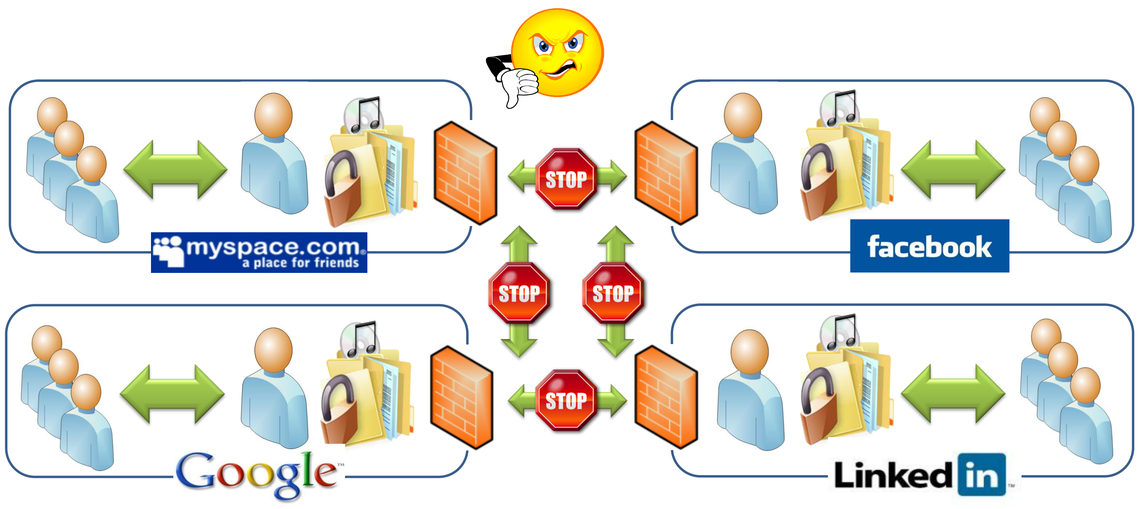
Towards Secure Web 2.0 User Content Sharing Beyond Walled Gardens

Student: San-Tsai Sun Supervisor: Konstantin Beznosov

Problem

❖ Lack of useful mechanisms for Web 2.0 users without special technical skills for sharing their content with each other in a controlled manner across content-hosting or application-service provider (CSP) boundaries.



Site-centric Walled Gardens

Approach

❖ Lit review to understand user sharing practices :
- Email is the most commonly used sharing mechanism
- Users tend to treat socially-defined classes of individuals the same when sharing

❖ Lit review to understand current sharing issues :
- Difficulties in selecting a common sharing mechanism with desired features
- Forgetting what has been shared and with whom
- Problem in knowing when new content was made available.

❖ Understand current sharing solutions provided by CSPs:
- Walled garden approach
- Secret-link approach

❖ Design and implement sharing mechanism based on:
- Existing Internet infrastructure and open protocols
- Distributed authorization mechanisms

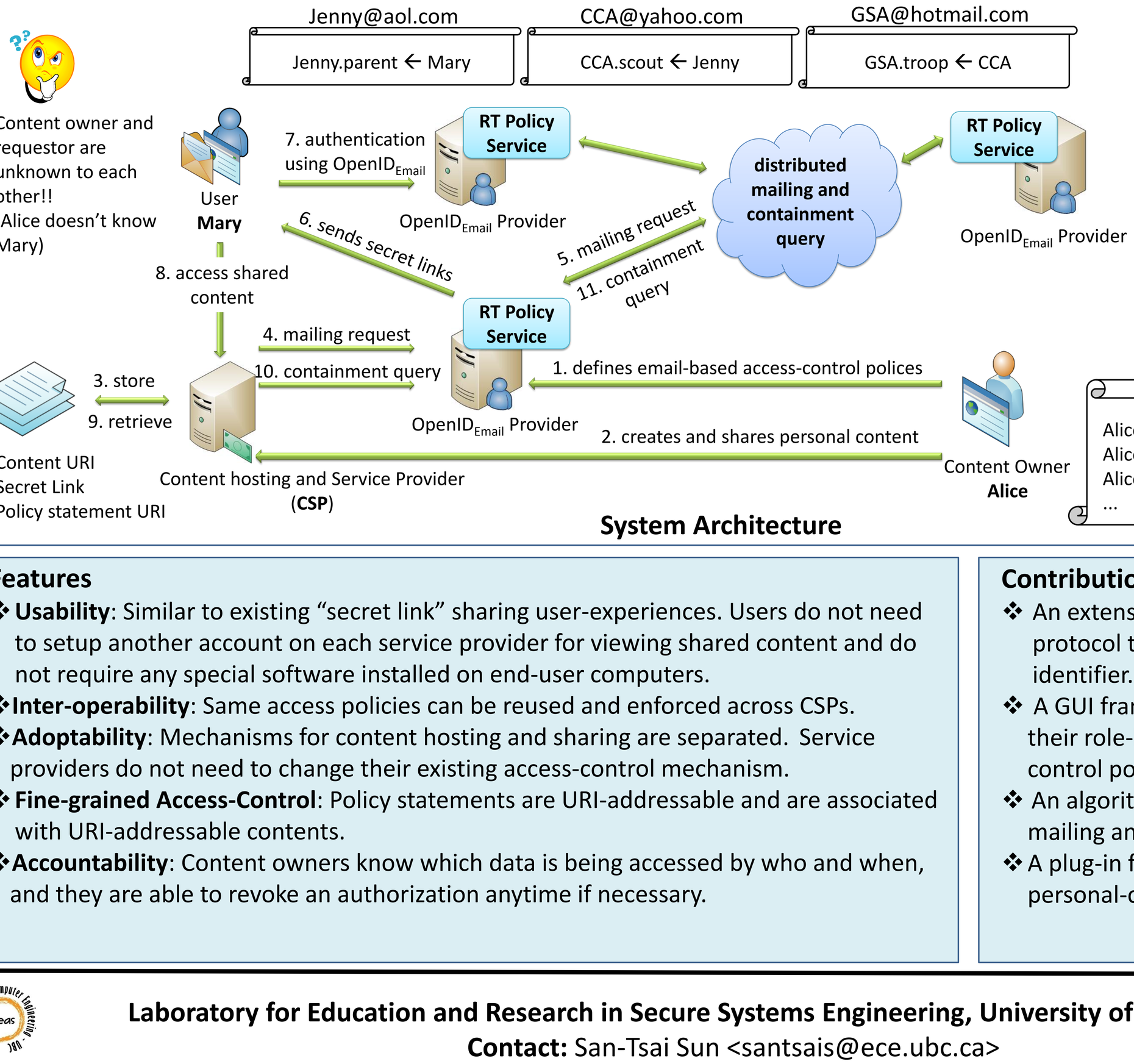
Usability and Inter-operability are key concerns

Design

Augment OpenID identity providers with two key components:

❖ **OpenID$_{email}$** : extends the existing OpenID protocol to enable OpenID identity providers to use email as an alternative identifier.

❖ **RT Policy Service**: provides services for internet users to organize their role-based trust-management access-control polices, and for CSPs to make access decisions.



System Architecture

❖ Scenario:
- Alice and Jenny are scouts in CCA club
- CCA is a certified member of GSA
- Mary is Jenny's Mother

❖ Access policy:
- Pictures of training events can only be seen by scouts in the same club and their parents

Alice@gmail.com

```
Alice.pic(training) ← CCA.scout
Alice.pic(training) ← CCA.scout.parent
Alice.pic(award) ← GSA.troop.scout
...
```

Features

❖ **Usability**: Similar to existing "secret link" sharing user-experiences. Users do not need to setup another account on each service provider for viewing shared content and do not require any special software installed on end-user computers.

❖ **Inter-operability**: Same access policies can be reused and enforced across CSPs.

❖ **Adoptability**: Mechanisms for content hosting and sharing are separated. Service providers do not need to change their existing access-control mechanism.

❖ **Fine-grained Access-Control**: Policy statements are URI-addressable and are associated with URI-addressable contents.

❖ **Accountability**: Content owners know which data is being accessed by who and when, and they are able to revoke an authorization anytime if necessary.

Contributions

❖ An extension to the existing OpenID protocol that uses email as an alternative identifier.

❖ A GUI framework for users to construct their role-based trust-management access-control polices.

❖ An algorithm and protocol for distributed mailing and containment queries.

❖ A plug-in for service providers to enable personal-content sharing.

Laboratory for Education and Research in Secure Systems Engineering, University of British Columbia
Contact: San-Tsai Sun <santsais@ece.ubc.ca>