A Software Product Line Approach for Handling Privacy Constraints in Web Personalization

Yang Wang and Alfred Kobsa
University of California, Irvine, USA

Outline
- Motivation
- Software product line
- Our privacy-enabling user modeling architecture
- An example
- Conclusion

Motivation
- Web personalization benefits both customers and vendors
- Privacy concerns counteract the personalization benefits
- How to dynamically balance personalization and privacy?

Aims and Key Characteristics
- Provide optimal personalization while respecting privacy laws, regulations, and users’ personal privacy preferences
- Leverage the flexibility of software product line to address combinatorial complexity of privacy constraints
- Apply state-of-the-art industry practice for managing software variants at run time

UniversalFriends.com
- Bridge physical distances
- Foster universal friendship
- Recommend personalized list of likely friends

Privacy Concerns
- Complex combinations of:
  - Users’ personal privacy preferences
  - International privacy laws (even trans-border)
  - Privacy regulations
users' privacy preferences

- "only collect my information if I give explicit consent!"
- "do not store my true name!"
- "do not track me!"

privacy laws

- EU data protection directive
- Asia-Pacific Economic Cooperation (APEC) privacy framework
- Organisation for Economic Co-operation and Development (OECD) privacy guidelines
- Over 30 countries already have their own privacy laws and more countries are coming

data protection laws – year 2003

- Sector standards (e.g., in USA)
  - Medical: HIPPA
  - Children: COPPA
  - Finance: Gramm-Leach-Bliley Act

- Self-regulation policies
  - TRUST e
  - Network Advertising Initiative
  - Chinese E-Commerce Trust Consortium

the research question

**how can personalized web-based systems maximize the personalization benefits while at the same time being compliant with the privacy constraints that are currently in effect?**

revisit the research question

**seeking a mechanism to dynamically select user modeling components that comply with the currently prevailing privacy constraints**
Institute for Software Research

PEP05

Yang Wang and Alfred Kobsa

A Software Product Line Approach for Handling Privacy Constraints in Web Personalization

user modeling component pool

<table>
<thead>
<tr>
<th>component</th>
<th>method used</th>
<th>inferential base</th>
<th>initial state</th>
<th>result state</th>
</tr>
</thead>
<tbody>
<tr>
<td>UMC1</td>
<td>rule-based reasoning</td>
<td>fuzzy reasoning</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>UMC2</td>
<td>fuzzy reasoning with uncertainty</td>
<td>yes</td>
<td>yes, low uncertainty</td>
<td></td>
</tr>
<tr>
<td>UMC3</td>
<td>fuzzy reasoning with uncertainty</td>
<td>yes</td>
<td>yes, low uncertainty</td>
<td></td>
</tr>
<tr>
<td>UMC4</td>
<td>rule-based reasoning</td>
<td>fuzzy reasoning</td>
<td>yes, high uncertainty</td>
<td></td>
</tr>
<tr>
<td>UMC5</td>
<td>rule-based reasoning</td>
<td>fuzzy reasoning</td>
<td>yes, high uncertainty</td>
<td></td>
</tr>
<tr>
<td>UMC6</td>
<td>one-time machine learning</td>
<td>fuzzy reasoning</td>
<td>yes, high uncertainty</td>
<td></td>
</tr>
<tr>
<td>UMC7</td>
<td>one-time machine learning</td>
<td>fuzzy reasoning</td>
<td>yes, high uncertainty</td>
<td></td>
</tr>
</tbody>
</table>

methods used:
- rule-based reasoning
- fuzzy reasoning
- one-time machine learning

UMC8

methods used:
- rule-based reasoning
- fuzzy reasoning with uncertainty

product line architecture

"The common architecture for a set of related products or systems developed by an organization." [Bosch, 2000]

a PLA includes:
- Stable core: basic functionalities
- Options: optional features/qualities
- Variants: alternative features/qualities

A particular architecture instance is selected from the product-line architecture

our approach

Selection Component

User Modeling Component

User Modeling Server

Option to include

User Models

an example

the privacy constraints
conclusions

- provide optimal personalization while respecting privacy laws, regulations and users’ personal privacy preferences
- leverage the flexibility of software product line to address combinatory complexity of privacy constraints
- apply state-of-the-art industry practice for managing software variants at run time

project status and future work

- currently prototyping the system
- systematically express privacy constraints
- a decentralized version
- privacy kernel

acknowledgements

- Alfred Kobsa
- André van der Hoek
- Eric Dashofy
- Yun Huang
- Norman Su
- Colleagues at CommerceNet