CERIAS

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.

Project Goals

The notion of purpose must play a major role in access control; i.e., access decisions should be made **based on purpose.**

The access control must be **fine-grained**; e.g., tuple-level and even cell-level.

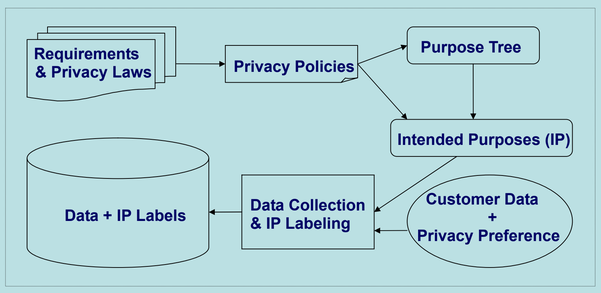
The access control must be **flexible**, yet it should not introduce too much overhead with respect to **storage/performance**.

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



Privacy Management Process

Purpose Tree

Element-Based

c_id	c_id_ip	name	name_ip	email	email_ip
1001	<{G}, >	John	<{G}, {M}>	john@aa.edu	<{P, S}, {M}>
1002	<{G}, >	Paul	<{G}, >	p23@oh.com	<{G}, >
1003	<{G}, >	Jack	<{G}, >	Jack03@very.net	<{G}, {T}>

Attribute-Based

c_id	street	city	state	zip	addr_ip
1001	232 Oval Drive	W.Lafayette	IN	47907	<{G}, {A, M}>
1002	433 State Road	Chicago	IL	46464	<{G}, >
1003	9898 First Ave	S. F.	CA	94037	<{G}, {T}>

Purpose Labeling

Purpose Labeling

1. Relation-based
A pair <R, ip>
2. Attribute-based
A set {<A_i, ip_i> | A_i • Attributes(R) • ip_i IP}
3. Tuple-based
A relation scheme Rtl (A_1, . . ., A_n, I)
4. Element-based
A relation scheme Rel (A_1, I_1, . . ., A_n, I_n)

Purpose Compliance

AP =>$_{PT}$ IP iff AP PIP* and AP AIP*
Data access is allowed only if AP=>$_{PT}$ IP

Examples

IP = <{Admin, Marketing}, {Third-Party}>

AP_1 = D-Email : AP_1 =>$_{PT}$ IP
AP_2 = T-Email : AP_2 >$_{PT}$ IP
AP_3 = Marketing : AP_3 >$_{PT}$ IP

Query Modification

Select name, phone
From customer
For Marketing

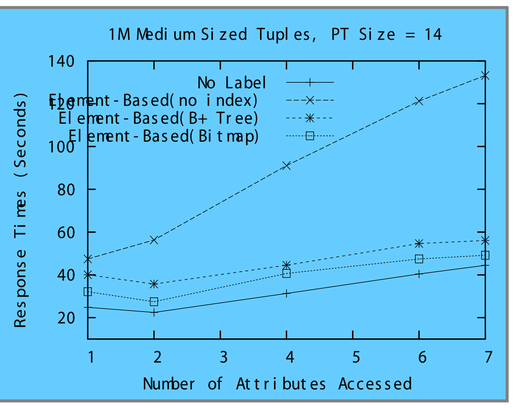
Customer table : Element-based
Marketing = '512'

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

Experiments

Partially implemented in Oracle

IP is stored as a bit string
Queries are modified manually
PL/SQL for compliance checks
Oracle VPD can be used
Performance improves with Index



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.

PURDUE UNIVERSITY

CERIAS®

Discovery Park e-Enterprise Center