Automated Trust Negotiation (ATN)

Research Seminar
05/11/2003

Daniel Olmedilla
Wolfgang Nejdl
Outline

- Introduction
- Trust Negotiation
- Workplan
- Conclusions
- References
Outline

- Introduction
- Trust Negotiation
- Workplan
- Conclusions
- References
Introduction

- Smart Space for Learning is built over a P2P infrastructure.

- P2P is a decentralized approach against other server-client approaches. Many advantages.

- Disadvantage: no centralized security entity exists. Trust management is more difficult.

- Trust management is necessary in order to be able to use booking, delivering or billing as services.

- Single sign on (SSO) is also needed
Outline

- Introduction
- Trust Negotiation
- Workplan
- Conclusions
- References
Automated Trust Negotiation

- Goal → protect resources from unauthorized access
- New approach to establishing trust between strangers
  - Initial trusting among nodes is not necessary
  - No need for registration (or even registration automatically)
- Use and interchange 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
- Automated Trust Negotiation → iterative exchange of digital credentials.
  - Iterative disclosure of policies and credentials
Credentials

- Describe one or more attributes of the owner asserted by the issuer.
- Each credential also contains the public key of the credential owner.
- As credentials contain sensitive information, they are not shown until the other part demonstrates that it is qualified to have such sensitive information.
- Policies are established in order to protect credentials: a policy must be fulfilled in order to access to the credential.
- Possibility of credentials at the attribute level (no irrelevant information is disclosed)
Control Access Policies

- Protect a resource or a credential
- Specify credentials that the other negotiation participant must provide in order to get access
- Focus the negotiation on those credentials actually needed to advance the negotiation.
- Several policies can be involved during the negotiation.
- Several policies for the same resource or credential.
- Policies over policies: protection of policies.
Users

- 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 e-mail if I buy a mp3 song in a music portal
- Users want assurance about what other nodes will do with their information
  - Policies can be used at the user side to give this control
ATN in ELENA

- Creation of an appropriate Trust Negotiation Agent (TNA)
- Each member of the ELENA Smart Space for Learning has one or use one of the Services that it provides
- Users have to login into the PLA and provide a policy (or select one of the available ones)
- PLA contain the information needed from the user.
- Single sign on at the PLA level and
  - No registration at LMS required or
  - Automated Registration at LMS
Example: policies

- LMS_A policy:
  - No requirements to show its ELENA membership credential.
  - Public access to resources
  - Only e-mail or full name required to access resources (statistic purpose)

- LMS_B policy:
  - No requirements to show its ELENA membership credential
  - Full name and credit card credential required to access the resources
  - Validated credit card credential from VISAAuthority required to access the resources

- User_A policy:
  - No requirements to give full name but never disclose the e-mail
  - ELENA membership credential required to give the credit card credential

- User_B policy:
  - ELENA membership credential required to give any personal information
  - Never disclose credit card credential
Examples (I)
Examples (& II)

Diagram:

- Resource?
- full name?
- full name
- credit card?
- elena?
- elena
- credit card
- resource
- valid
  - valid
Outline

- Introduction
- Trust Negotiation
- Workplan
- Conclusions
- References
Workplan

Prototype: one process simulating several peers
- Depth-first search Prolog meta-interpreter → Done
- Real simulation of several peers → Done
- Several strategies implemented
  - Depth-first search → Done
  - Breadth-first search → Done
  - Others?

Paper for WWW 2004 → In process

Next steps:
- RuleML Integration
- Real prototype with several processes (peers)
- Integration in Java
Outline

- Introduction
- Trust Negotiation
- Workplan
- Conclusions
- References
## Conclusions (I)

<table>
<thead>
<tr>
<th></th>
<th>Centralized: LDAP, Kerberos</th>
<th>Federated</th>
<th>Automatic Trust Negotiation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type</strong></td>
<td>Centralized: client/server</td>
<td>Decentralized</td>
<td>Decentralized: P2P</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: several different strategies</td>
</tr>
<tr>
<td><strong>User interactivity</strong></td>
<td>No user interactivity: only server policies</td>
<td>No user interactivity: only server policies</td>
<td>Node (User and Server) policies</td>
</tr>
<tr>
<td><strong>Credentials</strong></td>
<td>1 credential for each LMS (authentication data)</td>
<td>1 credential for each LMS (flexible data)</td>
<td>Possibility of any kind of credential (flexible data)</td>
</tr>
<tr>
<td><strong>Registration</strong></td>
<td>Required in each node manually</td>
<td>Replicated to each node 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.

- Decentralized? more suitable and valuable according to our approach and infrastructure with P2P networks.

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

- Easy integration of different strategies (ad-hoc strategies) for negotiation depending on the metainterpreter used

- High valuable collaborators:
  - Marianne Winslett (UIUC)
  - Other universities of USA
Outline

- Introduction
- Trust Negotiation
- Workplan
- Conclusions
- References
References

- An Introduction to Automated Trust Establishment. Marianne Winslett


- Automated Trust Negotiation Over the Internet. Ting Yu, Marianne Winslett, Kent Seamons.