Is OpenID too Open? Technical, Business, and Human Issues That Get in the Way of OpenID and Ways of Addressing Them

San-Tsai Sun

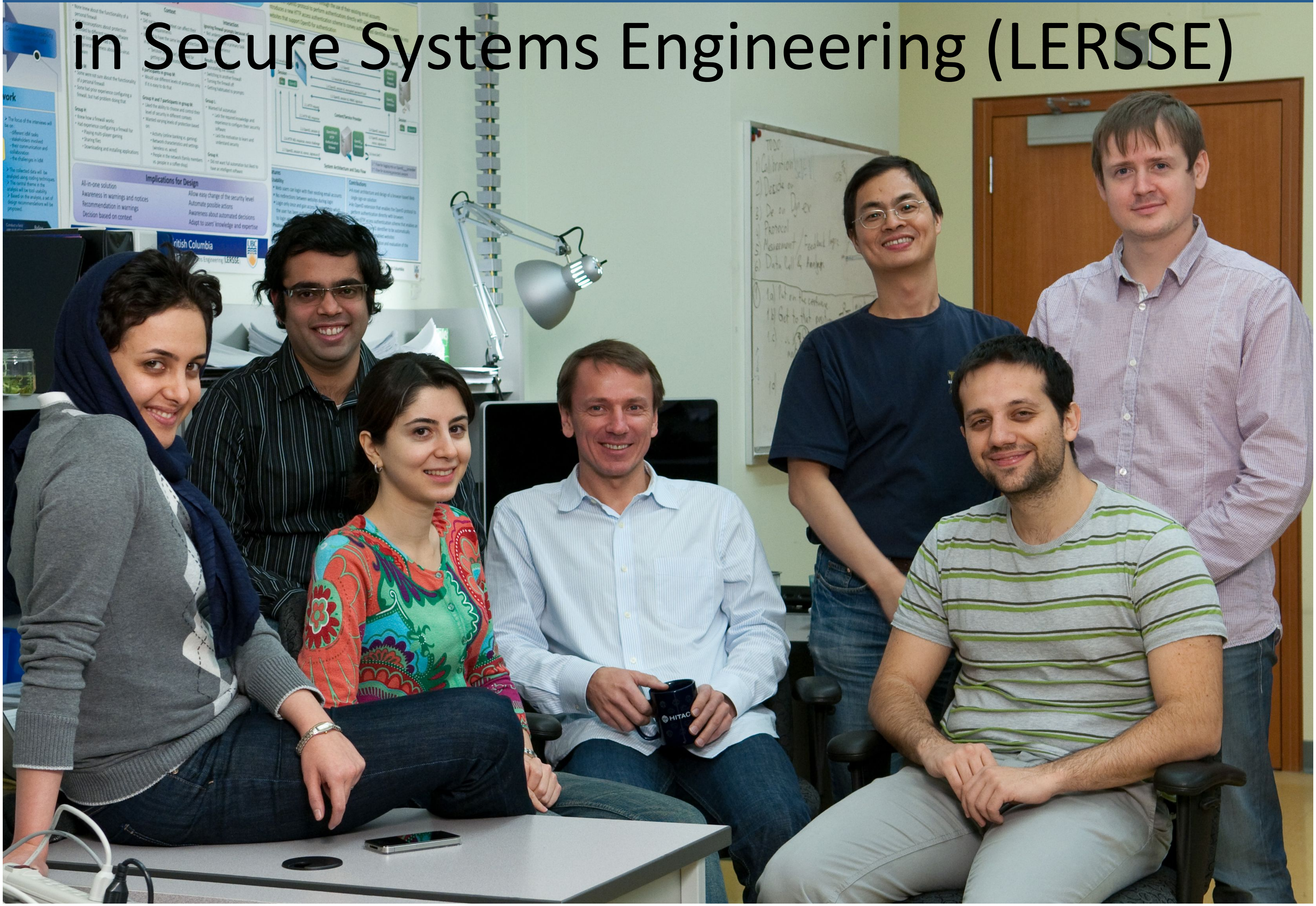
Konstantin (Kosta) Beznosov

a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

Laboratory for Education and Research in
Secure Systems Engineering (LERSSE)

Department of Electrical & Computer Engineering

Laboratory for Education and Research in Secure Systems Engineering (LERSSE)



LERSSE research

- access control
  - performance and availability
- security of online social networks
- usability of end-user security controls
  - personal firewalls
  - user account control (UAC) in Windows
- usability of IT security management
  - IT security administration
  - identity management
- web security
  - detection & prevention of SQL injection attacks
  - authentication
  - controlled sharing of user content

why web single sign on

1. many passwords to manage

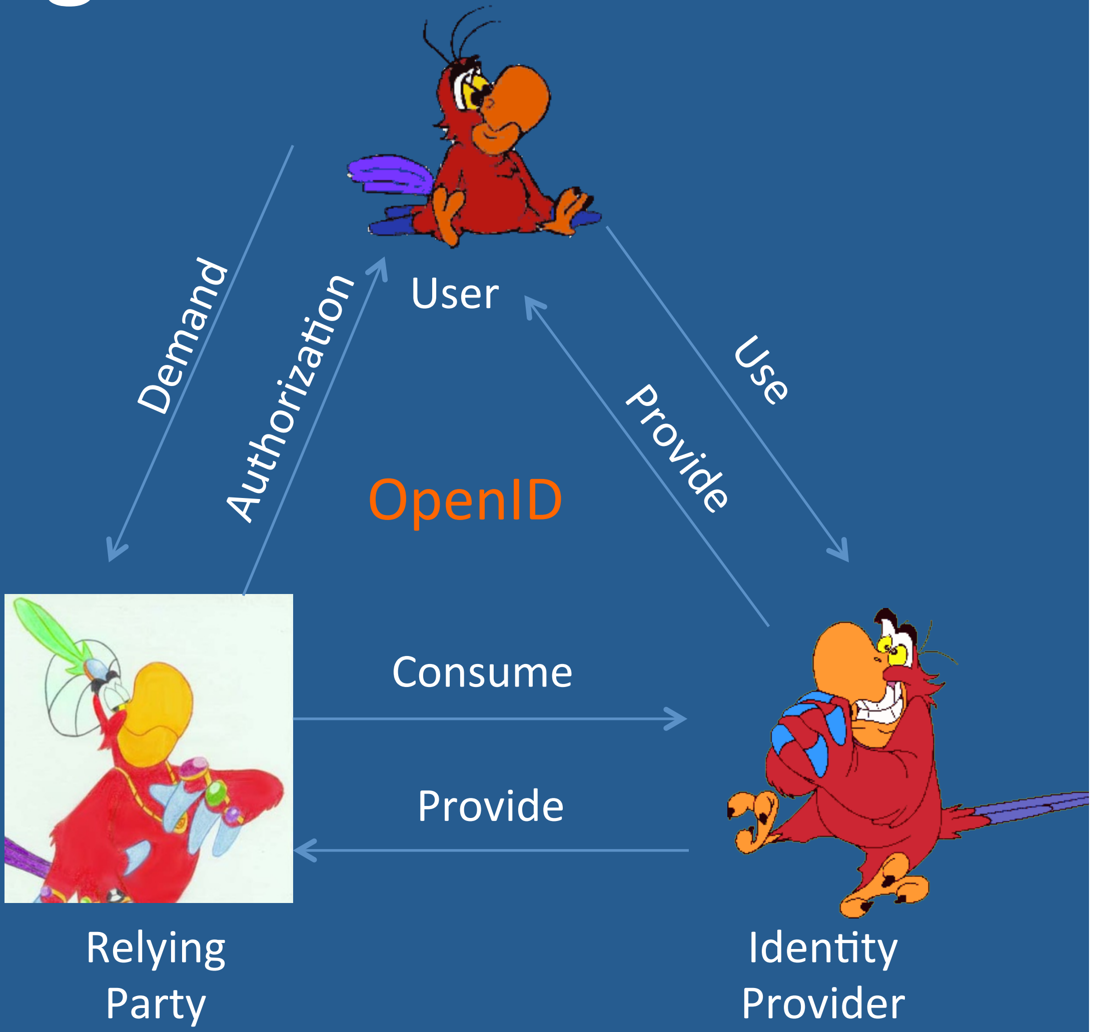
25 accounts
8 passwords per day [1]

2. multiple on-line profiles and information propagation

[1] D. Florencio and C. Herley. A large-scale study of web password habits. In Proc. of WWW '07, New York, NY, USA, 2007.

existing solutions

password managers



User

Demand

Authorization

Use

Provide

OpenID

Consume

Provide

Relying Party

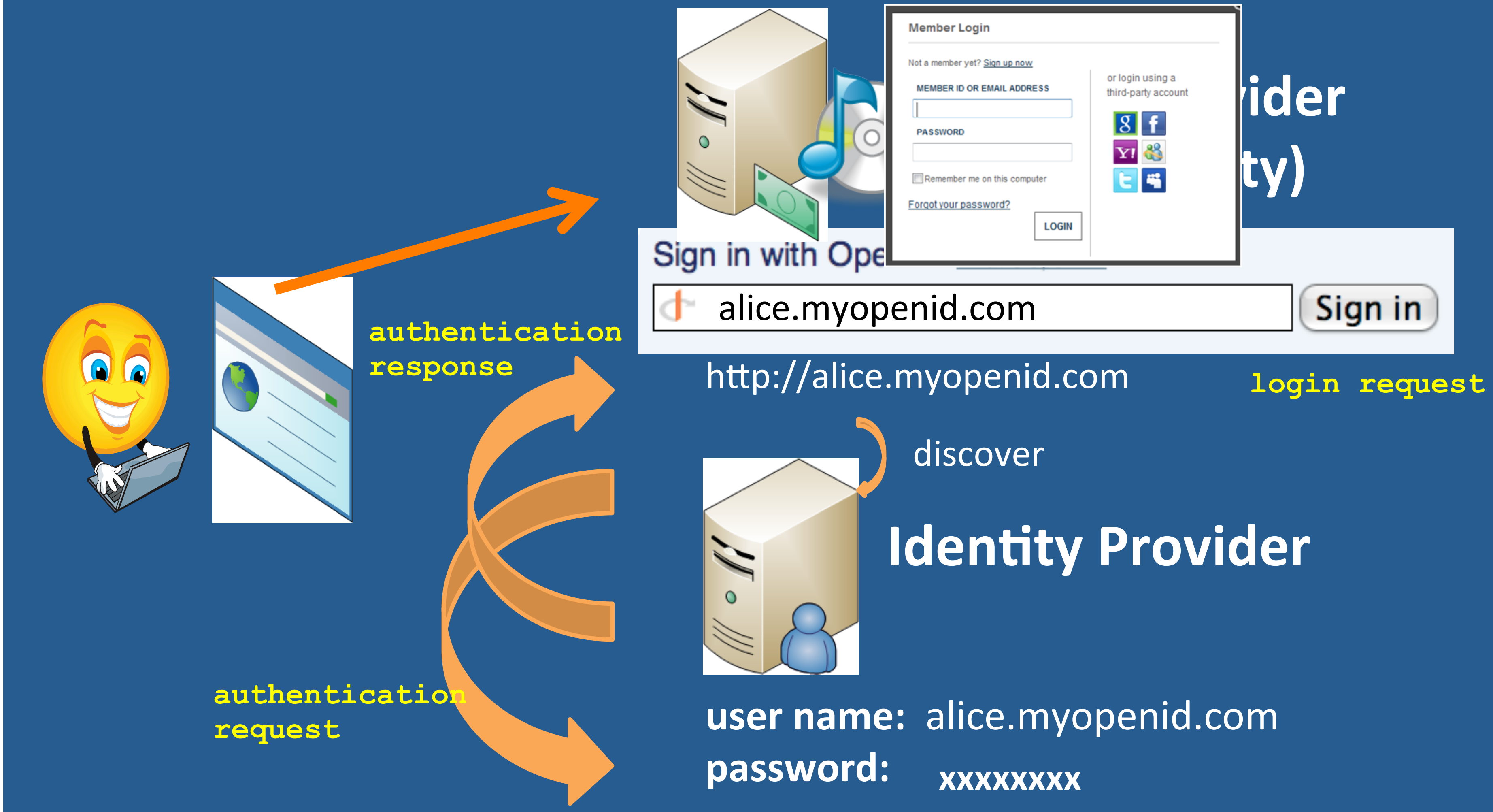
Identity Provider

OpenID

- open and user-centric Web single sign-on protocol
- OpenID Foundation (2007) [1]
  - Microsoft, Google, IBM, Yahoo, VeriSign, Facebook, PayPal, PingIdentity
- over **one billion** OpenID enabled user accounts provided by Google, Yahoo, AOL...[1]

[1] OpenID Foundation. http://openid.net/foundation

how OpenID works



Member Login

Not a member yet? Sign up now

MEMBER ID OR EMAIL ADDRESS

PASSWORD

□ Remember me on this computer

Forgot your password?

LOGIN

or login using a third-party account

Sign in with Ope

alice.myopenid.com

Sign in

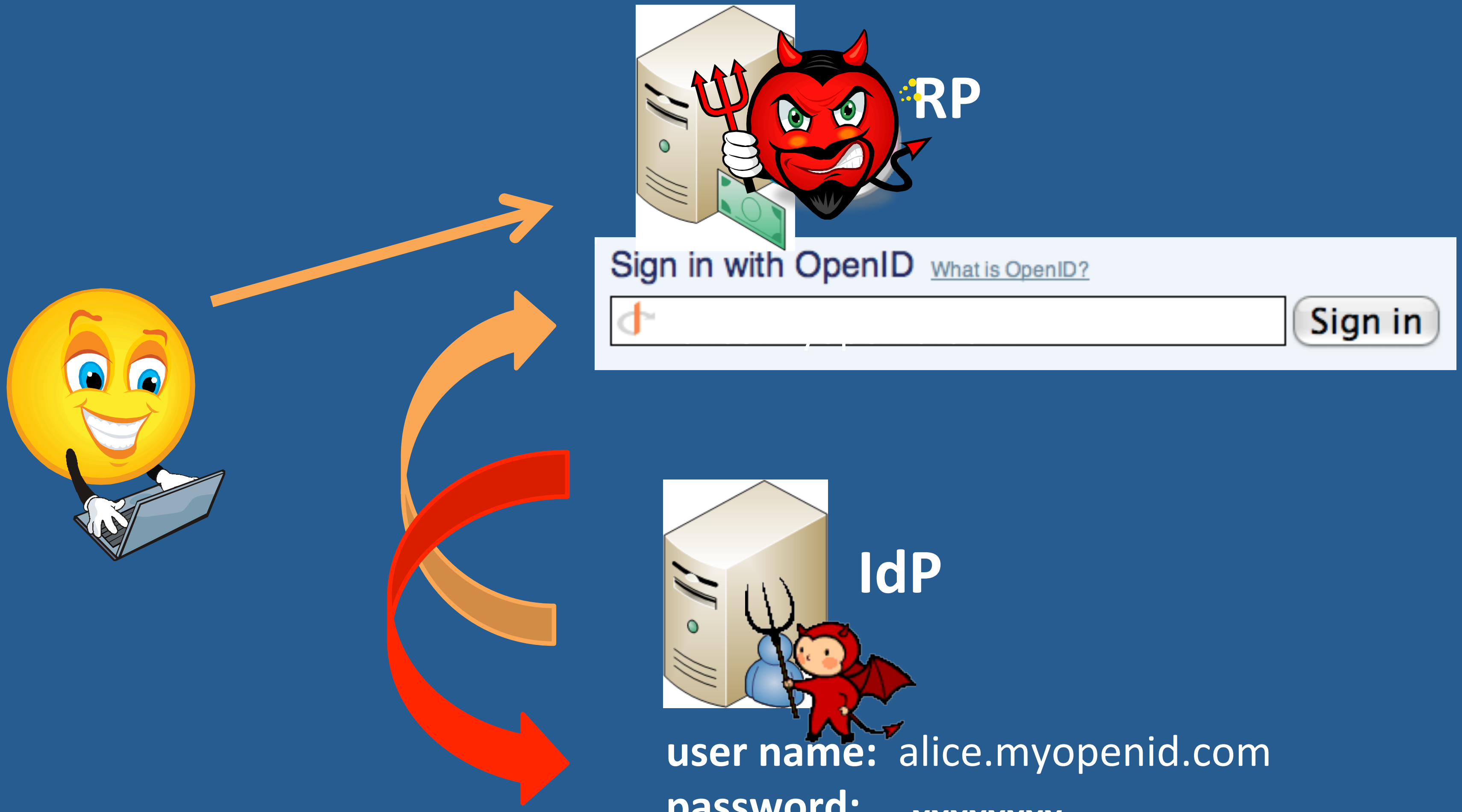
user name: alice.myopenid.com

password: xxxxxxxx

agenda

- technical vulnerabilities
- business concerns
- usability issues
- a way to a better web SSO
  - OpenID$_{\text{email}}$ enabled web browser

password phishing attacks

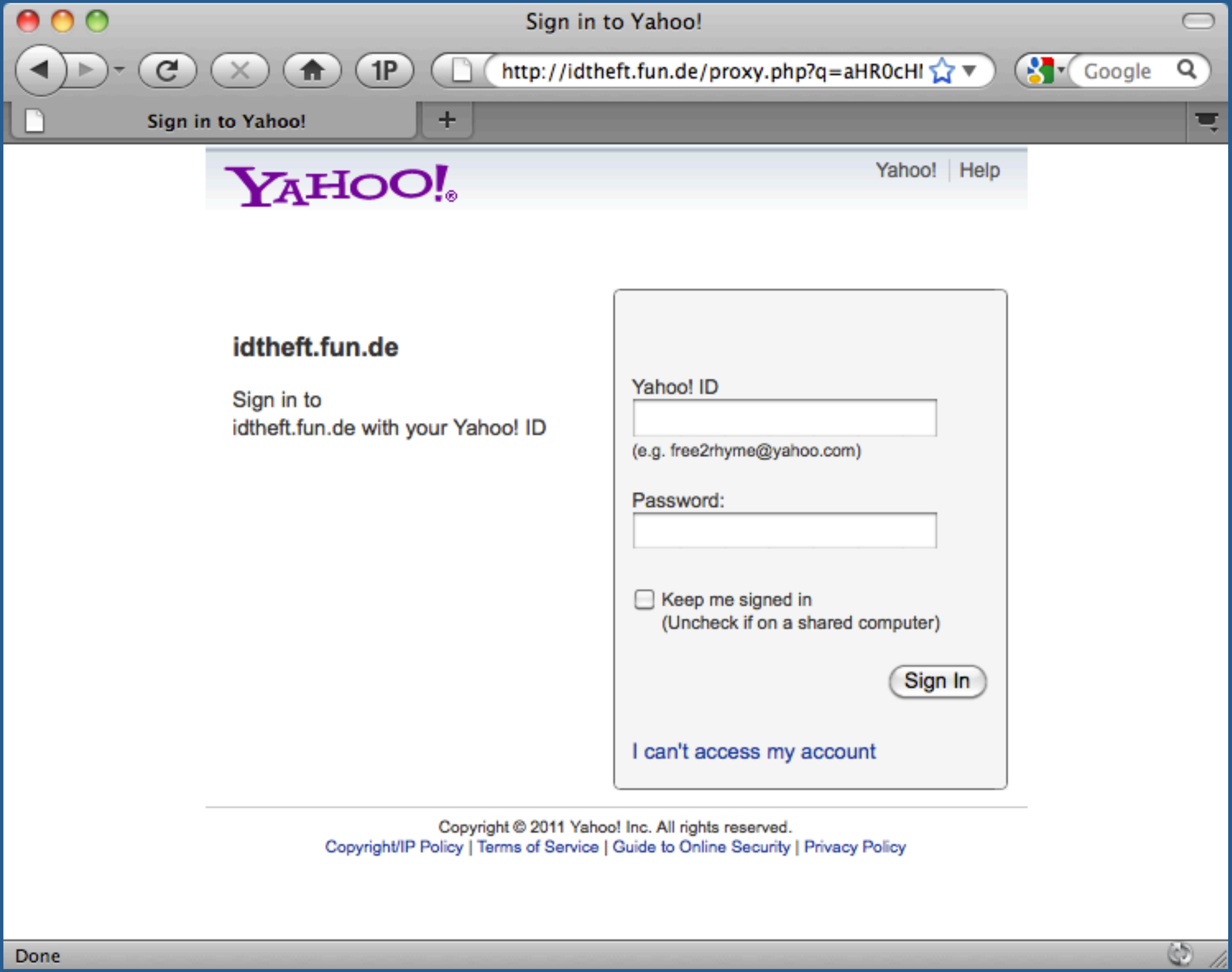


user name: alice.myopenid.com

password: xxxxxxxx

[1] B. Laurie. OpenID Phishing heaven.
[2] C. Messina. OpenID Phishing Brainstorm. http://wiki.openid.net/OpenID Phishing Brainstorm, 2009
[3] R. Dhamija, J. D. Tygar, and M. Hearst. Why Phishing works. In the Proceedings of CHI '06, New York, NY, USA, 2006.
[4] B. Adida. EmID: Web authentication by email address. In Proceedings of W2SP 2008, Oakland, California, USA, 2008.

users are vulnerable to phishing attacks



http://idtheft.fun.de/proxy.php?q=aHR0cH!

idtheft.fun.de

Sign in to
idtheft.fun.de with your Yahoo! ID

Yahoo! ID

(e.g. free2rhyme@yahoo.com)

Password:

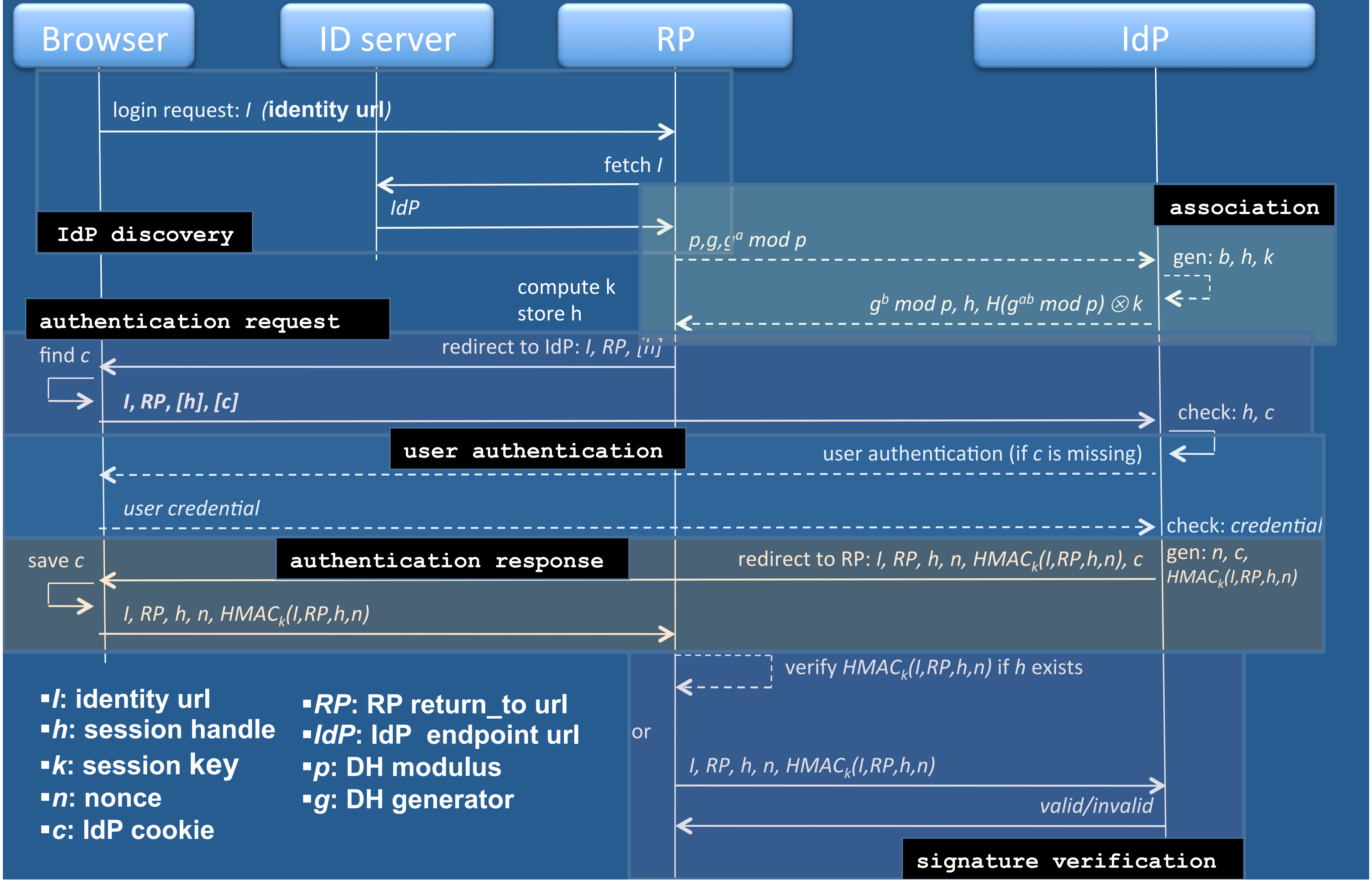
□ Keep me signed in
(Uncheck if on a shared computer)

I can't access my account

Copyright © 2011 Yahoo! Inc. All rights reserved.
Copyright/IP Policy | Terms of Service | Guide to Online Security | Privacy Policy

TECHNICAL VULNERABILITIES

OpenID sequence diagram



Browser

ID server

RP

IdP

login request: *I* (**identity url**)

fetch *I*

IdP

IdP discovery

association

p,g,g^a mod p

gen: *b, h, k*

compute k
store h

g^b *mod p, h,* $H(g^{ab} \bmod p) \otimes k$

authentication request

find *c*

redirect to IdP: *I, RP, [h]*

I, RP, [h], [c]

check: *h, c*

user authentication

user authentication (if *c* is missing)

user credential

check: *credential*

save *c*

authentication response

redirect to RP: *I, RP, h, n,* $HMAC_k(I,RP,h,n)$*, c*

gen: *n, c,* $HMAC_k(I,RP,h,n)$

I, RP, h, n, $HMAC_k(I,RP,h,n)$

verify $HMAC_k(I,RP,h,n)$ if *h* exists

or

I, RP, h, n, $HMAC_k(I,RP,h,n)$

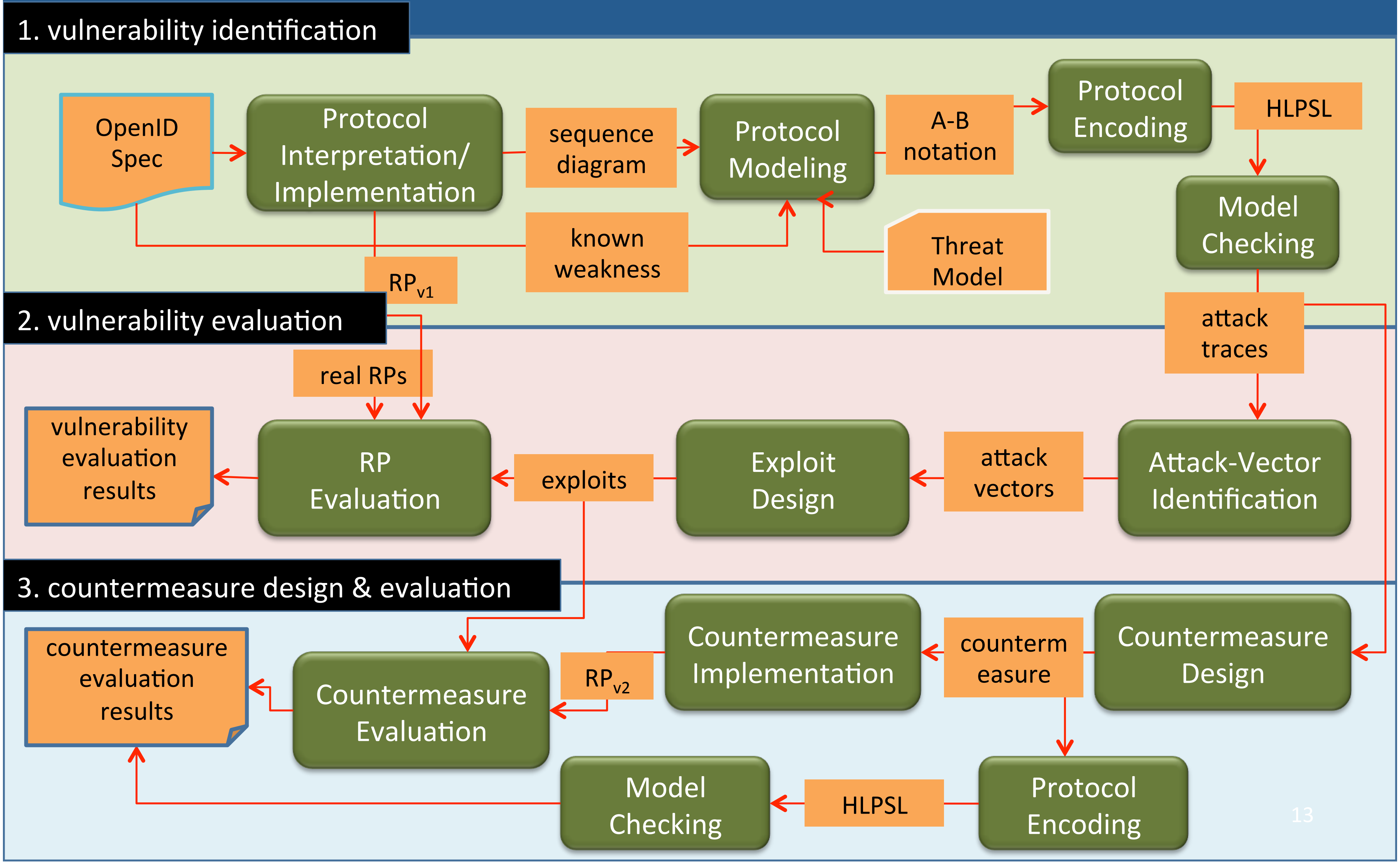
valid/invalid

signature verification

- ***I*: identity url**
- ***h*: session handle**
- ***k*: session key**
- ***n*: nonce**
- ***c*: IdP cookie**

- ***RP*: RP return_to url**
- ***IdP*: IdP endpoint url**
- ***p*: DH modulus**
- ***g*: DH generator**

security analysis methodology



1. vulnerability identification

OpenID Spec

Protocol Interpretation/ Implementation

sequence diagram

Protocol Modeling

A-B notation

Protocol Encoding

HLPSL

Model Checking

known weakness

Threat Model

RP_{v1}

attack traces

2. vulnerability evaluation

real RPs

vulnerability evaluation results

RP Evaluation

exploits

Exploit Design

attack vectors

Attack-Vector Identification

3. countermeasure design & evaluation

countermeasure evaluation results

Countermeasure Evaluation

RP_{v2}

Countermeasure Implementation

counterm easure

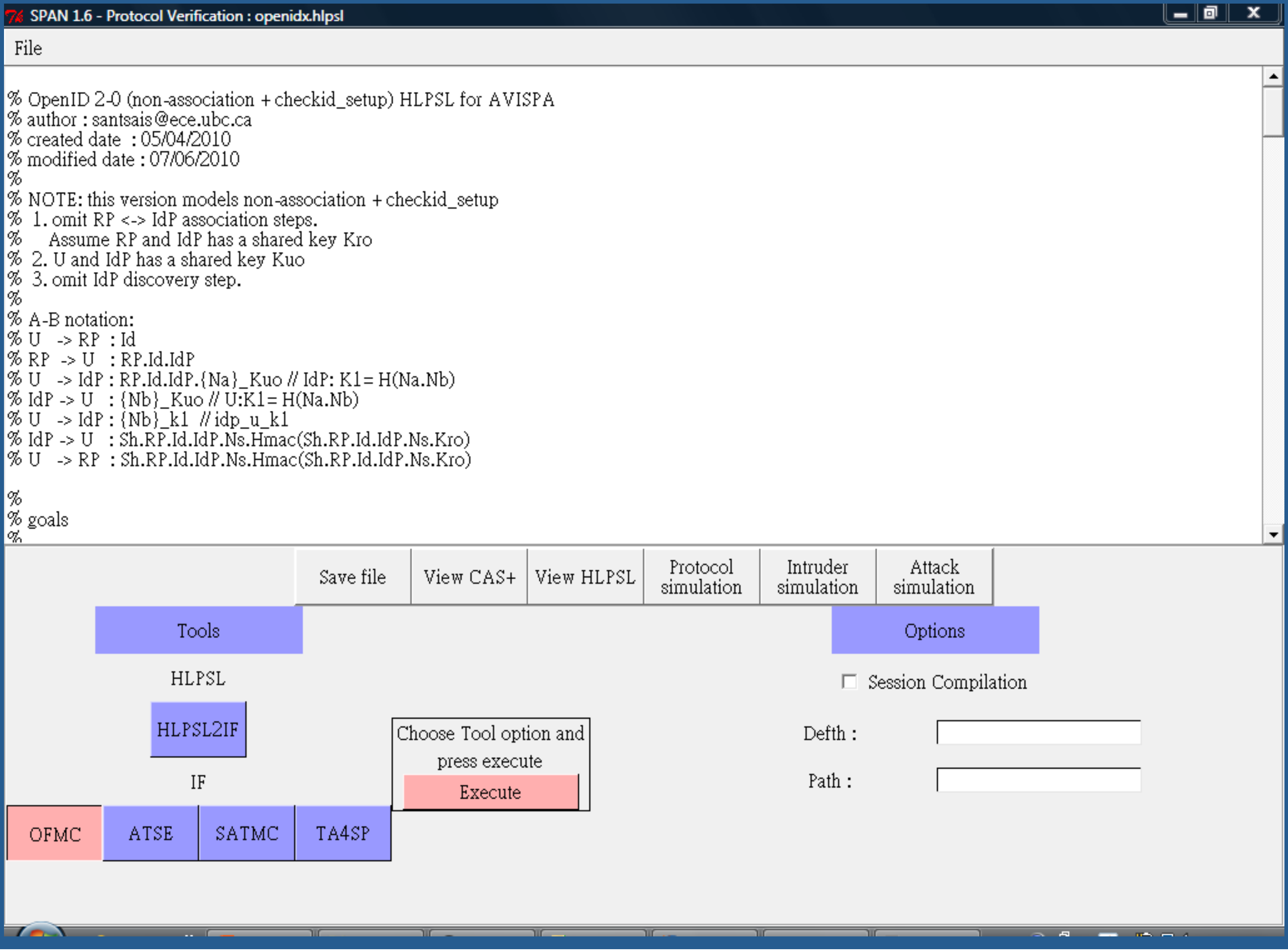
Countermeasure Design

Model Checking

HLPSL

Protocol Encoding

AVISPA



```
% OpenID 2-0 (non-association + checkid_setup) HLPSL for AVISPA
% author : santsais@ece.ubc.ca
% created date  : 05/04/2010
% modified date : 07/06/2010
%
% NOTE: this version models non-association + checkid_setup
%  1. omit RP <-> IdP association steps.
%     Assume RP and IdP has a shared key Kro
%  2. U and IdP has a shared key Kuo
%  3. omit IdP discovery step.
%
% A-B notation:
% U   -> RP  : Id
% RP  -> U   : RP.Id.IdP
% U   -> IdP : RP.Id.IdP.{Na}_Kuo // IdP: K1= H(Na.Nb)
% IdP -> U   : {Nb}_Kuo // U:K1= H(Na.Nb)
% U   -> IdP : {Nb}_k1  // idp_u_k1
% IdP -> U   : Sh.RP.Id.IdP.Ns.Hmac(Sh.RP.Id.IdP.Ns.Kro)
% U   -> RP  : Sh.RP.Id.IdP.Ns.Hmac(Sh.RP.Id.IdP.Ns.Kro)

%
% goals
%
```

adversary model

- adversary: non-RP or IdP associated attackers
- goal: unauthorized access/modification of users' data hosted on RP
- adversary types
  - web poster
    - post comments
  - web attacker:
    - setup a malicious website
    - send malicious links via spam
    - deliver malicious content via Ads network
    - exploit web vulnerabilities (i.e., XSS) of benign websites
  - network attacker:
    - setup an wireless access point
    - compromise client DNS resolution

assumptions

- RP, IdP, user machine, and browser are not compromised
- RP, IdP are not malicious
- user credentials on IdPs are secure
- cookies in the browser are secure (integrity and confidentiality)

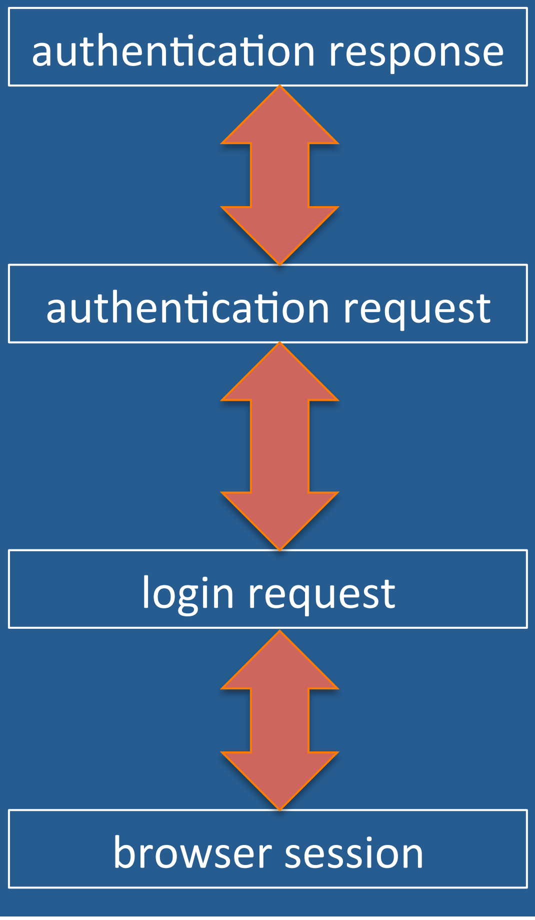
non-considered threats

- availability threat
  - DoS by sending massive concurrent auth requests to an IdP
  - DoS by sending massive concurrent auth responses to an RP
- identity spoofing
  - phishing attacks by RP
  - exploits vulnerabilities on IdP
- integrity of IdP discovery process
  - altering discovery information
  - compromise RP DNS resolution

demonstration of attacks

found weakness

authentication response acts as a one-time access token to an RP, but there is no binding chain



authentication response

authentication request

login request

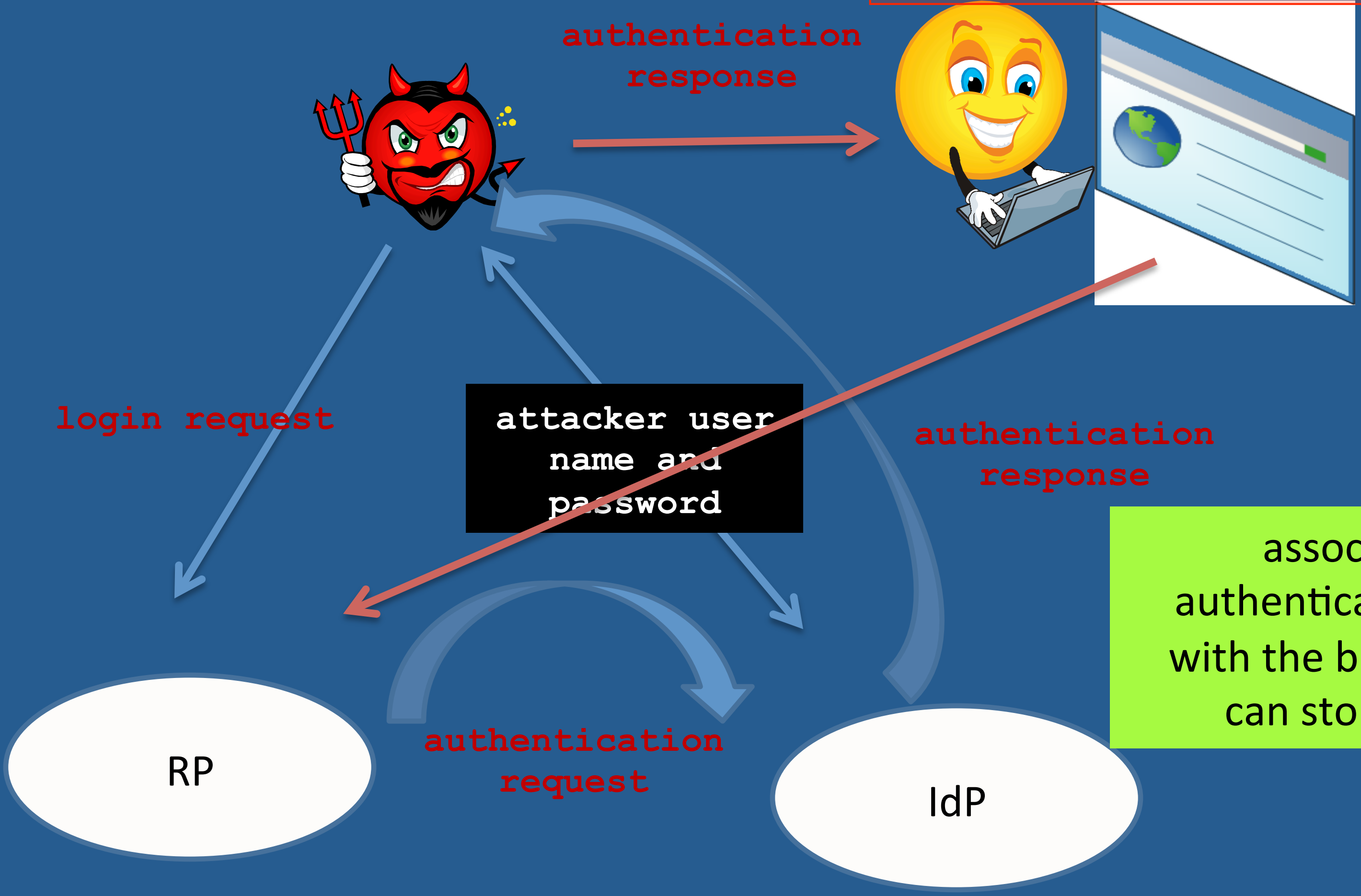
browser session

attack vectors

- CSRF
  - single sign-on (SSO) CSRF (force victim to login)
    - HTTP GET Auth Request CSRF[Web poster, Web attacker]
    - HTTP POST Login CSRF [Web attacker]
    - HTTP GET Login CSRF [Web poster, Web attacker]
  - account profile CSRF [Web poster, Web attacker]
  - login CSRF (login as attacker) [Web poster, Web attacker]
- authentication response interception
  - impersonation [Network attacker]
  - replay attack [Network attacker]

login CSRF: login as the attacker

```
<img src=“auth response”
style=“display:none”>
```



authentication response

login request

attacker user name and password

authentication response

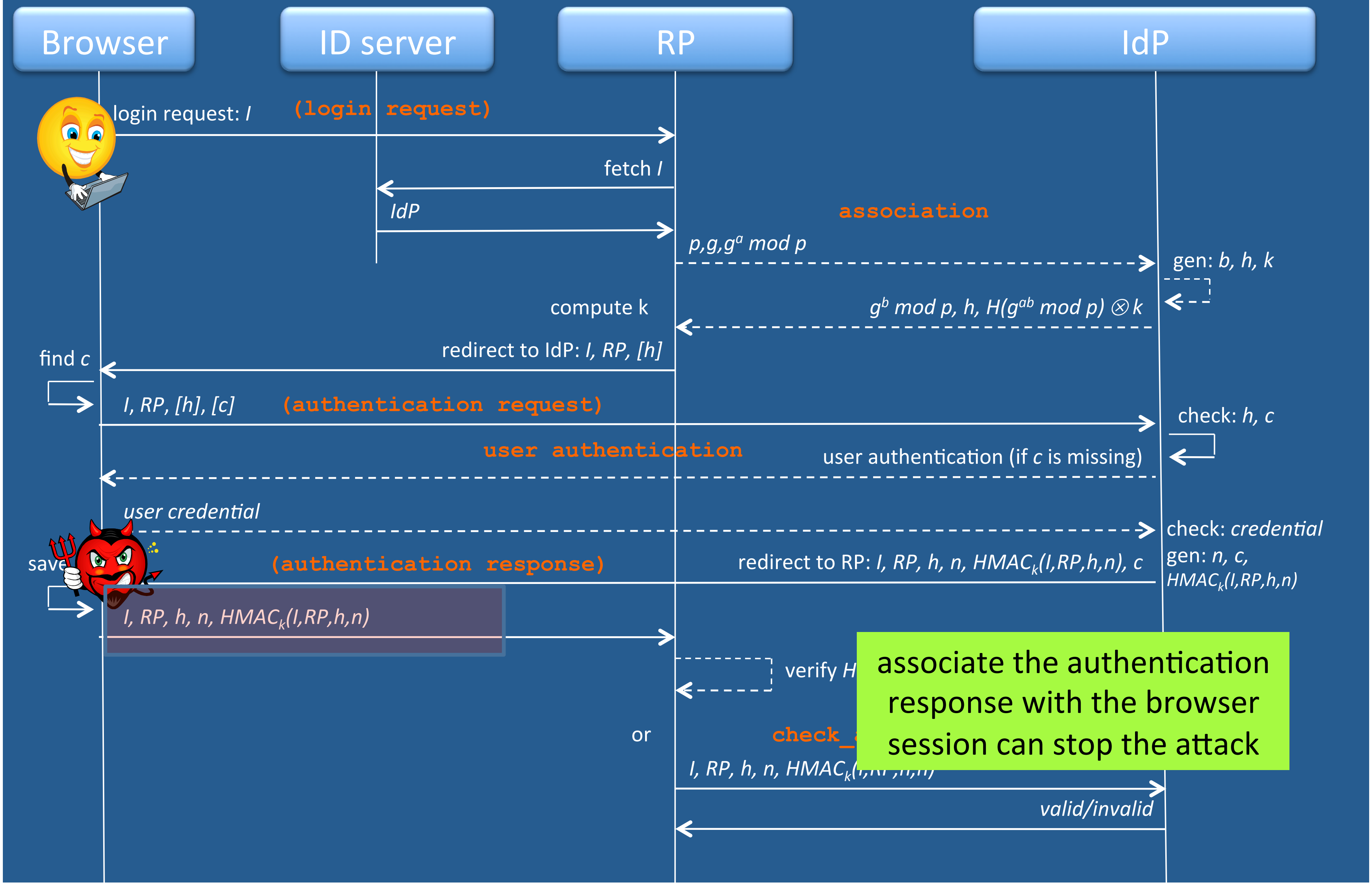
authentication request

RP

IdP

associating the authentication response with the browser session can stop the attack

impersonation and replay attack



associate the authentication response with the browser session can stop the attack

attack stats

- cross site request forgery (CSRF) attacks
  - single-sign-on CSRF (force victim to login) (70%)
  - account profile CSRF (50%)
  - login CSRF (login as attacker) (73%)
- authentication response interception
  - impersonation (67%)
  - replay attack (6%)

countermeasure

- when a new browser session initialized RP
  - generates a nonce N = HMAC(browser session id)
  - issues a new cookie C_N = N
  - appends a parameter P_N=N to the OpenID login form
- on a login request, IdP
  - checks if $P_N = C_N$ and C_N = HMAC(browser session id)
  - initiates a new authentication request
  - appends a parameter R_N=N to the **`return_to`** URL
- on an authentication response, RP
  - checks if $R_N = C_N$ and C_N = HMAC(browser session id)

characteristics of countermeasure

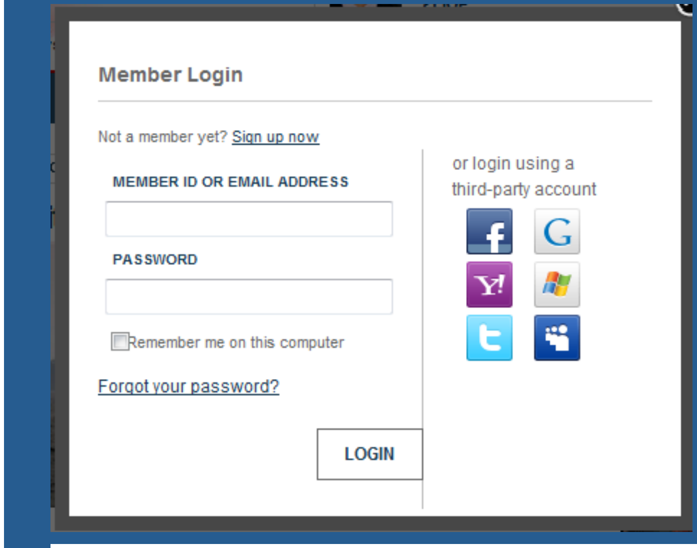
- compatible with existing OpenID
- does not require any additional storage on RP
- would not reveal browser session id
- protects from cookie overwrite

future work

- evaluate more RPs
- apply our methodology to other Web single sign-on protocol
  - Facebook Connect
  - Microsoft Live ID

USABILITY ISSUES

relying party user interfaces confusing



Member Login

Not a member yet? Sign up now

MEMBER ID OR EMAIL ADDRESS

PASSWORD

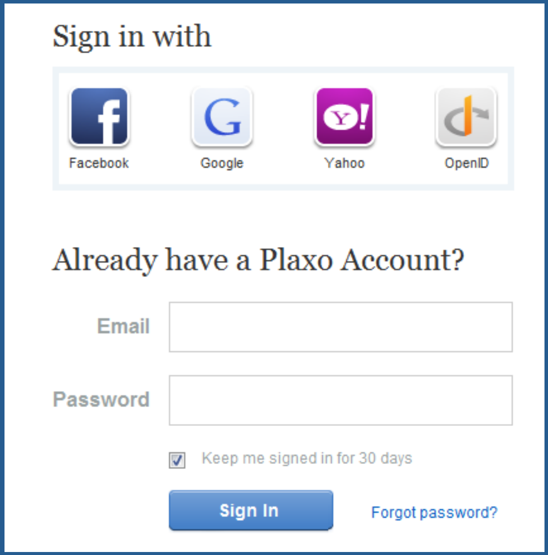
□ Remember me on this computer

Forgot your password?

LOGIN

or login using a third-party account

No single way of implementing OpenID enabled login form



Sign in with

Facebook Google Yahoo OpenID

Already have a Plaxo Account?

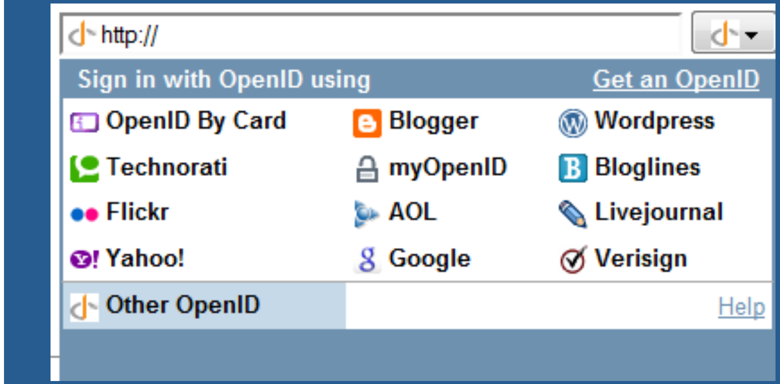
Email

Password

☑ Keep me signed in for 30 days

Sign In

Forgot password?



http://

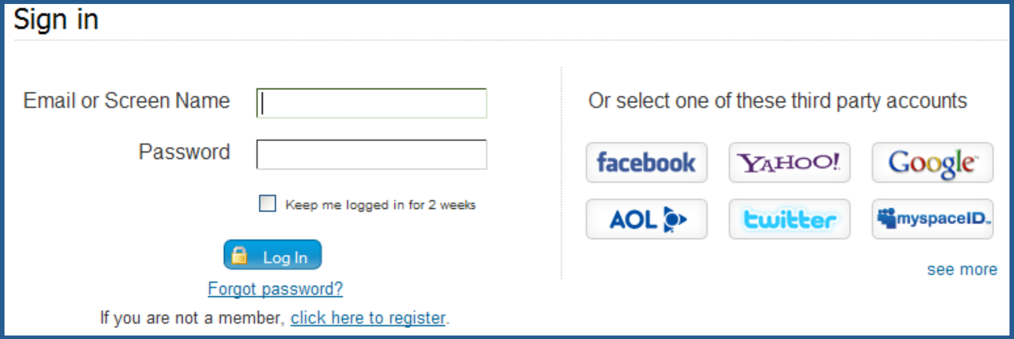
Sign in with OpenID using

Get an OpenID

OpenID By Card	Blogger	Wordpress
Technorati	myOpenID	Bloglines
Flickr	AOL	Livejournal
Yahoo!	Google	Verisign

Other OpenID

Help



Sign in

Email or Screen Name

Password

□ Keep me logged in for 2 weeks

Log In

Forgot password?

If you are not a member, click here to register.

Or select one of these third party accounts

facebook YAHOO! Google AOL twitter myspaceID

see more

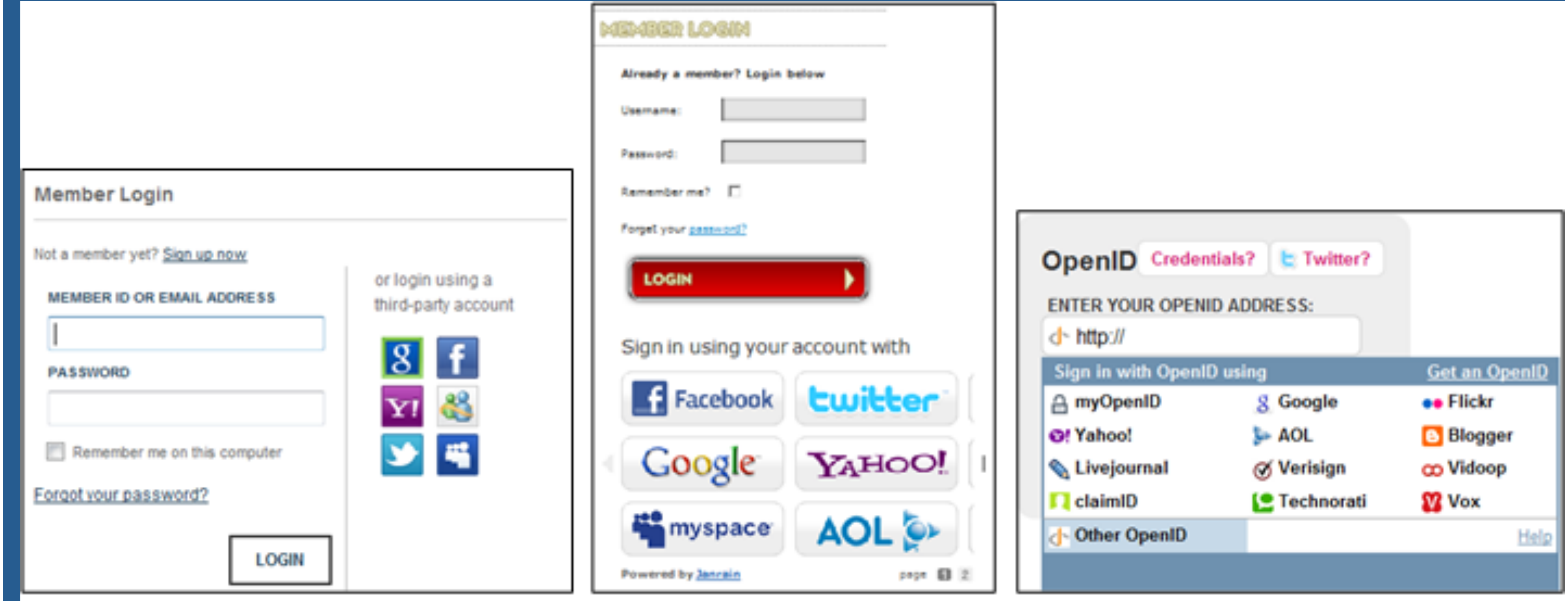
study participants

9 participants from UBC and Greater Vancouver

- 6 male & 3 female
- age: four 19-24 & five 25-34
- 8 fluent in English
- 8 with college or graduate degree
- all had more than 4 web accounts
- 2 used password managers
- 5 used UBC's campus-wide login (CWL) web SSO

study protocol 1/4

1. background questionnaire
2. sign-up and sign-in to three OpenID-supported web sites using using their existing account with an IdP.

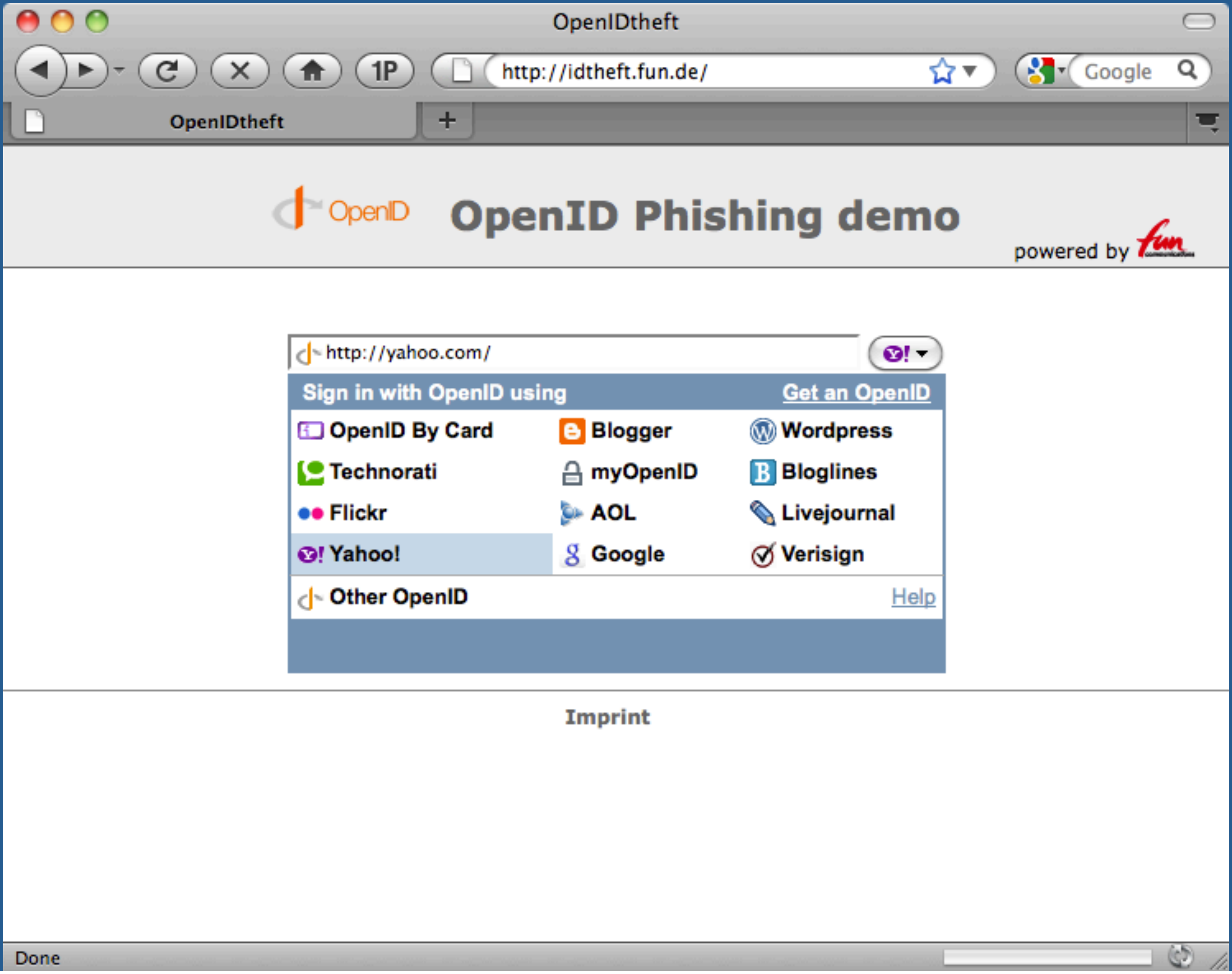


(a) (b) (c)

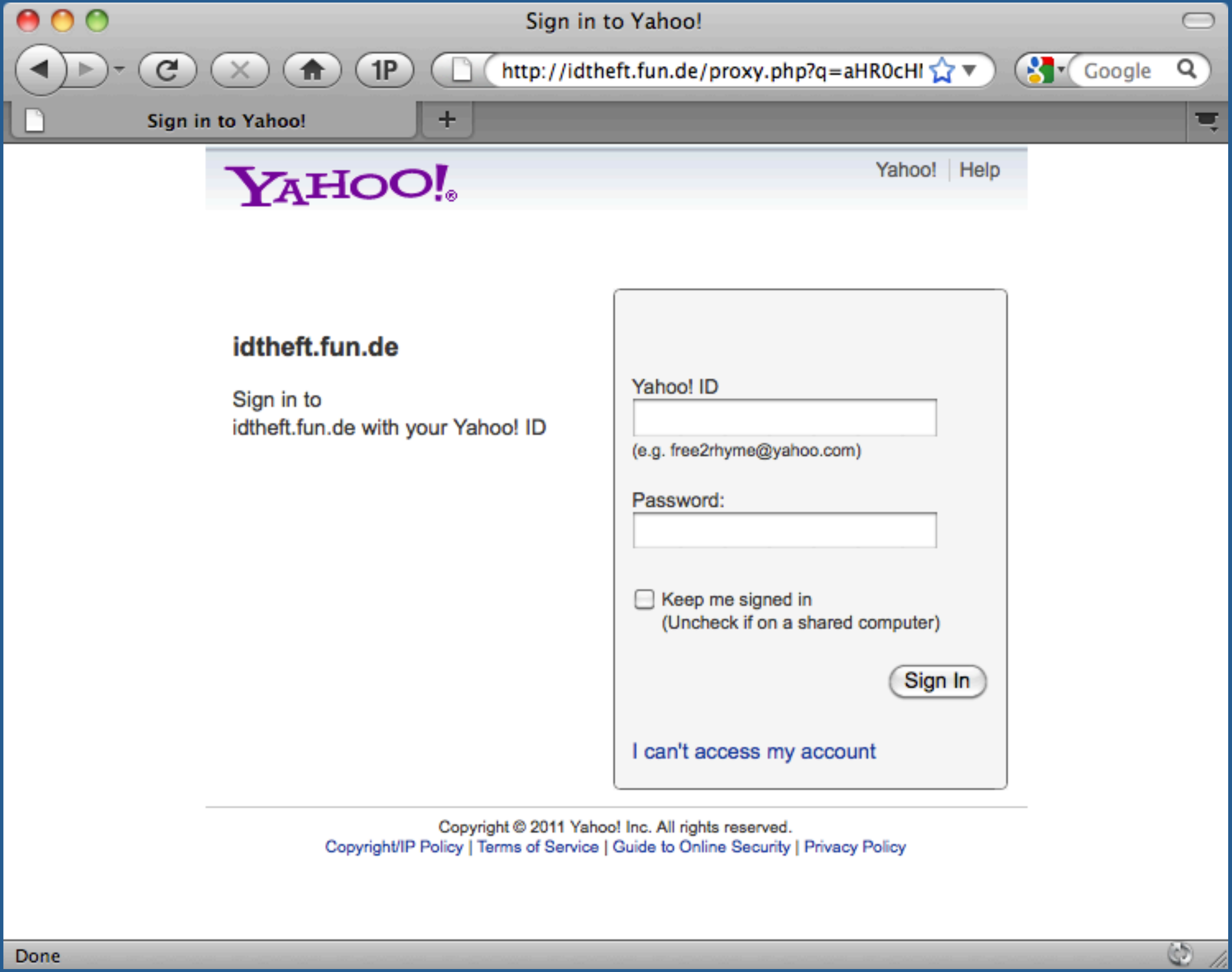
3. log out from all web sites, as on a public computer

study protocol 2/4

4.a browse to idtheft.fun.de and select Yahoo! as the account that you will use for login



study protocol 3/4



Sign in to Yahoo!

http://idtheft.fun.de/proxy.php?q=aHR0cH!

idtheft.fun.de

Sign in to
idtheft.fun.de with your Yahoo! ID

Yahoo! ID

(e.g. free2rhyme@yahoo.com)

Password:

□ Keep me signed in
(Uncheck if on a shared computer)

Sign In

I can't access my account

Copyright © 2011 Yahoo! Inc. All rights reserved.
Copyright/IP Policy | Terms of Service | Guide to Online Security | Privacy Policy

Done

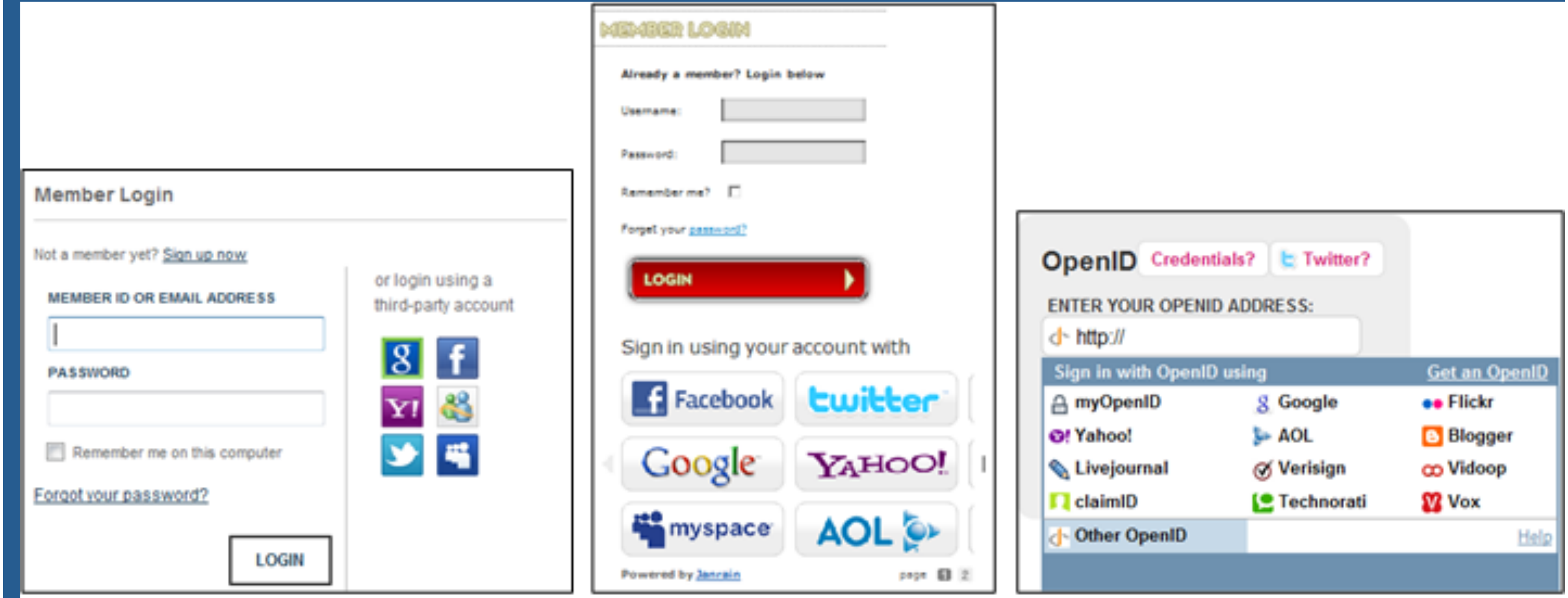
4.b try to find any way to tell that this is NOT the real Yahoo! website

study protocol 4/4

5. exit questionnaire
6. contextual interview

finding 1: incorrect initial mental model

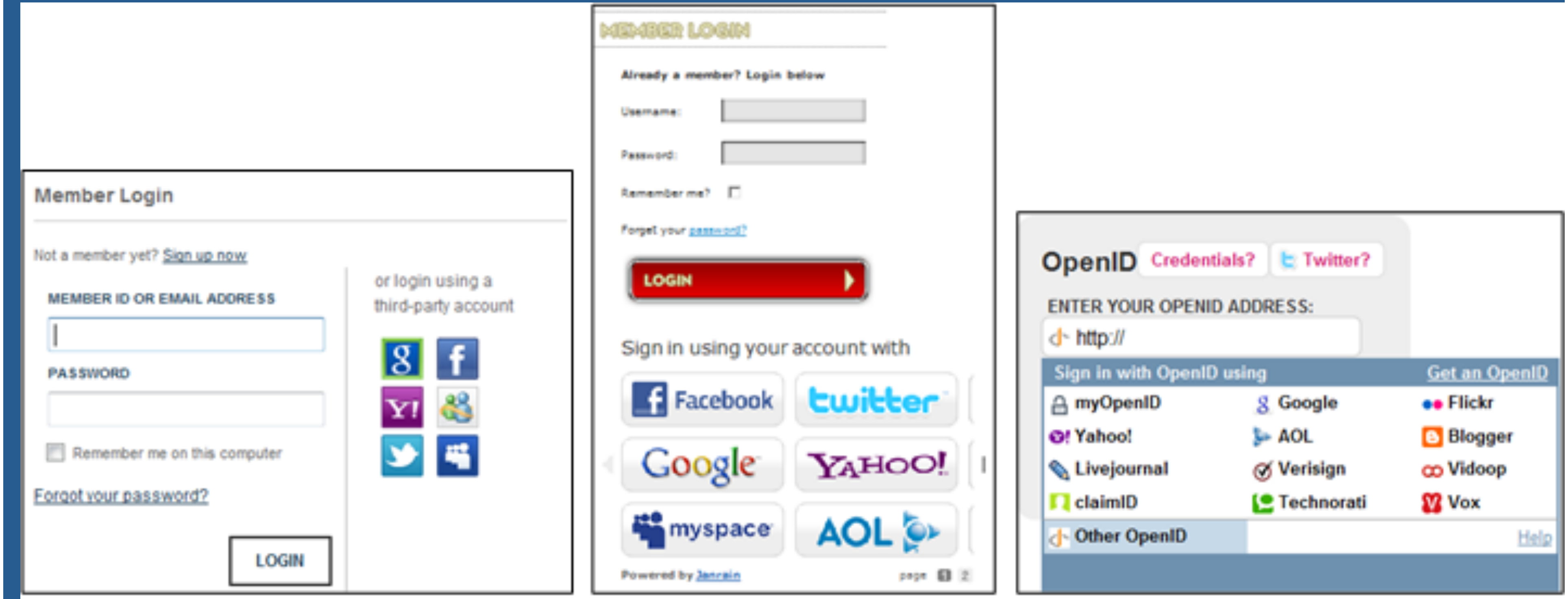
eight entered their IdP credentials directly into the RP's fields on **sign-up**



(a) (b) (c)

finding 2: wrong mental model derived from the login process

5 re-entered their IdP credentials directly into the RP's fields on **sign-in**

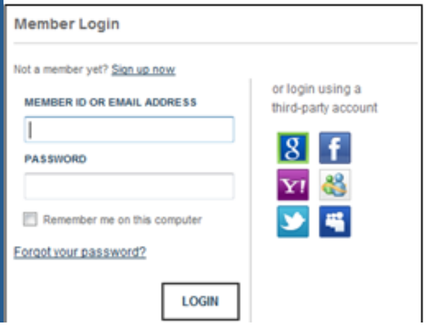


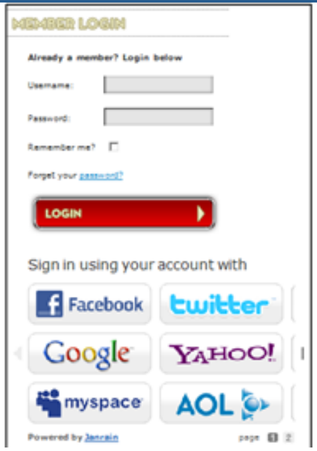
(a) (b) (c)

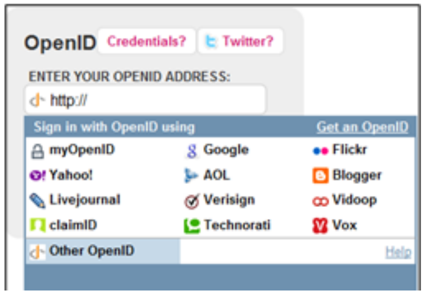
the website must have their Google or Yahoo user name and password already …

finding 3: bad affordance and visibility

1. 8 did not know they needed to click on one of the IdP icons to initiate the login process
2. 3 thought the IdP icons were Ads
3. 2 thought the website had teamed up with the IdPs for content sharing.
4. 2 thought the highlighted IdP icon was a cue for them to enter their Google or Yahoo email and password.


Member Login
Not a member yet? Sign up now
MEMBER ID OR EMAIL ADDRESS
PASSWORD
□ Remember me on this computer
Forgot your password?
LOGIN
or login using a third-party account
Y!





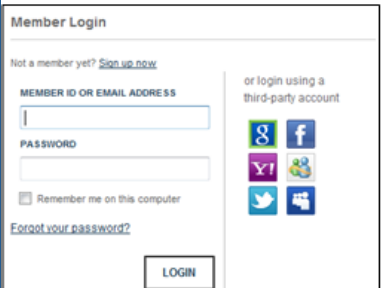
findings 4&5

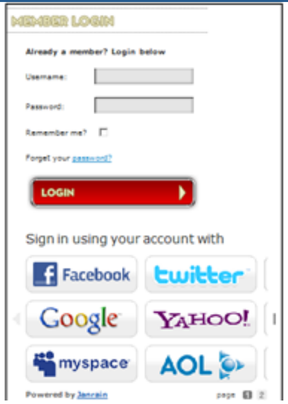
4. **IdP account association is confusing**

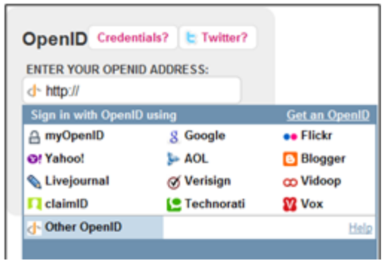
   Most believe that as soon as they were redirected back from the IdP, they were already logged in.

5. **Implicit IdP login concern**

   All were concerned that they had to explicitly log out from their IdP, in addition to the websites.

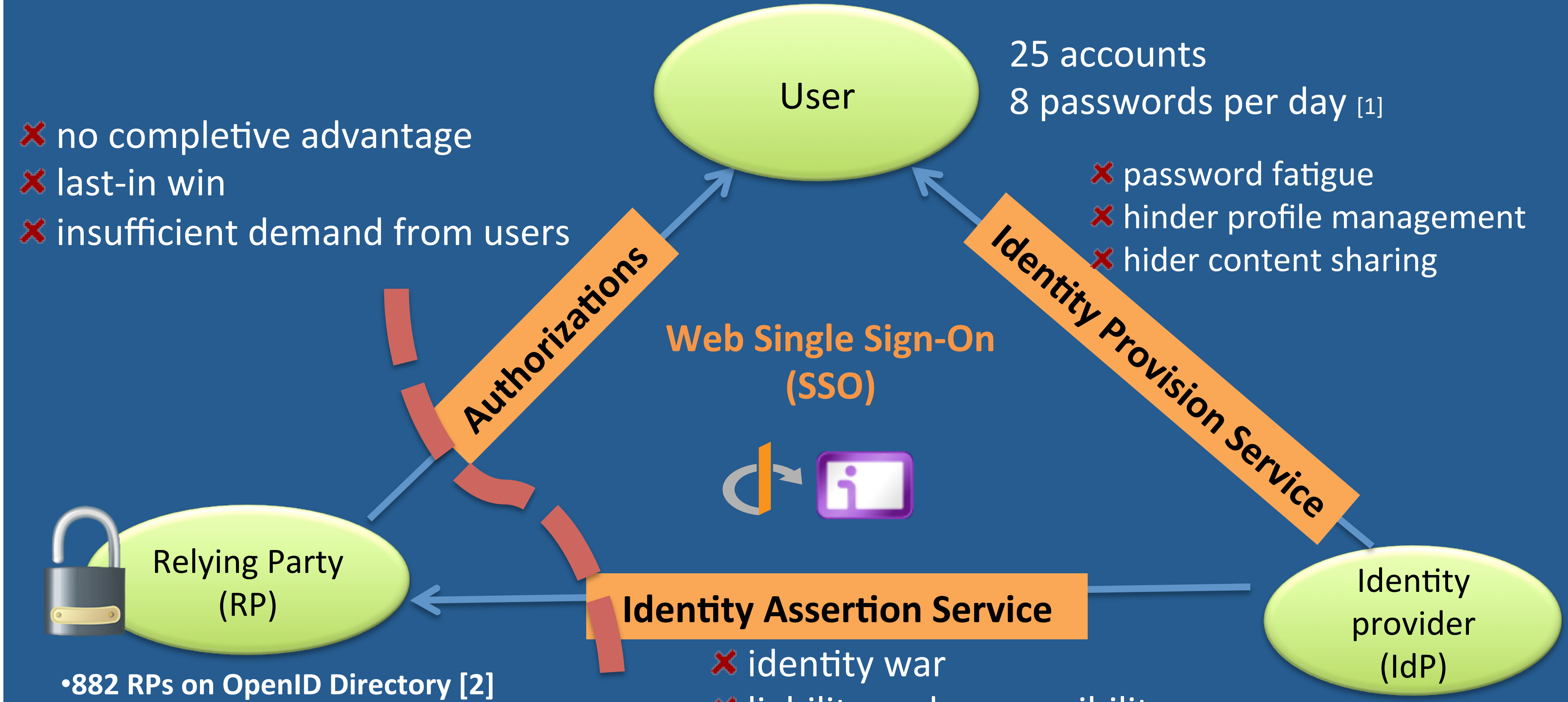

Member Login
Not a member yet? Sign up now
MEMBER ID OR EMAIL ADDRESS
PASSWORD
□ Remember me on this computer
Forgot your password?
LOGIN
or login using a third-party account





BUSINESS CONCERNS

summary



25 accounts
8 passwords per day [1]

- ✗ no completive advantage
- ✗ last-in win
- ✗ insufficient demand from users

- ✗ password fatigue
- ✗ hinder profile management
- ✗ hider content sharing

- ✗ identity war
- ✗ liability and responsibility

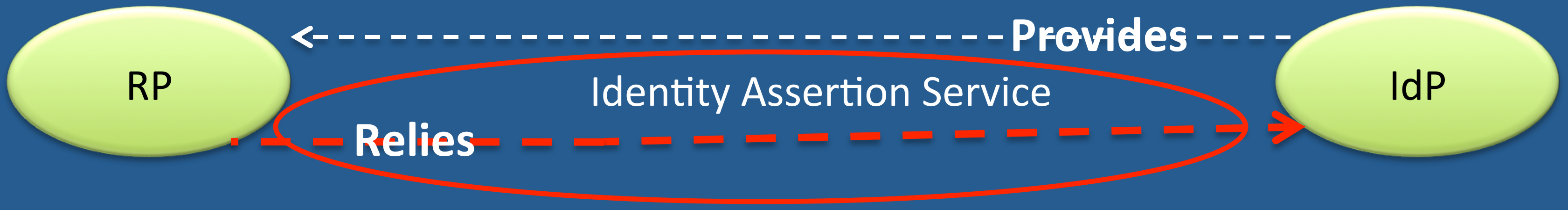
- **•882 RPs on OpenID Directory [2]**
- **•240 RPs on MyOpenID.com Directory [3]**
- **•40,000 claimed by JanRain [4] (no detailed result)**
- **•(< 0.018% of 213,000,000 websites [6])**
- **•InfoCard: almost no RP**

Google, Yahoo, AOL …

one billion keys

[1] D. Florencio and C. Herley. A large-scale study of web password habits. In Proc. of WWW '07, New York, NY, USA, 2007.
[2] OpenID Directory , http://openiddirectory.com/
[3] MyOpenID Directory, https://www.myopenid.com/directory
[4] Replying Party Stats, http://www.janrain.com/blogs/relying-party-stats-april-1st-2009
[5] Alexa Top 500 Global Sites, http://www.alexa.com/topsites/global
[6] August 2010 Web Server Survey, http://news.netcraft.com/archives/category/web-server-survey/

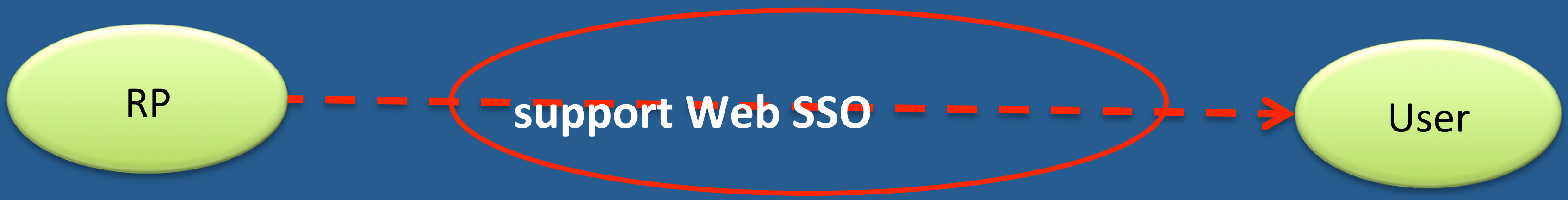
RPs do not want to ***rely on*** IdPs



- ✘ identity war [1] : rely on user data to survive
- ✘ need to trust IdPs [2, 3]
- ✘ RPs are liable and responsible for the loss when IdPs are compromised or unavailable [4]

[1] Phil Becker on Identity's First Big War: a history lesson. http://www.identityblog.com/?p=551
[2] A. Josang, M. A. Zomai, and S. Suriadi. Usability and privacy in identity management architectures. In the Proceedings of ACSW '07.
[3] R. Dhamija and L. Dusseault. The seven flaws of identity management: Usability and security challenges. IEEE Security and Privacy, 6:24-29, 2008.
[4] S. J. Murdoch and R. Anderson. Verified by visa and mastercard securecode: or, how not to design authentication. In Proc of Financial Cryptography and Data Security 2010.

web SSO does not provide RPs with **immediate business returns**



- no competitive advantage [1]
- confusing user experience could turn users away [2, 3, 4]
- rather wait for a critical mass

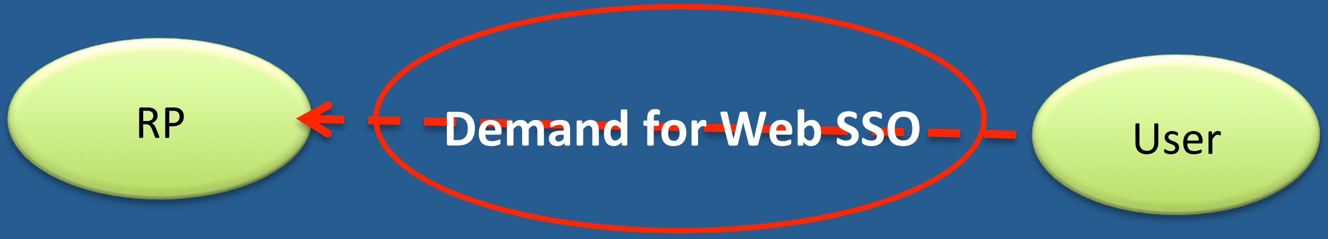
[1] Johannes Ernst. On OpenID's Relying Party Adoption Problem, http://netmesh.info/jernst/digital_identity/on-openids-relying-party-adoption-problem, 2008.

[2] R. Dhamija and L. Dusseault. The seven flaws of identity management: Usability and security challenges. IEEE Security and Privacy, 6:24-29, 2008.

[3] Beverly Freeman. Yahoo! OpenID:One Key, Many Doors. http://developer.yahoo.com/openid/openid-research-jul08.pdf

[4] Eric Sachs. Usability Research on Federated Login. http://sites.google.com/site/oauthgoog/UXFedLogin

insufficient driving force from users



- no urgent need
  - password manager [1]
  - no evidences for insecure password practices [2]
- security
  - single-point of failure [3]
  - phishing attacks [3, 4, 5]
- privacy [6]

Login CSRF	70%
Account CSRF	40%
Login as Attacker	75%
Impersonate	67%
Replay Attack	10%

[1] S. Gaw and E. W. Felten. Password management strategies for online accounts. In Proc. of SOUPS '06

[2] C. Herley. So long, and no thanks for the externalities: the rational rejection of security advice by users. In Proc. of NSPW '09.

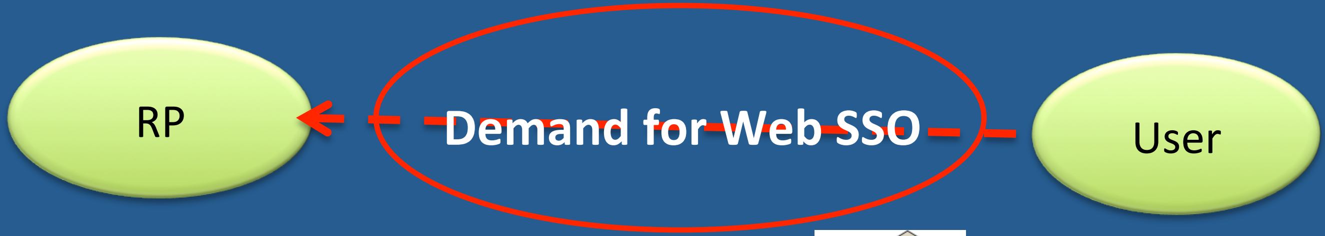
[3] R. Dhamija and L. Dusseault. The seven flaws of identity management: Usability and security challenges. IEEE Security and Privacy, 6:24-29, 2008.

[4] B. Laurie. OpenID Phishing heaven. http://www.links.org/?p=187

[5] C. Messina. OpenID Phishing Brainstorm. http://wiki.openid.net/OpenID Phishing Brainstorm, 2009.

[6] Learning the OpenID problems, http://mateusz.loskot.net/2008/05/14/learning-the-openid-problems/

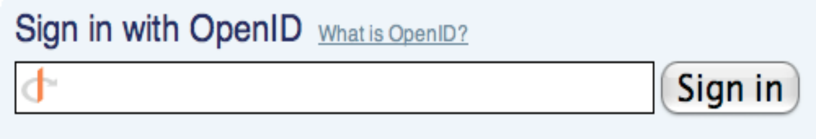
shared-identity sign-on rather than true Web SSO



shared-identity sign-on

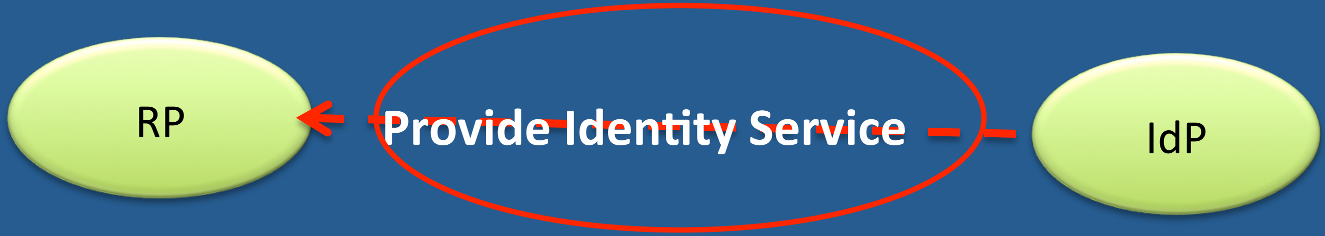
- ✗visit N+1 login UIs
- ✗pick an IdP N ways
- ✗consent N times
- ✗logout N+1 times

N RPs



1 IdP

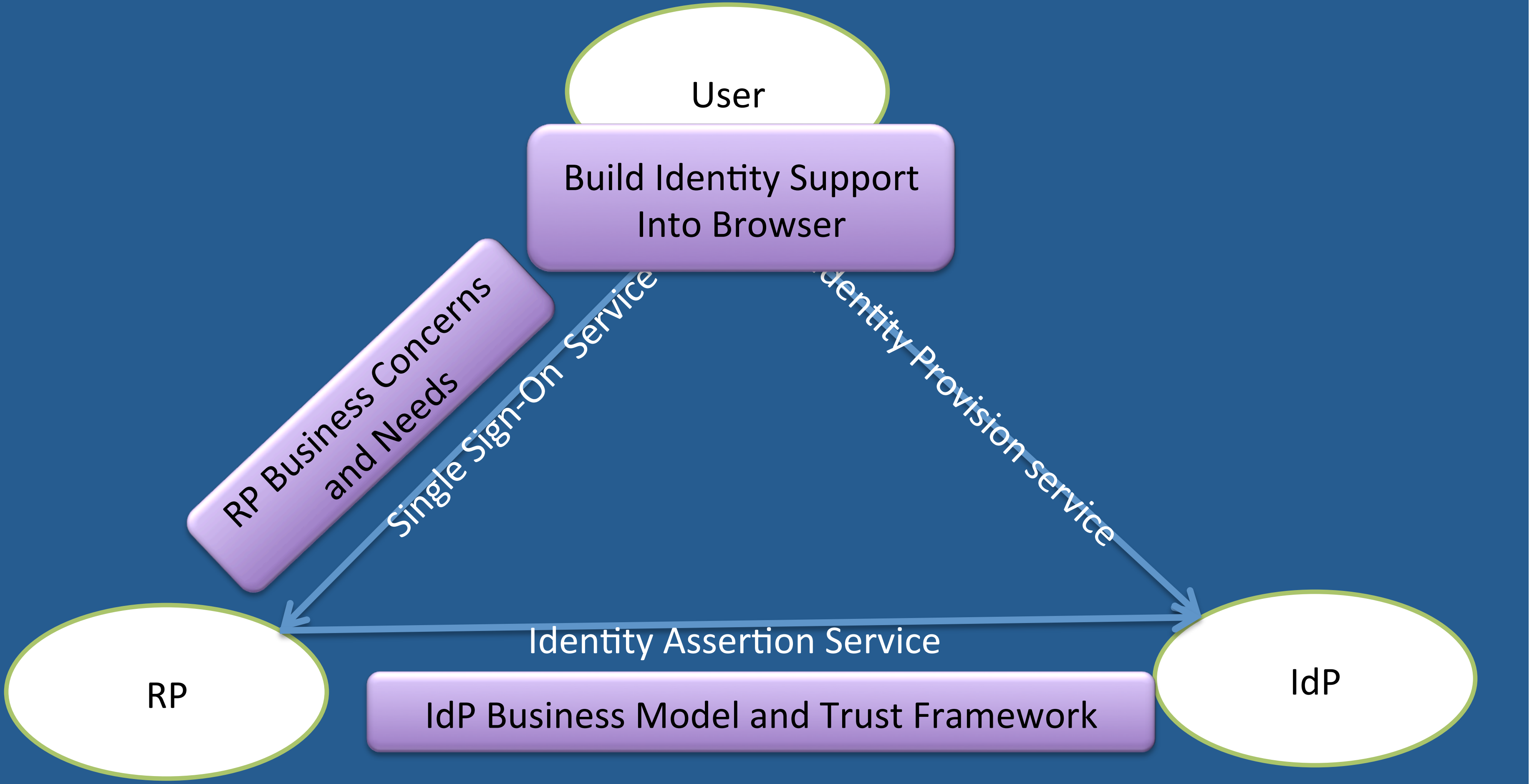
insufficient driving force from IdPs



- ✘ lack of proven business model [1]
- ✘ inherently difficult on the Web [4]
- ✘ people's privacy concerns [2,3]

[1] B. Blakley. The Information Card Landscape. Technical report, Burton Group, Febrary 2009
[2] Spiekermann, S., Cranor, L. F.: Engineering privacy. IEEE Transactions on Software Engineering, pp. 1-42. IEEE 2008.
[3] CBS News. Poll: Privacy rights under attack. http://www.cbsnews.com/stories/2005/09/30/opinion/polls/main894733.shtml, October 2005.
[4] http://en.wikipedia.org/wiki/On_the_Internet,_nobody_knows_you%27re_a_dog

recommendations


User
Build Identity Support Into Browser
RP Business Concerns and Needs
Single Sign-On Service
Identity Provision service
Identity Assertion Service
RP
IdP Business Model and Trust Framework
IdP

recommendation 1: understand RPs' business concerns

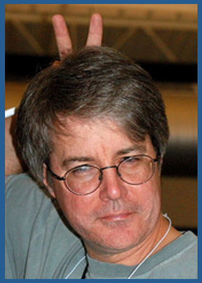
- Identity technology grew within corporation
  - reduces operational cost and streamline users' login experience
  - only needs cost justification but no business concerns
- Web SSO requires RPs to give up control over their users
  - users are important assets
  - **raises significant business concerns**

recommendation 1:
address RPs' business concerns

- **business needs**: How can Web SSO help RPs increase their revenue and serve their customers better?
- **liability and laws**: When IdPs fail, who is liable? Who should be called when customer support is needed?
- **terms and quality of service requirements for identity services**: How should RPs define and validate the accuracy of identity information?
- **models for monetizing identity services**: How and how much should RPs pay for the identity services provided by IdPs?
- **usability and user acceptance**: How can users be provided with consistent and usable login experiences?
- **privacy**: What are users' privacy concerns? How can RPs protect their privacy?

recommendation 2: identify IdP business models and build trust frameworks

- example: ***meta-identity*** service as a business model and a way to reduce privacy risks [1]



  - Bob's age over 18 vs. Bob is 51
  - clean credit history vs. credit history list
- example: Open Identity Exchange (Mar. 2010) [2]
  - trust framework: a certification program that enables a RP to trust the identity, security, and privacy policies of IdP
  - build trust in the exchange of online identity credentials across public and private sectors

[1 B. Blakley. The meta-identity system. http://notabob.blogspot.com/2006/07/meta-identity-system.html, July 2006.
[2] Open Identity Exchange. Building trust online identity. http://openidentityexchange.org/, March 2010.

summary of the issues

- technical issues
  - lack of binding between browser session, login form, authentication request and response lead to SSO and login CSRF, and replay vulnerabilities.
- human issues:
  - mental models for OpenID login-in are inadequate,
  - confusing association between IdP's and RP's accounts,
  - concerns about logout, privacy concerns
- business issues:
  - lack of business drivers for adoption
  - RPs are liable for IdPs' misbehavior but RPs don't trust IdPs
  - last-in wins, no competitive advantage
  - shared identity rather than SSO

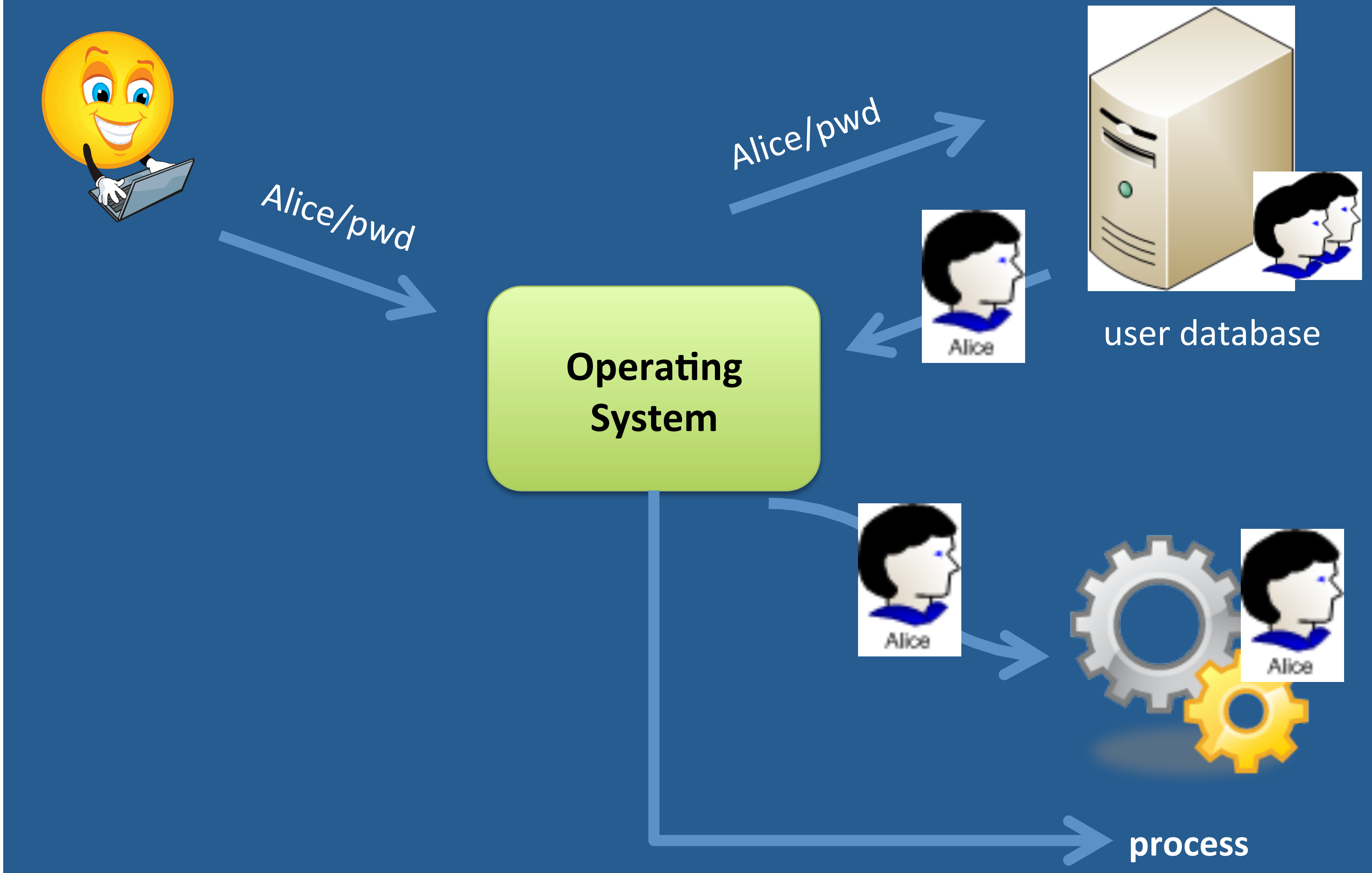
identity-enabled browser

- consistent and intuitive user experience
- raise the awareness of Web SSO
- acts as a platform for leveraging user data from IdPs to RPs
- shift shared-identity sign-on to true Web SSO
  - ✓visit 1 login UI
  - ✓gains access to all websites that she has an account
  - ✓logout 1 time

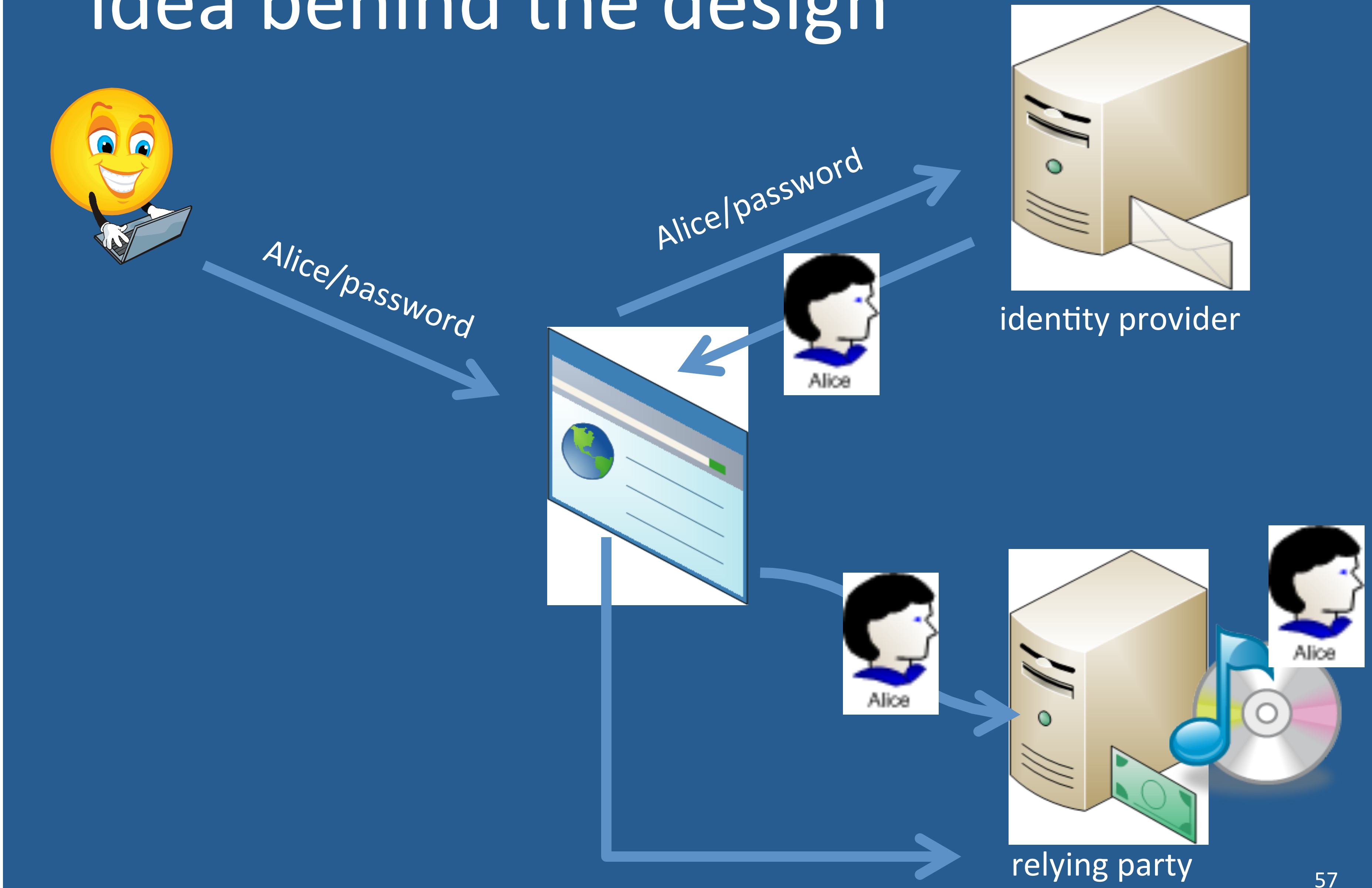
design considerations

- usable by average web users
- leverage one-billion existing OpenID-enabled keys
- should not require RPs to modify their login UI
- readily employable for emerging Web 2.0 applications
- should avoid relying on users' cognitive capability to detect phishing sites [1,2,3]
- must be secure in untrusted environments
  - compromised users' computers
  - malicious content and service providers
  - network traffic sniffing and modification

metaphor identity flow in OS



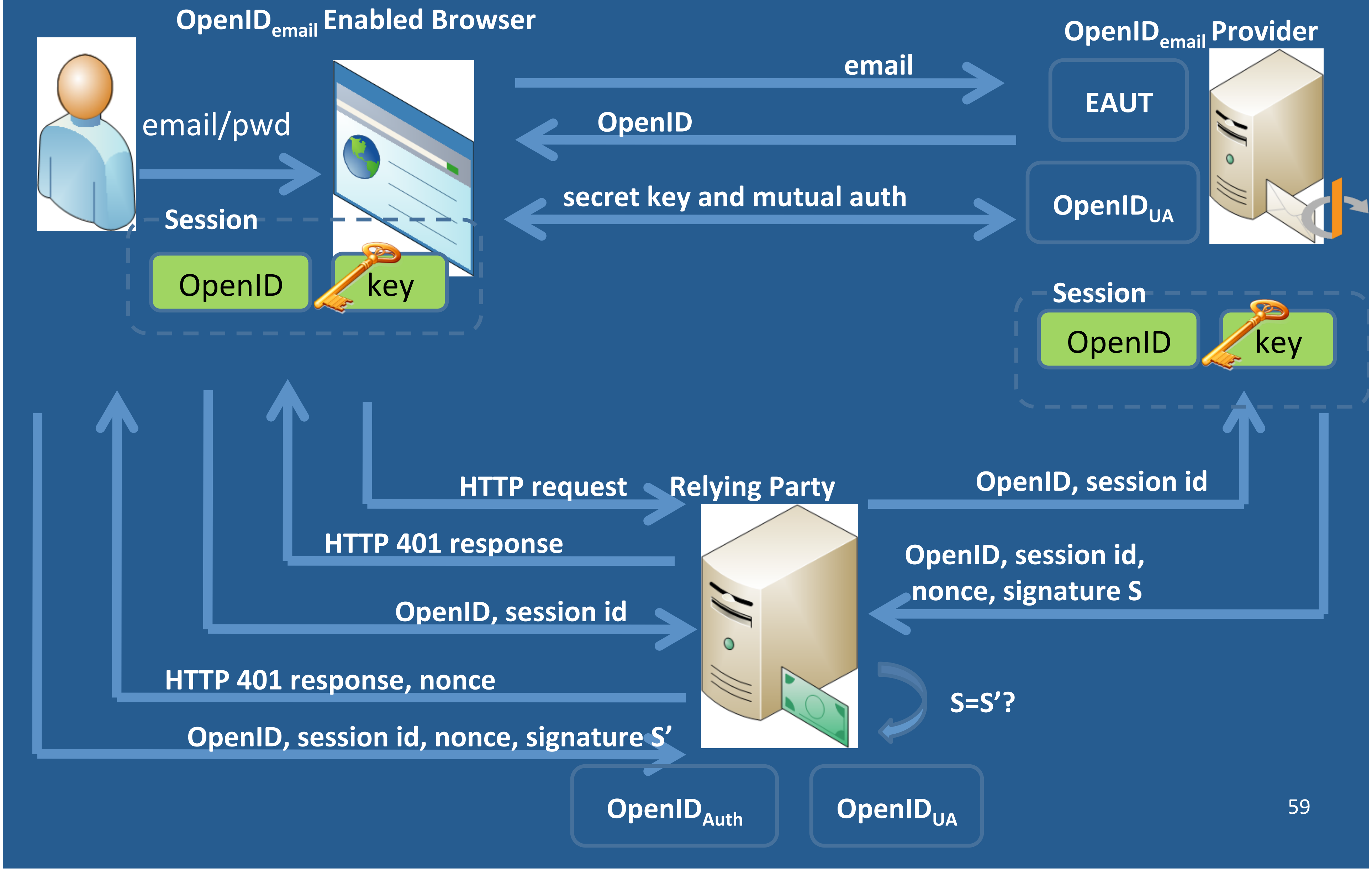
idea behind the design



approach

- builds OpenID support right into web browsers
- hides OpenID identifiers from users through the use of their existing email accounts
- extends the OpenID protocol to perform authentication directly with user-agents such as browsers (**OpenID$_{ua}$ extension**)
- introduces a new HTTP access authentication scheme to convey authenticated identities automatically into websites that support OpenID for authentication (**OpenIDAuth**)

architecture and data flows



$\text{OpenID}_{\text{email}}$ Enabled Browser
email/pwd
Session
OpenID
key
email
OpenID
secret key and mutual auth
$\text{OpenID}_{\text{email}}$ Provider
EAUT
$\text{OpenID}_{\text{UA}}$
Session
OpenID
key
HTTP request
Relying Party
OpenID, session id
HTTP 401 response
OpenID, session id,
nonce, signature S
OpenID, session id
HTTP 401 response, nonce
S=S'?
OpenID, session id, nonce, signature S'
$\text{OpenID}_{\text{Auth}}$
$\text{OpenID}_{\text{UA}}$

related project publications

- S. Sun, E. Pospisil, I. Muslukhov, N. Dindar, K. Hawkey, K. Beznosov. **OpenID-Enabled Browser: Towards Usable and Secure Web Single Sign-On. CHI Work-in-Progress**, May 7-11 2011, Vancouver BC, Canada. http://lersse-dl.ece.ubc.ca/record/251

- S. Sun, K. Hawkey, K. Beznosov. **OpenIDemail Enabled Browser: Towards Fixing the Broken Web Single Sign-On Triangle**. In Proceedings of the **ACM Workshop on Digital Identity Management (DIM)**, October 8 2010. http://portal.acm.org/citation.cfm?doid=1866855.1866868

- S. Sun, Y. Boshmaf, K. Hawkey, K. Beznosov. **A Billion Keys, but Few Locks: The Crisis of Web Single Sign-On**. In Proceedings of the **New Security Paradigms Workshop (NSPW)**, September 20-22, 2010. http://portal.acm.org/citation.cfm?doid=1900546.1900556

- S. Sun, K. Hawkey, K. Beznosov. **Secure Web 2.0 content sharing beyond walled gardens**. In Proceedings of the 25th **Annual Computer Security Applications Conference (ACSAC)**, pages 409-418, December 2009. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5380698

- S. Sun, K. Hawkey, K. Beznosov, **Towards Enabling Web 2.0 Content Sharing beyond Walled Gardens**, CSE, vol. 4, pp.979-984, **International Conference on Computational Science and Engineering**, 2009. http://www.computer.org/portal/web/csdl/doi/10.1109/CSE.2009.162

- S. Sun and K. Beznosov. **Open problems in Web 2.0 user content sharing**. In Proceedings of the **iNetSec Workshop**, pages 37-51, Zurich, Switzerland, April 23 2009. http://www.springerlink.com/content/an755ut08l63r965/

San-Tsai Sun

Dr. Kirstie Hawkey

lersse.ece.ubc.ca

Konstantin (Kosta) Beznosov

konstantin.beznosov.net