Password Managers, Single Sign-On, Federated ID: Have users signed up?

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

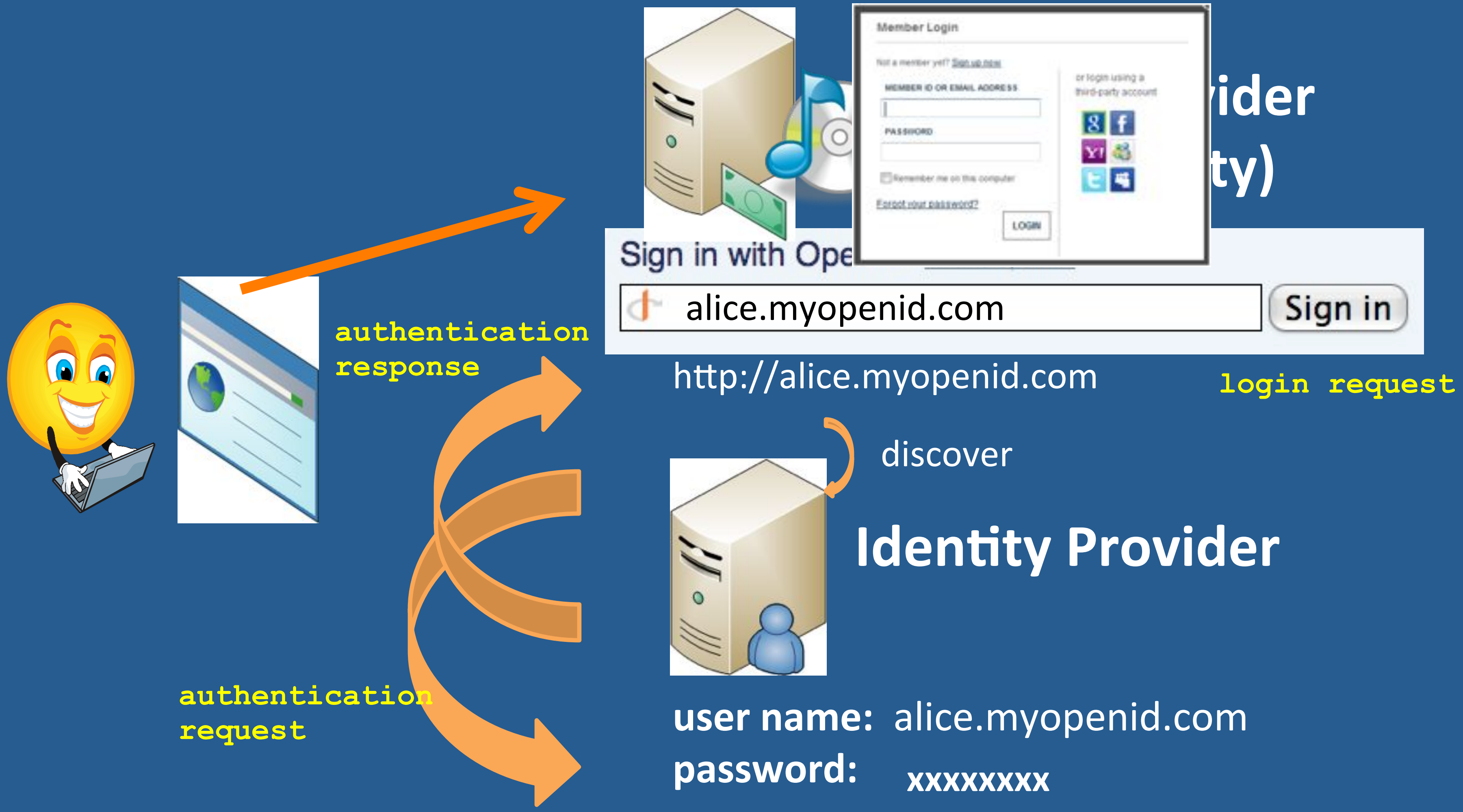
Open ID

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

vider

ty)

Sign in with Ope

alice.myopenid.com

Sign in

http://alice.myopenid.com

Identity Provider

user name: alice.myopenid.com

password: xxxxxxxx

HAVE USERS SIGNED UP?

NO

WHY HAVE NOT USERS SIGNED UP?

BECAUSE THEY CAN!

ha-ha!

if we really want to know, then why not to ask users?

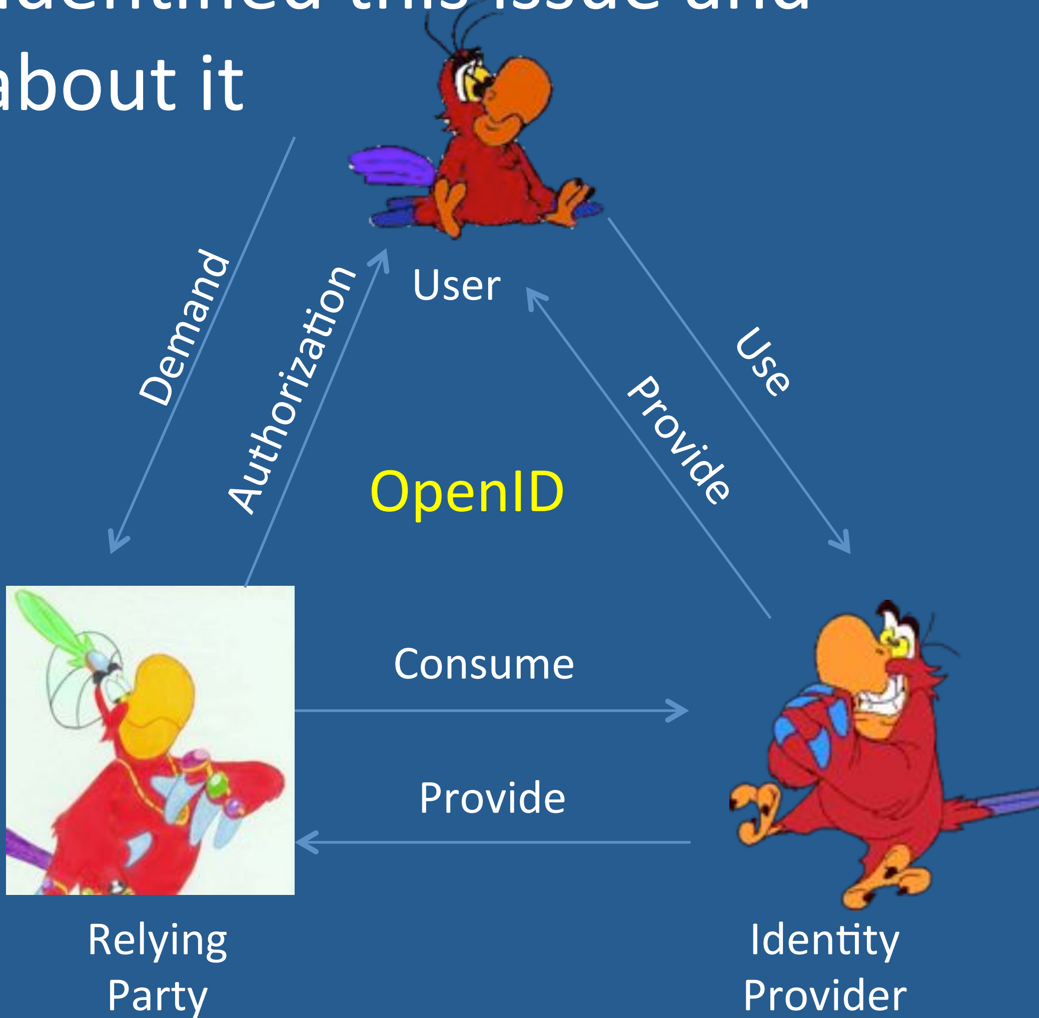
interviews with 51 participants

no perceived urgent need for Web SSO

- most are “comfortable” with weak or reused password
- 23% used the password manager feature in the browse

single-point of failure concern

- 26% of participants identified this issue and expressed concern about it



User

Demand

Authorization

Use

Provide

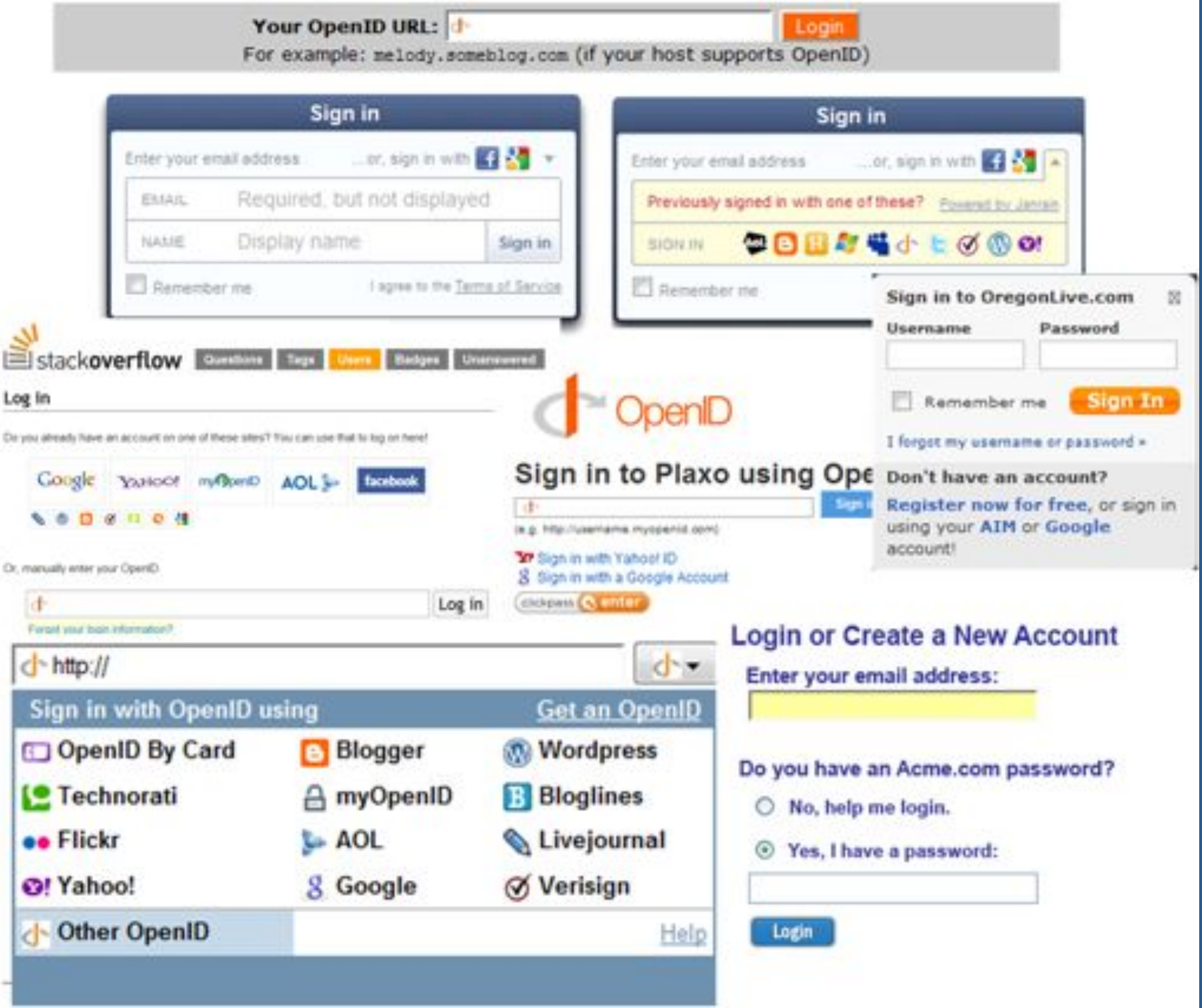
OpenID

Consume

Provide

Relying Party

Identity Provider



Your OpenID URL: Login
For example: melody.someblog.com (if your host supports OpenID)

Sign in

Enter your email address ...or, sign in with

EMAIL Required, but not displayed

NAME Display name Sign in

□ Remember me I agree to the Terms of Service

Sign in

Enter your email address ...or, sign in with

Previously signed in with one of these? Powered by Janrain

SIGN IN

□ Remember me

Sign in to OregonLive.com

Username Password

□ Remember me Sign In

I forgot my username or password »

Don't have an account?

Register now for free, or sign in using your AIM or Google account!

stackoverflow Questions Tags Users Badges Unanswered

Log In

Do you already have an account on one of these sites? You can use that to log on here!

Google Yahoo! myOpenID AOL facebook

Or, manually enter your OpenID

Log in

Forgot your login information?

OpenID

Sign in to Plaxo using Ope

Sign i

(e.g. http://username.myopenid.com)

Sign in with Yahoo! ID

Sign in with a Google Account

clickpass enter

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

Login or Create a New Account

Enter your email address:

Do you have an Acme.com password?

○ No, help me login.

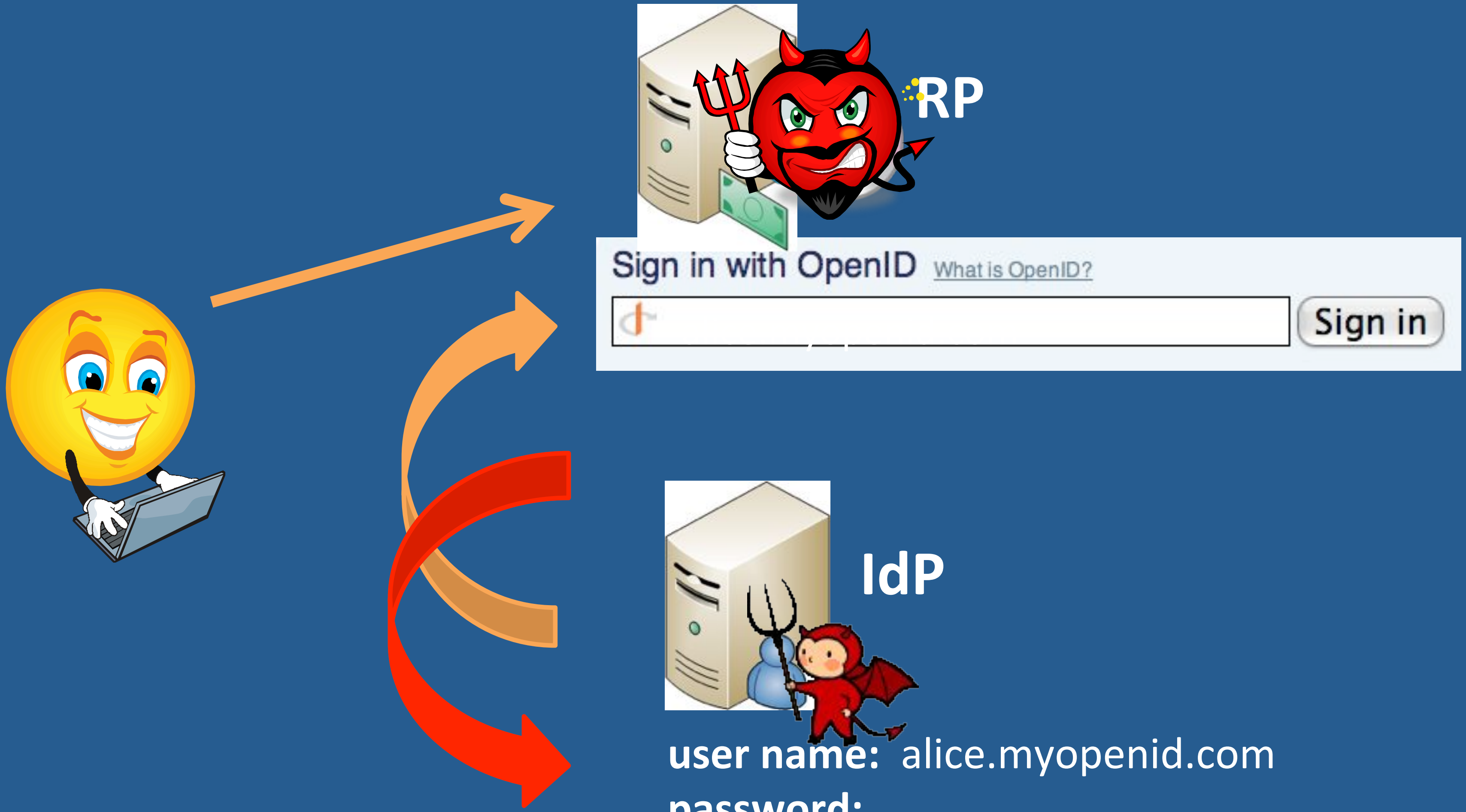
● Yes, I have a password:

Login

security misconceptions and incorrect mental models

- majority thought they were giving their user name and password to the RP websites directly
- some had the impression that their user name and password were stored on the local computer

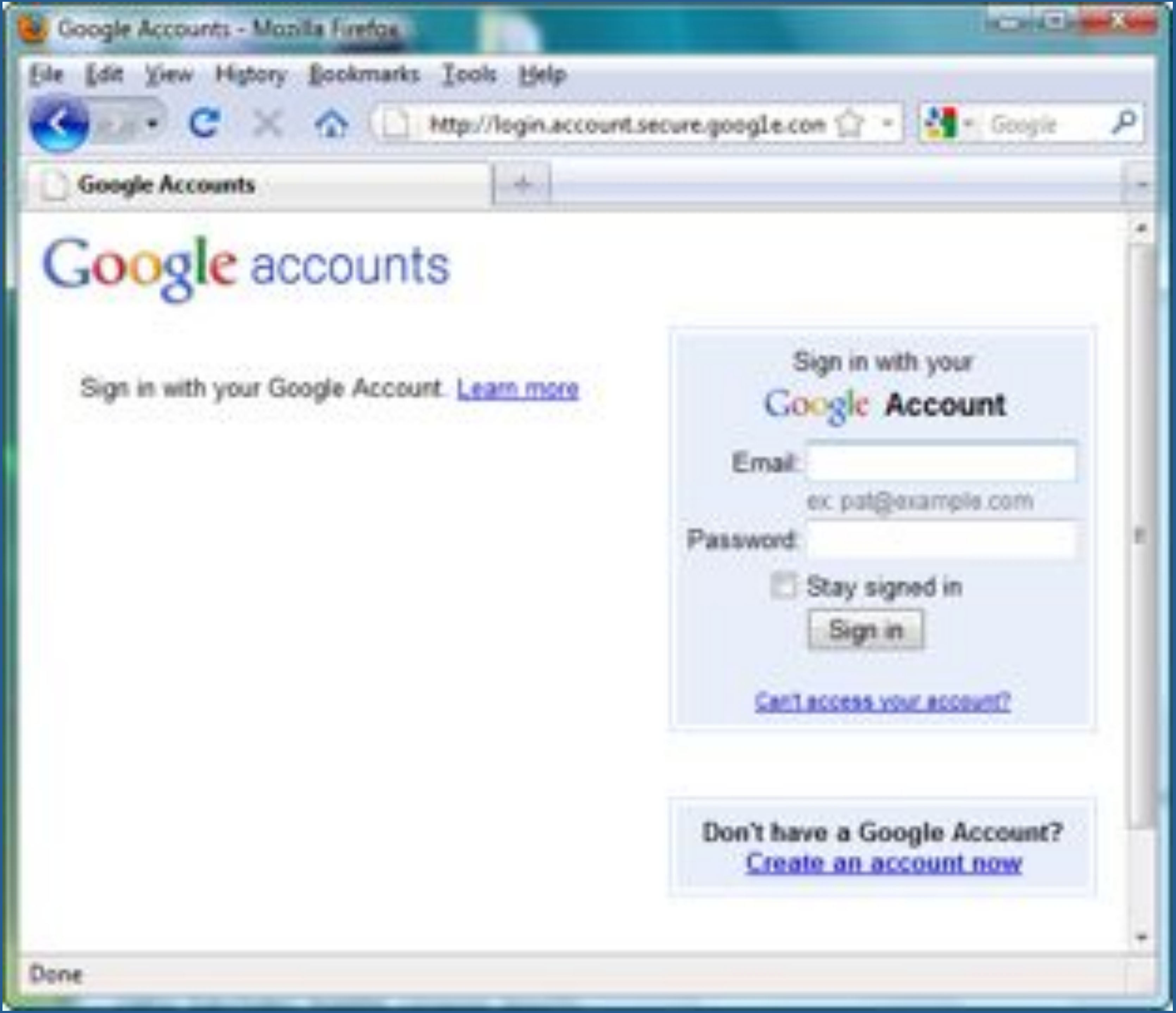
password phishing attacks



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.



http://login.account.secure.google.com

Google accounts

Sign in with your Google Account. Learn more

Sign in with your Google Account

Email:

ex: pat@example.com

Password:

□ Stay signed in

Can't access your account?

Don't have a Google Account?
Create an account now

phishing concerns

- once informed, all expressed great concerns about IdP phishing attacks
- even when prompted, half couldn't find any distinguishing features on a phishing login form

privacy concerns

- 40% were hesitant to consent to the release of personal profile information when prompted by the RP
- 26% requested and were provided with an anonymous OpenID account for the study

lack of user trust

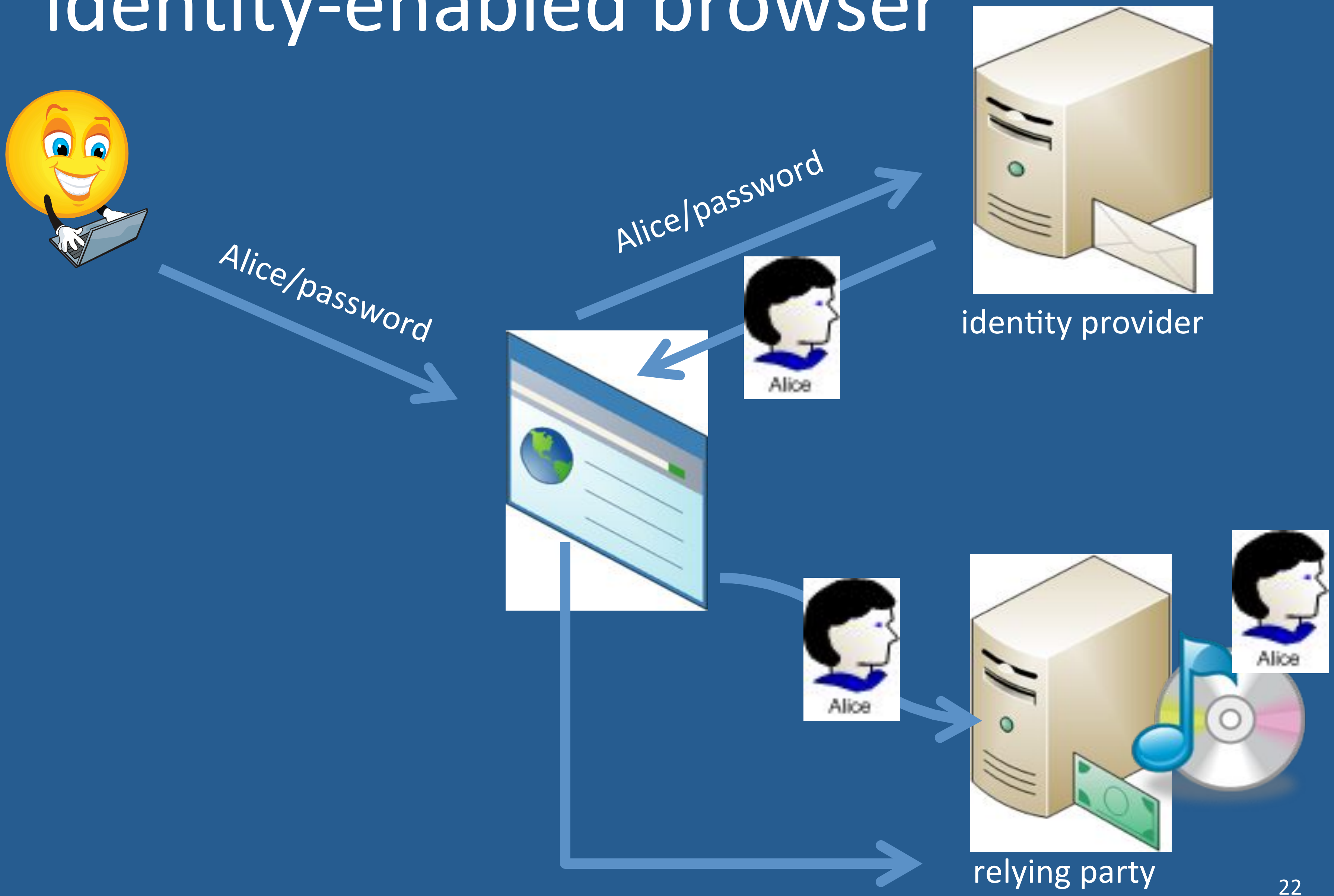
- 36% stated that they would not use SSO on websites that contain valuable personal information or involve potential monetary loss (e.g., banking, stock websites)
- many stated they would not use a Web SSO system on websites which they do not believe to be trustworthy or are not familiar with

account linking

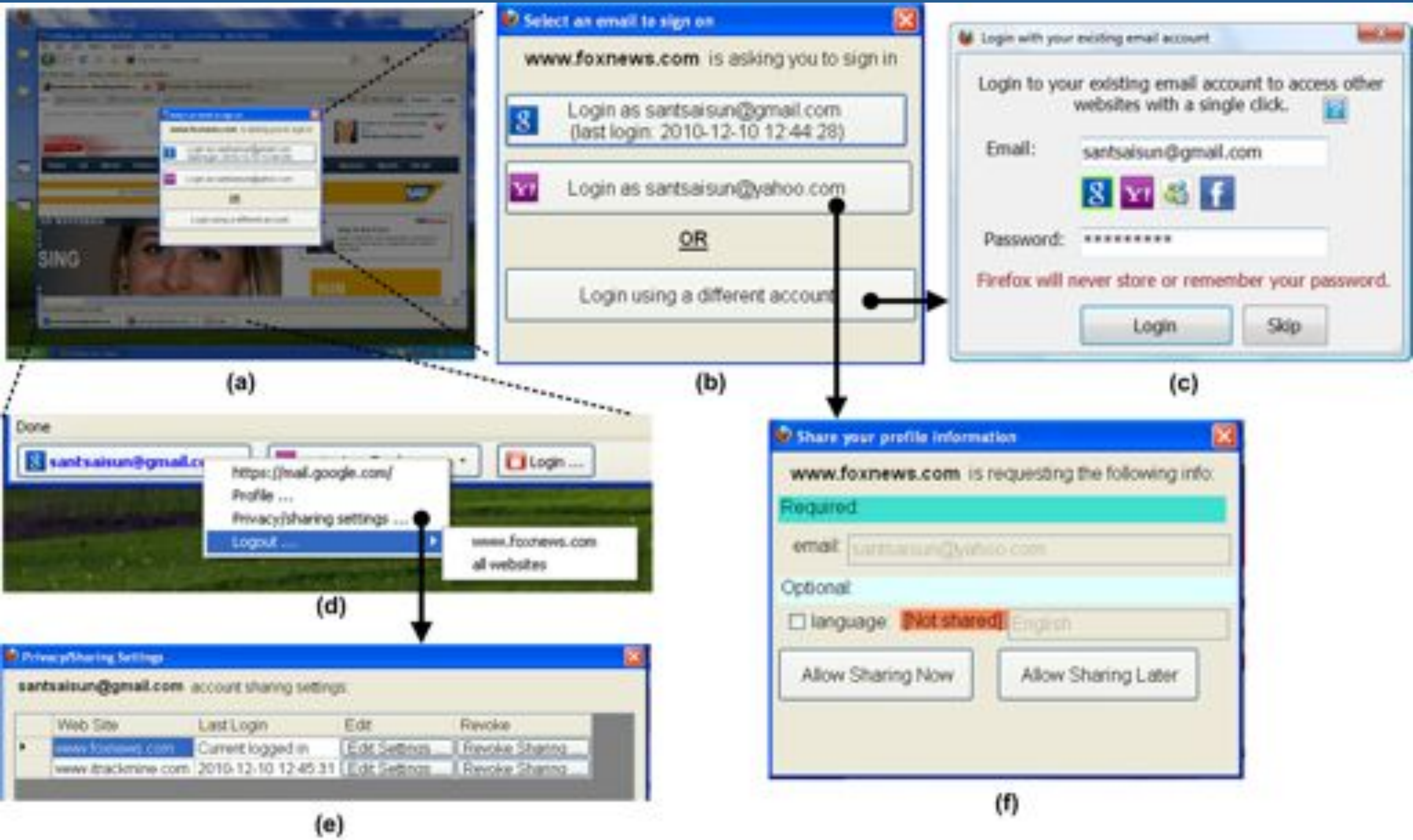
- most did not understand the purpose and concept of account linking
- they became confused and frustrated when they were prompted to create or associate an account on the RP website

ANY IDEAS?

identity-enabled browser



UI consistent across sites



(a)

Select an email to sign on

www.foxnews.com is asking you to sign in

Login as santsaisun@gmail.com (last login: 2010-12-10 12:44:28)

Login as santsaisun@yahoo.com

OR

Login using a different account

(b)

Login with your existing email account

Login to your existing email account to access other websites with a single click.

Email: santsaisun@gmail.com

Password: **********

Firefox will never store or remember your password.

Login | Skip

(c)

Done

santsaisun@gmail.co

Login ...

https://mail.google.com/

Profile ...

Privacy/sharing settings ...

Logout ...

www.foxnews.com

all websites

(d)

Privacy/Sharing Settings

santsaisun@gmail.com account sharing settings

Web Site	Last Login	Edit	Revoke
www.foxnews.com	Current logged in	Edit Settings	Revoke Sharing
www.itrackmine.com	2010-12-10 12:45:31	Edit Settings	Revoke Sharing

(e)

Share your profile information

www.foxnews.com is requesting the following info:

Required

email: santsaisun@yahoo.com

Optional

□ language [Not shared] English

Allow Sharing Now | Allow Sharing Later

(f)