Privacy Mechanisms for PEAS Workshop Panel

Prof.(Dr.) Yuh-Jong Hu

November-12-2007

hu@cs.nccu.edu.tw
Emerging Network Technology(ENT) Lab.
Department of Computer Science
National Chengchi University, Taipei, Taiwan
Grand Challenges for a General Privacy Mechanism

- A clear separation of enforceable privacy policy from privacy mechanism

- Having sound and complete (enforceable) privacy policies and mechanisms derived from legal privacy laws or regulations

- Auditing and verifying the compliance of legal privacy laws or regulations for enforceable privacy policy and mechanism

- Successful enforcement of interdomain privacy protection policy and mechanism, including flexible information flow exchange with composition of associated privacy policy and mechanism in the interdomain
Privacy Protection Techniques for Different Web Generation

Semantic Web
- Purpose Ontology
- Data User Ontology
- Role Ontology
- Data Access
- Data Object Ontology
- Record any access log
- Ontology data model storing digital trace, transaction data, and P3P ontology
- Server with P3P ontology
- Communicate with APPEL
- Client A3
- P3P (OWL/RDF)

Web 2.0
- Data access by Law
- Government
- Department of Enterprise
- Data Access by E-P3P
- Enterprise
- Data Access by E-P3P
- Database with Oracle VPD storing digital trace log, transaction data, and P3P
- Server with P3P
- Communicate with APPEL
- Client A2
- P3P (XML-Based)

Web 1.0
- Data access by Law
- Government
- Department of Enterprise
- Direct Access
- Enterprise
- Direct Access
- Database storing transaction data
- Communicate with user agreement
- Client A1
- 3rd party
- Data access and transfer by enterprise contract
Privacy Protection Problems of the Semantic Web

Whether current privacy policy and mechanism enforcement status will be improved or exacerbated using semantic web technologies is unknown because:

✔ Vast amount of collected data, privacy protection policies and mechanisms are not semantic web enabled

✔ Semantic enabled data and information are much more easy for bad guys to link together, which means...

✔ Some of existing ontologies+rules combinations do not allow us to easily specify negative assertions and permission deny in the privacy protection policies

✔ Ontology matching and merging are unavoidable for interdomain privacy protection. Furthermore, privacy protection policy composition are necessary.

✔ Dealing with a general privacy protection problem, including protection all of end user digital traces on the Web is very hard