.
Query answering for OWL-DL with rules.

J. Pan and I. Horrocks.
Web ontology reasoning with datatype groups.

The UCON$_{ABC}$ usage control model.

R. Pucella and V. Weissman.
A formal foundation for ODRL.

R. Rosati.
On the decidability and complexity of integrating ontologies and rules.
R. Rosati.

*DL+log: Tight integration of description logics and disjunctive Datalog.*


R. Rosati.

Integrating ontologies and rules: Semantic and computational issues.


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.


D. J. Weitzner et al.
Creating a policy-aware web: Discretionary, rule-based access for the world wide web.

T. Yu, A. N. Li, and I. Antón.
A formal semantics for p3p.