Policy Specification, Composition, and Conformance

Abstract

Secure but cooperative systems, privacy protection, and business rules for everybody: the Working Group on "Policy specification, composition, and conformance" aims at designing policy languages and policy-driven systems that enhance user privacy, Web service usability and protection, and improve user control on the policies applied by open systems and services.

Use Scenarios

Ann connects to a web service for the first time, therefore she does not know the service's policies governing access control, business rules and so on. The system has no information about Ann, and must acquire information about Ann before granting access to the service.

For example, is Ann an EU citizen? Is she at least 18 years old? And so on.

Ann does not necessarily need to provide manually the required information and credentials.To improve service usability and navigation ease, an automated personal assistant provides such data, obeying the privacy protection policy adopted by the user. For instance, Ann's credit card number shall be released only to services that provably belong to the Best Business Bureau Program. Moreover, the privacy policy may state that in certain contexts, Ann's permission must be explicitly asked for before releasing particular pieces of data.

Note the technical challenge underlying this framework: the server must be able to state its requests in a machine understandable way.

Since such conditions may involve sophisticated specifications of what kind of certifications and delegations are accepted, the request language must be flexible and powerful, but not computationally hard.

Now suppose that Ann's request is rejected. She may want to understand why, or how to get the required permissions, possibly submitting queries such as: "Why didn't you accept my ACM membership card? Would I get the special discount on financial product X if I were locally employed?"

Policies and queries to policies are often formulated by people with no training in computer science nor programming. However they can specify their policies and queries in a restricted fragment of natural language, as in: "Users can download the files in folder historical data if the creation date precedes 1/1/2000." Of course, both policy enforcement and query answering should require no additional „technical" information or coding, if policy specification is to be at reach for common users with no programming experience.

Mission

Security and privacy protection are often in conflict with system usability. Higher-quality and more competitive services can be built if we succeed in injecting some intelligence in the procedures that handle security and privacy policies. The burden of providing and gathering security-related information and certificates should be progressively moved from users to machines, by improving current interoperability techniques.

Another challenge is enhancing user control and awareness on system behaviour, be it determined by security/privacy policies, business rules, or quality-of-service rules. If common users are to specify their own rules and understand the automated decisions of systems and web services, then users must be given high-level tools - e.g. natural language parsers - to formulate policies and ask systems for explanations. Good explanation facilities may make a web service more competitive by attracting occasional users.

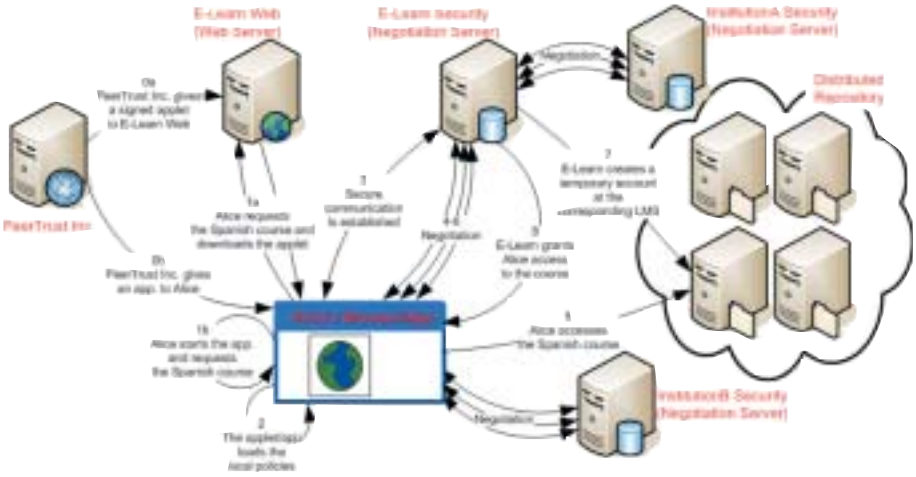
Through a rule-based approach, the working group aims both at giving users more control, and at reducing the cost of building and maintaining cooperative systems and services, by means of intelligent tools for generating as automatically as possible the dialogs with the users.

More information available at

http://rewerse.net/i2

Description of Research

Research activities covers several complementary threads. One line concerns trust management; by this we mean both techniques based on the negotiation of electronic credentials, and trust models based on reputation. Another line of research focuses on extending policy language implementations with high-level query answering and explanation facilities, as well as the ability of executing actions (to log interesting events, activate workflows, etc.) Last but not least, a crucial research activity is devoted to the controlled natural language front-end, to be adapted and extended to handle policy expressions and nonmonotonic reasoning.



Tools & Technologies

The Working Group is extending and adapting the rule-based trust management system PeerTrust
(http://www.learninglab.de/english/projects/peertrust.html)
and the Attempto Controlled English system (ACE) for natural language specification and query answering (http://www.ifi.unizh.ch/attempto/).

The underlying technologies involve standard Web technology - including Java - and lightweight Prolog technology, sometimes compiled directly on Java classes and bytecode. The Group's goals comprise compliance with the major Web standards for security, privacy and rules (e.g., XACML, P3P, and RuleML.)

Glossary

The word "**policy**" is used here in the broad sense of high-level specifications of a complex system behaviour, regulating in particular the interactions between different system parts. Thus, our understanding of the word "policy" encompasses security and privacy policies, business rules and quality-of-service specifications as special cases (to name a few).

"**Trust management**" deals with the problem of verifying properties of users, organizations, electronic resources and systems in a reliable way, even in the absence of a single centralized control. Flexibility is a key issue: users-system and system-system interactions are often occasional and hard to predict in our reference scenarios. Trust management involves both credential-based property verification and reputation -based trust assignment issues.

The expression "**Controlled natural language**" denotes unambiguous fragments of natural language, well suited to write executable specifications. Controlled natural language can be used by people with no particular training in computer programming, after learning a small number of simple rules, that explain which sentences are accepted and how they are understood by the system.

Contact Person

Dr. Piero A. Bonatti, Professor
Dip. di Scienze Fisiche
Università di Napoli Federico II
Complesso Universitario di Monte Sant' Angelo, Via Cinthia
80126 Napoli, IT

Phone: +39 081 676822
Email: bonatti@na.infn.it

http://people.na.infn.it/~bonatti

Members

Wolfgang Nejdl, Daniel Olmedilla (Hannover); Grigoris Antoniou (Heraklion); Nahid Shahmehri, Claudiu Duma, Eduard Turcan (Linköping); Piero A. Bonatti, Adriano Peron (Naples); Rolf Grütter, Joachim Peer (St. Gallen); Cristina Baroglio (Turin); Thomas Eiter, Roman Schindlauer, Hans Tompits (Vienna); Norbert E. Fuchs, Fabio Rinaldi, Gerold Schneider (Zurich)

Impressum

webXcerpt Software GmbH
REWERSE Technology Transfer
Aurbacherstr. 2, D-81541 Munich
http://rewerse.net

Contact: Andrea Kulas
ak@webxcerpt.com
Phone: +49 89 54 80 88 48

Responsible for the content:
Piero A. Bonatti
Dip. Di Scienze Fisiche
Università di Napoli Frederico II
Complesso Universitario di
Monte Sant' Angelo,
Via Cinthia, I-80126 Napoli
bonatti@na.infn.it
Phone: +39 081 676822

2004.11-300