Purpose Based Access Control for Privacy Protection

Elisa Bertino, Ninghui Li, Ji-Won Byun
CERIAS and Department of Computer Sciences, Purdue University
{bertino, Ninghui, byunj}@cs.purdue.edu

Motivations
Privacy policies are concerned with which data object is used for which purposes, rather than which users are performing which actions on which data objects.

“We will collect and use customer identifiable information for billing purposes and to anticipate and resolve problems with your service.”

The comfort level of privacy varies from individual to individual.

Definition of Purpose
Intended Purpose = AIP + PIP
Associated with data and regulate data usage
AIP: Purpose for which data access is allowed
PIP: Purpose for which data access is prohibited

Access Purpose
Associated with data access, i.e., queries
Purpose for accessing a particular data item

Purpose Compliance
AP =⇒ IP if AP =⇒ IP
Data access is allowed only if AP =⇒ IP

Examples
IP = {<Admin, Marketing>, (Third-Party>}
AP1 = D-Email : AP2 =⇒ IP
AP2 = T-Email : AP3 =⇒ IP
AP3 = Marketing : AP4 =⇒ IP

Purpose Labeling
1. Relation-based
   A pair <R, ip>
2. Attribute-based
   A set <{A}, ip> | {A} = Attributes(R) • ip, IP
3. Tuple-based
   A relation scheme Rel (A, . . . , A, l)
4. Element-based
   A relation scheme Rel (A, 1, . . . , A, l)

Query Modification
Select name, phone
From customer
Where comp_check(512, name_aip, name_pip)
and comp_check(512, phone_aip, phone_pip)

Future Work
Automatic management of intended purpose labels.
Compatibility with P3P.
Extend to cope with obligations and conditions.
Enforcement of the Sticky-policy requirement.
Investigation of Fine-grained Access Control.