University of British Columbia

Case Study: Security and Usability of Web Single Sign-On Systems

San-Tsai Sun

- uncovering novel vulnerabilities
- designing usable and practical countermeasures

- **PhD candidate**: web security
- **architect/consultant**: Web-based software and security engineering
- **certified instructor**: Microsoft, Sun Java, Trend Micro
- **web technology evangelist**: MVP, MSDN Regional Director Taiwan, TechED, DevDays, PDC, Java Two

outline

- **background and overview**
- Case 1: OpenID 2.0 security analysis
- Case 2: OAuth 2.0 security analysis
- Case 3: web SSO usability study

security design principles

1. Least Privilege
2. Fail-Safe Defaults
3. Economy of Mechanism
4. Complete Mediation
5. Open Design
6. Separation of Duty
7. Least Common Mechanism
8. Psychological Acceptability
9. Defense in depth
10. Question assumptions

usable security design principles

1. Path of Least Resistance
2. Active Authorization
3. Revocability
4. Visibility
5. Self-Awareness
6. Trusted Path
7. Expressiveness
8. Relevant Boundaries
9. Identifiability
10. Foresight

Professional Ajax

Author: Nicholas C. Zakas·Jeremy McPeak·Joe Fawcett

To get inside C#, Microsoft's new OO programming language, use A Preview of C# as a guide. It offers a preview of Visual Studio.NET and an overview of the .NET framework, and demonstrates how C# is integrated with ASP+, ADO+, and COM+ in .NET applications. You'll get examples of C# in action, too.

more

Windows Presentation Foundation

Author: Adam Nathan·Daniel Lehenbauer

Filling an important spot in the Wrox Programmer to Programmer series, Beginning Active Server Pages 3.0 is an excellent introduction to the new version of ASP released for the Windows 2000 platform. This guide expects no previous ASP knowledge or even previous Web development experience.

more

Microsoft .NET Framework 2.0 Windows Client

Author: Tony Northrup·Matthew A. Stoecker·Steven J. Stein

Use this book to build a robust infrastructure for powerful Web sites. Master programmers who write for Web Techniques, Dr. Dobb's Journal, Interactivity, Data Base Management Systems, Network, and Software Development have joined forces to tackle the latest round of web programming puzzles for you.

more

Red Hat Enterprise Linux 5

Author: Tony Northrup

Allaires ColdFusion is a powerful solution for developers wanting to build secure, scalable, and manageable Web applications. ColdFusion Fast & Easy Web Development takes a visual approach to learning this Web application server.

more

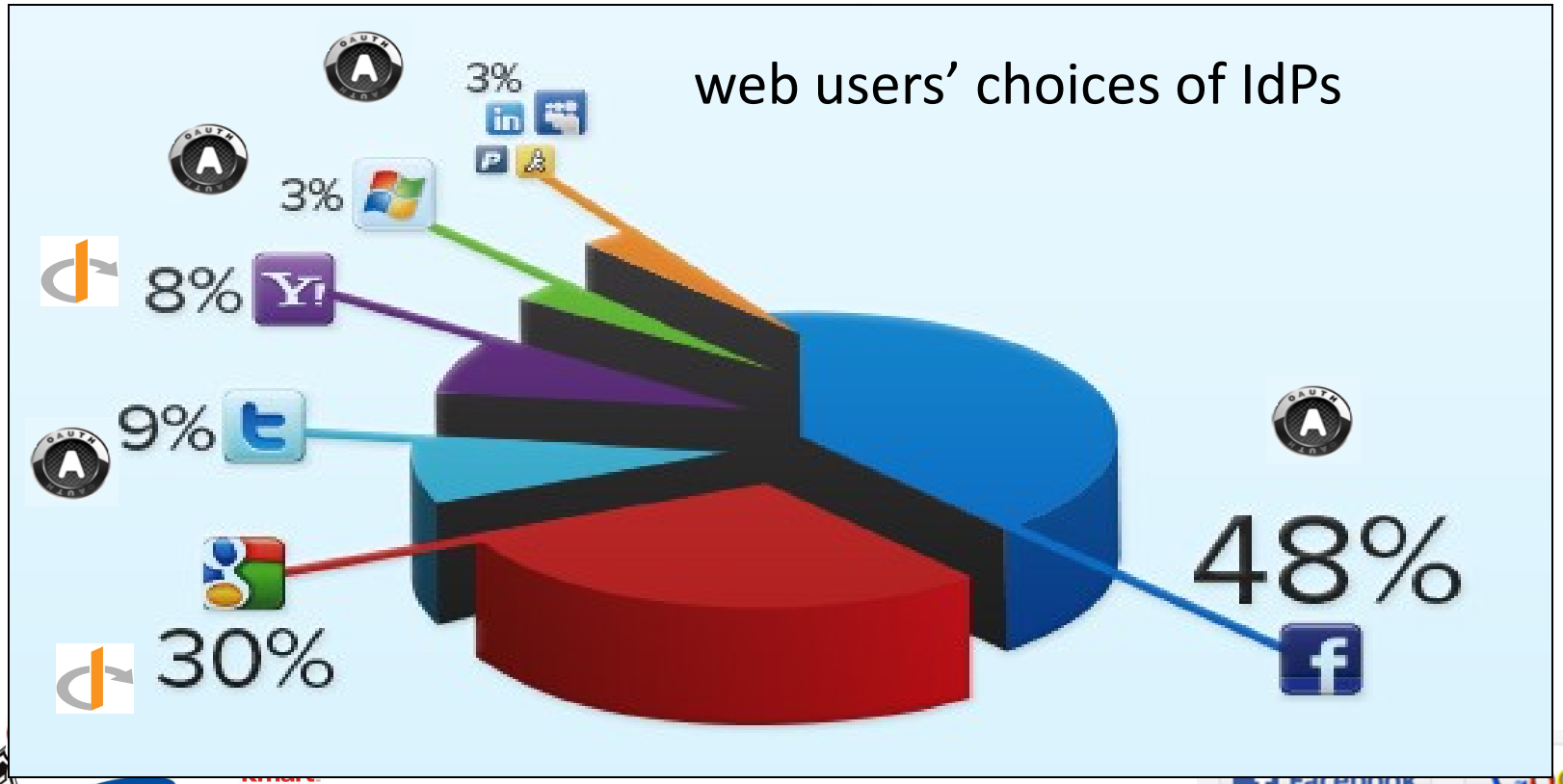
traditional site-centric architecture

25 accounts
8 passwords per day [1]

✘ password fatigue
✘ insecure password practices

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

OpenID and OAuth-based web single sign-on (SSO) systems



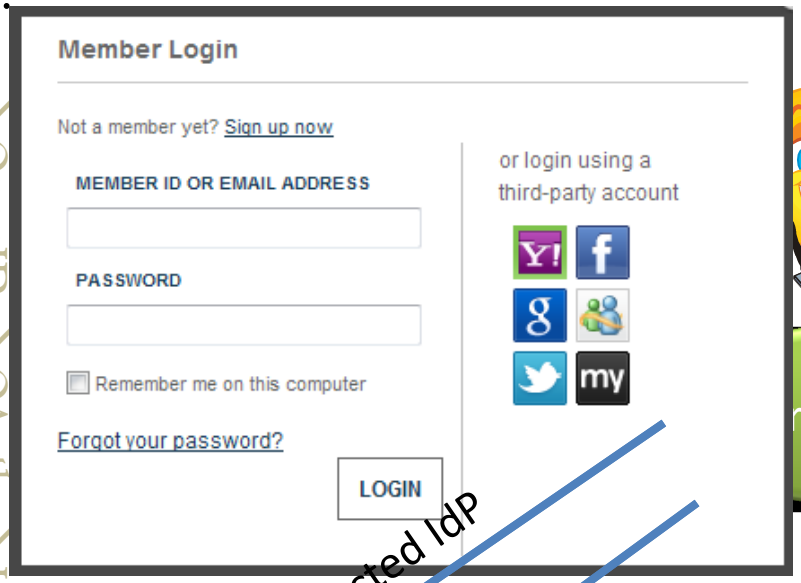
source: jainrain

Relying Party (RP)

Identity provider (IdP)

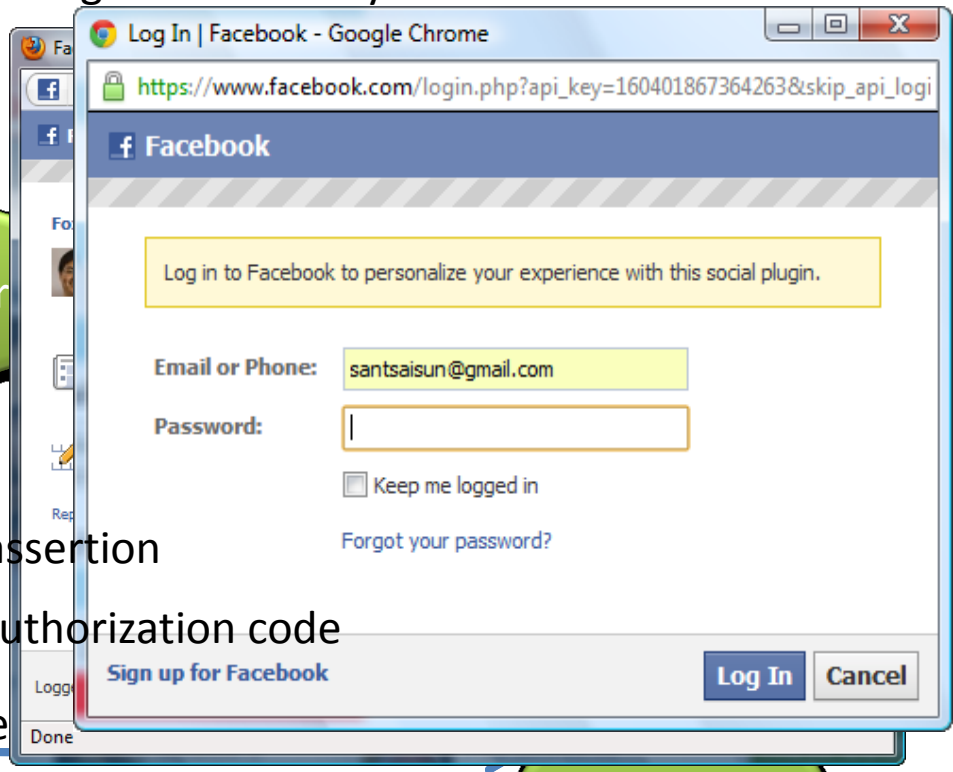
[1] http://janrain.com/blog/social-login-and-social-sharing-trends-across-the-web-for-q2-of-2012/

how OpenID and OAuth SSO works



skip authorization if granted already

skip authentication if user has logged into the IdP in the same browser



selected IdP

OpenID: attribute assertion

OAuth: access token or authorization code

OpenID: (optional) Diffie

RP

IdP

authz. code and app. secret

access token

API +access token

user profile

OAuth RP-to-IdP registration: unique app ID/secret key

challenges, assumptions, overall approach

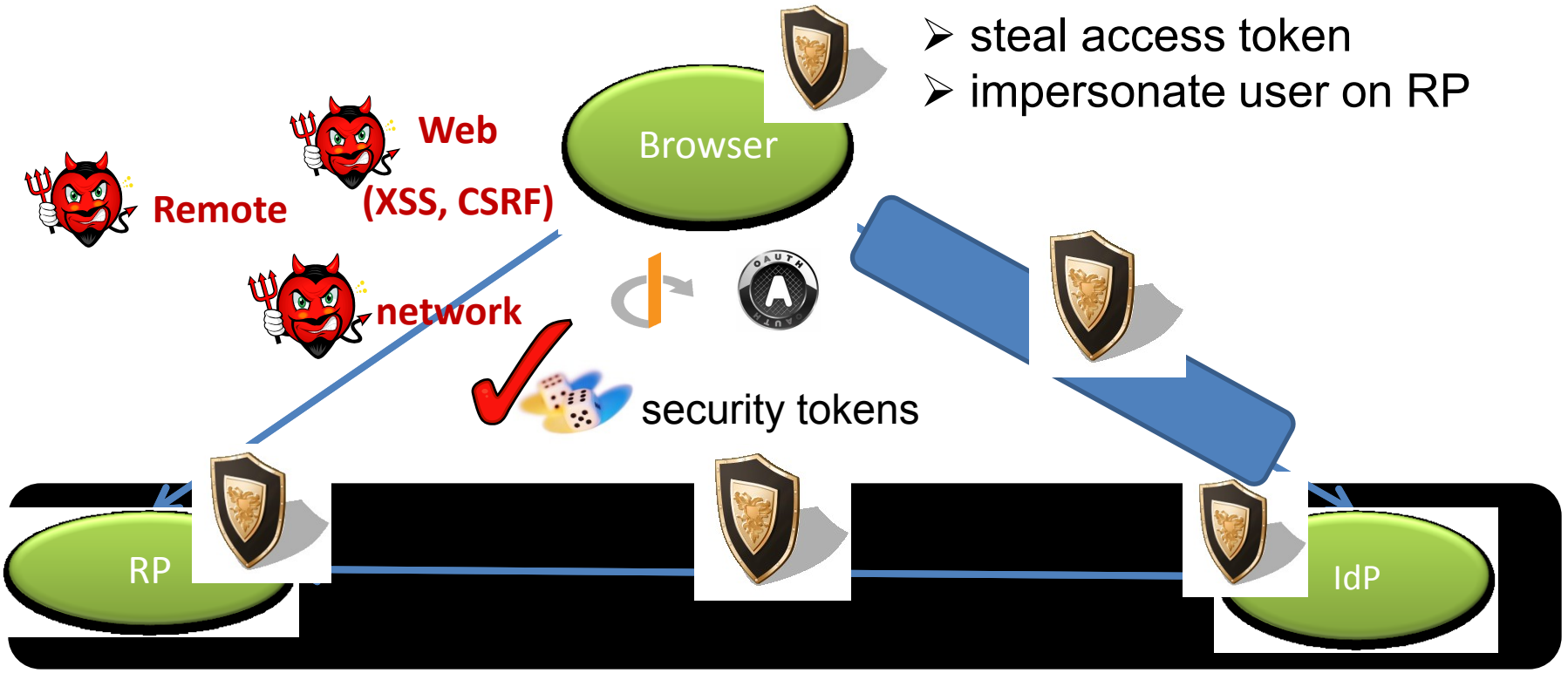
challenges:

- ✘ source code is not accessible
- ✘ situated between RP and IdP is hard
- ✘ realistic evaluation introduce actual harms

- ➢ identify weaknesses

browser relay messages

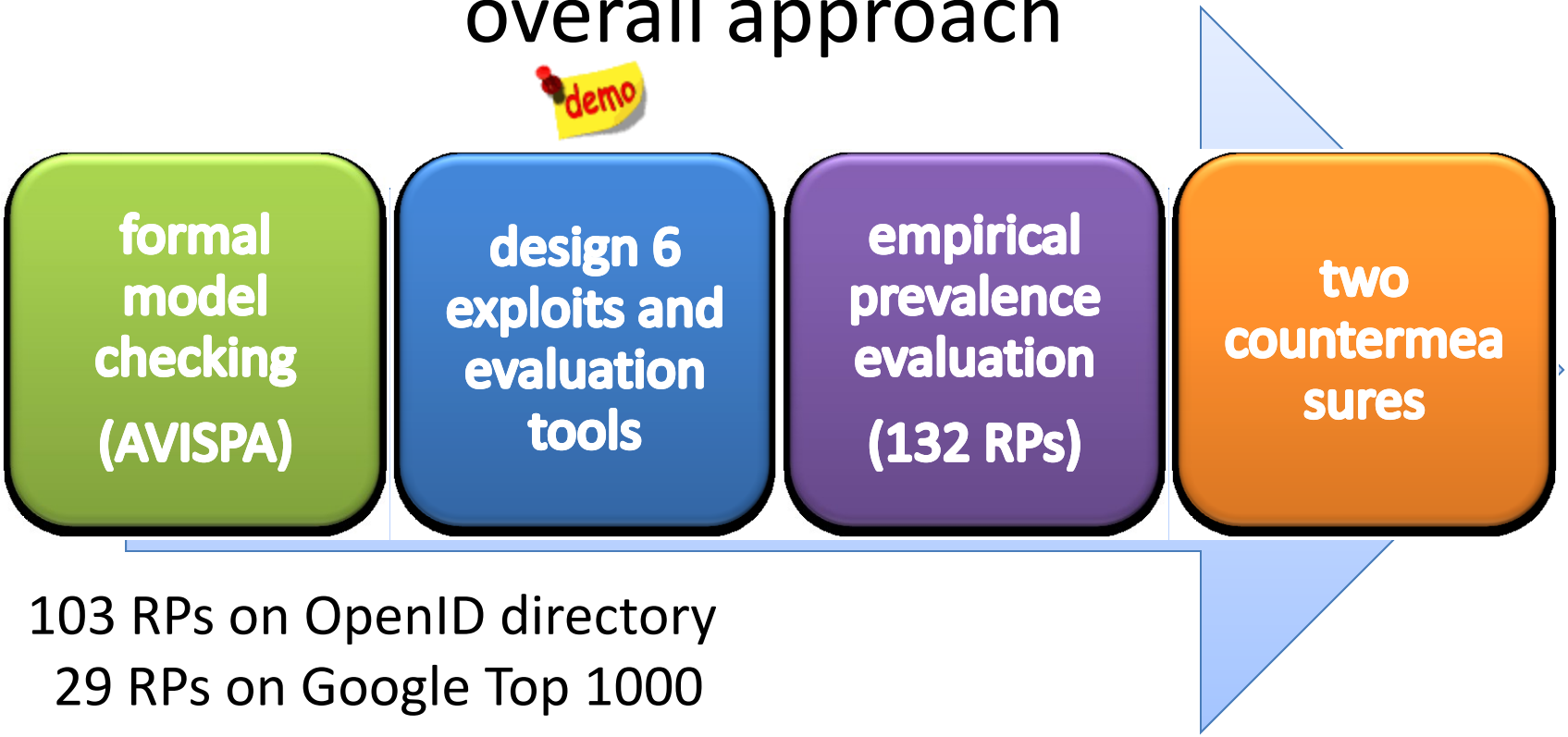
- ➢ steal access token
- ➢ impersonate user on RP



Formal Analysis and Empirical Evaluation for OpenID 2.0 Security

S. Sun, K. Hawkey, and K. Beznosov, "Systematically breaking and fixing OpenID security: Formal analysis, semi-automated empirical evaluation, and practical countermeasures," Computers & Security, 31(4):465-483, May 2012.

OpenID 2.0 security analysis overall approach

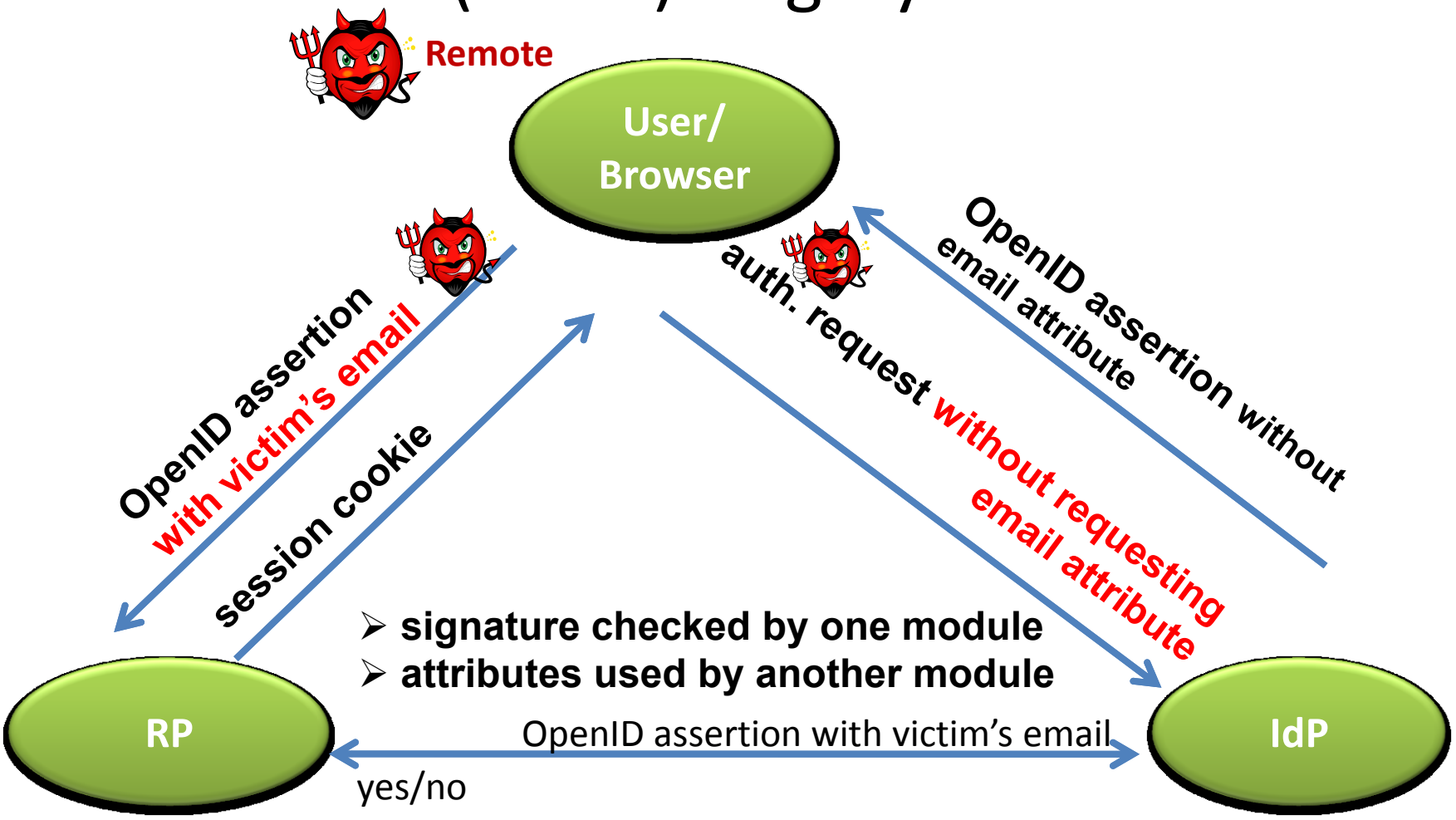


103 RPs on OpenID directory
29 RPs on Google Top 1000

three fundamental weaknesses:

- ✘ lack of **authenticity guarantee** of auth. request
- ✘ lack of **integrity guarantee** of auth. request
- ✘ lack of **contextual binding** between protocol messages and the browser

impersonation using profile attribute (email) forgery



use email address as identifier,
without checking whether the email is signed by the IdP

principles violated?

1. Least Privilege
2. Fail-Safe Defaults
3. Economy of Mechanism
4. Complete Mediation
5. Open Design
6. Separation of Duty
7. Least Common Mechanism
8. Psychological Acceptability
9. Defense in depth
10. Question assumptions

Empirical Security Analysis of OAuth 2.0-based SSO Systems

S. Sun and K. Beznosov, "The Devil is in the (implementation) details: An empirical security analysis of OAuth single sign-on systems," in Proceedings of 19th ACM Conference on Computer and Communications Security (CCS), October 2012.

OAuth 2.0-based SSO

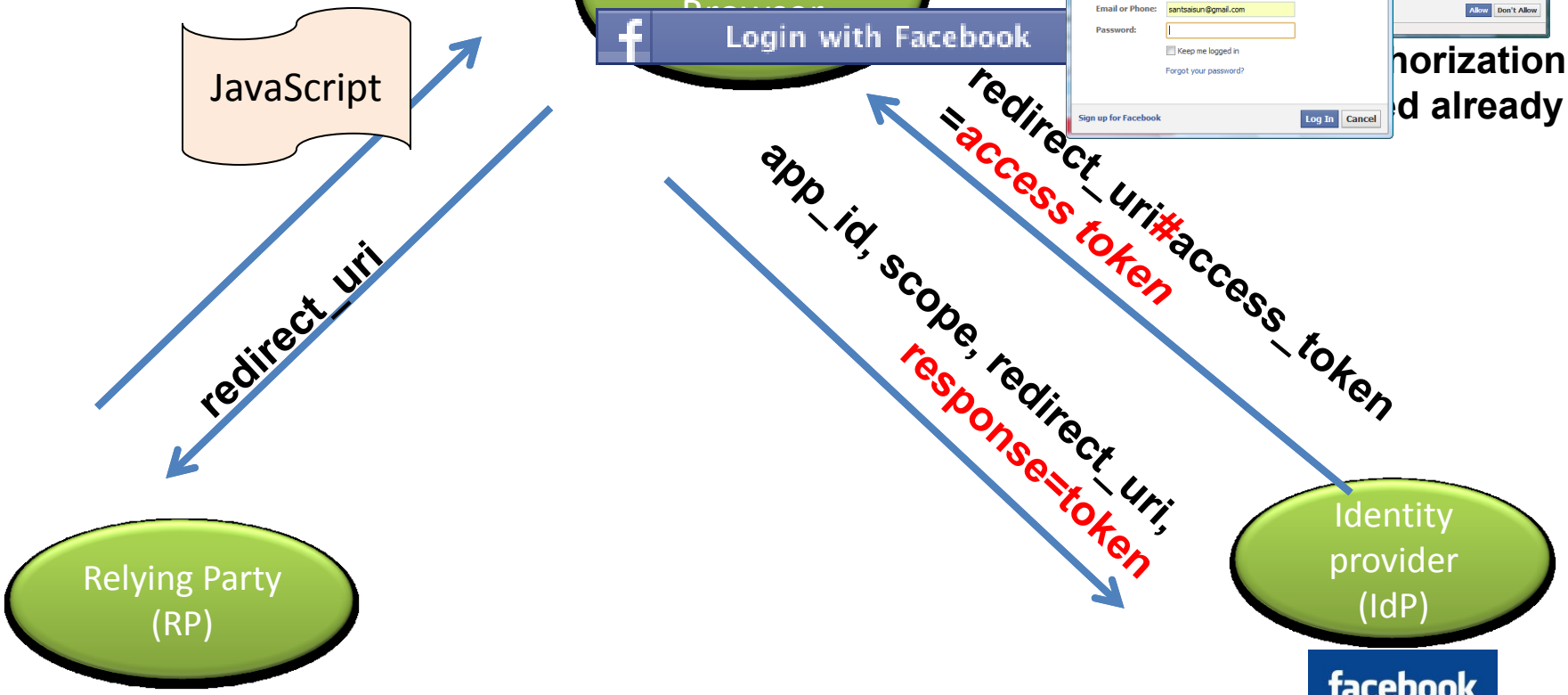
- **access token is the capability!**
  - **represent scope and duration of an authorization**
  - **used by RP to access identity information**
  - **temporary key to user account on IdP and RP**
- **server-flow: RP server-side**
- **client-flow: JavaScript/Rich-client**

client flow

`access_token = document.location.hash`

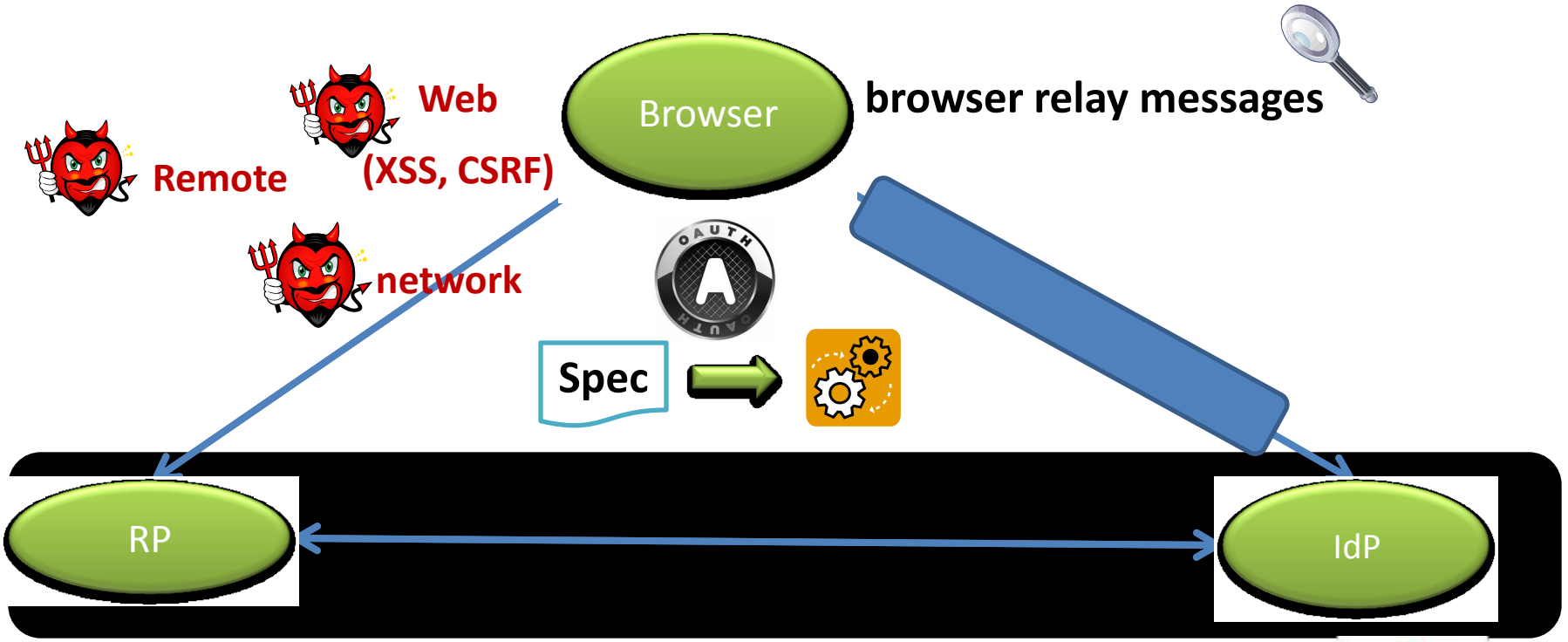
skip authentication if user has logged into the IdP in the same browser

horization if
d already



overall approach (OAuth 2.0)

- steal access token
  - harvest user data on IdP
  - act on behalf of victim
- impersonate user on RP
  - control user RP account



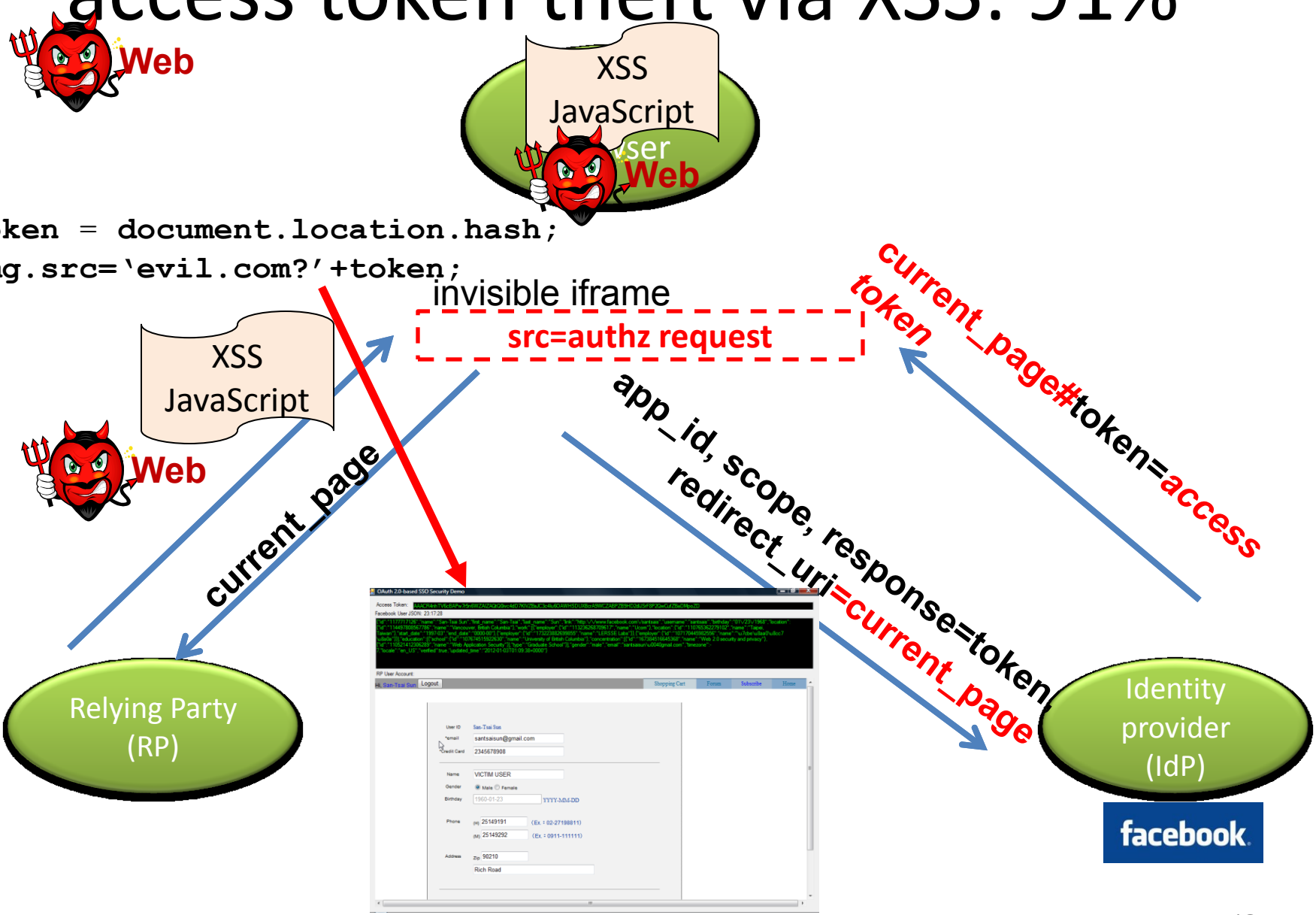
96 RPs listed on Google Top 1,000 Websites

- English-written
- support Facebook

Connect with Facebook

facebook Google Windows Live 7

access token theft via XSS: 91%



principles violated?

1. Least Privilege
2. Fail-Safe Defaults
3. Economy of Mechanism
4. Complete Mediation
5. Open Design
6. Separation of Duty
7. Least Common Mechanism
8. Psychological Acceptability
9. Defense in depth
10. Question assumptions

Investigating User's Perspective of Web Single Sign-On

- S. Sun, , E. Pospisil, I. Muslukhov, N. Dindar, K. Hawkey, and K. Beznosov, "Investigating user's perspective of web single sign-on: Conceptual gaps, alternative design and acceptance model," in minor revision, ACM Transactions on Internet Technology (TOIT), January 2012.
- S. Sun, E. Pospisil, I. Muslukhov, N. Dindar, K. Hawkey, and K. Beznosov, "What makes users refuse web single sign-on? An empirical investigation of OpenID," in Proceedings of Symposium on Usable Privacy and Security (SOUPS), July 2011.
- S. Sun, , E. Pospisil, I. Muslukhov, N. Dindar, K. Hawkey, K. Beznosov, "OpenID-Enabled Browser: Towards usable and secure web single sign-on," in Proceedings of the 29th International Conference Extended abstracts on Human Factors in Computing Systems (CHI), May 2011.

in-lab user study overall approach

exploratory study (9) | alternative interface design | formative study (7) | comparative study (35)

- understand web users' perceptions, concerns
- define requirements

- confirm findings from the exploratory study
- improve prototype and study design

- compare IDeB with current UI

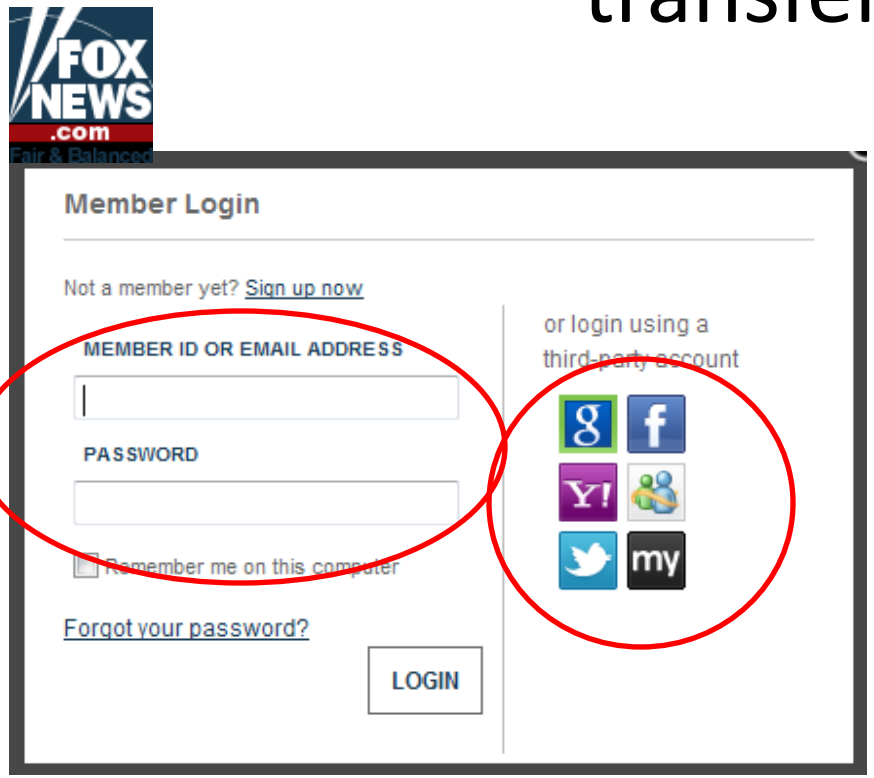
➢ screen participants for gender, age, student/non-student
➢ each participant was included only one study

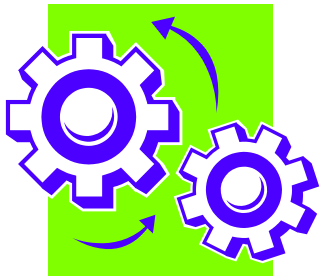
- identity-enabled browser (IDeB)
  - ➢ sign onto real-world RPs using SSO
  - ➢ IdP-phishing identification test
  - ➢ mental model drawing
  - ➢ semi-structured interview

main findings


FoxNews.com - Breaking News | Latest News | Current News - Mozilla Firefox
File Edit View History Bookmarks Tools Help
FoxNews.com - Breaking News | Late...
My Account
http://www.foxnews.com/
Google
Fox News
Fox Business
Small Business Center
Fox News Latino
Fox News Radio
Fox Nation
Account
FOX NEWS .com
Fair & Balanced
June 16, 2011 -- Updated at 7:17 PM ET
Search
ON AIR NOW »
FOX Report w/ Shepard Smith (cc)
News at the Speed of LIVE!
7p et
On Air Personalities »
The O'Reilly Factor (cc)
It's the "No Spin Zone!"
8p et
FULL COVERAGE
It's All Your Money • Rise of Freedom • On the Job Hunt
WATCH LIVE
Casey Anthony Trial
Home
Video
Politics
U.S.
Opinion
Entertainment
SciTech
Health
Leisure
World
Sports
On Air
UGLY
TO THE END
AP
WATCH FOXNEWS.COM LIVE
Foxnews.Com Replay June 16
Missed the show while it was on? Don't worry; we've got it on DVR. Watch the replay now.
Watch
Smelling the
ADVERTISEMENT
Weiner Resigns Over Sexting Scandal
• VIDEO: Weiner Announces Resignation | YOU DECIDE: After Sexting Scandal, Do You Trust Your Spouse Less?
• Stand by Your Man? The Different Decisions of Political Wives | VIDEO: Weiner's Ex Reacts
• Ex-Porn Star in Scandal Cashing In on 15 Minutes of Fame | SLIDESHOW: Anthony Weiner Resigns
• Dr. Manny's Advice for Weiner's Pregnant Wife | TIMELINE: Anthony Weiner Scandal
MARKETS
SPONSORED BY
Ameritrade
Transferring data from tag.admeld.com...

misleading affordance and negative transfer effect



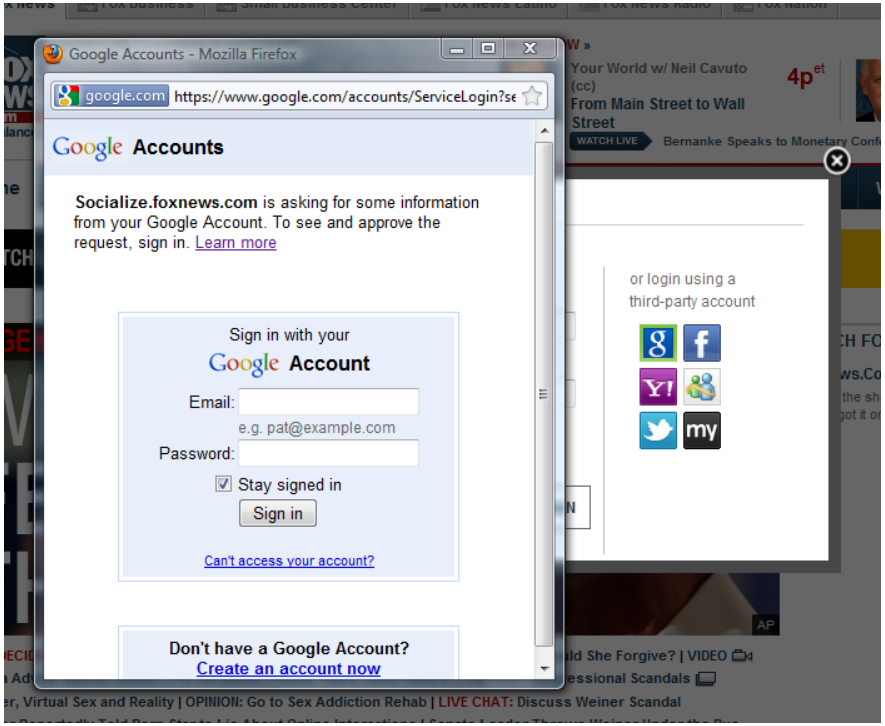


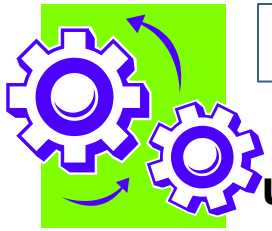
click on icon to select an IdP

enter one of their user name and password listed on the right-hand side

most participants entered their Google or Yahoo email and password into the traditional login form directly.

security misconception





user

user name/ password

IdP

RP

profile

user

user name/ password

IdP

user name/ password

RP

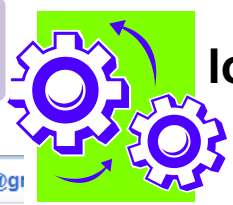
profile

"The website is going to have my Google email and password!!"

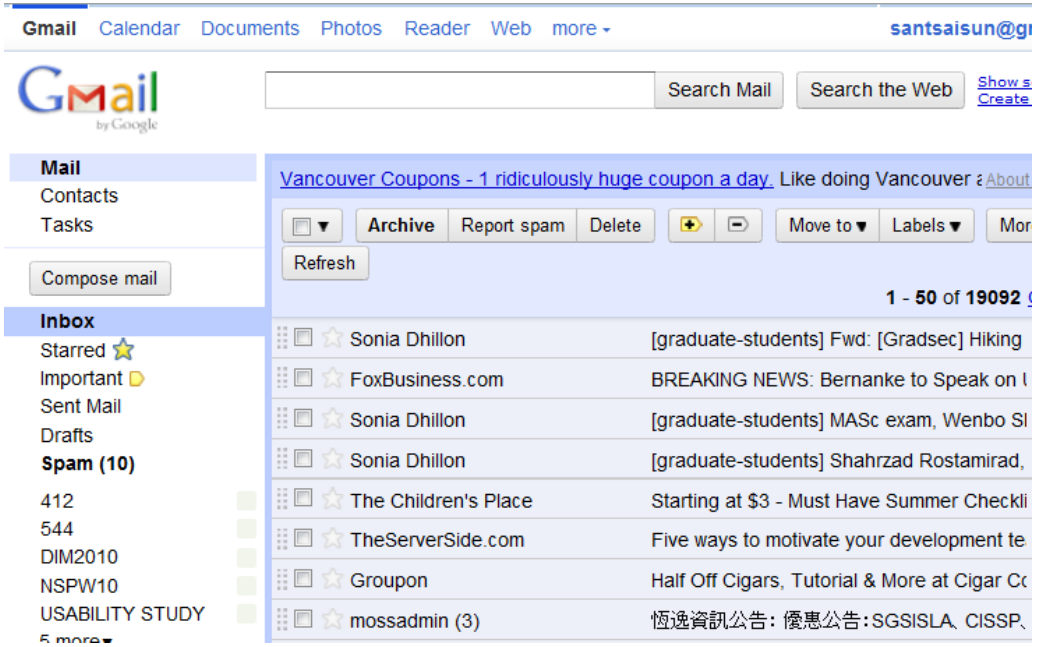
implicit IdP login concern

log out all RP websites

check email



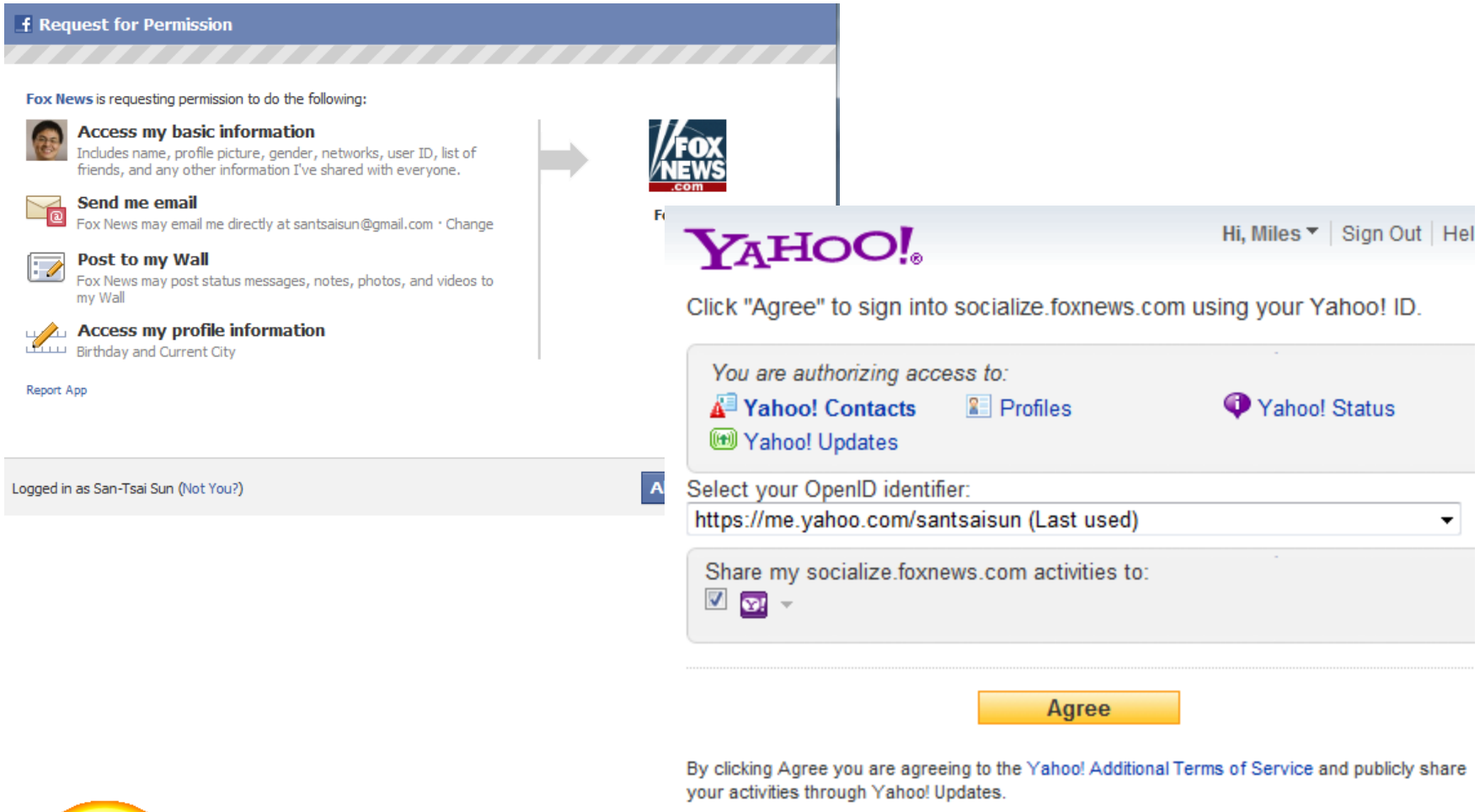
log into **RP** and **IdP**



log into **RP** only

"why Gmail did not ask me to sign in!!"
"what if I just left this computer?"

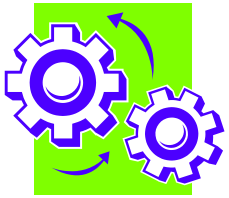
privacy concern

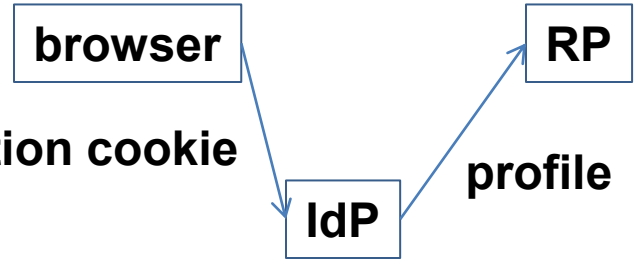


"I would normally say NO !!"

security misconception confirm

in the same browser session, only one IdP login prompt for a specific IdP





log back into FOX NEWS .com Fair & Balanced

"Fox News remembers my Google password!!"

"why no IdP login prompt?"

"my password has been stored some where!!"

usable security design principles?

1. Path of Least Resistance
2. Active Authorization
3. Revocability
4. Visibility
5. Self-Awareness
6. Trusted Path
7. Expressiveness
8. Relevant Boundaries
9. Identifiability
10. Foresight