Privacy Preserving Data Sharing Policy for National Security Enforcement

Prof. Dr. Yuh-Jong Hu

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

Oct-21st-2010

FP7 RISE Project Taiwan Conference


Part I

General Issues


Motivations

1. Enforcing national security usually requires data sharing
2. Data sharing needs to collect and integrate data from multiple autonomous data sources
3. While enforcing national security how do we ensure privacy-preserving data sharing?
4. To achieve national security, data sharing policy might be enforced in a single judicial domain or across judicial borders


Purposes of Data Sharing

- Data sharing as a research topic in computer science field for more than a decade
- Privacy-preserving data sharing is another research challenge.
- The original purpose of data sharing is to achieve an effective and efficient data usage from multiple autonomous data sources.
- The emerging purpose of data sharing is to prevent and combat terrorism and other serious crimes by using the following data:
  - Passenger Name Records (PNR)
  - SWIFT financial data under the TFTP


East Meets West (I)

- Why using data sharing to implement international security cooperation is so difficult?
  1. Paradox of human rights and national security
  2. Differences of culture and society
  3. Consensus of privacy protection concepts
  4. Reconciliation of different laws
  5. Effectiveness of data sharing to fight against the terrorism
  6. Gap from bilateral agreements to a real policy implementation


East Meets West (II)

- Two questions wait for your answers:
  1. To achieve national security, can we learn from recent EU and U.S. good/bad experiences on the establishment processes of bilateral agreements based on the 12 EU-U.S. data sharing principles?
  2. Is it possible (and necessary) to consider Asia as another area to participate the data sharing and international security program to fight against the terrorism and serious crimes?

East Meets West (II)

- Two questions wait for your answers:
  1. To achieve national security, can we learn from recent EU and U.S. good/bad experiences on the establishment processes of bilateral agreements based on the 12 EU-U.S. data sharing principles?
  2. Is it possible (and necessary) to consider Asia as another area to participate the data sharing and international security program to fight against the terrorism and serious crimes?

Related Information

- Transatlantic Security: Data Sharing and Privacy Protection, July 8, 2010.
- EU-US High Level Contact Group on information sharing and privacy and personal data protection, EU US Summit, 12 June 2008.
- The EU PNR Framework decision proposal: Towards completion of the PNR processing scene in Europe, *Computer Law & Security Review*, 26, 2010, pp. 368-376.
- Anything but SWIFT: Why Data Sharing is Still a Problem for the EU, *AICGS ISSUEBRIEF*, May, 2010.


The 12 EU-U.S. Data-Sharing Principles

- Purpose specification/purpose limitation
- Integrity/data quality
- Relevant and necessary/proportionality
- Information security
- Special categories of personal information (sensitive data)
- Accountability
- Independent and effective oversight
- Individual access and rectification
- Transparency and notice
- Redress
- Automated individual decisions
- Restrictions on onward transfers to third countries

–High Level Contact Group on information sharing and privacy and personal data protection, EU US Summit, 12 June 2008.

The 12 EU-U.S. Data-Sharing Principles

- Purpose specification/purpose limitation
- Integrity/data quality
- Relevant and necessary/proportionality
- Information security
- Special categories of personal information (sensitive data)
- Accountability
- Independent and effective oversight
- Individual access and rectification
- Transparency and notice
- Redress
- Automated individual decisions
- Restrictions on onward transfers to third countries

–High Level Contact Group on information sharing and privacy and personal data protection, EU US Summit, 12 June 2008.

Research Goals

- A representation of data sharing, privacy protection, and national security policies in computer languages based on regulations, laws, and agreements
- Mitigating the gap from regulations, laws, and agreements to the real enforcement in computer systems
- Legalizing the computer-based policies derived from human regulations, laws, and agreements without causing ambiguity for policy representation and enforcement
- Exploiting the processes of legitimate law enforcement to collect, use, retain, and share personal information
- Resolving possible conflicts between different computer-enabled policies derived from original regulations, laws, and agreements


Research Goals

- A representation of data sharing, privacy protection, and national security policies in computer languages based on regulations, laws, and agreements
- Mitigating the gap from regulations, laws, and agreements to the real enforcement in computer systems
- Legalizing the computer-based policies derived from human regulations, laws, and agreements without causing ambiguity for policy representation and enforcement
- Exploiting the processes of legitimate law enforcement to collect, use, retain, and share personal information
- Resolving possible conflicts between different computer-enabled policies derived from original regulations, laws, and agreements


Research Goals

- A representation of data sharing, privacy protection, and national security policies in computer languages based on regulations, laws, and agreements
- Mitigating the gap from regulations, laws, and agreements to the real enforcement in computer systems
- Legalizing the computer-based policies derived from human regulations, laws, and agreements without causing ambiguity for policy representation and enforcement
- Exploiting the processes of legitimate law enforcement to collect, use, retain, and share personal information
- Resolving possible conflicts between different computer-enabled policies derived from original regulations, laws, and agreements


Research Goals

- A representation of data sharing, privacy protection, and national security policies in computer languages based on regulations, laws, and agreements
- Mitigating the gap from regulations, laws, and agreements to the real enforcement in computer systems
- Legalizing the computer-based policies derived from human regulations, laws, and agreements without causing ambiguity for policy representation and enforcement
- Exploiting the processes of legitimate law enforcement to collect, use, retain, and share personal information
- Resolving possible conflicts between different computer-enabled policies derived from original regulations, laws, and agreements

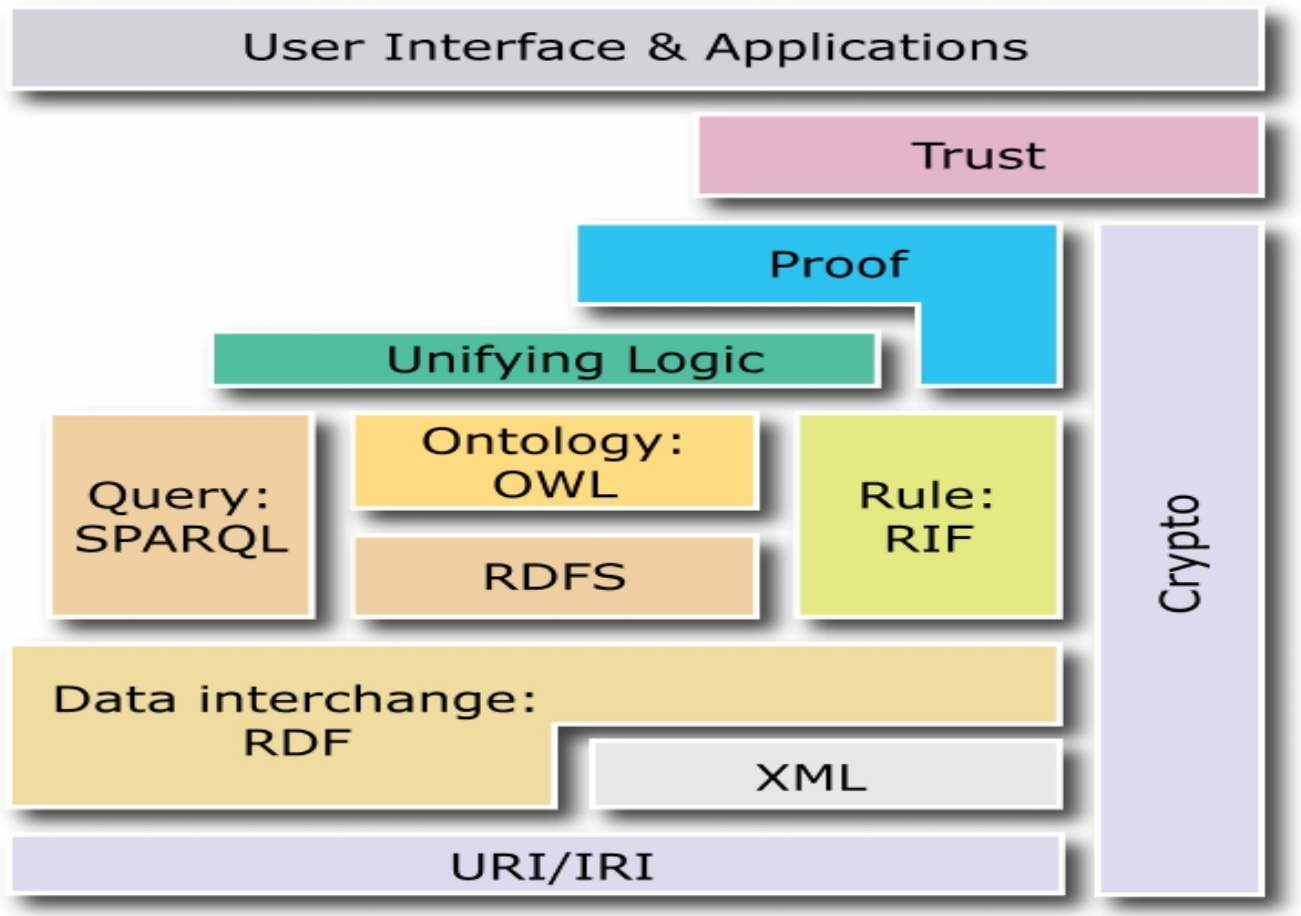

Research Goals

- A representation of data sharing, privacy protection, and national security policies in computer languages based on regulations, laws, and agreements
- Mitigating the gap from regulations, laws, and agreements to the real enforcement in computer systems
- Legalizing the computer-based policies derived from human regulations, laws, and agreements without causing ambiguity for policy representation and enforcement
- Exploiting the processes of legitimate law enforcement to collect, use, retain, and share personal information
- Resolving possible conflicts between different computer-enabled policies derived from original regulations, laws, and agreements


Part II

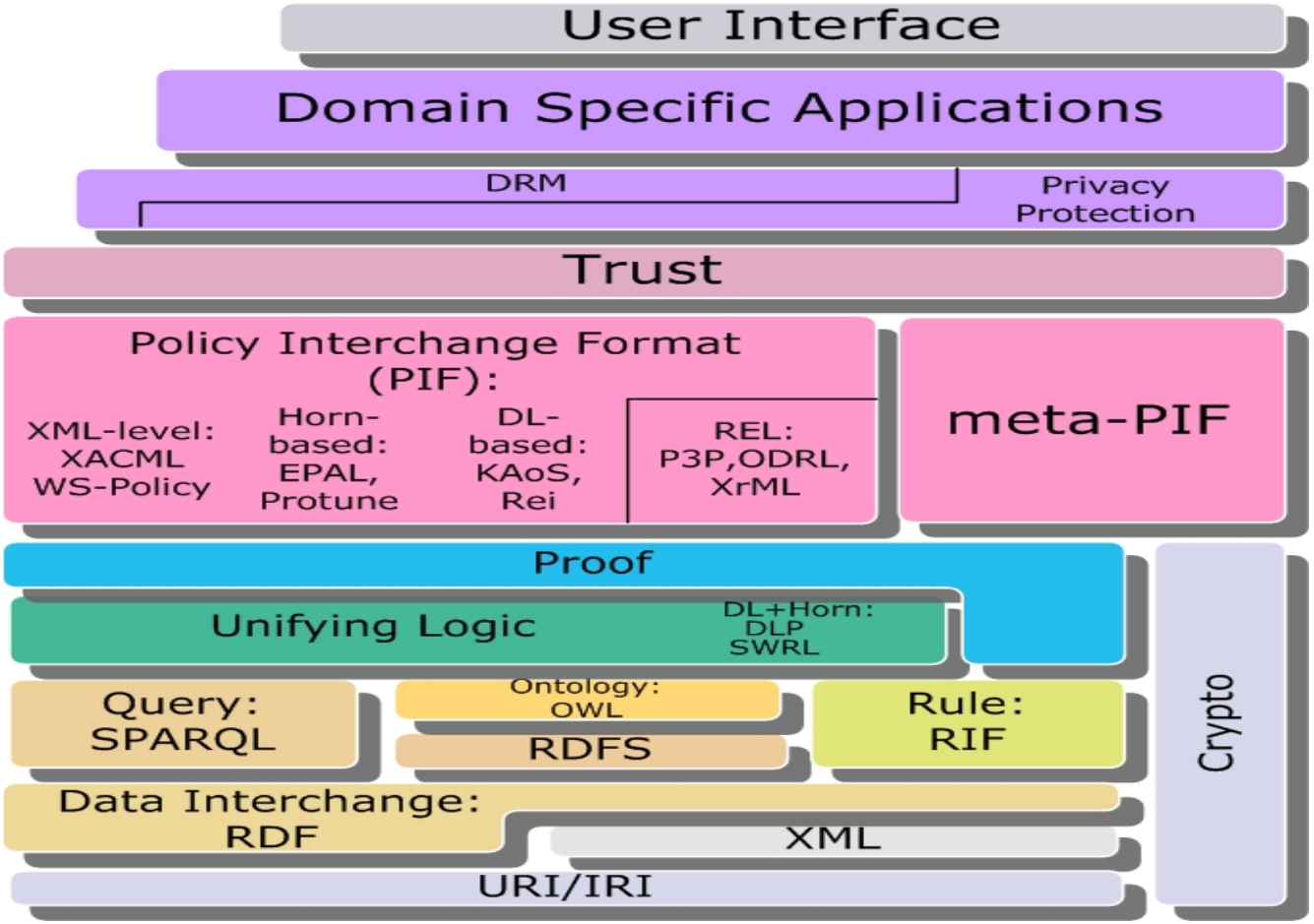
Technique Issues


Semantic Web Layer Cake



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

SemPIF Extends Semantic Web Architecture



Policy Representation

Natural Language

- Pros: Human readable and understandable
- Cons: Machine unfriendly but no formal semantics for the machine

Pure First Order Logic (FOL)

- Pros: Formal and clear syntax and semantics
- Cons: Machine unfriendly, possibly undecidable computation complexity, and policy writer (reader) needs to be a logician


Policy Representation

Natural Language

- Pros: Human readable and understandable
- Cons: Machine unfriendly but no formal semantics for the machine

Pure First Order Logic (FOL)

- Pros: Formal and clear syntax and semantics
- Cons: Machine unfriendly, possibly undecidable computation complexity, and policy writer (reader) needs to be a logician

Policy Representation (conti.)

Rights Expression Languages

- Pros: Machine processing of 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 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 Policy in Computer Languages?

Definition

- 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 for the context of policy

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


Semantics-Enabled Policy in Computer Languages (conti.)

Policy semantics can be created from the following semantic web languages

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

What Do You Mean Meta-Policy?

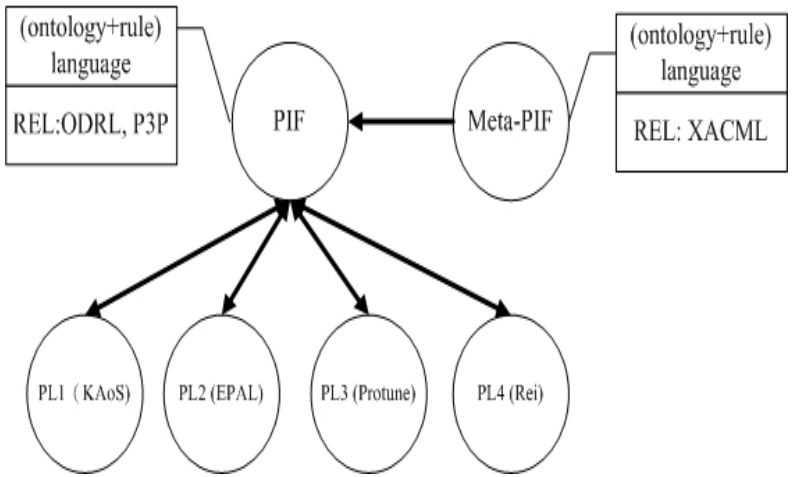
Definition

- A policy about policies
- Enforcing naming/adding/deleting/updating/integration of policy management services
- Setting up policy priority to coordinate, enforce, negotiate, and conflict resolution of policies

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


Policy Management Services in Meta-Policy

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



Conclusion and Further Study

1. Enforcing semantics-enabled policies in computer languages to support privacy protection and national security policies still needs further study.
2. A long way to go for Asia countries (maybe except Australia and Japan) to participate the data sharing program with EU and US within an umbrella data-protection agreement.
3. Expecting to learn some experiences from the establishment processes of EU-U.S. data sharing and privacy protection bilateral agreements.

Conclusion and Further Study

1. Enforcing semantics-enabled policies in computer languages to support privacy protection and national security policies still needs further study.
2. A long way to go for Asia countries (maybe except Australia and Japan) to participate the data sharing program with EU and US within an umbrella data-protection agreement.
3. Expecting to learn some experiences from the establishment processes of EU-U.S. data sharing and privacy protection bilateral agreements.

Conclusion and Further Study

1. Enforcing semantics-enabled policies in computer languages to support privacy protection and national security policies still needs further study.
2. A long way to go for Asia countries (maybe except Australia and Japan) to participate the data sharing program with EU and US within an umbrella data-protection agreement.
3. Expecting to learn some experiences from the establishment processes of EU-U.S. data sharing and privacy protection bilateral agreements.