Outline

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

- Introduction
- What is Trust Negotiation
- How does it work
- Conclusions & Further Work
- References
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 and e-mail

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

- E-Book sells that book so 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
System Requirements

- Traditional distributed environments
  - Close environments
    - Providers and requesters are known in advance
  - Server has to trust the client
    - Unidirectional (registration): take-it-or-leave-it
  - Is information gathered real?

- WWW, P2P, GRID, etc...
  - Dynamic networks
    - Nodes are usually not known in advance
  - Trust between strangers is needed
  - Bi-directional access control required
User Requirements

- Users do not want to register at any site (tedious task)

- Users want control over what information they disclose and set levels of privacy
  - E.g. My first name has not the same level than my credit card number

- Users do not want to give irrelevant information
  - E.g. Give my address if I buy a mp3 song in a music portal

- Users 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
- Conclusions & Further Work
- References
Trust Negotiation

- Goal → 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

student(alice) @ uniHanover

- Describe one or more attributes of the owner asserted by 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.

- Possibility of credentials at the attribute level (no irrelevant information is disclosed)

- Typically based on public/private key cryptography
Control Access Policies

freeAccess(Course, Requester) ← student(Requester) @ uniHanover

- Protect a resource or a credential
  - A policy must be fulfilled in order to get access

- Focus the negotiation on those credentials actually needed to advance the negotiation
  - Specify credentials that the other negotiation participant must provide

- Various policies can be involved during the negotiation and various policies for the same resource or credential.
Negotiation Strategies

- A negotiation may have various different paths to succeed

- Each party may define a different strategy
  - More or less restrictive
  - Faster or slower

- Strategies must be compatible
  - Family of strategies
Extra Features

- Prolog based inference engine
  - Minerva
  - XSB under development

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

- RuleML import/export facility
  - Policies encoded into RuleML files

- Security Agents implemented
  - App. Based
  - Browser based: no extra software required
Outline

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

E-Learn offers free Spanish course to police officers of California

1. Alice requests to access E-Learn's Spanish course at no charge
2. E-Learn asks Alice to show a police badge issued by the California State Police to prove that she is a police officer, and her driver's license to prove that she is living in the state of California
3. Alice is willing to disclose her driver's license to anyone, so she sends it to E-Learn. However, she considers her police badge to contain sensitive information. She tells E-Learn that in order to see her police badge, E-Learn must prove that it belongs to the Better Business Bureau.
4. Fortunately, E-Learn does have a BBB membership card. The card contains no sensitive information, so E-Learn discloses it to Alice
5. Alice now believes that she can trust E-Learn and discloses her police badge to E-Learn
6. After verifying that the badge is valid and that Alice owns it and the driver's license, E-Learn gives Alice the free registration for this course
Policy Examples

E-Learn:
freeEnroll(Course, Requester) $ Requester →
policeOfficer(Requester) @ csp @ Requester,
rdfType(Course, ‘http://…/elena#Course’),
dcLanguage(Course, ‘es’),
creditUnits(Course, X),
X <= 1.

Alice:
policeOfficer(alice) @ csp $ Requester →
member(Requester) @ bbb @ Requester
| signedBy [csp].
Scenario Network Diagram

**0a** PeerTrust Inc. gives a signed applet to E-Learn Web

**0b** PeerTrust Inc. gives an app. to Alice

**1a** Alice requests the Spanish course and downloads the applet

**1b** Alice starts the app. and requests the Spanish course

**2** The applet/app loads the local policies

**3** Secure communication is established

**4-6** Negotiation

**7** E-Learn creates a temporary account at the corresponding LMS

**8** E-Learn grants Alice access to the course

**9** Alice accesses the Spanish course

**InstitutionA Security (Negotiation Server)**

**InstitutionB Security (Negotiation Server)**

**Distributed Repository**

**E-Learn Web (Web Server)**

**E-Learn Security (Negotiation Server)**

**Alice's Browser/App**
Scenario Interaction Diagram

Alice

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

E-Learn
Outline

- Introduction
- What is Trust Negotiation
- How does it work
- Conclusions & Further Work
- References
## Conclusions (I)

<table>
<thead>
<tr>
<th></th>
<th>Centralized: (LDAP, Kerberos)</th>
<th>Federated (e.g. Liberty Alliance)</th>
<th>Trust Negotiation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type</strong></td>
<td>Centralized</td>
<td>Decentralized</td>
<td>Decentralized</td>
</tr>
<tr>
<td><strong>Initial trusting required</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td><strong>Strategies</strong></td>
<td>No strategy</td>
<td>Unique strategy</td>
<td>Flexible: different strategies</td>
</tr>
<tr>
<td><strong>User interactivity</strong></td>
<td>No user interactivity: only server policies</td>
<td>User might have limited policies</td>
<td>Node (User and Server) policies</td>
</tr>
<tr>
<td><strong>Registration</strong></td>
<td>Required in each node manually</td>
<td>Required or replicated automatically</td>
<td>No required (possible automatically)</td>
</tr>
</tbody>
</table>
Conclusions (& II)

- E-commerce needs a scalable approach that allows automatic on-line pre-registration, or does away entirely away with the need of pre-registration.

- More suitable and valuable for Distributed Environments (decentralized) and even required for Open Distributed Environments

- Horn Logic (e.g. PROLOG) allows to create policies easily and with flexibility

- Easy integration of different strategies for negotiation

- Semantic metadata can be used in policy definition
Further work

- Add support for SAML (message interchange)
- Integrate XSB Prolog inference engine
- Loop detection during negotiation
- Extensions to
  - Semantic Web Services
  - GRID technologies
- Cashing of credentials
- Create a set of policies for a specific domain
Outline

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

- PeerTrust project page: http://www.learninglab.de/deutsch/projekte/peertrust.html

