SWPW 2005 – Galway, Ireland

REWERSE reasoning on the web

REWERSE Working Group I2

The REWERSE View on Policies

Piero Bonatti, November 7th, 2005

REWERSE WG I2 - policy language

Contents

- The view of REWERSE on **policies for the Semantic Web**
  - Important features
  - Technical **challenges**
- **REWERSE** is one of the 2 EU NoE devoted to the SW
  - focussed on rule-based techniques
  - policies identified as crucial area
  - WG I2 devoted to policy *specification, composition, conformance*

What is a Policy

For us the term *policy* covers:

- Security policies & Trust management
- Business rules
- Quality of Service directives
- ...
  - *more about this in the panel*

All these policies make decisions based on similar pieces of information (evidence)

- user age, nationality, customer profile, identity, reputation...

Many Policies, One Framework

It is appealing to integrate all these notions in one framework

- One common infrastructure
  - for **interoperability** and **decision making**
- Where policies can be harmonized & coordinated

Challenge: harmonize and integrate different requirements

- procedural (ECA) vs. declarative semantics
- top-down, bottom-up derivation strategies
- deduction vs. abduction ...

Strong, Soft, and Lightweight Evidence

How can individuals *prove* their eligibility?

- Strong evidence, e.g. **digital credentials**
- Soft evidence, e.g. **numerical reputation measures**
- Lightweight evidence, e.g. **unsigned declarations**

They should be integrated for balancing:

- trust level
- risk level
- computational costs
- **usability (fetching credentials, personal assistants)**

(see also the paper in the workshop proceedings)

Strong, Soft, and Lightweight Evidence

Challenges:

- Research on reputation models still in early stage
  - new models keep being introduced
  - vulnerabilities (e.g., to coalitions)
  - **adopt parametric frameworks?** (current choice of REWERSE)
- Interoperability
  - lightweight evidence can be based on any web contents
  - how to explain requirements in a machine-understandable way?
  - **a standard semantic web issue – ontologies**
  - **still lightweight?...**

Trust Management (TM)

- Encode trust
  - already discussed in a more general setting (*evidence*)
- Acquire / submit evidence, encode requests
  - **negotiations**
- Make decisions, execute actions
  - rule-based
  - **provisional policies**

There exists much work on TM

- **Are (semantic) web scenarios different from those considered by the TM community?**
- **Any difference in their requirements?**

Formulating information requests

A Semantic Web approach:

- **Publish policies** (rules) describing which information is needed to get services, facilities, credentials, ...
  - eligibility criteria, user classes, and other auxiliary concepts
  - in fact peers are exchanging their **ontologies**
- A new idea?
  - **No:** see CCS 2000
  - Ontologies are based on minimal shared knowledge: X.509+rule semantics
    - **This makes the approach plausible even in short-mid time**
    - Very important for Semantic Web ideas

Publishing rules

Not *all* rules!

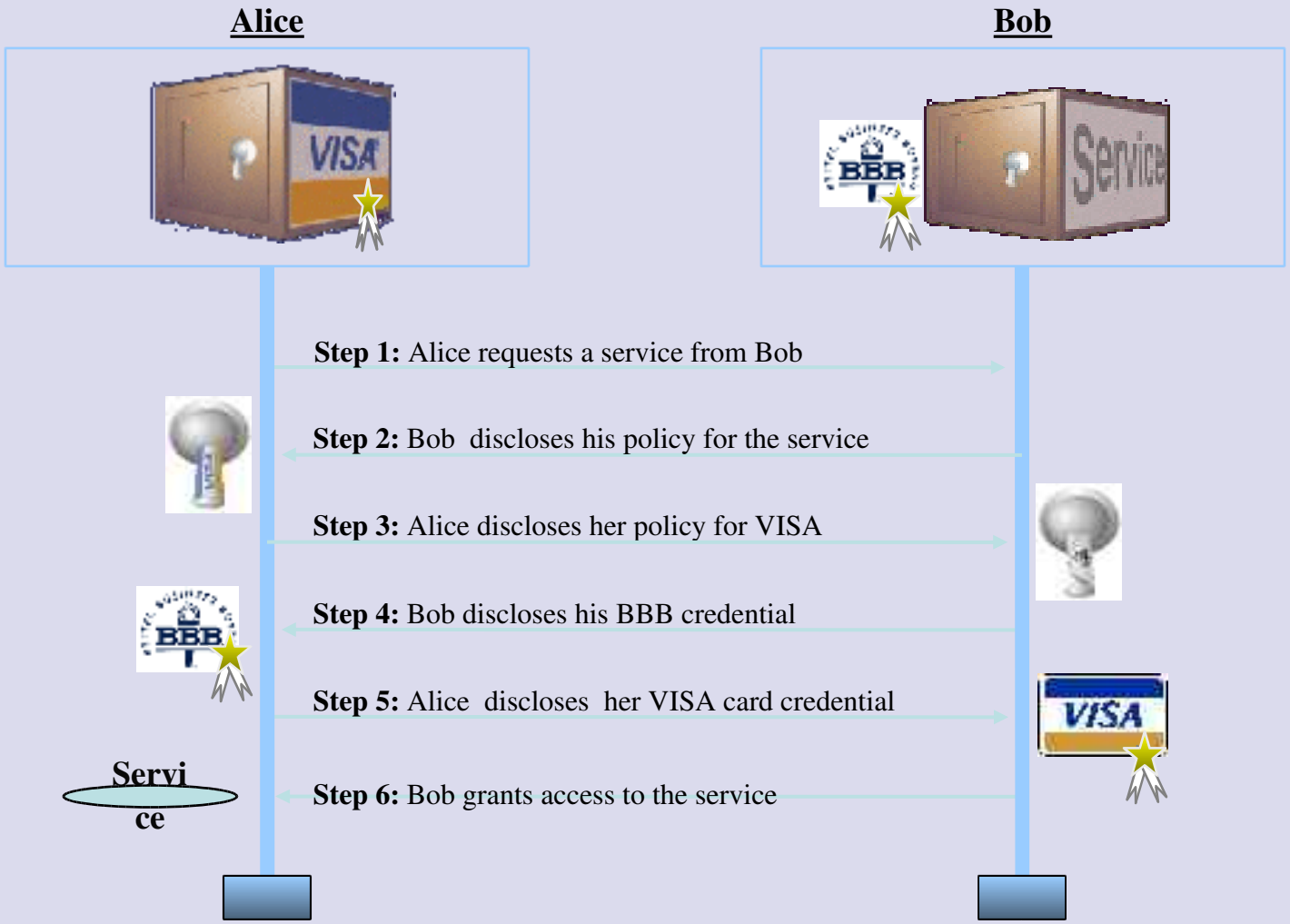
- Policies are sensitive even in “personal” scenarios
  - “Picture 12.jpg can be seen only by my best friends”
  - How would an “ordinary” friend react to a denial?...
- Personal information sharing scenarios are not different from standard TM scenarios
- More policy rules can be disclosed as more information about the peer is gathered
  - it encourages multiple iterations

Negotiations

Multiple steps motivated by

- The need for incremental information release
  - sensitive policies
  - minimizing personal information disclosure
- Counter-requests of the peer asking for a resource
  - “how are you handling the information I'm giving you?”
  - proving certifications

Negotiations



Stateful Negotiations?

Some researchers argue they are undesirable on the web

- Saving states on the peers is not strictly necessary
  - disclosed information can be replicated in each message
  - although messages get longer
- In practice important web sites adopt stateful transactions
  - despite heavy traffic load
- Would it be better to have stateful web protocols?
  - probably lead more robust and secure
  - think of cookie-related vulnerabilities

Summarizing

Trust Management: What's new?

- Apparently, only a more corageous approach to lightweight evidence

Challenges: all open challenges in TM, including:

- "policy interoperability": guaranteeing negotiation success when policies "theoretically" permit it
- optimal negotiations: which strategies / policy features minimize the amount and the sensitivity of disclosed information
- more generally: making concrete decisions in the choice space given by regulations

Cooperative policy enforcement

Crucial for the success of a web service

- Never say "*no*"!
- Encourage first-time users

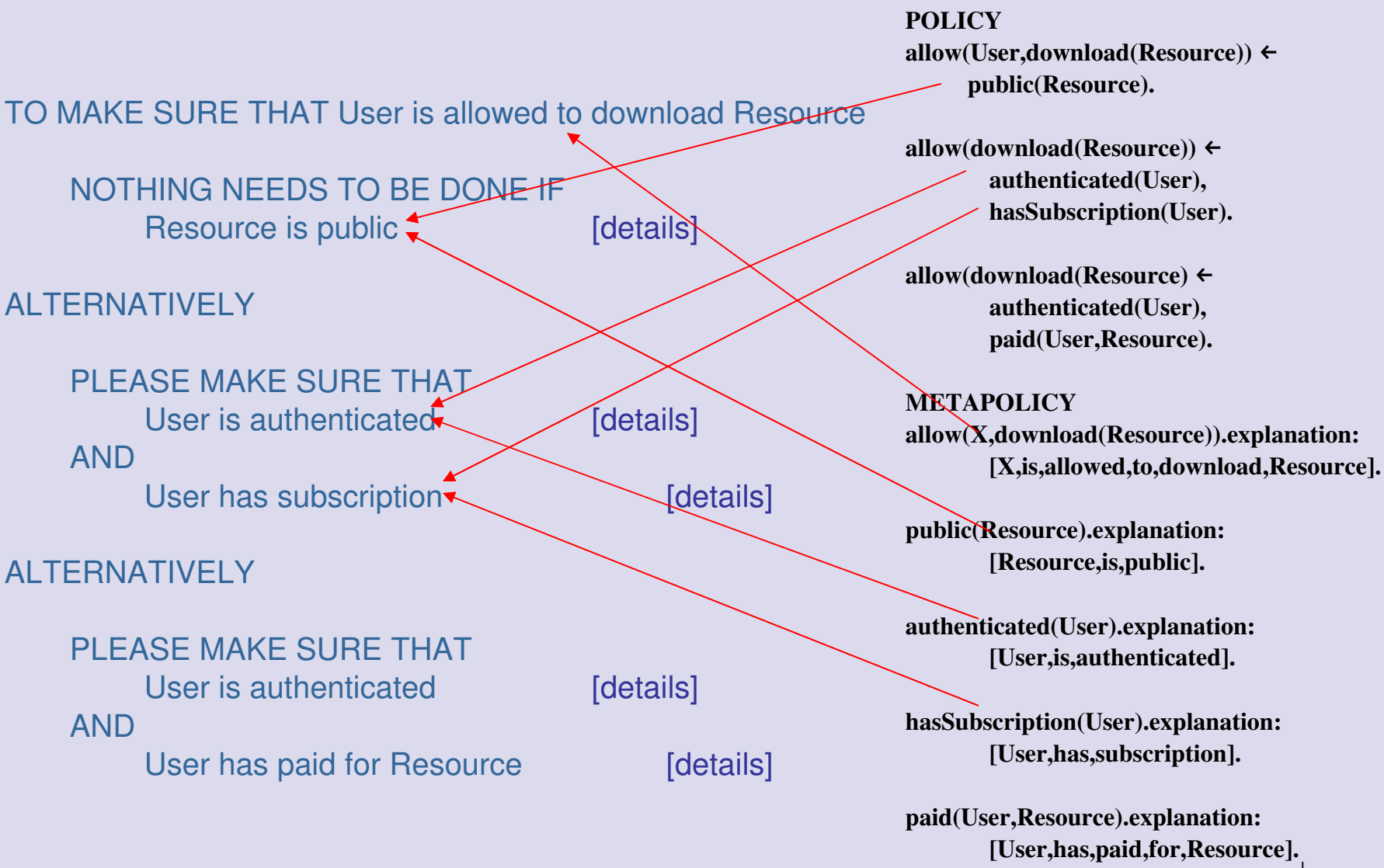
- Explain policy decisions
  - Advanced queries: Why / why not
- Guide users in acquiring missing permissions
  - Activate registration procedures
  - Provide instructions
  - Advanced queries: how-to, what-if
- Enhance users **awareness** about the policy applied by their system
  - A necessary precondition for fully exploiting the system's security mechanisms

Explanation mechanism

Main challenge:

- Finding the right tradeoff between
  - Explanation quality
  - Framework instantiation effort
    - The framework needs to be adapted to each application domain
    - Reduce the need for specialized staff

Explanation mechanism (how to)



Explanation mechanism (why not)

"authenticated" depends on a credential. "hasSubscription" depends on "authenticated"

I CAN'T PROVE THAT
it is allowed to download paper14.pdf
BECAUSE

Rule [r3] is not applicable:
THERE IS NO User SUCH THAT
User is authenticated [details]

Pruning: User is not authenticated so it makes no sense to inspect her subscriptions

AND

Rule [r4] is not applicable:
THERE IS NO User SUCH THAT
User is authenticated [details]
MOREOVER
THERE IS NO User SUCH THAT
User has paid for paper14.pdf [details]

POLICY

[r3]: allow(download(Resource)) ←
authenticated(User),
hasSubscription(User).

[r4]: allow(download(Resource) ←
authenticated(User),
paid(User,Resource).

METAPOLICY

allow(download(Resource)).explanation:
[it,is,allowed,to,download,Resource].

public(Resource).explanation:
[Resource,is,public].

authenticated(User).explanation:
[User,is,authenticated].

hasSubscription(User).explanation:
[User,has,subscription].

paid(User,Resource).explanation:
[User,has,paid,for,Resource].

Controlled natural language specifications

- Our goal is formulating rules such as:
  - "*Academic users can download the files in folder historical_data whenever their creation date precedes 1942*"
  - Internal format: rules
- Very important for giving users **greater control** on the policy applied by their system
  - A necessary precondition for fully exploiting the system's security mechanisms

REWERSE's policy framework

PROTUNE

- First attempt at tackling all the aforementioned issues simultaneously
- Metapolicies for driving negotiations declaratively
  - e.g. Rule sensitivity, action execution time
- and for instantiating the framework in application scenarios
  - New actions and responsible actors
  - Verbalization directives
- Integrating legacy software and numerical reputations
- Explanation mechanism

Implementations

Extensions and improvements of

- The Trust Management System **PeerTrust**
  - http://www.learninglab.de/english/projects/peertrust.html
- **Attempto Controlled English system (ACE)**
  - for natural language specification
  - for query answering
  - http://www.ifi.unizh.ch/attempto/

Members of WG I2

G. Antoniou	- Heraklion
M. Baldoni	- Torino
C. Baroglio	- Torino
P.A. Bonatti	- Napoli (coord.)
C. Duma	- Linkoeping
T. Eiter	- Wien
N. Fuchs	- Zurich
A. Martelli	- Torino
W. Nejdl	- Hannover
D. Olmedilla	- Hannover
J. Peer	- St. Gallen
V. Patti	- Torino
N. Shahmehri	- Linkoeping

QUESTIONS?

Metapolicy examples

table(Key,Data).evaluation:immediate ← ground(Key).

logged(Msg,File).action:'echo'+Msg+'>'+File.

credential(_).ontology:URI.

abbrev(_).explanation:"this condition checks…"

Publications

Publications

Important REWERSE related …

- Rita Gavriloaie, Wolfgang Nejdl, Daniel Olmedilla, Kent Seamons, Marianne Winslett. No Registration Needed: How to Use Declarative Policies and Negotiation to Access Sensitive Resources on the Semantic Web. In *Proc. of 1st European Semantic Web Symposium*, May. 2004, Heraklion, Greece
- S. Staab, B. Bhargava, L. Lilien, A. Rosenthal, M. Winslett, M. Sloman, T. S. Dillon, E. Chang, F. K. Hussain, W. Nejdl, D. Olmedilla, V. Kashyap The Pudding of Trust IEEE Intelligent Systems Journal, Vol. 19(5), pp. 74-88, Sep./Oct. 2004
- Abraham Bernstein, Esther Kaufmann, Norbert E. Fuchs, June von Bonin Talking to the Semantic Web - A Controlled English Query Interface for Ontologies Proceedings of the 14th Workshop on Information Technology and Systems, December 11-12, 2004, Washington D.C., USA
- C. Duma, N. Shahmehri, E. Turcan, "Resilient Trust for Peer-to-Peer Based Critical Information Infrastructures", 2nd International Conference on Critical Infrastructures (CRIS 2004), Grenoble, France, 2004.

Publications

Important REWERSE related …

- P.A. Bonatti. Abduction over unbounded domains via ASP. *Proc. of the European Conf. on Artificial Intelligence* (ECAI-04), 288-292, IOS Press, 2004.
- M. Baldoni, C. Baroglio, A. Martelli, V. Patti, and C. Schifanella. Verifying protocol conformance for logic-based communicating agents. In J. Leite and P. Torroni, editors, Pre-Proc. of Fifth International Workshop on Computational Logic in Multi-Agent Systems, CLIMA V, pages 82-97, Lisbon, Portugal, 2004.
- Eikemeier, C., Gruetter, R., Fierz, W. (2004, September 14). On a Surveillance Service for Drug Prescription using Distributed Patient Records and a P2P Infrastructure. 49. Jahrestagung der Deutsche Gesellschaft fuer Medizinische Informatik, Biometrie und Epidemiologie (gmds2004), Innsbruck, September 2004.
- P.A. Bonatti. On the Decidability of Containment of Recursive Datalog Queries Preliminary report. *Proc. of PODS 2004*, pp. 297-306

  Note: A foundational study related to forthcoming deliverables on policy validation and composition.
- More publications on rewerse.net.

Mission

Working Group I2 aims at designing **policy languages** and **policy-driven systems** that exploit **semantic web techniques** to enhance user privacy, web service usability and protection, and improve user control on the policies applied by open systems and services.

Security & Privacy Protection

- often in conflict with system usability
- providing & gathering security-related inform. or certificates
  - goal: progressively moved from users to machines

Enhancing **User Control & Awareness** on System Behavior

- common users
  - specify their own rules
  - understand the automated decisions of the system
  - ⇨ are given high-level tools (e.g. natural language parsers)
    - to formulate policies and to ask systems for explanations
- **explanation facilities**
  - attract occasional users
  - ⇨ may make a web service more competitive