No Registration Needed: How to Use Declarative Policies and Negotiation to Access Sensitive Resources on the Semantic Web


1st European Semantic Web Symposium
Heraklion, Greece, 12th May. 2004
Outline

- Introduction
- What is Trust Negotiation
- How does it work
- Further Work
Outline

- Introduction
- What is Trust Negotiation
- How does it work
- Further Work
Motivation: Buying in Internet

- Bob wants to access an electronic AI book at “E-Book Store” (a website he found while surfing in Internet)

- Previously, E-Book requires Bob to register providing full name, age, complete address, telephone and e-mail.

- Bob does not mind to give his full name and age but he does not like to provide his complete address, telephone and e-mail. However, he does not have any other option so he does it (although he does not provide his real address and telephone).

- E-Book sells that book. Therefore now it asks Bob to provide his credit card information. Bob would not mind to buy the book because it is not too expensive and he is really interested in reading it. However, he has never heard about E-Book so he decides to not buy it.
Requirements

Systems
- Traditional distributed environments
  - Close environments: providers and requesters are known in advance
  - Server must trust the client: unidirectional (registration)
- WWW, P2P, GRID: dynamic networks
  - Nodes are usually not known in advance
  - Trust between strangers is needed
  - Bi-directional access control required

Users
- Do not want to register at any site (tedious task)
- Want control over what information they disclose and to set levels of privacy
  - E.g. My first name has not the same level than my credit card number
- Want assurance about what other nodes will do with their information
  - They want to know about the other party
Outline

- Introduction
- What is Trust Negotiation
- How does it work
- Further Work
Trust Negotiation

- Goal → to protect resources from unauthorized access
- New approach to establishing trust between strangers
  - Initial trust among nodes is not necessary
  - No need for registration (or even registration automatically)
- Use of credentials: online analogue to the paper credentials in real life
- Negotiation according to policies
  - Access control policies can be used in both sides (requester and provider)
- Delegation
- Trust Negotiation → trust is established gradually through an iterative exchange of digital credentials
Credentials and Policies

- Property-based credentials
  - Describe one or more properties / attributes of the owner asserted by the issuer, signed with the private key of the issuer
  - As credentials contain sensitive information, they are not shown until the other part demonstrates that it is qualified to have such sensitive information
  - E.g. student(‘Alice Smith’) @ ‘Hanover University’

- Access Control Policies
  - Protect a resource or a credential
  - Specify credentials that the other negotiation participant must provide in order to get access
  - Several policies can be involved during the negotiation
  - Several policies for the same resource or credential
  - Policies can be protected like any other resource
  - E.g. freeAccess(Course,User) ← student(User) @ ‘Hanover University’
Trust Negotiation among Peers on the Web

Designed a policy language to express trust negotiation
- Delegation, policy protection, negotiation strategies
- Based on guarded distributed logic programs

Developed a run-time system for automated trust negotiation
- Based on Prolog meta interpreter embedded as Java library in Applet / Server (WWW) or Peer-to-Peer (Edutella) environment

Use RDF in policies
- Use of metadata information into policies
- E.g. access(Resource, Requester) ← dcCreator(Resource, Requester)

RuleML import/export facility
- Policies encoded in RuleML

Currently two application areas
- eLearning (ELENA, EU/FP5 @ L3S)
- Emergency management (ITR @ DAIS/UIUC (M. Winslett))
Outline

- Introduction
- What is Trust Negotiation
- How does it work
- Further Work
Example scenario

Step 1: Alice requests to access E-Learn’s free Spanish course
Step 2: E-Learn replies with policy protecting this resource
  - Requests driver’s licence to prove California residence status
  - Requests police badge to prove police officer status
Step 3: Alice views her driver’s license as non-critical, but needs to protect her police officer credential
  - Discloses driver’s license
  - Requests E-Learn membership proof from the Better Business Bureau
Step 4: E-Learn agrees
  - Discloses Better Business Bureau membership card
Step 5: Alice finds her policy satisfied
  - Discloses police badge
Step 6: E-Learn finds its policy satisfied
  - Makes Spanish course available
Policy Examples

E-Learn:
freeEnroll(Course, Requester) $ Requester →
  policeOfficer(Requester) @ 'California State Police' @ Requester,
  rdfType(Course, 'http://.../elena#Course'),
  dcLanguage(Course, 'es'),
  creditUnits(Course, X),
  X <= 1.

Alice:
  policeOfficer('Alice Smith') @ 'California State Police' $ Requester →
  member(Requester) @ 'Better Business Bureau' @ Requester
  | signedBy ['California State Police'].

Daniel Olmedilla
May 12, 2004
Network Diagram
Interaction Diagram

```
freeEnroll(spanish101,alice)

driversLicense(alice) @ caDMV ?
< driversLicense(alice) @ caDMV >

policeOfficer(alice) @ csp ?
member(eLearn) @ bbb ?
< member(eLearn) @ bbb >
< policeOfficer(X) @ csp < policeOfficer(X) @ chp >, < policeOfficer(alice) @ chp >

access granted
```
Outline

- Introduction
- What is Trust Negotiation
- How does it work

- Further Work
Further work

- User-friendly parser for policies
- Integrate XSB Prolog inference engine
- Loop detection during negotiation
- Extensions to
  - Semantic Web Services
  - GRID technologies
    - J. Basney, W. Nejdl, D. Olmedilla, V. Welch, M. Winslett
      Negotiating Trust on the Grid
      2nd Workshop on Semantics in P2P and Grid Computing at the
- Cashing of credentials
Questions?