Single Sign-On for the Internet:
A Security Story

eugene@tsyrklevich.name
vlad902@gmail.com

BlackHat USA, Las Vegas 2007
How do you manage your 169 Web 2.0 accounts today?
Does your “SSO” consist of

A login
(e.g. johndoe)

+ 

2 passwords
(one insecure for web 2.0 sites and one secure for banking sites)

?
Attack #1

a. Fail a user’s login

b. Observe the user try every single combination of their username and password, including the secure password..
Lesson #1

Complexity breeds insecurity
One login to rule them all…

…a story about reducing complexity
Proves that a user owns a URL

You get to choose who manages your identity
e.g. http://john.doe.name/ or http://jonny.myopenid.com/
Answers the who? question (authentication)

are you john.doe.name?

Does NOT answer the what? (authorization)

is john.doe.name allowed to access this page?
How?
(demo)
Sign in with OpenID

http://eugene.tsyrklevich.name

Examples:
http://you.myopenid.com/
http://username.livejournal.com/
http://first.last.name/
=example.iname

Don't have an OpenID? Sign up to get one now.
https://www.myopenid.com/signin_password?uid=020cd1b19

Username: http://eugene.tsyrklevich.name/
Password: [enter password]

Sign In | Cancel
A site identifying as http://jyte.com/ has asked us for confirmation that http://eugene.tsyrlievich.name/ is your identity URL.
Newest claims
Showing 1 to 10 of 30689 total. Next 10

Cheese.  By darraghq.myopenid.com 1 minute ago

The Jerry Springer show is the most democratic show on television.  By darraghq.myopenid.com 6 minutes ago

I have read "The Attention Economy: The Natural Economy of the Net" by Michael H. Goldhaber.  By Ivan FXS 25 minutes ago
That was easy!
Oh. Never mind.
Let’s start at the beginning
Attack #2 – Which one are you?

http://nsa.gov:1/, http://nsa.gov:2/, ...

https://192.168.1.15/internal/auth?ip=1.1.1.1

http://localhost:8080/

http://www.youtube.com/largemovie.flv

http://www.tarpit.com/cgi-bin/hang.pl

file:///dev/null
Lesson #2

Flexibility and security do not get along

(or, why it’s important to be less flexible and more paranoid)
Everybody loves crypto

“associate mode”
Why is crypto required?

to protect request & response URLs
Shared symmetric key is generated using Diffie-Hellman

POST /server HTTP/1.0
Host: www.myopenid.com
Content-type: application/x-www-form-urlencoded
Content-length: 504

openid.mode=associate&openid.assoc_type=HMAC-SHA1&
openid.session_type=DH-SHA1&
openid.db_consumer_public=QVl0vpfJ31QmJPmvHFs6gIHE63FliBDAPH%2F693Uk3arIaMvhVcLx4kQyQhy5G0O0OJvVNwsVciFVxN0%2BiuKnFtmPn7gjgq3yjKzf5NT5iDz35QZx1Z7WGWVgGRyIYyrNne1RgKJu3EvpMHDhL7KxwCyq%2B2gIsOjwezBD8KVyuXM%3D&openid.db_modulus=ANz5OguIOXLsDhmYmsWizjEOHTdxfo2Vcbt2I3MYZuYe91ouJ4mLBX%2BYkcLiemOcPym2CBRYHNOyyjmG0mg3Bvd9RcLn5S3IHHoXGHblzqdLFEi%2F368Ygo79JRnxTkXjgmY0rxlJ5bU1zIKaSDuKdi%2BXUkKJX8Fvf8W8vsixYOr&openid.db_gen=Ag%3D%3D
Attack #3 - Diffie-Hellman is vulnerable to man-in-the-middle attacks!

The spec suggests running DH over https to improve protocol security

So what’s the point of using DH in the first place?
Lesson #3

Home brewed crypto is a no no

(or, why you should stick to https)
Where are you going?
This way! No, that way!

Location: http://www.myopenid.com/server?
openid.assoc_handle=%7BHMAC-SHA1%7D%7B4..&
openid.identity=http%3A%2F%2Fjohn.doe.name%2F&
openid.mode=checkid_setup&
openid.return_to=http%3A%2F%2Fwww.somesite.com%2F&
Attack #4a
Phishing with malicious RPs
Attack #4b
Phishing with malicious URL hosts
Lesson #4

Phishers 1 – OpenID 0

(or, why Johnny will never learn to read URLs)
Let me in!

1. Login with OpenID url
2. Download OpenID url
3. Negotiate crypto keys
4. Redirect
5. Enter password
6. Authorize RP
7. Redirect

John Doe

OpenID-enabled Web 2.0 site aka RP (e.g. www.jyte.com)

Identity Provider aka IdP (e.g. www.myopenid.com)

John Doe's URL host (e.g. http://john.doe.name)
Once signed in, you will no longer need to re-enter your password for other OpenID enabled sites

Convenient, eh?
In other words…

your identity provider receives and processes ALL your login requests on your behalf

…privacy, anyone?
Lesson #5

OpenID makes privacy difficult

(or, why some paranoid users might want to use one OpenID login per site)
Not another redirect!

1. Login with OpenID url
2. Download OpenID url
3. Negotiate crypto keys
4. Redirect
5. Enter password
6. Authorize RP
7. Redirect

John Doe

Identity Provider aka IdP (e.g. www.myopenid.com)

OpenID-enabled Web 2.0 site aka RP (e.g. www.jyte.com)

John Doe's URL host (e.g. http://john.doe.name)
Attack #6 – Replay attack

Location: http://www.somesite.com/finish_auth.php?
openid.assoc_handle=%7BHMAC-HA1%7D%7B47bb..&
openid.identity=http%3A%2F%2Fjohn.doe.name%2F&
openid.mode=id_res&
openid.return_to=http%3A%2F%2Fwww.somesite.com&
openid.sig=vbUyND6n39Ss8IkpKl19RT83O%2F4%3D&
openid.signed=mode%2Cidentity%2Creturn_to&
nonce=wVso75KH
Problems with Nonces

a. Not part of the OpenID spec (v1)

b. Do not actually protect against active attackers!
Lesson #6

Nonces are nonsense

(or, why you must be drinking absolut kool-aid if you believe nonces will protect you against an active attacker)
I am secure once I am logged in though, right?
Attack #7 – Cross-site request forgery

<html><body>

<iframe id="login" src="http://bank.com/login?openid_url=john.doe.name" width="0" height="0"></iframe>

<iframe id="transfer" src="http://bank.com/transfer_money?amount=100&to=attacker" width="0" height="0"></iframe>

</body></html>
Lesson #7

OpenID robs you of control

(or IdP, not RP, makes the security decisions)
Is it really all that bad?! 

No!

OpenID can make your logins far more secure than they are today!
How?!

Only one service to secure so we can afford to use

- Client-side certificates
- SecurID
- Smartcards
Lesson #8

There is only 1 front door with OpenID

(or, how I got over my privacy and learnt to love OpenID)
Lessons Learnt

1. Complexity breeds insecurity
2. Flexibility and security do not get along
3. Home brewed crypto is a no no
4. Phishers 1 – OpenID 0
5. OpenID makes privacy difficult
6. Nonces are nonsense
7. OpenID robs you of control
8. There is only 1 front door with OpenID
Is OpenID doomed?
Absolutely not
It’s a great system solving a very real problem
But its security and privacy concerns need further thought
Thanks!

Try it today.

http://www.openid.net/
http://www.freeyourid.com/

eugene@tsyrklevich.name
vlad902@gmail.com
Primary adoption vector:
grassroots, Web 2.0 applications

URL-based (OpenID)

OpenID/SAML convergence!?

Digital Identity

Invisible (SAML/Liberty)
Primary adoption vector:
internal IT needs of the enterprise

Card-based (WS-Trust)
Primary adoption vector:
CardSpace bundled with Windows Vista

User-centric