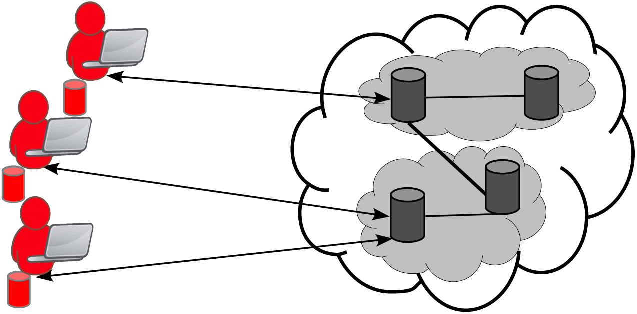
Privacy and Data Protection in Emerging Scenarios

Security, Privacy, and Data Protection Laboratory
Dipartimento di Informatica
Università degli Studi di Milano

Privacy of users



Privacy of users

Privacy of users' identities

Users may wish to remain anonymous or to not disclose much information about themselves when operating in the cloud

- Anonymous communication techniques (e.g., Mix networks, onion routing, Tor, Crowds)
- Privacy in location-based services [ACCDS-11, ALS-12]
- Attribute-based access control [ACCDS-11, BS-02, DFJPPS-12]
  - instead of declaring their identities, users prove they satisfy properties needed for the access
  - changes the way access control process works
- Support for user-privacy preferences in information disclosure [ACCM-12, ADFPS-10a, ADFPS-10b, ADFPS-12, CCKT-05, KOB-08, YFAR-08]

User empowerment

Users may want to specify policies regulating information disclosed:

- when using external servers for sharing/disseminating their own resources (e.g., Facebook)
- when releasing information in digital interactions (e.g., releasing credit card to access a service)

Two aspects of protection:

- direct release regulates to whom, when, for what purpose a user agrees to release information
- secondary usage regulates usage and further dissemination of user information by the receiving parties (e.g., P3P)

User empowerment

Users may want to specify policies regulating information disclosed:

- when using external servers for sharing/disseminating their own resources (e.g., Facebook)
- when releasing information in digital interactions (e.g., releasing credit card to access a service)

Two aspects of protection:

- direct release regulates to whom, when, for what purpose a user agrees to release information
- secondary usage regulates usage and further dissemination of user information by the receiving parties (e.g., P3P)

Direct release – Several contributions (1)

The research community has been very active and produced several approaches for regulating interactions among unknown parties through the definition of attribute-based access control mechanisms

- What users can do depend on assertions (attributes) they can prove presenting certificates
- Access control does not return “yes/no” anymore, but responds with requirements that the requestor must satisfy to get access
- Not only the server needs to be protected …
  - clients want guarantees too (e.g., privacy)

    ⟹ some form of negotiation may be introduced

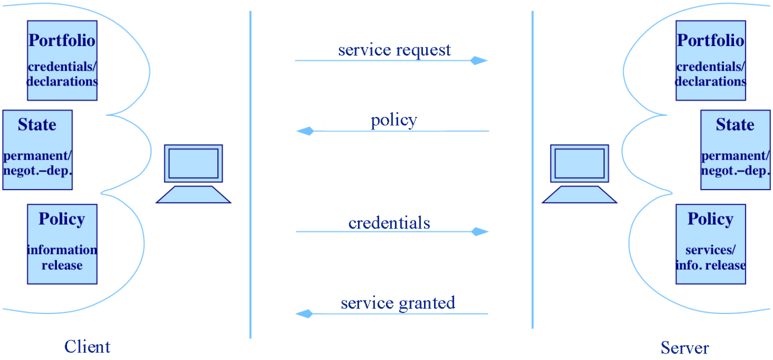
Direct release – Several contributions (2)

Large body of proposals (e.g., [BS-02; LWBW-08 WCJS-97, YWS-03]) addressing:

- credential/attribute-based policy specifications
- policy evaluation with partial information
- policy confidentiality support
- policy communication and dialog
- negotiation strategies and trust management
- evaluation of termination, correctness, no improper information disclosure in the negotiation

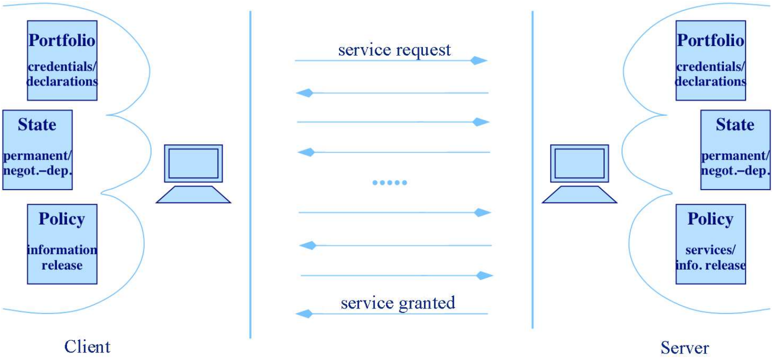
$\Longrightarrow$ typically using logic-based languages

Interactive access control



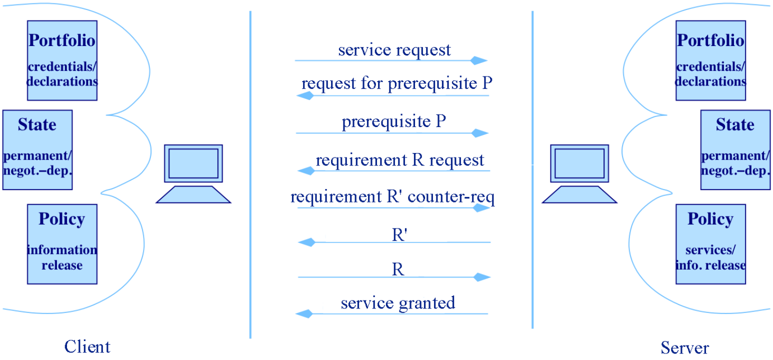
- No conditions by the client

Interactive access control



- No conditions by the client
- Multi-step negotiation

Interactive access control



- No conditions by the client
- Multi-step negotiation
- Two-step interaction

Existing/emerging technologies supporting ABAC

- U-Prove/Idemix: provide advance credential management technologies (selective release, proof of possession, …)

- XACML: standard today for interoperation of access control policies
    - expressive but with limited features for reasoning about digital certificates (e.g., attribute nationality should be certified by a passport) or policy dialog

User privacy preferences

Access control specifications do not always fit well with the problem at the client (user) side

+ they are expressive and powerful

+ they allow users to specify whether some information can be or cannot be released

– they do not allow users to express the fact that they might prefer to release some information over other when given the choice

$\Longrightarrow$ Need to provide users with means to effectively define privacy preferences on the release of their information

User privacy preferences: Desiderata – 1

- Context-based preferences
  - e.g., “I want to disclose my credit card to financial servers in the context of payment transactions only”
- Forbidden disclosures
  - e.g., “I do not want to release both my name and my nickname”
- Sensitive associations
  - e.g., “The association between my zip code and my date of birth is more sensitive than the two pieces of information singularly taken”
- Limited disclosure
  - e.g., “I do not mind saying that I am older than 30 but I do not want to release my age”

User privacy preferences: Desiderata – 2

- Instance-based preferences
  - e.g., “I prefer to release my credit card over my bank account if the credit card expires in less than one year”
- History-based preferences
  - e.g., “I prefer to release my county over my phone if you already have my zip code”
- Proof-based preferences
  - e.g., “I prefer to release the proof that I have an Italian passport rather than releasing the passport itself”
- Non-linkability preferences
  - e.g., “I prefer to release the piece of information that, merged with the other party knowledge, identifies me the less”
- . . .

User privacy preferences: Some approaches

- Cost-sensitive trust negotiation

- Point-based trust management model

- Logic-based minimal credential disclosure

- Privacy preferences in credential-based interactions

Cost-Sensitive Trust Negotiation

W. Chen, L. Clarke, J. Kurose, D. Towsley, “Optimizing Cost-Sensitive Trust-Negotiation Protocols,” in *Proc. of INFOCOM*, Miami, FL, USA, March 2005.

Cost-sensitive trust negotiation – 1

- Two parties (client and server) interact with each other to establish mutual trust by the exchange of credentials

  $\Longrightarrow$ trust negotiation protocol

- The disclosure of a credential is regulated by a policy that specifies the prerequisite conditions that must be satisfied to disclose the credential

- Credentials and policies are associated with a cost

  $\Longrightarrow$ more sensitive credentials/policies have higher cost

- The goal is to minimize the total sensitivity cost of credentials and policies disclosed during a trust negotiation

Cost-sensitive trust negotiation – 2

Policies

Client:

- $c_1 \leftarrow s_1$
- $c_2 \leftarrow s_3$
- $c_3 \leftarrow s_2$
- $c_4 \leftarrow s_2$

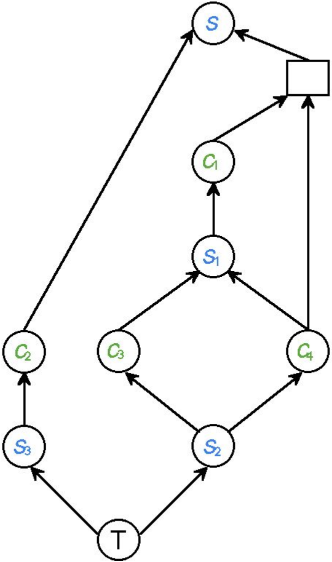
Server:

- $s \leftarrow (c_1 \wedge c_4) \vee c_2$
- $s_1 \leftarrow c_3 \vee c_4$
- $s_2 \leftarrow$ TRUE
- $s_3 \leftarrow$ TRUE

Costs

- cost(c_1)=2
- cost(c_2)=7
- cost(c_3)=2
- cost(c_4)=1
- cost(s)=5
- cost(s_1)=2
- cost(s_2)=0
- cost(s_3)=0

Policy graph



Cost-sensitive trust negotiation – 2

Policies	Costs	Policy graph

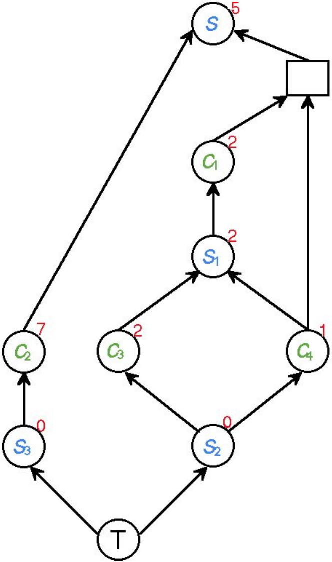
Client:

- $c_1 \leftarrow s_1$
- $c_2 \leftarrow s_3$
- $c_3 \leftarrow s_2$
- $c_4 \leftarrow s_2$

Server:

- $s \leftarrow (c_1 \wedge c_4) \vee c_2$
- $s_1 \leftarrow c_3 \vee c_4$
- $s_2 \leftarrow$ TRUE
- $s_3 \leftarrow$ TRUE

- cost(c_1)=2
- cost(c_2)=7
- cost(c_3)=2
- cost(c_4)=1
- cost(s)=5
- cost(s_1)=2
- cost(s_2)=0
- cost(s_3)=0



Cost-sensitive trust negotiation – 2

Policies

Client:

- $c_1 \leftarrow s_1$
- $c_2 \leftarrow s_3$
- $c_3 \leftarrow s_2$
- $c_4 \leftarrow s_2$

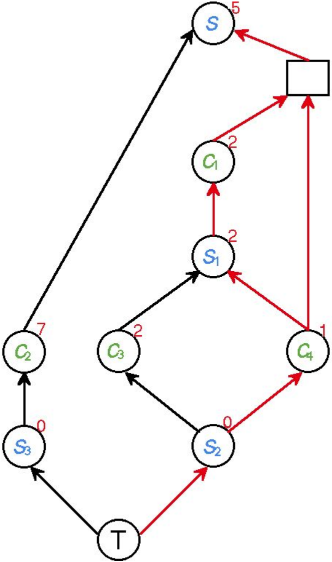
Server:

- $s \leftarrow (c_1 \wedge c_4) \vee c_2$
- $s_1 \leftarrow c_3 \vee c_4$
- $s_2 \leftarrow$ TRUE
- $s_3 \leftarrow$ TRUE

Costs

- cost(c_1)=2
- cost(c_2)=7
- cost(c_3)=2
- cost(c_4)=1
- cost(s)=5
- cost(s_1)=2
- cost(s_2)=0
- cost(s_3)=0

Policy graph



Cost-sensitive trust negotiation – 3

- Provide a mechanism for regulating the release of credentials according to their sensitivity
- Put focus on negotiation rather than on client control
- Support only coarse-grain (credentials) specifications; sensitive associations as well as forbidden releases cannot be expressed
- Possession-sensitive credentials (e.g., dialysis certificate) are not considered
- Minimizing overall cost (client + server) has limited applicability
- Linear combination of costs may not be always desirable

Point-based Trust Management Model

D. Yao, K.B. Frikken, M.J. Atallah, R. Tamassia, “Private Information: To Reveal or not to Reveal,” in *ACM TISSEC*, vol. 12, no. 1, October 2008.

Point-based trust management model – 1

How to get a New York Driver License . . .

- Documents that prove your name are assigned a point value; you must present identification that totals **six points or more**:
    - US Passport or Passport Card [4 points]
    - Certificate of Naturalization (Form N-550, N-570) [3 points]
    - Certificate of Citizenship (Form N-560 and N-561) [3 points]
    - NYS Certificate of Title [2 points]
    - US Social Security Card [2 points]
    - Bank statement [1 point]
    - . . .

Point-based trust management model – 2

- A server associates a given number of points with each credential
    - represent the trustworthiness of its holder
    - the points associated with credentials are private
- A server requires a minimum total threshold of points before granting a client access to a resource
    - the threshold is private
- A client values each of its credentials with a private score
    - indicates the sensitivity of the credential and should be kept private

Goal: find a subset of the client credentials that satisfies the threshold fixed by the server and that has minimum privacy value to the client

Point-based trust management model – 3

Threshold of accessing a resource: 10

SERVER

	College ID	Driver's license	Credit card	SSN
Point value	3	6	8	10

CLIENT

	College ID	Driver's license	Credit card	SSN
Sensitivity score	10	30	50	100

Point-based trust management model – 3

Threshold of accessing a resource: 10

SERVER

	College ID	Driver's license	Credit card	SSN
Point value	3	6	8	10

CLIENT

	College ID	Driver's license	Credit card	SSN
Sensitivity score	10	30	50	100

Client's options:

- SSN [Points: 10; Sensitivity: 100]

Point-based trust management model – 3

Threshold of accessing a resource: 10

SERVER

	College ID	Driver's license	Credit card	SSN
Point value	3	6	8	10

CLIENT

	College ID	Driver's license	Credit card	SSN
Sensitivity score	10	30	50	100

Client's options:

- SSN [Points: 10; Sensitivity: 100]
- College ID, Credit card [Points: 11; Sensitivity: 60]

Point-based trust management model – 3

Threshold of accessing a resource: 10

SERVER

	College ID	Driver's license	Credit card	SSN
Point value	3	6	8	10

CLIENT

	College ID	Driver's license	Credit card	SSN
Sensitivity score	10	30	50	100

Client's options:

- SSN [Points: 10; Sensitivity: 100]
- College ID, Credit card [Points: 11; Sensitivity: 60]
- Driver's license, Credit card [Points: 14; Sensitivity: 80]

Point-based trust management model – 3

Threshold of accessing a resource: 10

SERVER

	College ID	Driver's license	Credit card	SSN
Point value	3	6	8	10

CLIENT

	College ID	Driver's license	Credit card	SSN
Sensitivity score	10	30	50	100

Client's options:

- SSN [Points: 10; Sensitivity: 100]
- College ID, Credit card [Points: 11; Sensitivity: 60]
- Driver's license, Credit card [Points: 14; Sensitivity: 80]

Point-based trust management model – 4

Problem

- The problem consists in fulfilling the access threshold while disclosing the least amount of sensitive information (Credential Selection Problem)

Solution

- The problem is converted into a knapsack problem and solved with a dynamic programming approach
- A secure two-party dynamic programming protocol is used for solving the knapsack problem
  - the server and user jointly compute the optimal sum of privacy scores for the released credentials without revealing their private parameters
  - the protocol uses homomorphic encryption

Point-based trust management model – 5

- The solution can model only the additive characteristic of privacy

- The client and server must agree on the universe of possible credential types (it may compromise the confidentiality of the server policy)

- Support only coarse-grain (credential) specification; sensitive associations as well as forbidden releases cannot be expressed

- Put focus on negotiation rather than on client control

Logic-based Minimal Credential Disclosure

P. Kärger, D. Olmedilla, W.-T. Balke, “Exploiting Preferences for Minimal Credential Disclosure in Policy-Driven Trust Negotiations,” in *Proc. of SDM*, Auckland, New Zealand, August 2008.

Logic-based minimal credential disclosure – 1

- Parties are involved in a trust negotiation where the release of credentials is regulated by given policies
- Each credential contains a single attribute
- By matching the policies of the involved parties, several negotiation paths (i.e., credential disclosure sets) will make the negotiation succeed
- Logic-based approach for users to specify privacy preferences exploited for selecting a negotiation path

Logic-based minimal credential disclosure – 2

Alice's policy

$c_{name} \leftarrow \text{TRUE}$

$c_{bdate} \leftarrow c_{bbb}$

$c_{telephone} \leftarrow c_{bbb}$

$c_{email} \leftarrow c_{bbb}$

$c_{pcode} \leftarrow c_{bbb}$

$c_{id} \leftarrow c_{bbb}$

$c_{passport} \leftarrow c_{bbb}$

$c_{bname} \leftarrow c_{bbb} \wedge c_{osc}$

$c_{baccount} \leftarrow c_{bbb} \wedge c_{osc}$

$c_{credit\_card} \leftarrow c_{bbb} \wedge c_{osc}$

$c_{pin} \leftarrow c_{bbb} \wedge c_{osc}$

On-line book shop's policy

$$\begin{aligned}
\text{purchase} &\leftarrow p_{register} \wedge p_{payment} \\
p_{register} &\leftarrow (c_{name} \wedge c_{bdate} \wedge \\
&\quad (c_{email} \vee c_{pcode})) \vee \\
&\quad c_{id} \vee c_{passport} \vee \\
&\quad ((c_{name} \vee c_{email}) \wedge c_{id}) \\
p_{payment} &\leftarrow (c_{bname} \wedge c_{baccount}) \vee \\
&\quad (c_{credit\_card} \wedge c_{pin}) \\
c_{bbb} &\leftarrow \text{TRUE} \\
c_{osc} &\leftarrow \text{TRUE}
\end{aligned}$$

Negotiation paths

	name	bdate	telephone	email	pcode	id	passport	bname	baccount	credit_card	pin
S_1	×	×		×				×	×		
S_2	×	×		×						×	×
S_3	×	×			×			×	×		
S_4	×	×			×					×	×
S_5						×		×	×		
S_6						×				×	×
S_7							×	×	×		
S_8							×			×	×
S_9	×					×		×	×		
S_{10}	×					×				×	×
S_{11}				×		×		×	×		
S_{12}				×		×				×	×

Logic-based minimal credential disclosure – 2

Alice's policy

$$
\begin{aligned}
c_{name} &\leftarrow \text{TRUE} \\
c_{bdate} &\leftarrow c_{bbb} \\
c_{telephone} &\leftarrow c_{bbb} \\
c_{email} &\leftarrow c_{bbb} \\
c_{pcode} &\leftarrow c_{bbb} \\
c_{id} &\leftarrow c_{bbb} \\
c_{passport} &\leftarrow c_{bbb} \\
c_{bname} &\leftarrow c_{bbb} \wedge c_{osc} \\
c_{baccount} &\leftarrow c_{bbb} \wedge c_{osc} \\
c_{credit\_card} &\leftarrow c_{bbb} \wedge c_{osc} \\
c_{pin} &\leftarrow c_{bbb} \wedge c_{osc}
\end{aligned}
$$

On-line book shop's policy

$$
\begin{aligned}
\text{purchase} &\leftarrow p_{register} \wedge p_{payment} \\
p_{register} &\leftarrow (c_{name} \wedge c_{bdate} \wedge \\
&\quad (c_{email} \vee c_{pcode})) \vee \\
&\quad c_{id} \vee c_{passport} \vee \\
&\quad ((c_{name} \vee c_{email}) \wedge c_{id}) \\
p_{payment} &\leftarrow (c_{bname} \wedge c_{baccount}) \vee \\
&\quad (c_{credit\_card} \wedge c_{pin}) \\
c_{bbb} &\leftarrow \text{TRUE} \\
c_{osc} &\leftarrow \text{TRUE}
\end{aligned}
$$

Negotiation paths

	name	bdate	telephone	email	pcode	id	passport	bname	baccount	credit_card	pin
S_1	×	×		×				×	×		
S_2	×	×		×						×	×
S_3	×	×			×			×	×		
S_4	×	×			×					×	×
S_5						×		×	×		
S_6						×				×	×
S_7							×	×	×		
S_8							×			×	×
S_9	×					×		×	×		
S_{10}	×					×				×	×
S_{11}				×		×		×	×		
S_{12}				×		×				×	×

Disclosure sets are represented as binary vectors

$\Longrightarrow$ 0 means do not disclose; 1 means disclose

Logic-based minimal credential disclosure – 2

Alice's policy

$$\begin{aligned}
c_{name} &\leftarrow \text{TRUE} \\
c_{bdate} &\leftarrow c_{bbb} \\
c_{telephone} &\leftarrow c_{bbb} \\
c_{email} &\leftarrow c_{bbb} \\
c_{pcode} &\leftarrow c_{bbb} \\
c_{id} &\leftarrow c_{bbb} \\
c_{passport} &\leftarrow c_{bbb} \\
c_{bname} &\leftarrow c_{bbb} \wedge c_{osc} \\
c_{baccount} &\leftarrow c_{bbb} \wedge c_{osc} \\
c_{credit\_card} &\leftarrow c_{bbb} \wedge c_{osc} \\
c_{pin} &\leftarrow c_{bbb} \wedge c_{osc}
\end{aligned}$$

On-line book shop's policy

$$\begin{aligned}
\text{purchase} &\leftarrow p_{register} \wedge p_{payment} \\
p_{register} &\leftarrow (c_{name} \wedge c_{bdate} \wedge \\
&\quad (c_{email} \vee c_{pcode})) \vee \\
&\quad c_{id} \vee c_{passport} \vee \\
&\quad ((c_{name} \vee c_{email}) \wedge c_{id}) \\
p_{payment} &\leftarrow (c_{bname} \wedge c_{baccount}) \vee \\
&\quad (c_{credit\_card} \wedge c_{pin}) \\
c_{bbb} &\leftarrow \text{TRUE} \\
c_{osc} &\leftarrow \text{TRUE}
\end{aligned}$$

Negotiation paths

	name	bdate	telephone	email	pcode	id	passport	bname	baccount	credit_card	pin
S_1	1	1	0	1	0	0	0	1	1	0	0
S_2	1	1	0	1	0	0	0	0	0	1	1
S_3	1	1	0	0	1	0	0	1	1	0	0
S_4	1	1	0	0	1	0	0	0	0	1	1
S_5	0	0	0	0	0	1	0	1	1	0	0
S_6	0	0	0	0	0	1	0	0	0	1	1
S_7	0	0	0	0	0	0	1	1	1	0	0
S_8	0	0	0	0	0	0	1	0	0	1	1
S_9	1	0	0	0	0	1	0	1	1	0	0
S_{10}	1	0	0	0	0	1	0	0	0	1	1
S_{11}	0	0	0	1	0	1	0	1	1	0	0
S_{12}	0	0	0	1	0	1	0	0	0	1	1

Disclosure sets are represented as binary vectors

$\Longrightarrow$ 0 means do not disclose; 1 means disclose

Logic-based minimal credential disclosure – 3

- Default preference: not disclosing a credential is preferred to disclosing it

  $\Longrightarrow 0 \succ_i 1$, with i the i-th credential

- Disclosure sets are compared according to the Pareto composition ($\succ_P$)
  - S_i dominates S_j if S_i shows better or equal values than S_j with respect to all credential preferences and is strictly better with respect to at least one credential

    Example

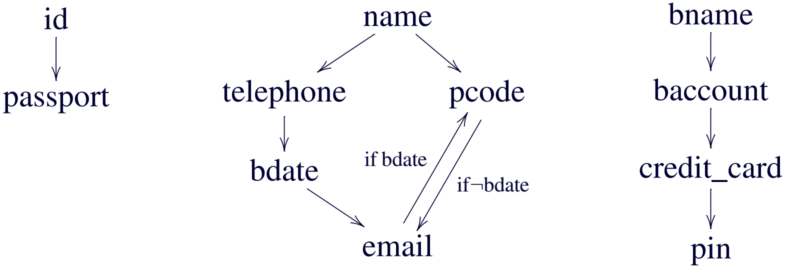
    S_5: [**0**,0,0,0,0,1,0,1,1,0,0] S_9: [**1**,0,0,0,0,1,0,1,1,0,0]

    $S_5[i] = S_9[i], i = 2, \ldots, 11$ and $S_5[1] \succ_1 S_9[1]$

    $\Longrightarrow S_5$ dominates S_9 ($S_5 \succ_P S_9$)

Logic-based minimal credential disclosure – 4

- Hierarchies specify (possibly contextual) user preferences on the release of credentials ($c_i \to c_j$ means that the user prefers to release c_i over c_j)



- Transitive combination of preferences
    - e.g., a disclosure set containing bname and baccount is preferred than a disclosure set containing credit_card and pin

Logic-based minimal credential disclosure – 5

Disclosure sets

	name	bdate	telephone	email	pcode	id	passport	bname	baccount	credit_card	pin
S_1	1	1	0	1	0	0	0	1	1	0	0
S_2	1	1	0	1	0	0	0	0	0	1	1
S_3	1	1	0	0	1	0	0	1	1	0	0
S_4	1	1	0	0	1	0	0	0	0	1	1
S_5	0	0	0	0	0	1	0	1	1	0	0
S_6	0	0	0	0	0	1	0	0	0	1	1
S_7	0	0	0	0	0	0	1	1	1	0	0
S_8	0	0	0	0	0	0	1	0	0	1	1
S_9	1	0	0	0	0	1	0	1	1	0	0
S_{10}	1	0	0	0	0	1	0	0	0	1	1
S_{11}	0	0	0	1	0	1	0	1	1	0	0
S_{12}	0	0	0	1	0	1	0	0	0	1	1

Logic-based minimal credential disclosure – 5

Disclosure sets

	name	bdate	telephone	email	pcode	id	passport	bname	baccount	credit_card	pin
S_1	1	1	0	1	0	0	0	1	1	0	0
S_2	1	1	0	1	0	0	0	0	0	1	1
S_3	1	1	0	0	1	0	0	1	1	0	0
S_4	1	1	0	0	1	0	0	0	0	1	1
S_5	**0**	0	0	0	0	1	0	1	1	0	0
S_6	0	0	0	0	0	1	0	0	0	1	1
S_7	0	0	0	0	0	0	1	1	1	0	0
S_8	0	0	0	0	0	0	1	0	0	1	1
S_9	**1**	0	0	0	0	1	0	1	1	0	0
S_{10}	1	0	0	0	0	1	0	0	0	1	1
S_{11}	0	0	0	1	0	1	0	1	1	0	0
S_{12}	0	0	0	1	0	1	0	0	0	1	1

Pareto composition

S_5 dominates S_9 since $0 \succ_{name} 1$

Logic-based minimal credential disclosure – 5

Disclosure sets

	name	bdate	telephone	email	pcode	id	passport	bname	baccount	credit_card	pin
S_1	1	1	0	1	0	0	0	1	1	0	0
S_2	1	1	0	1	0	0	0	0	0	1	1
S_3	1	1	0	0	1	0	0	1	1	0	0
S_4	1	1	0	0	1	0	0	0	0	1	1
S_5	0	0	0	0	0	1	0	1	1	0	0
S_6	0	0	0	0	0	1	0	0	0	1	1
S_7	0	0	0	0	0	0	1	1	1	0	0
S_8	0	0	0	0	0	0	1	0	0	1	1
S_9	1	0	0	0	0	1	0	1	1	0	0
S_{10}	1	0	0	0	0	1	0	0	0	1	1
S_{11}	0	0	0	1	0	1	0	1	1	0	0
S_{12}	0	0	0	1	0	1	0	0	0	1	1

Pareto composition

S_5 dominates S_9 since $0 \succ_{name} 1$

Logic-based minimal credential disclosure – 5

Disclosure sets

	name	bdate	telephone	email	pcode	id	passport	bname	baccount	credit_card	pin
S_1	1	1	0	1	0	0	0	1	1	0	0
S_2	1	1	0	1	0	0	0	0	0	1	1
S_3	1	1	0	0	1	0	0	1	1	0	0
S_4	1	1	0	0	1	0	0	0	0	1	1
S_5	0	0	0	**0**	0	1	0	1	1	0	0
S_6	0	0	0	0	0	1	0	0	0	1	1
S_7	0	0	0	0	0	0	1	1	1	0	0
S_8	0	0	0	0	0	0	1	0	0	1	1
S_9	1	0	0	0	0	1	0	1	1	0	0
S_{10}	1	0	0	0	0	1	0	0	0	1	1
S_{11}	0	0	0	**1**	0	1	0	1	1	0	0
S_{12}	0	0	0	1	0	1	0	0	0	1	1

Pareto composition

S_5 dominates S_9 since $0 \succ_{name} 1$

S_5 dominates S_{11} since $0 \succ_{email} 1$

Logic-based minimal credential disclosure – 5

Disclosure sets

	name	bdate	telephone	email	pcode	id	passport	bname	baccount	credit_card	pin
S_1	1	1	0	1	0	0	0	1	1	0	0
S_2	1	1	0	1	0	0	0	0	0	1	1
S_3	1	1	0	0	1	0	0	1	1	0	0
S_4	1	1	0	0	1	0	0	0	0	1	1
S_5	0	0	0	0	0	1	0	1	1	0	0
S_6	0	0	0	0	0	1	0	0	0	1	1
S_7	0	0	0	0	0	0	1	1	1	0	0
S_8	0	0	0	0	0	0	1	0	0	1	1
S_9	1	0	0	0	0	1	0	1	1	0	0
S_{10}	1	0	0	0	0	1	0	0	0	1	1
S_{11}	0	0	0	1	0	1	0	1	1	0	0
S_{12}	0	0	0	1	0	1	0	0	0	1	1

Pareto composition

S_5 dominates S_9 since $0 \succ_{name} 1$
S_5 dominates S_{11} since $0 \succ_{email} 1$

Logic-based minimal credential disclosure – 5

Disclosure sets

	name	bdate	telephone	email	pcode	id	passport	bname	baccount	credit_card	pin
S_1	1	1	0	1	0	0	0	1	1	0	0
S_2	1	1	0	1	0	0	0	0	0	1	1
S_3	1	1	0	0	1	0	0	1	1	0	0
S_4	1	1	0	0	1	0	0	0	0	1	1
S_5	0	0	0	0	0	1	0	1	1	0	0
S_6	**0**	0	0	0	0	1	0	0	0	1	1
S_7	0	0	0	0	0	0	1	1	1	0	0
S_8	0	0	0	0	0	0	1	0	0	1	1
S_9	1	0	0	0	0	1	0	1	1	0	0
S_{10}	**1**	0	0	0	0	1	0	0	0	1	1
S_{11}	0	0	0	1	0	1	0	1	1	0	0
S_{12}	0	0	0	1	0	1	0	0	0	1	1

Pareto composition

S_5 dominates S_9 since $0 \succ_{name} 1$

S_5 dominates S_{11} since $0 \succ_{email} 1$

S_6 dominates S_{10} since $0 \succ_{name} 1$

Logic-based minimal credential disclosure – 5

Disclosure sets

	name	bdate	telephone	email	pcode	id	passport	bname	baccount	credit_card	pin
S_1	1	1	0	1	0	0	0	1	1	0	0
S_2	1	1	0	1	0	0	0	0	0	1	1
S_3	1	1	0	0	1	0	0	1	1	0	0
S_4	1	1	0	0	1	0	0	0	0	1	1
S_5	0	0	0	0	0	1	0	1	1	0	0
S_6	0	0	0	0	0	1	0	0	0	1	1
S_7	0	0	0	0	0	0	1	1	1	0	0
S_8	0	0	0	0	0	0	1	0	0	1	1
S_9	1	0	0	0	0	1	0	1	1	0	0
S_{10}	1	0	0	0	0	1	0	0	0	1	1
S_{11}	0	0	0	1	0	1	0	1	1	0	0
S_{12}	0	0	0	1	0	1	0	0	0	1	1

Pareto composition

S_5 dominates S_9 since $0 \succ_{name} 1$
S_5 dominates S_{11} since $0 \succ_{email} 1$
S_6 dominates S_{10} since $0 \succ_{name} 1$

Logic-based minimal credential disclosure – 5

Disclosure sets

	name	bdate	telephone	email	pcode	id	passport	bname	baccount	credit_card	pin
S_1	1	1	0	1	0	0	0	1	1	0	0
S_2	1	1	0	1	0	0	0	0	0	1	1
S_3	1	1	0	0	1	0	0	1	1	0	0
S_4	1	1	0	0	1	0	0	0	0	1	1
S_5	0	0	0	0	0	1	0	1	1	0	0
S_6	0	0	0	**0**	0	1	0	0	0	1	1
S_7	0	0	0	0	0	0	1	1	1	0	0
S_8	0	0	0	0	0	0	1	0	0	1	1
S_9	1	0	0	0	0	1	0	1	1	0	0
S_{10}	1	0	0	0	0	1	0	0	0	1	1
S_{11}	0	0	0	1	0	1	0	1	1	0	0
S_{12}	0	0	0	**1**	0	1	0	0	0	1	1

Pareto composition

S_5 dominates S_9 since $0 \succ_{name} 1$

S_5 dominates S_{11} since $0 \succ_{email} 1$

S_6 dominates S_{10} since $0 \succ_{name} 1$

S_6 dominates S_{12} since $0 \succ_{email} 1$

Logic-based minimal credential disclosure – 5

Disclosure sets

	name	bdate	telephone	email	pcode	id	passport	bname	baccount	credit_card	pin
S_1	1	1	0	1	0	0	0	1	1	0	0
S_2	1	1	0	1	0	0	0	0	0	1	1
S_3	1	1	0	0	1	0	0	1	1	0	0
S_4	1	1	0	0	1	0	0	0	0	1	1
S_5	0	0	0	0	0	1	0	1	1	0	0
S_6	0	0	0	0	0	1	0	0	0	1	1
S_7	0	0	0	0	0	0	1	1	1	0	0
S_8	0	0	0	0	0	0	1	0	0	1	1
S_9	1	0	0	0	0	1	0	1	1	0	0
S_{10}	1	0	0	0	0	1	0	0	0	1	1
S_{11}	0	0	0	1	0	1	0	1	1	0	0
S_{12}	0	0	0	1	0	1	0	0	0	1	1

Pareto composition

S_5 dominates S_9 since $0 \succ_{name} 1$
S_5 dominates S_{11} since $0 \succ_{email} 1$
S_6 dominates S_{10} since $0 \succ_{name} 1$
S_6 dominates S_{12} since $0 \succ_{email} 1$

Logic-based minimal credential disclosure – 5

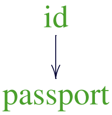
Disclosure sets

	name	bdate	telephone	email	pcode	id	passport	bname	baccount	credit_card	pin
S_1	1	1	0	1	0	0	0	1	1	0	0
S_2	1	1	0	1	0	0	0	0	0	1	1
S_3	1	1	0	0	1	0	0	1	1	0	0
S_4	1	1	0	0	1	0	0	0	0	1	1
S_5	0	0	0	0	0	**1**	**0**	1	1	0	0
S_6	0	0	0	0	0	**1**	**0**	0	0	1	1
S_7	0	0	0	0	0	**0**	**1**	1	1	0	0
S_8	0	0	0	0	0	**0**	**1**	0	0	1	1
S_9	1	0	0	0	0	1	0	1	1	0	0
S_{10}	1	0	0	0	0	1	0	0	0	1	1
S_{11}	0	0	0	1	0	1	0	1	1	0	0
S_{12}	0	0	0	1	0	1	0	0	0	1	1

Hierarchical preferences

S_5 dominates S_7

S_6 dominates S_8



id

passport

Logic-based minimal credential disclosure – 5

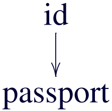
Disclosure sets

	name	bdate	telephone	email	pcode	id	passport	bname	baccount	credit_card	pin
S_1	1	1	0	1	0	0	0	1	1	0	0
S_2	1	1	0	1	0	0	0	0	0	1	1
S_3	1	1	0	0	1	0	0	1	1	0	0
S_4	1	1	0	0	1	0	0	0	0	1	1
S_5	0	0	0	0	0	1	0	1	1	0	0
S_6	0	0	0	0	0	1	0	0	0	1	1
S_7	0	0	0	0	0	0	1	1	1	0	0
S_8	0	0	0	0	0	0	1	0	0	1	1
S_9	1	0	0	0	0	1	0	1	1	0	0
S_{10}	1	0	0	0	0	1	0	0	0	1	1
S_{11}	0	0	0	1	0	1	0	1	1	0	0
S_{12}	0	0	0	1	0	1	0	0	0	1	1

Hierarchical preferences

S_5 dominates S_7

S_6 dominates S_8



id

passport

Logic-based minimal credential disclosure – 5

Disclosure sets

	name	bdate	telephone	email	pcode	id	passport	bname	baccount	credit_card	pin
S_1	1	**1**	0	**1**	**0**	0	0	1	1	0	0
S_2	1	**1**	0	**1**	**0**	0	0	0	0	1	1
S_3	1	**1**	0	**0**	**1**	0	0	1	1	0	0
S_4	1	**1**	0	**0**	**1**	0	0	0	0	1	1
S_5	0	0	0	0	0	1	0	1	1	0	0
S_6	0	0	0	0	0	1	0	0	0	1	1
S_7	0	0	0	0	0	0	1	1	1	0	0
S_8	0	0	0	0	0	0	1	0	0	1	1
S_9	1	0	0	0	0	1	0	1	1	0	0
S_{10}	1	0	0	0	0	1	0	0	0	1	1
S_{11}	0	0	0	1	0	1	0	1	1	0	0
S_{12}	0	0	0	1	0	1	0	0	0	1	1

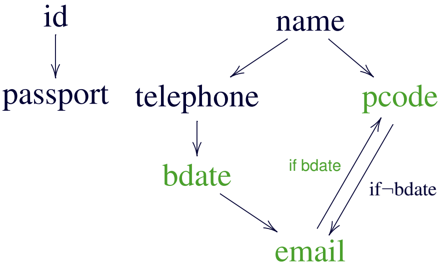
Hierarchical preferences

S_5 dominates S_7

S_6 dominates S_8

S_1 dominates S_3

S_2 dominates S_4



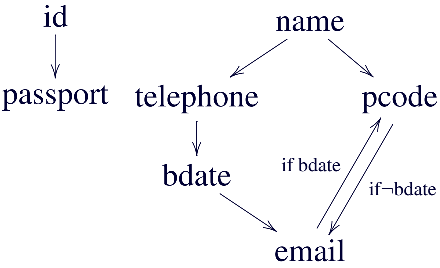
Logic-based minimal credential disclosure – 5

Disclosure sets

	name	bdate	telephone	email	pcode	id	passport	bname	baccount	credit_card	pin
S_1	1	1	0	1	0	0	0	1	1	0	0
S_2	1	1	0	1	0	0	0	0	0	1	1
S_3	1	1	0	0	1	0	0	1	1	0	0
S_4	1	1	0	0	1	0	0	0	0	1	1
S_5	0	0	0	0	0	1	0	1	1	0	0
S_6	0	0	0	0	0	1	0	0	0	1	1
S_7	0	0	0	0	0	0	1	1	1	0	0
S_8	0	0	0	0	0	0	1	0	0	1	1
S_9	1	0	0	0	0	1	0	1	1	0	0
S_{10}	1	0	0	0	0	1	0	0	0	1	1
S_{11}	0	0	0	1	0	1	0	1	1	0	0
S_{12}	0	0	0	1	0	1	0	0	0	1	1

Hierarchical preferences

S_5 dominates S_7
S_6 dominates S_8
S_1 dominates S_3
S_2 dominates S_4



Logic-based minimal credential disclosure – 5

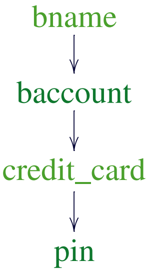
Disclosure sets

	name	bdate	telephone	email	pcode	id	passport	bname	baccount	credit_card	pin
S_1	1	1	0	1	0	0	0	**1**	**1**	**0**	**0**
S_2	1	1	0	1	0	0	0	**0**	**0**	**1**	**1**
S_3	1	1	0	0	1	0	0	1	1	0	0
S_4	1	1	0	0	1	0	0	0	0	1	1
S_5	0	0	0	0	0	1	0	**1**	**1**	**0**	**0**
S_6	0	0	0	0	0	1	0	**0**	**0**	**1**	**1**
S_7	0	0	0	0	0	0	1	1	1	0	0
S_8	0	0	0	0	0	0	1	0	0	1	1
S_9	1	0	0	0	0	1	0	1	1	0	0
S_{10}	1	0	0	0	0	1	0	0	0	1	1
S_{11}	0	0	0	1	0	1	0	1	1	0	0
S_{12}	0	0	0	1	0	1	0	0	0	1	1

Transitive combination of preferences

S_1 dominates S_2

S_5 dominates S_6



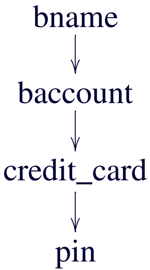
Logic-based minimal credential disclosure – 5

Disclosure sets

	name	bdate	telephone	email	pcode	id	passport	bname	baccount	credit_card	pin
S_1	1	1	0	1	0	0	0	1	1	0	0
S_2	1	1	0	1	0	0	0	0	0	1	1
S_3	1	1	0	0	1	0	0	1	1	0	0
S_4	1	1	0	0	1	0	0	0	0	1	1
S_5	0	0	0	0	0	1	0	1	1	0	0
S_6	0	0	0	0	0	1	0	0	0	1	1
S_7	0	0	0	0	0	0	1	1	1	0	0
S_8	0	0	0	0	0	0	1	0	0	1	1
S_9	1	0	0	0	0	1	0	1	1	0	0
S_{10}	1	0	0	0	0	1	0	0	0	1	1
S_{11}	0	0	0	1	0	1	0	1	1	0	0
S_{12}	0	0	0	1	0	1	0	0	0	1	1

Transitive combination of preferences

S_1 dominates S_2
S_5 dominates S_6



Logic-based minimal credential disclosure – 5

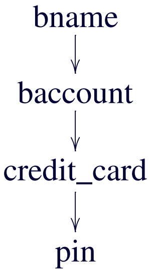
Disclosure sets

	name	bdate	telephone	email	pcode	id	passport	bname	baccount	credit_card	pin
S_1	1	1	0	1	0	0	0	1	1	0	0
S_2	1	1	0	1	0	0	0	0	0	1	1
S_3	1	1	0	0	1	0	0	1	1	0	0
S_4	1	1	0	0	1	0	0	0	0	1	1
S_5	0	0	0	0	0	1	0	1	1	0	0
S_6	0	0	0	0	0	1	0	0	0	1	1
S_7	0	0	0	0	0	0	1	1	1	0	0
S_8	0	0	0	0	0	0	1	0	0	1	1
S_9	1	0	0	0	0	1	0	1	1	0	0
S_{10}	1	0	0	0	0	1	0	0	0	1	1
S_{11}	0	0	0	1	0	1	0	1	1	0	0
S_{12}	0	0	0	1	0	1	0	0	0	1	1

Transitive combination of preferences

S_1 dominates S_2

S_5 dominates S_6



bname

baccount

credit_card

pin

$\Longrightarrow$ user has to choose between S_1, S_5

Logic-based minimal credential disclosure – 6

- Users are still involved in choosing the disclosure set
- Assume only attributes (does not reason about credentials)
- The specification of preferences among groups of attributes is not always easy
- Possession-sensitive credentials are not considered
- Forbidden releases (e.g., the release of name, bdate, and pcode is forbidden) are not supported

Privacy Preferences in Credential-based Interactions

C.A. Ardagna, S. De Capitani di Vimercati, S. Foresti, S. Paraboschi, P. Samarati, "Minimizing Disclosure of Private Information in Credential-Based Interactions: A Graph-Based Approach," in *Proc. of PASSAT*, Minneapolis, MN, USA, August 2010.

C.A. Ardagna, S. De Capitani di Vimercati, S. Foresti, S. Paraboschi, P. Samarati, "Supporting Privacy Preferences in Credential-Based Interactions," in *Proc. of WPES*, Chicago, IL, USA, October 2010.

C.A. Ardagna, S. De Capitani di Vimercati, S. Foresti, S. Paraboschi, P. Samarati, "Minimising Disclosure of Client Information in Credential-Based Interactions," in *IJIPSI*, vol. 1, no. 2/3, 2012.

Goal of the work

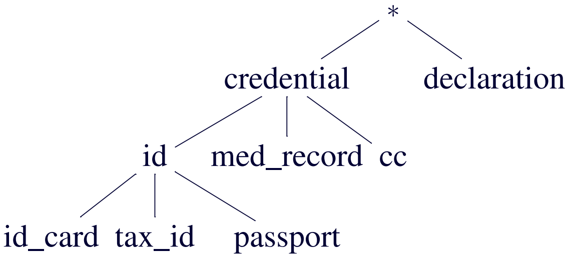
Enable users to effectively regulate disclosure of their properties and credentials

- identify requirements and concepts that need to be captured
- organize user's properties and credentials in the user portfolio
- enable user to specify how much she values the disclosure of different components of the portfolio
- provide possible technical approaches for supporting user's preferences
- provide a basis for investigating user-friendly/user-understandable approaches for regulating release of user's properties

Client portfolio modeling

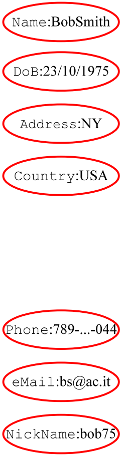
- The information of the client forms a client portfolio
- Credential: certificate issued and signed by a third party
  - certifies a set of properties
  - has a type, an identifier, and an issuer
- Declaration: property stored as a self-signed credential
- Hierarchy of abstractions of credential types $\mathscr{H}(\mathscr{T}, \preceq_{isa})$ (e.g., *id_card*$\preceq_{isa}$*id*, *id*$\preceq_{isa}$*credential*)

An example of hierarchy of credential types



Client portfolio – Properties

- Credential-independent: the value depends only on the credential's owner (e.g., birth date)


Name:BobSmith

DoB:23/10/1975

Address:NY

Country:USA

Phone:789-...-044

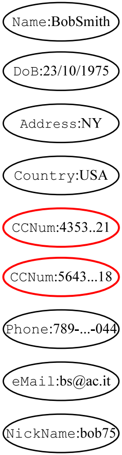
eMail:bs@ac.it

NickName:bob75

Client portfolio – Properties

- Credential-independent: the value depends only on the credential's owner (e.g., birth date)

- Credential-dependent: the value depends on the certifying credential (e.g., credit card number)



Name:BobSmith

DoB:23/10/1975

Address:NY

Country:USA

CCNum:4353..21

CCNum:5643...18

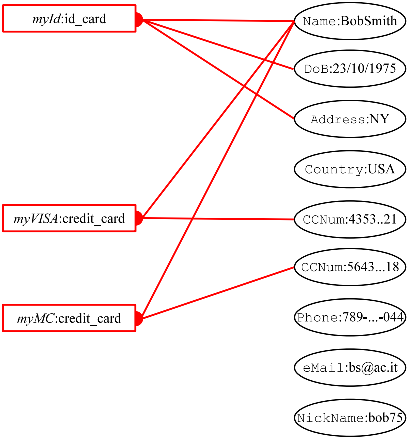
Phone:789-...-044

eMail:bs@ac.it

NickName:bob75

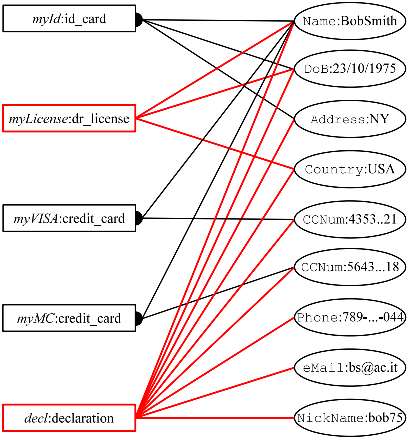
Client portfolio – Credentials

- Atomic: released as a whole (e.g., X.509)



Client portfolio – Credentials

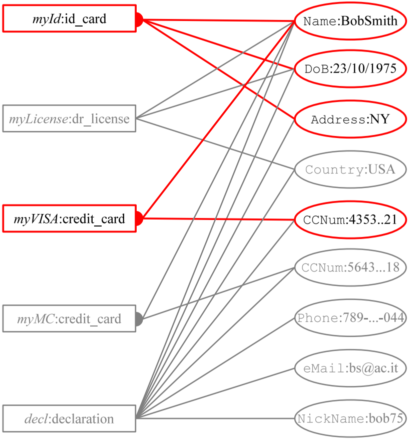
- Atomic: released as a whole (e.g., X.509)
- Non-atomic: properties can be selectively released, proof-of-possession can be certified (e.g., Idemix, U-Prove)



Disclosure

A disclosure is a subset of the client portfolio that satisfies:

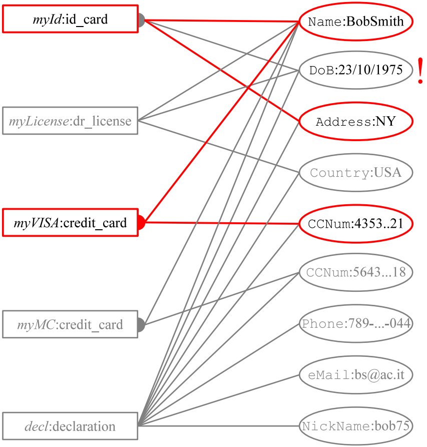
- certifiability: each property is certified by a credential
- atomicity: if a property of an atomic credential is disclosed, all its properties are disclosed



Disclosure

A disclosure is a subset of the client portfolio that satisfies:

- certifiability: each property is certified by a credential
- atomicity: if a property of an atomic credential is disclosed, all its properties are disclosed



Does not satisfy atomicity!

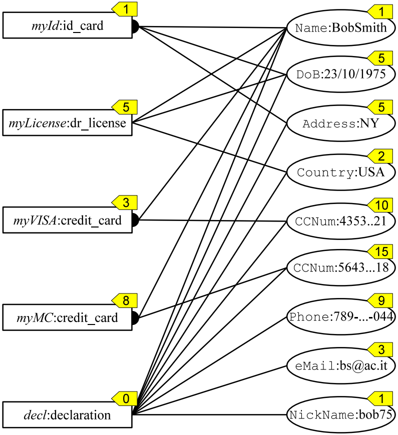
Portfolio sensitivity

- Different portfolio components have different sensitivity
  - the client may prefer to disclose some properties or credentials
- Sensitivity labels express privacy requirements:
  - partial order relationship $\succeq$
  - arbitrary composition operator $\oplus$
    (the composition of two sensitivity labels $\lambda_1 \oplus \lambda_2$ is a sensitivity label)
- We assume sensitivity labels to be integer values, composed through the $+$ operator

Sensitivity of properties and credentials

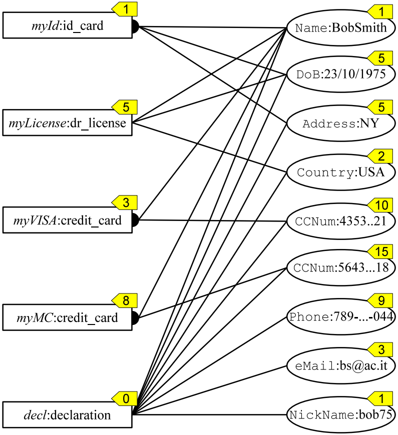
Specify how a client values information in her portfolio

- $\lambda(A)$: sensitivity of property A individually taken
- $\lambda(c)$: sensitivity of the existence of credential c



Sensitivity of associations

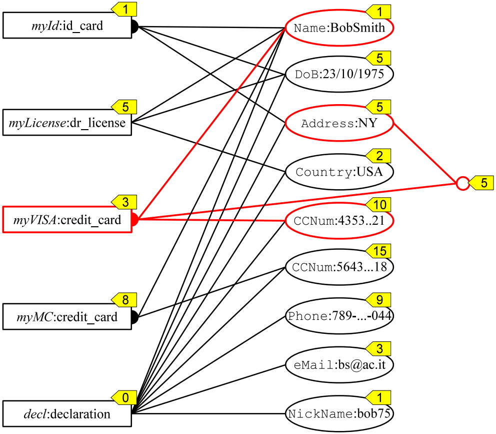
$\lambda(A)$: sensitivity of an association $A=\{A_i,\ldots,A_j,c_k,\ldots,c_n\}$, whose joint release carries:



Sensitivity of associations

$\lambda(A)$: sensitivity of an association A=$\{A_i,\ldots,A_j,c_k,\ldots,c_n\}$, whose joint release carries:

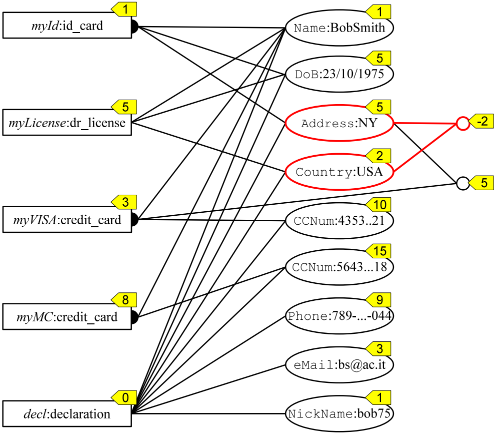
- more information than the release of each element in A
  $\Longrightarrow$ sensitive view



Sensitivity of associations

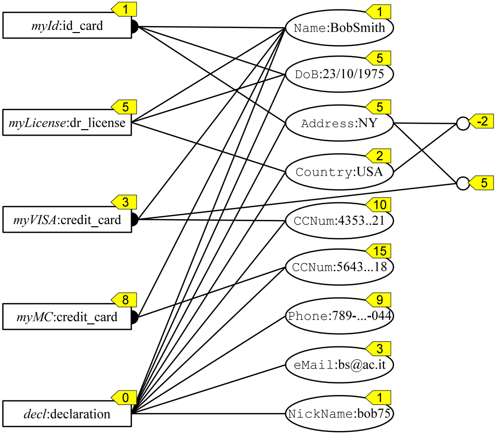
$\lambda(A)$: sensitivity of an association $A=\{A_i,\ldots,A_j,c_k,\ldots,c_n\}$, whose joint release carries:

- more information than the release of each element in A $\Longrightarrow$ sensitive view
- less information than the release of each element in A $\Longrightarrow$ dependency



Disclosure constraints

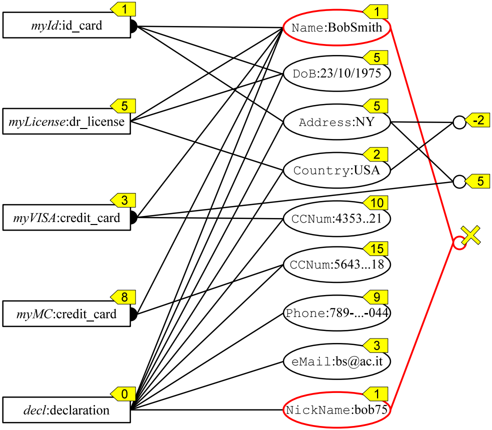
Set $A=\{A_i,\ldots,A_j,c_k,\ldots,c_n\}$ of elements whose release must be controlled



Disclosure constraints

Set $A=\{A_i,\ldots,A_j,c_k,\ldots,c_n\}$ of elements whose release must be controlled

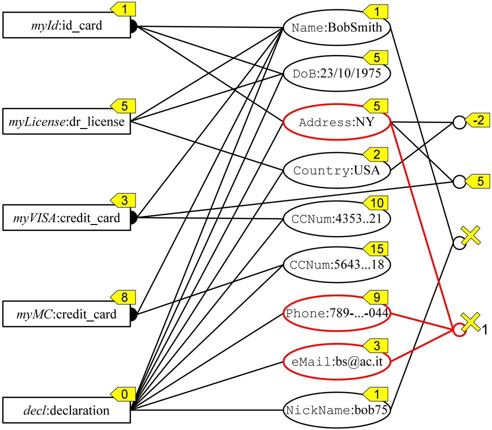
- forbidden view: the release of A is prohibited



Disclosure constraints

Set $A=\{A_i,\ldots,A_j,c_k,\ldots,c_n\}$ of elements whose release must be controlled

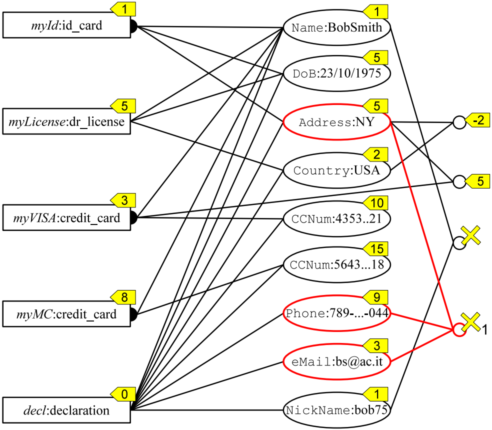
- forbidden view: the release of A is prohibited
- disclosure limitation: at most n elements in A can be released



Disclosure constraints

Set $A = \{A_i, \ldots, A_j, c_k, \ldots, c_n\}$ of elements whose release must be controlled

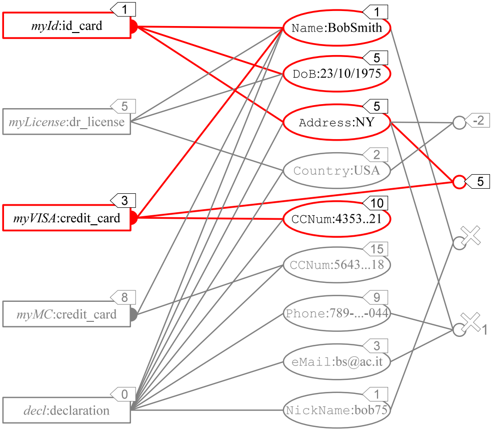
- forbidden view: the release of *A* is prohibited
- disclosure limitation: at most n elements in *A* can be released



A disclosure is valid if no disclosure constraint is violated

Disclosure sensitivity

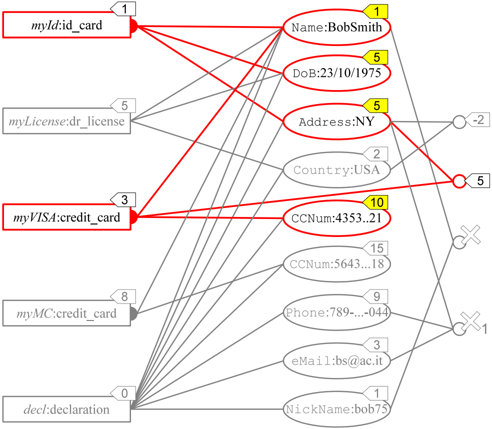
The sensitivity $\lambda(\mathscr{D})$ of a disclosure $\mathscr{D}$ is the sum of the sensitivity labels of released:



Disclosure sensitivity

The sensitivity $\lambda(\mathscr{D})$ of a disclosure $\mathscr{D}$ is the sum of the sensitivity labels of released:

- properties

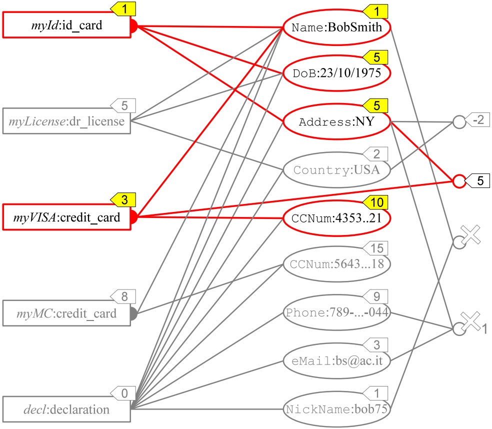


$\lambda(\mathscr{D})$ = 1+5+5+10

Disclosure sensitivity

The sensitivity $\lambda(\mathscr{D})$ of a disclosure $\mathscr{D}$ is the sum of the sensitivity labels of released:

- properties
- credentials

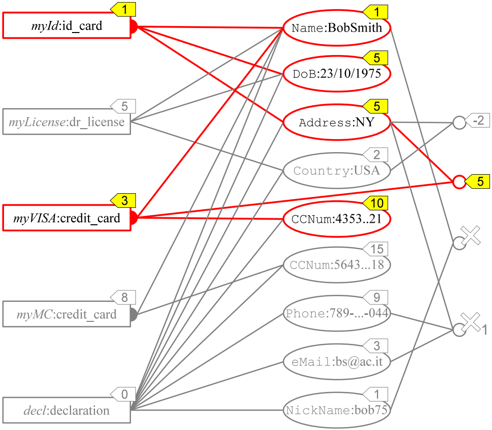


$\lambda(\mathscr{D})$ = 1+5+5+10+1+3

Disclosure sensitivity

The sensitivity $\lambda(\mathscr{D})$ of a disclosure $\mathscr{D}$ is the sum of the sensitivity labels of released:

- properties
- credentials
- associations



$$\lambda(\mathscr{D}) = 1+5+5+10+1+3+5 = 30$$

Server request

Request $\mathscr{R}$: disjunction of simple requests

- Simple request R: conjunction of terms
  - term r=$type.\{A_1, \ldots, A_m\}$: disclosure of $\{A_1, \ldots, A_m\}$ from c s.t. $type(c) \preceq_{isa} type$

    $\Longrightarrow$ *type* is an abstraction of credential type *type*(c) in $\mathscr{H}$

Example

$\mathscr{R} = r_1 \wedge r_2$

$r_1 = id.\{\texttt{Name},\texttt{Address}\}$

$r_2 = cc.\{\texttt{Name},\texttt{CCNum}\}$

Min-disclosure problem

A disclosure $\mathscr{D}$:

- satisfies $\mathscr{R}$ if it satisfies at least a R in $\mathscr{R}$
- satisfies R if, $\forall$ r=*type*.$\{A_1,\ldots,A_m\}$ in R, it includes c s.t.:
  - c certifies $\{A_1,\ldots,A_m\}$
  - *type*(c)$\preceq_{isa}$*type*

Min-disclosure problem

$\mathscr{R}$ = *id*.{`Name`,`Address`} ∧ *cc*.{`Name`,`CCNum`}

A disclosure $\mathscr{D}$:

- satisfies $\mathscr{R}$ if it satisfies at least a R in $\mathscr{R}$

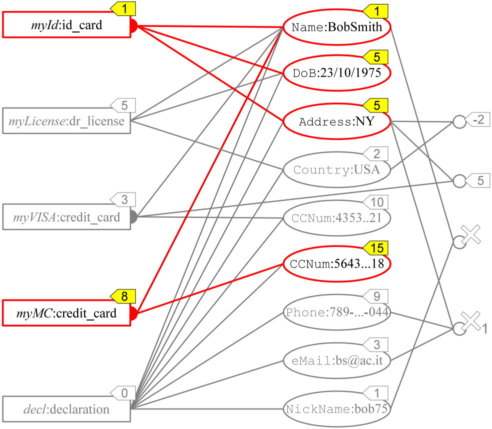
- satisfies R if, $\forall$ r=$type.\{A_1,\ldots,A_m\}$ in R, it includes c s.t.:
    - c certifies $\{A_1,\ldots,A_m\}$
    - $type(c) \preceq_{isa} type$

Min-disclosure problem

$\mathscr{R}$ = *id*.{Name,Address} ∧ *cc*.{Name,CCNum}

A disclosure $\mathscr{D}$:

- satisfies $\mathscr{R}$ if it satisfies at least a R in $\mathscr{R}$
- satisfies R if, ∀ r=*type*.$\{A_1, \ldots, A_m\}$ in R, it includes c s.t.:
    - c certifies $\{A_1, \ldots, A_m\}$
    - $type(c) \preceq_{isa} type$



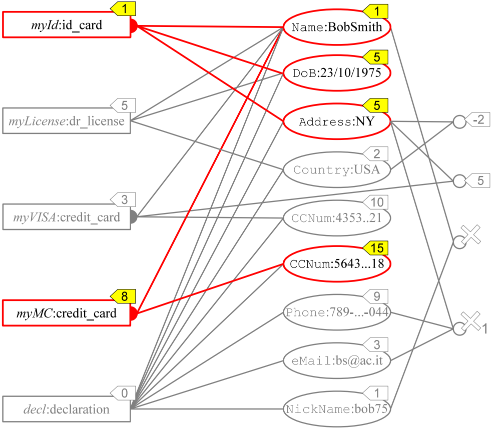
$\lambda(\mathscr{D})$ = 1+8+1+5+5+15 = 35

Min-disclosure problem

A disclosure $\mathscr{D}$:

- satisfies $\mathscr{R}$ if it satisfies at least a R in $\mathscr{R}$
- satisfies R if, $\forall$ r=*type*.$\{A_1,\ldots,A_m\}$ in R, it includes c s.t.:
  - c certifies $\{A_1,\ldots,A_m\}$
  - $type(c) \preceq_{isa} type$
- is minimum if $\nexists$ a valid disclosure $\mathscr{D}'$ s.t. $\mathscr{D}'$ satisfies $\mathscr{R}$ and $\lambda(\mathscr{D}')<\lambda(\mathscr{D})$

$\mathscr{R}$ = *id*.{Name,Address} ∧ *cc*.{Name,CCNum}



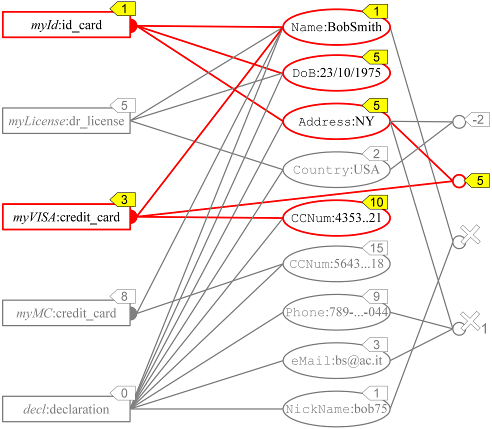
$\lambda(\mathscr{D})$ = 35 $\Longrightarrow$ $\mathscr{D}$ is not minimum

Min-disclosure problem

A disclosure $\mathscr{D}$:

- satisfies $\mathscr{R}$ if it satisfies at least a R in $\mathscr{R}$
- satisfies R if, $\forall$ r=$type.\{A_1,\ldots,A_m\}$ in R, it includes c s.t.:
    - c certifies $\{A_1,\ldots,A_m\}$
    - $type(c) \preceq_{isa} type$
- is minimum if $\nexists$ a valid disclosure $\mathscr{D}'$ s.t. $\mathscr{D}'$ satisfies $\mathscr{R}$ and $\lambda(\mathscr{D}')<\lambda(\mathscr{D})$

$\mathscr{R}$ = id.{Name,Address} ∧ cc.{Name,CCNum}



$\lambda(\mathscr{D}')$ = 30 $\Longrightarrow$ $\mathscr{D}'$ is minimum

Computing a minimal disclosure

The problem of computing a disclosure that minimizes release of information is NP-hard

- exploit graph-based representation of portfolio and requests, providing heuristics based on graph-matching [ADFPS-10a]
- exploit Max-SAT representation of the problem and existing SAT solver [ADFPS-10b]

Work to be investigated – 1

- Enable derivation of sensitivity levels of properties (e.g., based on identity exposure)
- Support specifications in terms of preferences (e.g., my id_card is less sensitive than my passport)
- Sensitivity labels assigned to proofs (provided by non-atomic credentials)
- Support referring to existence of a credential (without releasing it)
- Allow recipient/context-based sensitivity specifications (e.g., dialysis certificates is less sensitive if released to a doctor than to a generic server)
- User-intuitive approaches for expressing preferences (and possibly translate them to sensitivity labels)

Work to be investigated – 2

- Consideration of previous disclosures
- Type vs instance mismatch (server talks about classes, users refer to instances)
- Integration with server-side solutions and more expressive server requests [ADFNPPSV-10]

Server-side open issues – 1

On the server-side there is still work to do to increase expressiveness. Today XACML:

- does not provide a support for expressing and reasoning about digital certificates in the specification of the authorization policies:
    - e.g., “attribute nationality should be certified by a passport”
- does not have support for abstractions
    - e.g., “id_document is an abstraction including credentials {identity_card, driver_license, passport}”

C. Ardagna, S. De Capitani di Vimercati, S. Paraboschi, E. Pedrini, P. Samarati, M. Verdicchio, “Expressive and Deployable Access Control in Open Web Service Applications,” in *IEEE TSC*, vol. 4, no. 2, April-June 2011.

Server-side open issues – 2

- does not have support for policy dialog (to communicate policies to users):
  - condition (e.g., “identity_card.age $>$ 18”)
  - predicate (e.g., “identity_card.age $>$”)
  - property (e.g., “identity_card.age”)
  - credential (e.g., “identity_card”)
  - none (nothing can be disclosed about the condition)
- does not have support for recursive conditions:
  - for expressing policies based on chains of credentials/properties
  - for supporting delegation and recursion (e.g., “the certification authority signing a user’s credential has been directly or indirectly delegated by a particular authority preferred by the server”)

References – 1

- [ACCDS-11] C.A. Ardagna, M. Cremonini, S. De Capitani di Vimercati, P. Samarati, “An Obfuscation-based Approach for Protecting Location Privacy,” in *IEEE TDSC*, vol. 8, no. 1, January-February 2011.
- [ACCM-12] A. Armando, A. Contento, D. Costa, M. Maratea, “Minimum Disclosure as Boolean Optimization: New Results,” in *Proc. of RCRA*, Rome, Italy, June 2012.
- [ADFNPPSV-10] C.A. Ardagna, S. De Capitani di Vimercati, S. Foresti, G. Neven, S. Paraboschi, F.-S. Preiss, P. Samarati, M. Verdicchio, “Fine-Grained Disclosure of Access Policies,” in *Proc. of ICICS*, Barcelona, Spain, December 2010.
- [ADFPS-10a] C.A. Ardagna, S. De Capitani di Vimercati, S. Foresti, S. Paraboschi, P. Samarati, “Minimizing Disclosure of Private Information in Credential-based Interactions: A Graph-based Approach,” in *Proc. of PASSAT*, Minneapolis, MN, USA, August 2010.
- [ADFPS-10b] C.A. Ardagna, S. De Capitani di Vimercati, S. Foresti, S. Paraboschi, P. Samarati, “Supporting Privacy Preferences in Credential-Based Interactions,” in *Proc. of WPES*, Chicago, IL, USA, October 2010.
- [ADFPS-12] C.A. Ardagna, S. De Capitani di Vimercati, S. Foresti, S. Paraboschi, P. Samarati, “Minimising Disclosure of Client Information in Credential-Based Interactions,” in *IJIPSI*, vol. 1, no. 2/3, 2012.

References – 2

- [ADPPSV-11] C. Ardagna, S. De Capitani di Vimercati, S. Paraboschi, E. Pedrini, P. Samarati, M. Verdicchio, “Expressive and Deployable Access Control in Open Web Service Applications,” in *IEEE TSC* vol. 4, no. 4, April-June 2011.
- [ALS-12] C.A. Ardagna, G. Livraga, P. Samarati, “Protecting Privacy of User Information in Continuous Location-Based Services,” in *Proc. of CSE*, Paphos, Cyprus, December 2012.
- [BS-02] P. Bonatti, P. Samarati, “A Uniform Framework for Regulating Service Access and Information Release on the Web,” in *JCS*, vol. 10, no. 3, 2002.
- [CCKT-05] W. Chen, L. Clarke, J. Kurose, D. Towsley, “Optimizing Cost-Sensitive Trust-Negotiation Protocols,” in *Proc. of INFOCOM,* Miami, FL, USA, March 2005.
- [DFJPPS-12] S. De Capitani di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, G. Psaila, P. Samarati, “Integrating Trust Management and Access Control in Data-Intensive Web Applications,” in *ACM TWEB*, vol. 6, no. 2, May 2012.
- [KOB-08] P. Kärger , D. Olmedilla, W.-T. Balke, “Exploiting Preferences for Minimal Credential Disclosure in Policy-Driven Trust Negotiations,” in *Proc. of SDM*, Auckland, New Zealand, August 2008.

References – 3

- [LWBW-08] A. J. Lee, M. Winslett, J. Basney, V. Welch, “The Traust Authorization Service,” in *ACM TISSEC*, vol. 11, no. 1, February 2008.
- [WCJS-97] M. Winslett, N. Ching, V. Jones, I. Slepchin, “Assuring Security and Privacy for Digital Library Transactions on the Web: Client and Server Security Policies, in *Proc. of ADL*, Washington, DC, USA, May 1997.
- [WL-06] W.H. Winsborough, N. Li, “Safety in Automated Trust Negotiation,” in *ACM TISSEC*, vol. 9, no. 3, August 2006.
- [YFAR-08] D. Yao, K. Frikken, M. Atallah, R. Tamassia, “Private Information: To reveal or Not to Reveal,” in *ACM TISSEC*, vol. 12, no. 1, October 2008.
- [YWS-03] T. Yu, M. Winslett, K.E. Seamons, “Supporting Structured Credentials and Sensitive Policies trough Interoperable Strategies for Automated trust,” in *ACM TISSEC*, vol. 6, no. 1, February 2003.