Motivation & Goals

Motivation

- Internet users hardly know who handled their data, and how
- User-centric Identity Management system are becoming popular to deal with SSO + Privacy + User Control
- Yet, these systems present shortcomings in regards to trust
  - Hardly applicable to distributed environments
- Reputation Management Systems present an elegant alternative to manage trust
- Users may find out the behavior of entities before interacting with them
**Motivation & Goals**

**Goals**

G Improve Identity Management solutions with Reputation Models aiming user-centricity, adaptability and privacy

G1. Study the *state of the art* of user-centric identity management systems and reputation management systems

G2. Identify challenges that the *integration of both concepts* raises in distributed environments

G3. **Design solutions** toward achieving that integration

G4. Focus on **accuracy, dynamism and privacy** as key drivers

G5. Analyze the behavior of such solutions, through **experiments**, considering malicious users and entities.

---

**Background**

- **State of the Art**
  - Identity management state of the art analysis
  - Integration between user-centric Identity Management system and Reputation Systems study

- **Accuracy & Dynamism**
  - ROMEO Simulator
  - Reputation Management in distributed IdM (OpenID)
  - Dynamic and Flexible Selection

- **Privacy**
  - Advanced Care Coordination Platform
  - Bridging the Trust Gap in eHealth Environments

- **User-centric reputation & privacy**
  - Towards privacy-preserving reputation management for Hybrid Broadcast Broadband applications
Enhancing User-Centric Identity Management Systems with Reputation Models in Distributed Environments

Background | Reputation Management in OpenID | Dynamic & Flexible selection | Reputation in eHealth | Private & customized reputation
---|---|---|---|---
Identity Management State of the Art

<table>
<thead>
<tr>
<th>Requirement / Model</th>
<th>Control via IdP</th>
<th>Identity selector</th>
<th>Zero-knowledge</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality</td>
<td>Successfully</td>
<td>Successfully</td>
<td>Successfully</td>
</tr>
<tr>
<td>Single Sign-On</td>
<td>Successfully</td>
<td>Successfully</td>
<td>Successfully</td>
</tr>
<tr>
<td>Auditing</td>
<td>Successfully</td>
<td>Successfully</td>
<td>Limited</td>
</tr>
<tr>
<td>Strong authentication</td>
<td>Limited</td>
<td>Successfully</td>
<td>Successfully</td>
</tr>
<tr>
<td>Justifiable parties (trust)</td>
<td>Limited</td>
<td>Limited</td>
<td>Successfully</td>
</tr>
<tr>
<td>End-user consent</td>
<td>Limited</td>
<td>Successfully</td>
<td>Successfully</td>
</tr>
<tr>
<td>Control of data</td>
<td>Limited</td>
<td>Successfully</td>
<td>Successfully</td>
</tr>
<tr>
<td>Usability</td>
<td>Successfully</td>
<td>Limited</td>
<td>Limited</td>
</tr>
<tr>
<td>Attribute revocation</td>
<td>Successfully</td>
<td>Limited</td>
<td>Limited</td>
</tr>
<tr>
<td>Self-asserted attributes</td>
<td>Limited</td>
<td>Successfully</td>
<td>Successfully</td>
</tr>
<tr>
<td>Minimal disclosure</td>
<td>Limited</td>
<td>Limited</td>
<td>Successfully</td>
</tr>
</tbody>
</table>

Integration between Identity Management & Reputation Systems

- Reputation management systems base trust on recommendations
- Fit with user-centric Identity Management drawbacks
  - Reliability
  - Trustworthiness
  - Dynamism
- Raise numerous open questions
Enhancing User-Centric Identity Management Systems with Reputation Models in Distributed Environments

State of the Art
- Integration between user-centric Identity Management system and Reputation Systems study

Accuracy & Dynamism
- Reputation Management in distributed IdM (OpenID)
- Dynamic and Flexible Selection

Privacy
- Advanced Care Coordination Platform
- Bridging the Trust Gap in eHealth Environments

User-centric reputation & privacy
- Towards privacy-preserving reputation management for Hybrid Broadcast Broadband applications

OpenID Overview
- Access service
- Redirect user for authentication
- Log-in process (user sends credentials)
- Redirect back with Token
- Service retrieval
Enhancing User-Centric Identity Management Systems with Reputation Models in Distributed Environments

OpenID Overview + Reputation Management

Access service
Redirect user for authentication
Log-in process (user sends credentials)
Service Provider Reputation information
Redirect back with Token
Service retrieval
Send recommendation

Request Service Provider recommendations
Aggregate recommendations

Reputation Computation Engines

• Different ways of aggregating recommendations

Average
Weighted Average
Preferences Weighted Average
User Weighted Average

University of Murcia
31st October 2014

Ginés Dólera Tormo
PhD Thesis
Enhancing User-Centric Identity Management Systems with Reputation Models in Distributed Environments

Ginés Dólera Tormo
PhD Thesis

31st October 2014

University of Murcia

Experiments Results

<table>
<thead>
<tr>
<th>System Conditions</th>
<th>Computation Engine</th>
<th>Number of Users</th>
<th>Number of OPs</th>
<th>User Participation</th>
<th>Network Resources</th>
<th>Computer Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average</td>
<td>++</td>
<td>++</td>
<td>++</td>
<td>++</td>
<td>++</td>
<td>++</td>
</tr>
<tr>
<td>Weighted Average</td>
<td>+</td>
<td>++</td>
<td>+</td>
<td>++</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>Preferences</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Weighted Average</td>
<td>-</td>
<td>+</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Users Weighted Average</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>--</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Performance Measurements</th>
<th>Computation Engine</th>
<th>Accuracy</th>
<th>User Satisfaction</th>
<th>Adaptability</th>
<th>Behavior with malicious users</th>
<th>Behavior with malicious OPs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average</td>
<td>+</td>
<td>--</td>
<td>++</td>
<td>++</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>Weighted Average</td>
<td>++</td>
<td>--</td>
<td>++</td>
<td>+</td>
<td>+</td>
<td>++</td>
</tr>
<tr>
<td>Preferences</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Weighted Average</td>
<td>++</td>
<td>++</td>
<td>--</td>
<td>++</td>
<td>++</td>
<td>++</td>
</tr>
<tr>
<td>Users Weighted Average</td>
<td>++</td>
<td>++</td>
<td>++</td>
<td>++</td>
<td>++</td>
<td>++</td>
</tr>
</tbody>
</table>

Reputation Management in OpenID
Dynamic & Flexible selection
Reputation in eHealth
Private & customized reputation

Background

ROMEO Simulator

Results: Accuracy | User Satisfaction
Show Standard deviation | Show Full | Show Last | 100

Result Chart

[Graph with data points]

Scenario Configuration: [Parameters]

Control Panel
Export Chart | Load Scenario | Save Scenarios | N Steps: 100 | Reset Scenarios | Run | New Scenario
Stop
Enhancing User-Centric Identity Management Systems with Reputation Models in Distributed Environments

Ginés Dólera Tormo
PhD Thesis

State of the Art

Integration between user-centric Identity Management system and Reputation Systems study

Accuracy & Dynamism

Reputation Management in distributed IdM (OpenID)

ROMEO Simulator

Dynamic and Flexible Selection

Privacy

Advanced Care Coordination Platform

Bridging the Trust Gap in eHealth Environments

User-centric reputation & privacy

Towards privacy-preserving reputation management for Hybrid Broadcast Broadband applications

Solution Architecture Overview

Reputation Computation Engines Pool

Recommendation Database

Reputation Computation Engine 1

status=active

Reputation Computation Engine 2

status=active

Reputation Computation Engine n

status=active

System Conditions

SC₁, SC₂, ..., SCₙ

Performance Measurements

PM₁, PM₂, ..., PMₙ

Inference Rules

R₁, R₂, ..., Rₙ

Engine Selector

Monitor

Define

Evaluate
**Enhancing User-Centric Identity Management Systems with Reputation Models in Distributed Environments**

**Ginés Dólera Tormo**
**PhD Thesis**

**University of Murcia**
**31st October 2014**

---

**Fuzzy Sets and Smooth Transition**

- **Inference rules defined using fuzzy sets**

  - Very High
  - High
  - Medium
  - Low
  - Very Low

- **Smooth transition**

**Experiments Results**

- **Accuracy of different models in a dynamic environment**

- **User Weighted Average**
- **Preferences Weighted Average**
- **Weighted Average**
- **Dynamic computation engine**
- **Transition time**
Enhancing User-Centric Identity Management Systems with Reputation Models in Distributed Environments

Ginés Dólera Tormo
PhD Thesis

State of the Art
Identity management state of the art analysis
Integration between user-centric Identity Management system and Reputation Systems study

Accuracy & Dynamism
Reputation Management in distributed IdM (OpenID)
Dynamic and Flexible Selection

Privacy
Advanced Care Coordination Platform
Bridging the Trust Gap in eHealth Environments

User-centric reputation & privacy
Towards privacy-preserving reputation management for Hybrid Broadcast Broadband applications

Scenario Elements Overview
Reputation Goals
• Users get CSPs reputation
• CSPs and APs get reputation of each other
• Weighted Average Reputation

Privacy Goals
• Recommendations remain private
• Recommenders remain private
• Recommenders weights remain private
Enhancing User-Centric Identity Management Systems with Reputation Models in Distributed Environments

**Advanced Care Coordinator Platform**

1. **Patient** requests assistance
2. Care Coordinator (Identity Provider) selects care service provider
3. Care Service Provider requests access to Patient Info
4. Care Giver requests access to Patient’s home and provides help
5. Patient provides feedback

**Privacy-preserving Recommendations Aggregation**

\[ \text{Aggregate recommendations} = \sum_{i=1}^{n} \varepsilon(\omega_{ui}) \cdot Rec_{ui} \]

\[ \varepsilon(\omega_{ui}) \]

\[ \varepsilon(\text{Reputation}) \]

\[ \varepsilon(\omega_{ui} \cdot Rec_{ui}) \]
Enhancing User-Centric Identity Management Systems with Reputation Models in Distributed Environments

State of the Art

Integration between user-centric Identity Management system and Reputation Systems study

Accuracy & Dynamism

Reputation Management in distributed IdM (OpenID)

Dynamic and Flexible Selection

Privacy

Advanced Care Coordination Platform

Bridging the Trust Gap in eHealth Environments

Towards privacy-preserving reputation management for Hybrid Broadcast Broadband applications
Privacy-preserving Properties

<table>
<thead>
<tr>
<th></th>
<th>Identity Provider</th>
<th>Application Store</th>
</tr>
</thead>
<tbody>
<tr>
<td>real users’ identity</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>similarity between users</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>users’ recommendations</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>relate two users’ interactions</td>
<td>✓</td>
<td>✗</td>
</tr>
</tbody>
</table>

Solution Overview

- End user
- Log-in
- Reputation request
- Reputation response
- Provides feedback
- Identity Provider
  - pseudo id (p-ID)
  - Decrypts similarities and aggregates feedbacks accordingly
  - Stores feedback
  - Sends encrypted feedback
  - Updates similarities and stores encrypted feedback
- App Store
  - Provides encrypted similarities
  - Similarity request (p-ID, other p-IDs)
Enhancing User-Centric Identity Management Systems with Reputation Models in Distributed Environments

Update Encrypted Similarities

- Sends encrypted feedback, \( \text{App Store} \)
- Identity Provider

\[ \text{update}(\text{similarity}_{i,j}, \text{feedback}_i) \]

- do they match?
  - yes
    - \( \varepsilon(\text{result}) = \varepsilon(0) \)
    - \( \varepsilon(\text{result}) = \varepsilon(1) \)
  - no
    - \( \varepsilon(\text{result}) = \varepsilon( \text{result} ) + \varepsilon( \text{result} ) \)

State of the Art

- Identity management state of the art analysis
- Integration between user-centric Identity Management system and Reputation Systems study

Accuracy & Dynamism

- Reputation Management in distributed IdM (OpenID)
- Dynamic and Flexible Selection

Privacy

- Advanced Care Coordination Platform
- Bridging the Trust Gap in eHealth Environments

User-centric reputation & privacy

- Towards privacy-preserving reputation management for Hybrid Broadcast Broadband applications
Conclusions & Future Work

Future Work

- Bring developed mechanisms into a standardization body
- Enhancing the proposed solutions in order to assist administrators
- Study applicability and scope of advanced cryptographic techniques to preserve users' privacy
- Analyzing how presented integration could be applied to other contexts
Contributions Summary

**Book Chapters**


**Journals with Impact Factor**


- Ginés Dólora Tormo, Félix Gómez Mármol, Gregorio Martínez Pérez, "Dynamic and flexible selection of a reputation mechanism for heterogeneous environments", *Elsevier Future Generation Computer Systems*, Special Issue on Trustworthy Data Fusion and Mining in Internet of Things, 2014 [IF=2.639, Q1]


Contributions Summary

Conferences


Contributions Summary

International Patents

• Joao Girao, Brigitta Lange, Nils Gruschka, Ginés Dólera Tormo, Félix Gómez Mármol, "Method to support an advanced home services coordination platform", US 20130304488 A1, 14/11/2013

• Ginés Dólera Tormo, Félix Gómez Mármol, "System and Method for determining a Reputation Mechanism", WO 2013/117224 A1, 08/02/2012
Contributions Summary

Complementary Work

- Journal with impact factor
  
  
  

- Open Source Software (protected with Intellectual Property Rights)
  - **OpenXKMS**: Open source implementation of the W3C Recommendation of the XML Key Management Specification 2.0
  
  - **UMU-XACML-Editor**: Graphical editor for access control policy definition based on the XACML standard
  
  - **Mistral-IdM**: Identity management implementation with advanced authentication and authorization features, based on standards (SAML, XACML and XKMS)
  
  - **SAMLUtil**: Helper implementation to provide common SAML functionality
  
  - **Identity Aggregator**: Identity Manager between multiple stakeholders
  
  - **XACML WebPAP**: User-friendly web-based Policy Administration Point for the XACML standard
Contributions Summary

Summary

<table>
<thead>
<tr>
<th>Category</th>
<th>Quantity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Book chapters</td>
<td>1</td>
</tr>
<tr>
<td>Published Journal with impact factor</td>
<td>8 (4 included in the thesis + 4 complementary)</td>
</tr>
<tr>
<td>Conferences</td>
<td>2</td>
</tr>
<tr>
<td>International Patents</td>
<td>2</td>
</tr>
<tr>
<td>Open Source Projects</td>
<td>6</td>
</tr>
</tbody>
</table>

Thanks for your attention