Beyond Passwords

Identity 2.0: promises, policies, threats

Lisa Dusseault
CommerceNet Fellow
Applications Area Director, IETF
Agenda

• Identity 2.0
  – Promises
  – Payoffs
  – Policies

• Threats to third-party authentication
  – How and why phishing/pharming works
  – Possible next steps
Web 2.0: Explosion of services

What user authentication options do new sites have?

- HTTP Authentication dialogs suck
  - Not enough context
- Password forms different everywhere
- More passwords makes users miserable
- User enrollment is a barrier: effort, spam and privacy concerns
Identity 2.0

3rd-party IDs for the whole Web

User POV

– Why create an account for each Web service?
– Instead, use a major account to provide secure identity to many other services
– Fewer passwords to remember
– Give out email address less often
Identity 2.0 Working Systems

- **Federated, browser-based**: OpenID, LID
  - Apache Heraldry…
- **Centralized, browser-based**:
  - Yahoo BBAuth, MS Passport/LiveID
- **Federated, OS-based**: Microsoft Infocard
- **All of the above**: Liberty Alliance
- **Payment Systems, other**:
  - Google Checkout, PayPal, Amazon S3: not discussed
General architecture and terms

1. Client needs to authenticate to relying party: choose identity

2. Relying party verifies identity with provider

3. Identity provider verifies:
   - valid user/ID
   - desired action
Browser-based workflow (not logged in)

Browser

Request Service

ID: lisa@

Redirect

Pwd: ***

Redirect

Relying Party

Ask for ID

Ask to Verify ID

Identity Provider

Request Password

Check Password

Send Assertion

Provide Service
New possibilities for Web Apps

• How:
  – Install Web server extensions
  – Yahoo, Deutsch Telecom: sign up as application or partner

• Why, who:
  – What’s in it for the relying party?
Promises

1. Avoid overhead of maintaining passwords
2. Avoid overhead of verifying email
3. Easier user enrollment
4. Reduce comment spam, inappropriate content and similar contributor problems?
5. Get user profile information (postal code, reputation)?
6. Better mashups?
Promise: No password maintenance

Reality: Yes!

- Avoid management of users forgetting passwords
- Avoid risks of password leaks
- Still want to maintain user information?
  - Local Database to map ID to local information
  - Preferences, history, etc
Promise: Avoid email verification

Reality: Depends on Policies

- Some IDPs do email verification for you
  - Yahoo does
  - Some federated IDPs do (Verisign yes, MyOpenID no)
  - Not an explicit assertion during identity validation

- Some identity claims are self-generated
  - MS Infocard allows new identities to be locally created
  - A federated IDP could be run by anybody

- Web service policy: must each user have email?
Promise: Easier User Enrollment

Reality: Mostly yes, but has tradeoffs

- Only works for users with identities
  - Did they need to download any software?
  - Do users trust these systems?
- Works if IDP makes sign in and validation steps smooth
- Tradeoffs
  - No user email known
  - Looser relationship
  - Lower barrier to entry can mean less trust
Promise: Reduce Spam

Reality: Mostly NO

- Centralized? Depends on IDP policy
  - Is it easy to get new ID to avoid blacklist?
  - What action taken with reported spammers? (e.g. None)
- Federated? Can’t even know IDP policy
  - Open to countless free IDs: poor blacklistability
  - No reputation information available yet
- Whitelists are just the same
  - Management overhead, filtering newcomers
Promise: Get User Profile
Privacy is bigger concern to IDP

• Yahoo: no profile info, not even username
• Infocard: possibly
  – If user entered data and if they agree to release
• OpenID, LID and other federated?
  – Not for a while yet
  – Reputation: even further away
• IDP goals counter to goals of Relying Party
Promise: Better Mashups

Reality: Explain how exactly?

- Even cross-identifying user may not work
  - Depends on policy, e.g., Yahoo’s user hashes
  - Depends on user choices, e.g., using different identities

- Identification $\not\equiv$ Authorization
  - How does knowing user’s identity get you access to their data on another service?
Promises weakened by Risks

• User fear
  – Reduced sign-up for identities
  – Reduced reliance for important things

• Compromised ID $\rightarrow$ erodes trust in IDP
  – Trust in entire system erodes too
  – Relationships are fragile

• Why do I worry? (Why should you?)
Pharming or Honeypot Attack

Attacker

Honeypot

Fake IDP

Client

Fake IDP looks like real one of course

Browser redirects: not evident to user
Honeypot Workflow

Browser

- Request Service
- Ask for ID
- Fake verify request
- ID: lisa@

Can user detect difference?

FAKE IDP

- Request Password
- Save Password!

May query real IDP to generate realistic form
MITM attack for 3rd-party IDPs

Attacker

Honeypot or pharm | Fake client
Fake IDP

Real IDP

Redirecting browser

Browser
Other attacks

- DNS poisoning
- MITM attack on a relying party
  - To obtain application ID if that’s needed
- Cookie abuse
  - Get client’s cookie for session on IDP
- Combine with social attacks
Why fall for it? Step 1

Incendiary Blog Post
The mounties are no use investigating cyber-crime; their horses can’t even use computers!

Post a reply?
Identify yourself

☐ OpenID identity: [http://lisa.example.net]

☐ BigCorp identity

Go
2. User sees what they expect

Sign In
You must sign in to authenticate as “http://lisa.example.net”
Password: *********

Sign In  Cancel

Done

www.notexample.net
3. No hint of password compromised

Comment:
I can’t believe what you said in your post on the RCMP! Of course they don’t use their horses when investigating cyber-crime.
To start using this service...

1. **Step 1: Sign in to Yahoo!**
   Yahoo! encourages folks with new ideas to work with Yahoo!’s own tools and services to make them even better and more useful for you. You’ll need to sign in to allow them to work with the personal information that you keep with Yahoo!.

2. **Step 2: Give your permission.**
   After you sign in we’ll ask you to give us permission to share your personal data with the developer of this service.

---

Copyright © 2006 Yahoo! Inc. All rights reserved. Copyright/IP Policy | Terms of Service | Guide to Online Security

NOTICE: We collect personal information on this site. To learn more about how we use your information, see our Privacy Policy.
Why Phishing Works

Paper by Rachna Dhamija, CommerceNet Fellow

- A great phishing site can fool 90% of test participants
- Indicators are ignored (status bar, URL)
- This applies to pharming, honeypots, too
Flow + 3rd-party login = more phishing

- Flow
  - User is goal directed: Task Fixation
  - More likely to proceed through its steps
- Third-party login: gives users the habit of jumping from a Web service to a login form
- Result:
  - Phishers engage users in a goal
  - Then meet expectations to proceed through steps
How trusted is a 3rd party identifier?

- Popularity of any specific IDP makes supporting it attractive
  - Also makes it attractive to attackers
- What % compromised identities is a problem?
- Policies of IDP matter
  - Can erode trust in uncompromised identities
- IDPs have much work to secure their logins…
What IDPs can do today

1. Convince users to customize
   - Security skins, status messages
2. Very careful with cookies, certificates
3. Police the net for social attacks, honeypots

Only big IDPs may be able to do this
Can IDP prevent MITM?

You must sign in to authenticate as “http://lisa.example.net”
Password: ******

Never provide your password unless you see the picture you provided.
Pretend Unusual Circumstances

Sign-in System Maintenance

Important alert! Due to a recent upgrade, all users must sign in again before we can proceed to verify identity. Temporarily, all user images are unavailable. You may choose to wait for user images to be available before proceeding.

Your ID:  http://lisa.example.net
Password:  ******

Sign In

Done

www.notexample.net  

US 2006
What else can be done?

• Upgrade browsers: GUI, protocol, other
  – Forms, redirects, and native support for proxies make phishing hard to prevent

• Or use OS
  – Microsoft Infocard doesn’t use forms, redirects or proxies
  – Serious work on trusted UI
  – Possible virtualization attacks
Upgrade browsers: GUI

- Problems:
  - Entire GUI is spoofable: whole-window feature
  - Login forms just like other forms: too customizable
  - Login dialogs not customizable enough

- Possible solutions:
  - Hybrid between login forms and dialogs
  - E.g. Rachna’s Security Skins
Upgrade Browsers: Protocols

Not enough to just upgrade GUI

• Fix Cookies
  – More rigorous limitations on cookie use
  – Internet-Drafts by Pettersen

• Link authentication with certificate verification

• Fix Digest authentication
  – Clearer spec: IETF effort

• New Authentication mechanisms
  – Browser MUST know when doing 3rd-party auth
  – Support logout explicitly
Beyond Passwords!

- If client doesn’t send password, the password can’t be compromised
- New HTTP Authentication mechanisms
  - No popular IETF specs so far
- TLS client certificates
  - Specs exist -- but need better usability and consistency
- Newer protocols
  - E.g. Microsoft’s WS-* suite, Liberty Alliance
Summary

Considering Identity 2.0 features?

• Understand your goals
  – Which goals are met by which kinds of identities

• Understand and minimize risks

• Experiment

• Participate
  – In standards development
  – In improving browsers: demand better
Links page

- OpenID: [http://openid.net/](http://openid.net/)
- Liberty Alliance standard deployments: [http://www.projectliberty.org/news_events/events/iddy_awards](http://www.projectliberty.org/news_events/events/iddy_awards)
- HTTP authentication, cookie discussions: [http://lists.w3.org/Archives/Public/ietf-http-wg/](http://lists.w3.org/Archives/Public/ietf-http-wg/)

Where to find these links and the presentation (soon): [http://blog.commerce.net/](http://blog.commerce.net/)
Extra slides
Browser-based workflow (logged in)

Browser

- Request Service
- ID: lisa@

Relying Party

- Ask for ID
- Ask to Verify ID

Identity Provider

- Verify cookie with ID
- Send Assertion

Redirect: client adds cookie

Redirect

Provide Service