# OpenID

Mark Heiges

Center for Tropical and Emerging Global Diseases

mheiges@uga.edu

# Agenda

- what is an OpenID
- how OpenID works
- demos
- developer perspective
- the dark-side

# Traditional Sign Up, Sign On

- Register for an account
- wait for email verification
- First Login
  - setup profile
- Next website: Rinse, repeat

# Traditional Sign Up, Sign On

- Proliferation of account names and passwords to manage
- Password security in someone else's hands

# What is an OpenID

- URL or XRI that functions as your identity

  http://mheiges.myopenid.com

  =mheiges

# OpenID, how does it work?

- You claim you own a URL
- You prove that claim

# demos

# Benefits of OpenID

- Fewer usernames and passwords
- Control over your online identity
  - you pick a provider you trust
  - can change providers later
- Minimize password security risk
  - password not stored by content provider
- Accelerate sign up at websites

source: http://openid.net/

# Simple Registration Extension (sreg)

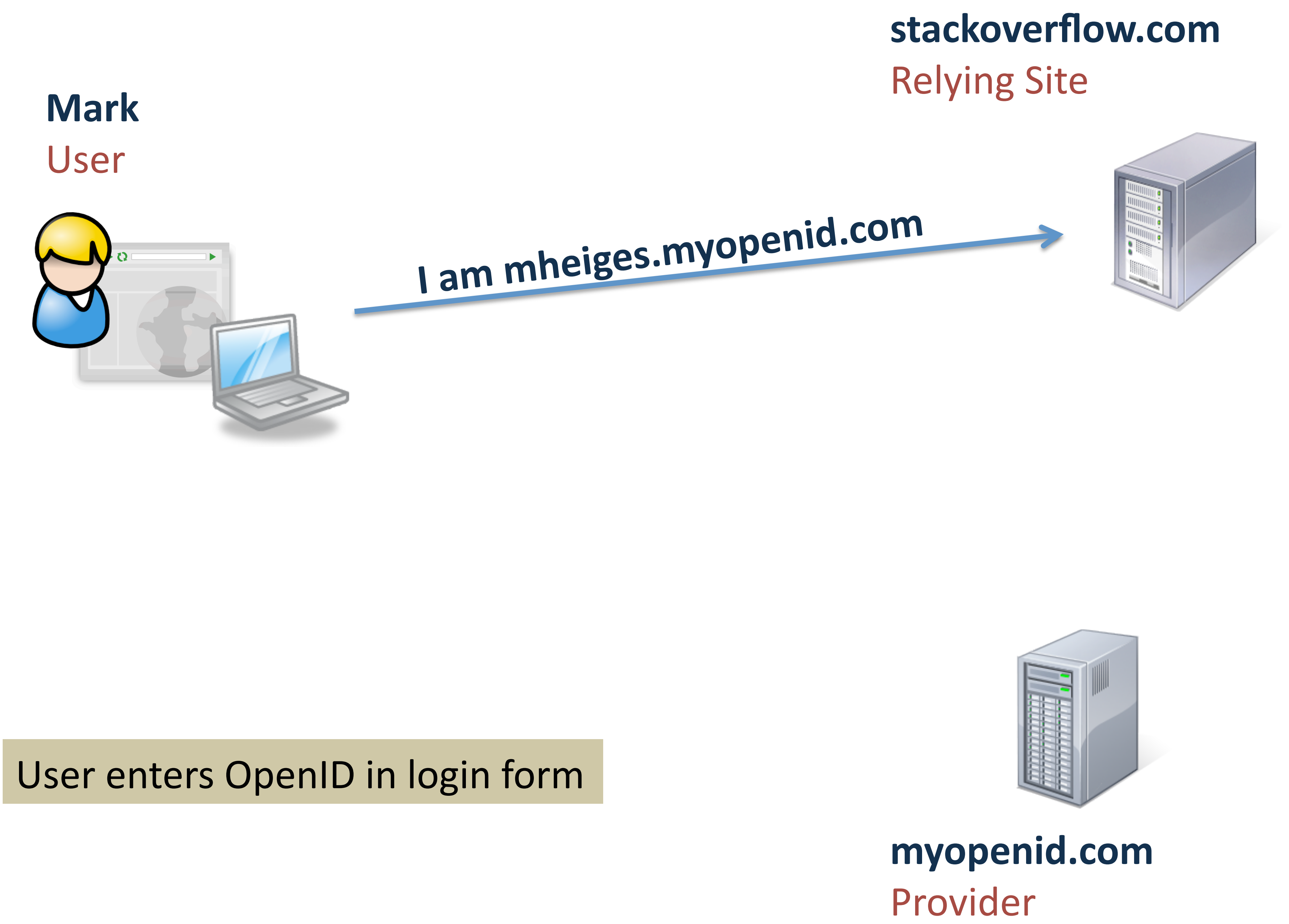
- nickname
- email
- fullname
- dob
- gender
- postcode
- country
- language
- timezone

# OpenID Protocol Flow

# A couple of terms

- **Relying site** (formerly, 'Consumer')
  - site asking for login
  - stackexchange.com

- **OpenID Provider** (OP)
  - site managing your identity
  - myopenid.com



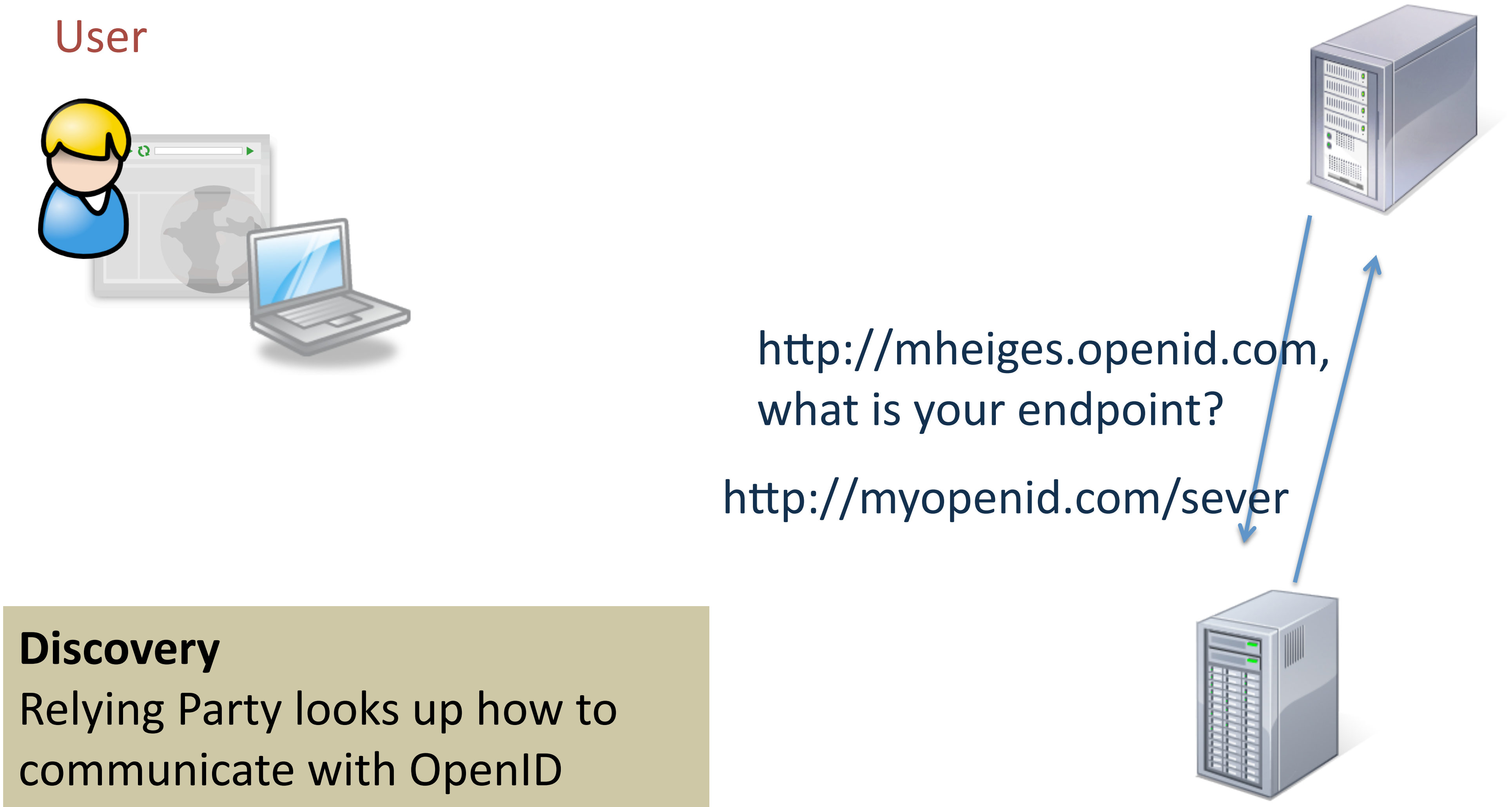
**stackoverflow.com**
Relying Site

**Mark**
User

**I am mheiges.myopenid.com**

**myopenid.com**
Provider

User enters OpenID in login form



**stackoverflow.com**
Relying Site

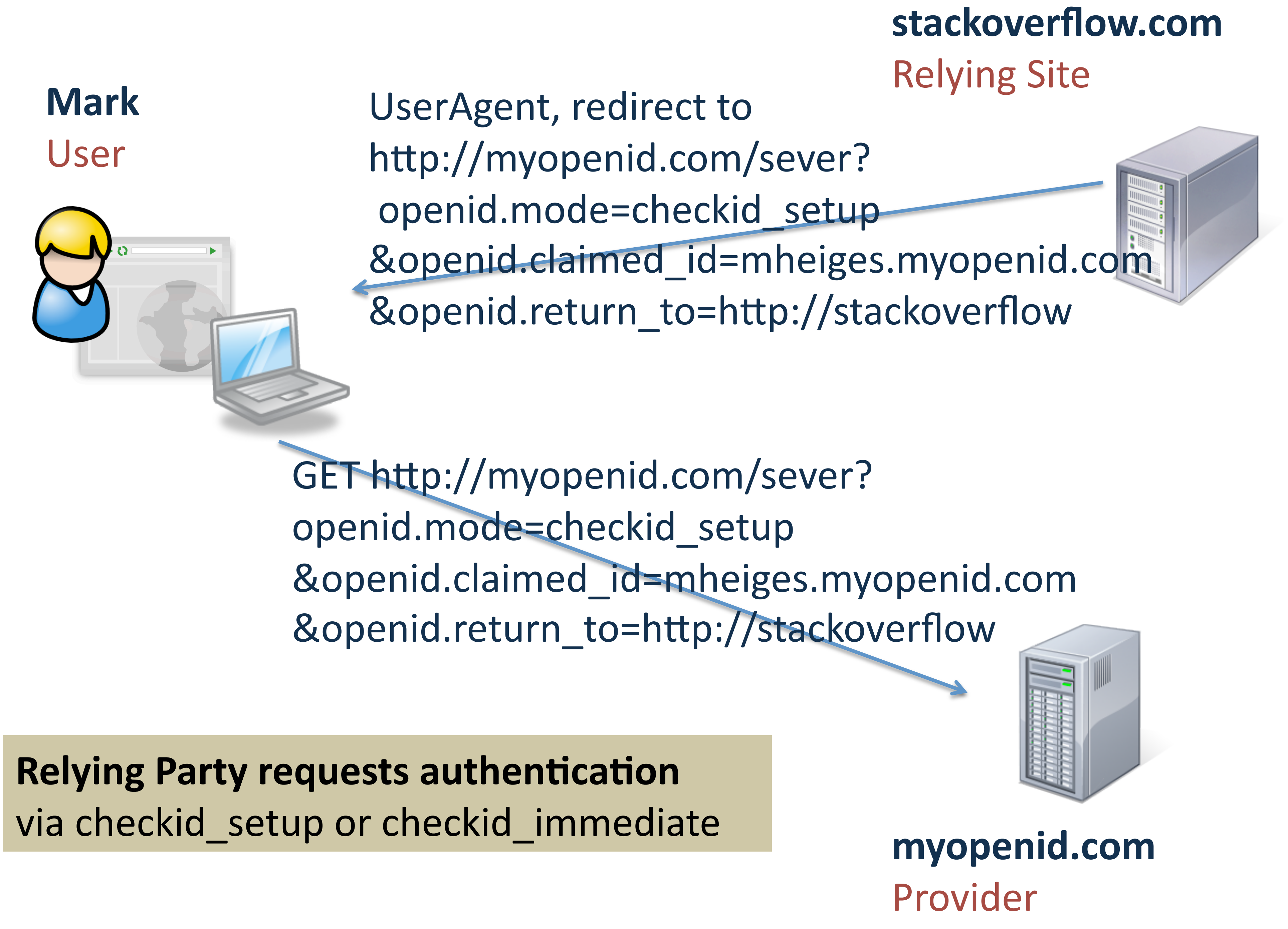
**Mark**
User

http://mheiges.openid.com,
what is your endpoint?

http://myopenid.com/sever

**myopenid.com**
Provider

**Discovery**
Relying Party looks up how to communicate with OpenID Provider



**Mark**
User

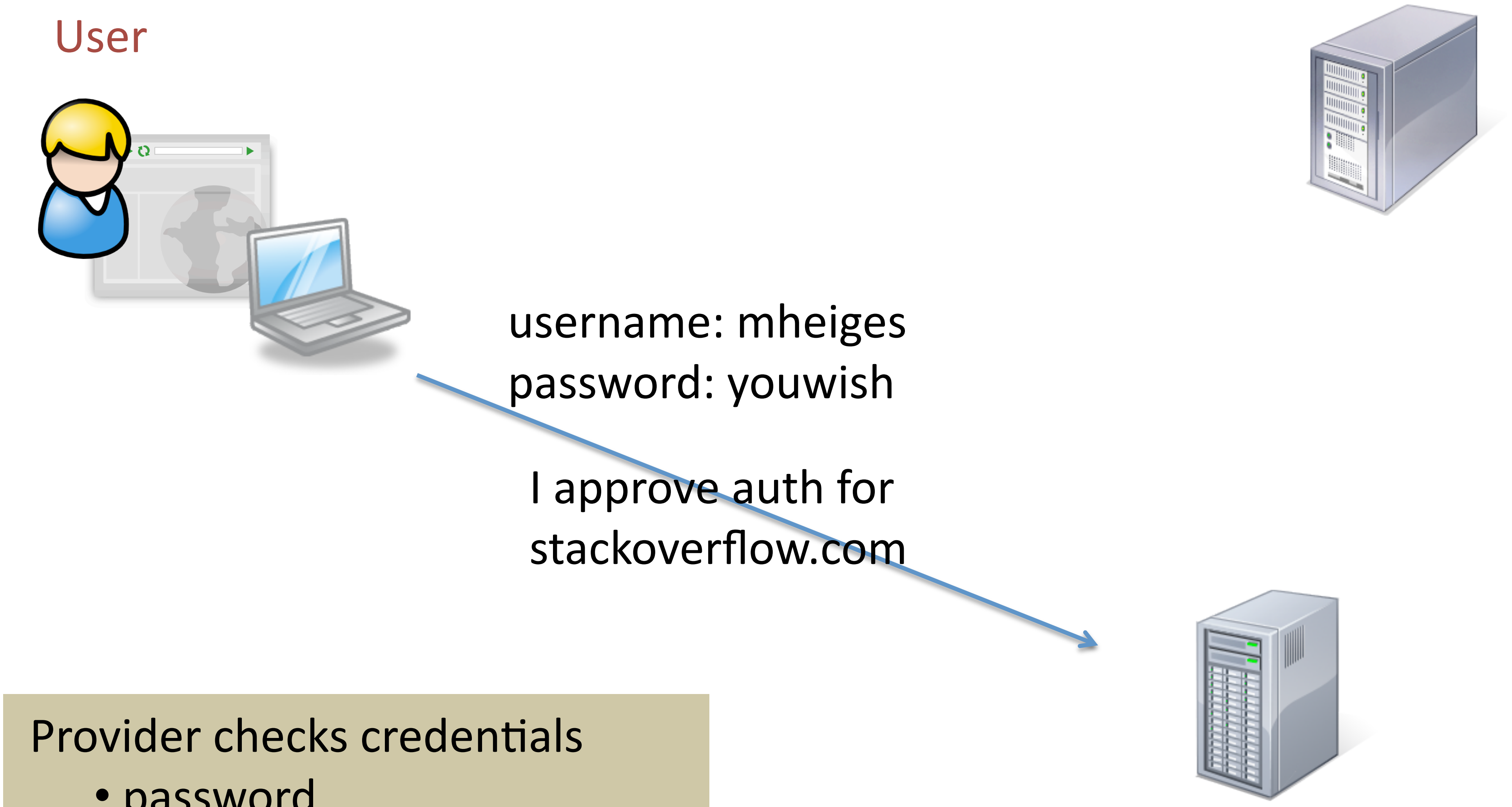
**stackoverflow.com**
Relying Site

UserAgent, redirect to
http://myopenid.com/sever?
openid.mode=checkid_setup
&openid.claimed_id=mheiges.myopenid.com
&openid.return_to=http://stackoverflow

GET http://myopenid.com/sever?
openid.mode=checkid_setup
&openid.claimed_id=mheiges.myopenid.com
&openid.return_to=http://stackoverflow

**myopenid.com**
Provider

**Relying Party requests authentication**
via checkid_setup or checkid_immediate



**stackoverflow.com**
Relying Site

**Mark**
User

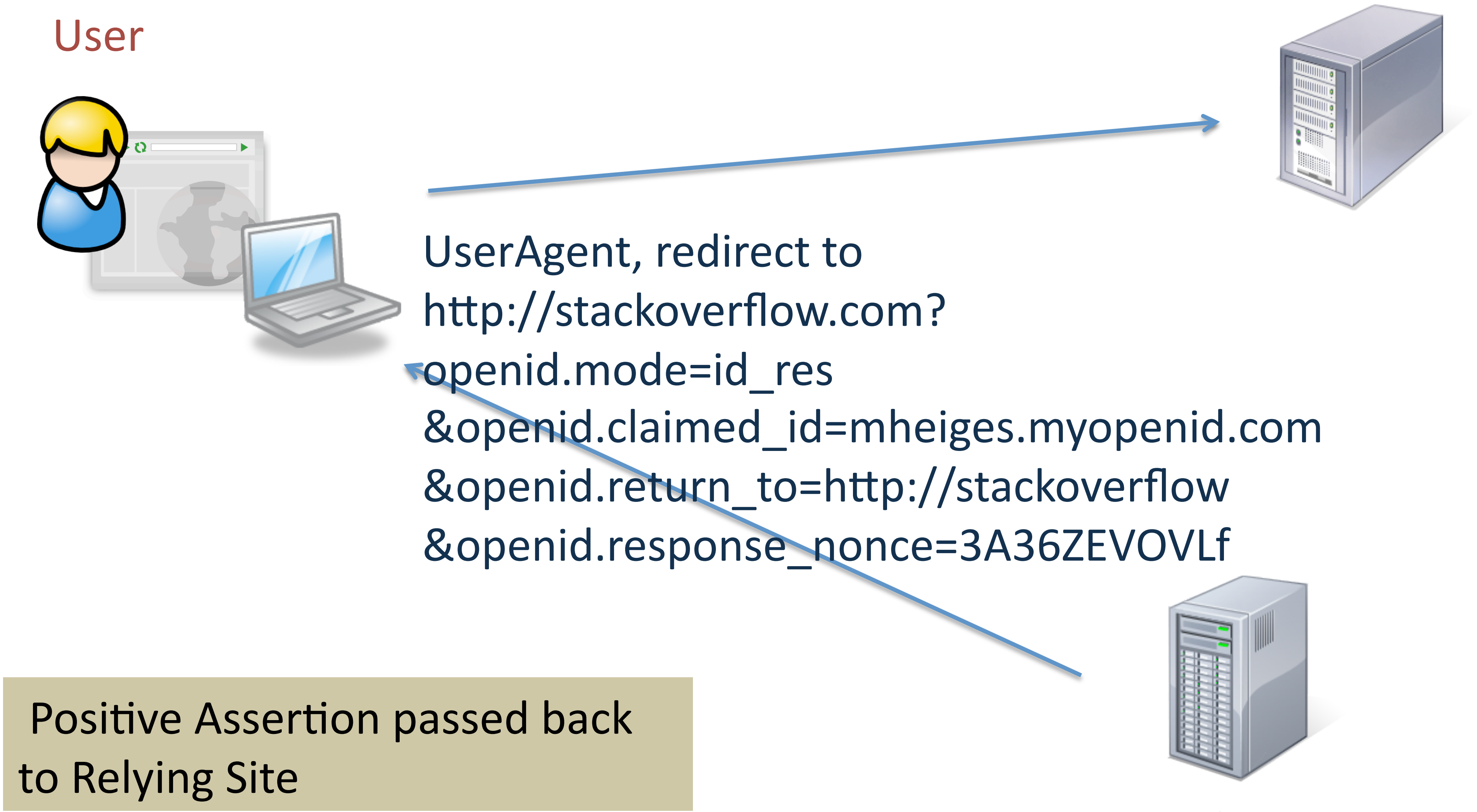
username: mheiges
password: youwish

I approve auth for
stackoverflow.com

**myopenid.com**
Provider

Provider checks credentials

- password
- signed cookie



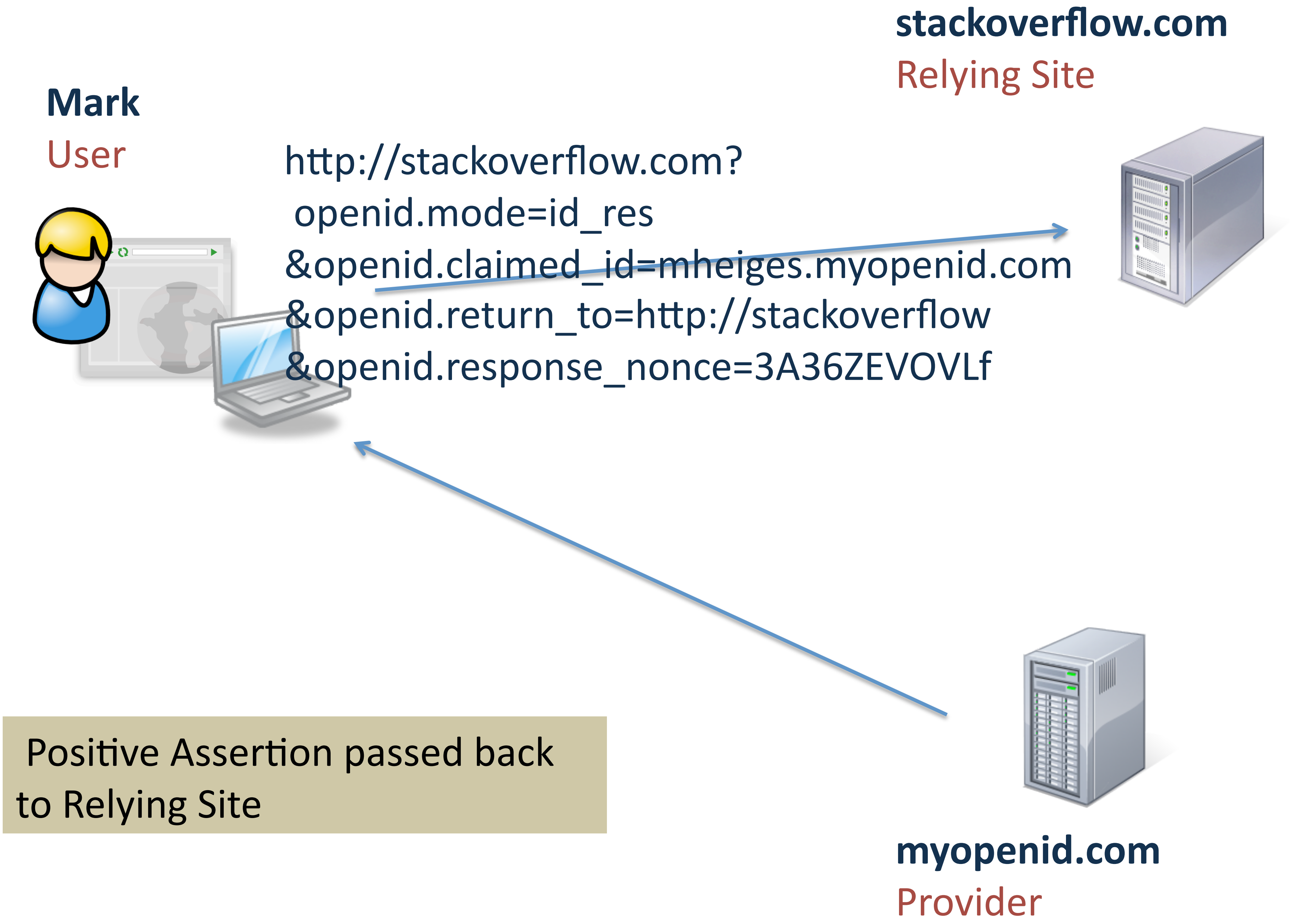
**Mark**
User

**stackoverflow.com**
Relying Site

UserAgent, redirect to
http://stackoverflow.com?
openid.mode=id_res
&openid.claimed_id=mheiges.myopenid.com
&openid.return_to=http://stackoverflow
&openid.response_nonce=3A36ZEVOVLf

**myopenid.com**
Provider

Positive Assertion passed back to Relying Site



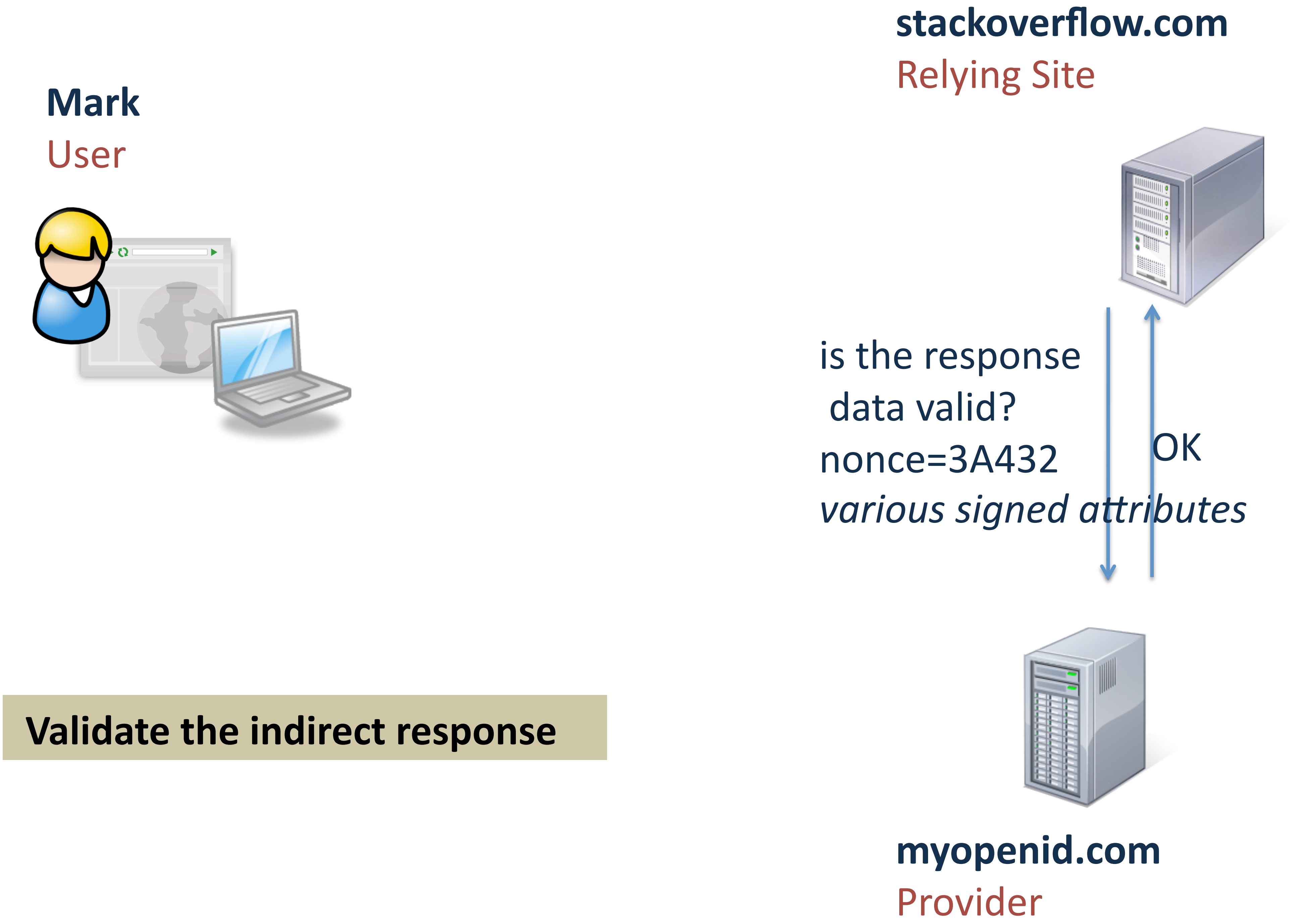
**stackoverflow.com**
Relying Site

**Mark**
User

http://stackoverflow.com?
openid.mode=id_res
&openid.claimed_id=mheiges.myopenid.com
&openid.return_to=http://stackoverflow
&openid.response_nonce=3A36ZEVOVLf

**myopenid.com**
Provider

Positive Assertion passed back to Relying Site



**stackoverflow.com**

Relying Site

**Mark**

User

is the response data valid?

nonce=3A432

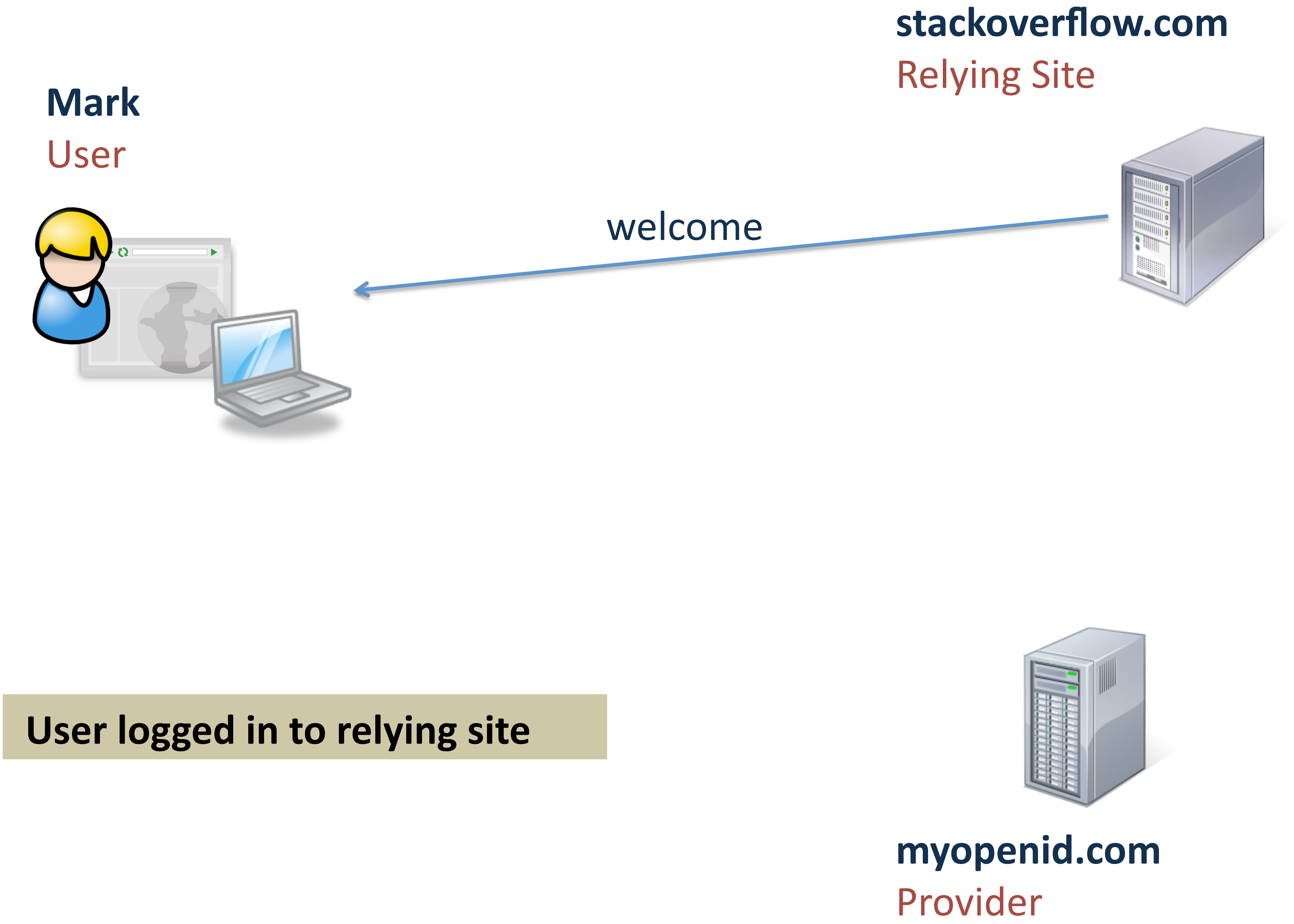
*various signed attributes*

OK

**myopenid.com**

Provider

**Validate the indirect response**



**stackoverflow.com**
Relying Site

**Mark**
User

welcome

**myopenid.com**
Provider

**User logged in to relying site**

# Where do I get an OpenID?

- from third-party Provider
  - myopenid.com
  - *OP-local identifier*
- use your own website + third-party provider
  - mark.heiges.us
  - mheiges.myweb.uga.edu
  - *claimed identity*
- use your own website + own provider

# Where do I get an OpenID?

- from third-party Provider
  - mheiges.myopenid.com
  - OP-local identifier
- use your own website + third-party provider
  - mark.heiges.us
  - mheiges.myweb.uga.edu
  - claimed identity
- use your own website + own provider

# OpenID Providers

- myopenid.com
- Verisign Personal Identity Portal
  - username.pip.verisignlabs.com
- LiveJournal
  - username.livejournal.com
- wordpress.com
  - username.wordpress.com
- aol.com
  - openid.aol.com/screenname
- Google
  - www.google.com/accounts/o8/id

# A look at what providers provide

demo

# Where do I get an OpenID?

- from third-party Provider
  - myopenid.com
  - *OP-local identifier*
- use your own website + third-party provider
  - mark.heiges.us
  - mheiges.myweb.uga.edu
  - claimed *identity*
- use your own website + own provider

# Delegation

- Your own domain URL delegates to provider

- demo
  - mark.heiges.us
  - openid.delegate
  - XRD

# Where do I get an OpenID?

- from third-party Provider
  - myopenid.com
  - *OP-local identifier*
- use your own website + third-party provider
  - mark.heiges.us
  - mheiges.myweb.uga.edu
  - *claimed identity*
- use your own website + own provider

# Host Your Own Provider Software

- janrain.com
  - libraries - PHP, Ruby, Python, Java, .NET
  - commercial SaaS

- SimpleID (php)

- Many subtleties in spec, avoid writing your own library

# Testing Provider Software & Delegation Configurations

- http://test-id.org/OP/Sreg.aspx
- http://puffypoodles.com

# Adding OpenID Sign-in To Your Site

Issues to be aware of

- OpenID 1.0
- OpenID 2.0
- OpenID 2.0 + extensions
- OAuth + extensions
- buggy, incomplete OP implementations

# Adding OpenID Sign-in To Your Site

- janrain.com software
  - libraries - PHP, Ruby, Python, Java, .NET
  - commercial SaaS

- http://openid.net

- Many subtleties in spec, avoid writing your own library

# Adding OpenID Sign-in To Your Site

- CMS Support
  - Moodle
  - Wordpress
  - Drupal
  - MediaWiki
  - phpBB
  - Redmine (useless)

# Criticisms of OpenID

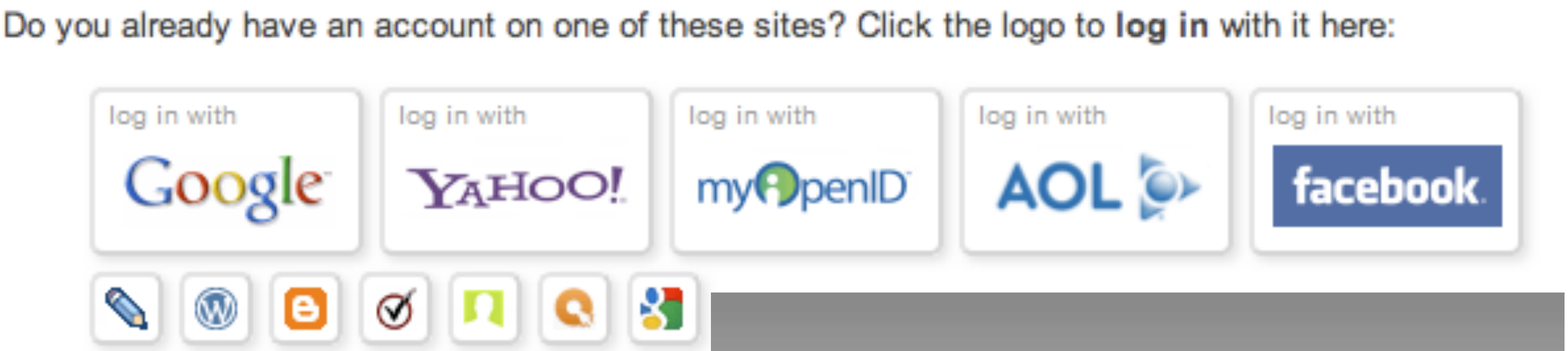
# User Adoption

- wtf is OpenID?
- URL? My identity is a website?
- I have to get an account somewhere else?

# User Adoption

- Users are already familiar with email addresses as logins
- Users already have accounts with major online services
  - Google
  - Yahoo
  - Facebook
- Why not use those?

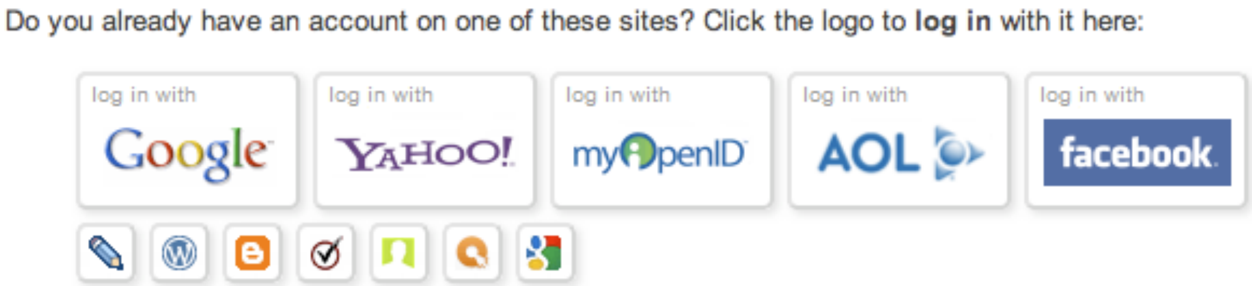
# The NASCAR  Interface



Do you already have an account on one of these sites? Click the logo to **log in** with it here:

# The NASCAR Problem

- users have too many choices
- may not make the same choice on next visit



Do you already have an account on one of these sites? Click the logo to **log in** with it here:

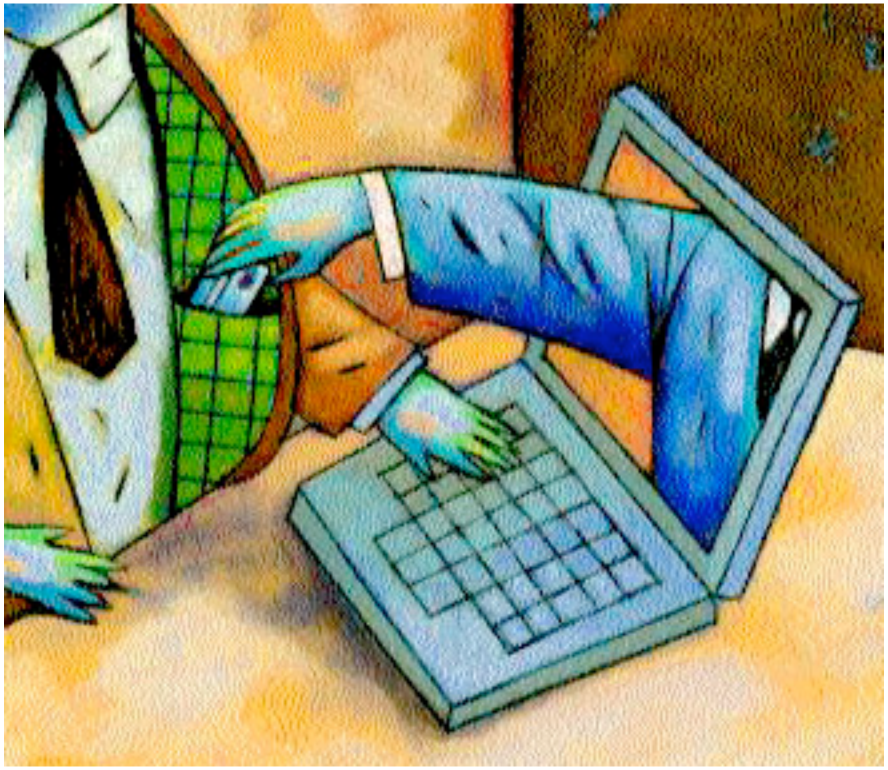
# Password Management,
# Is it really a problem?

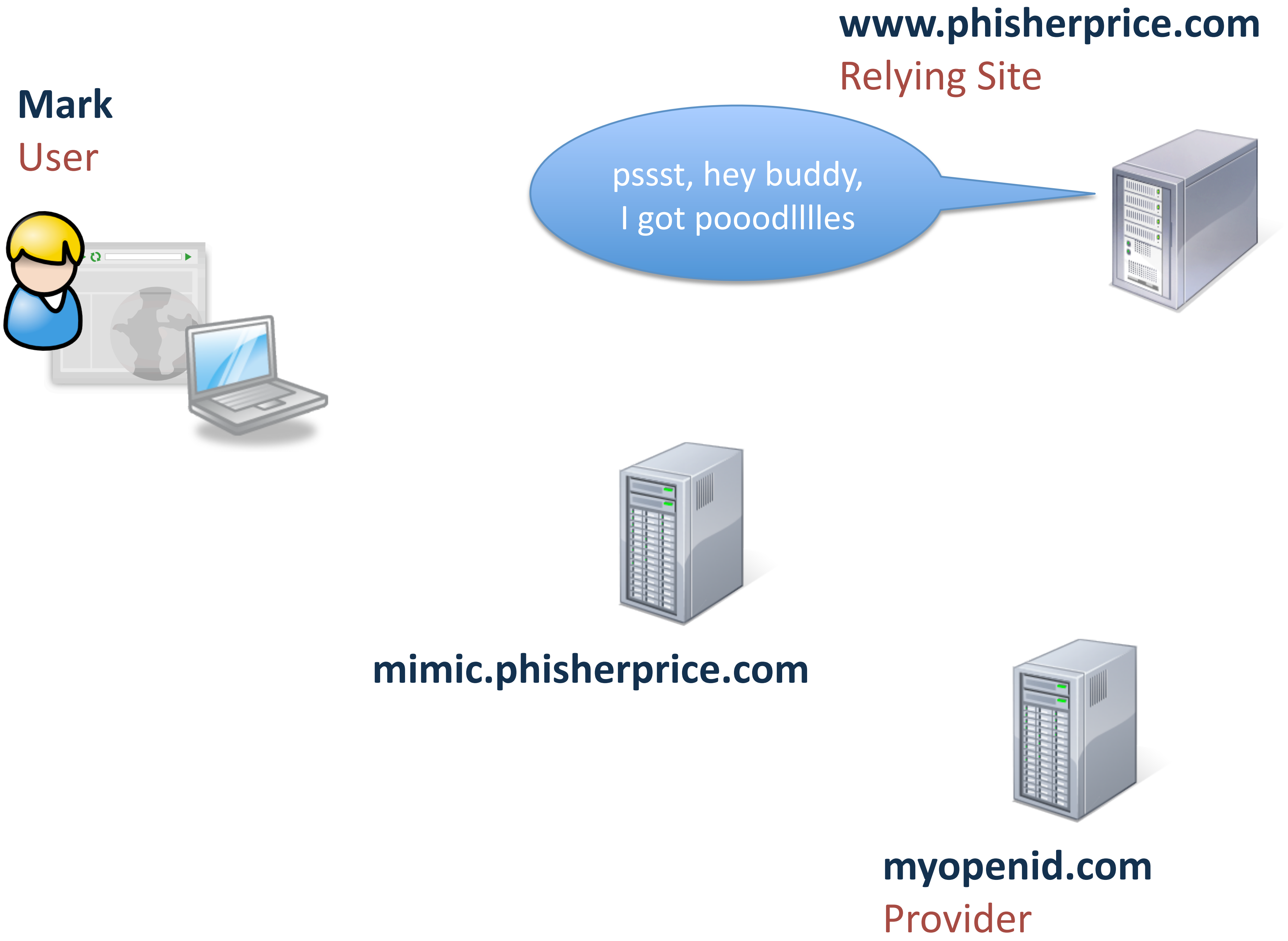
- browser/OS keychain
- plugins - LastPass, KeePass
- same password everywhere
- autofill

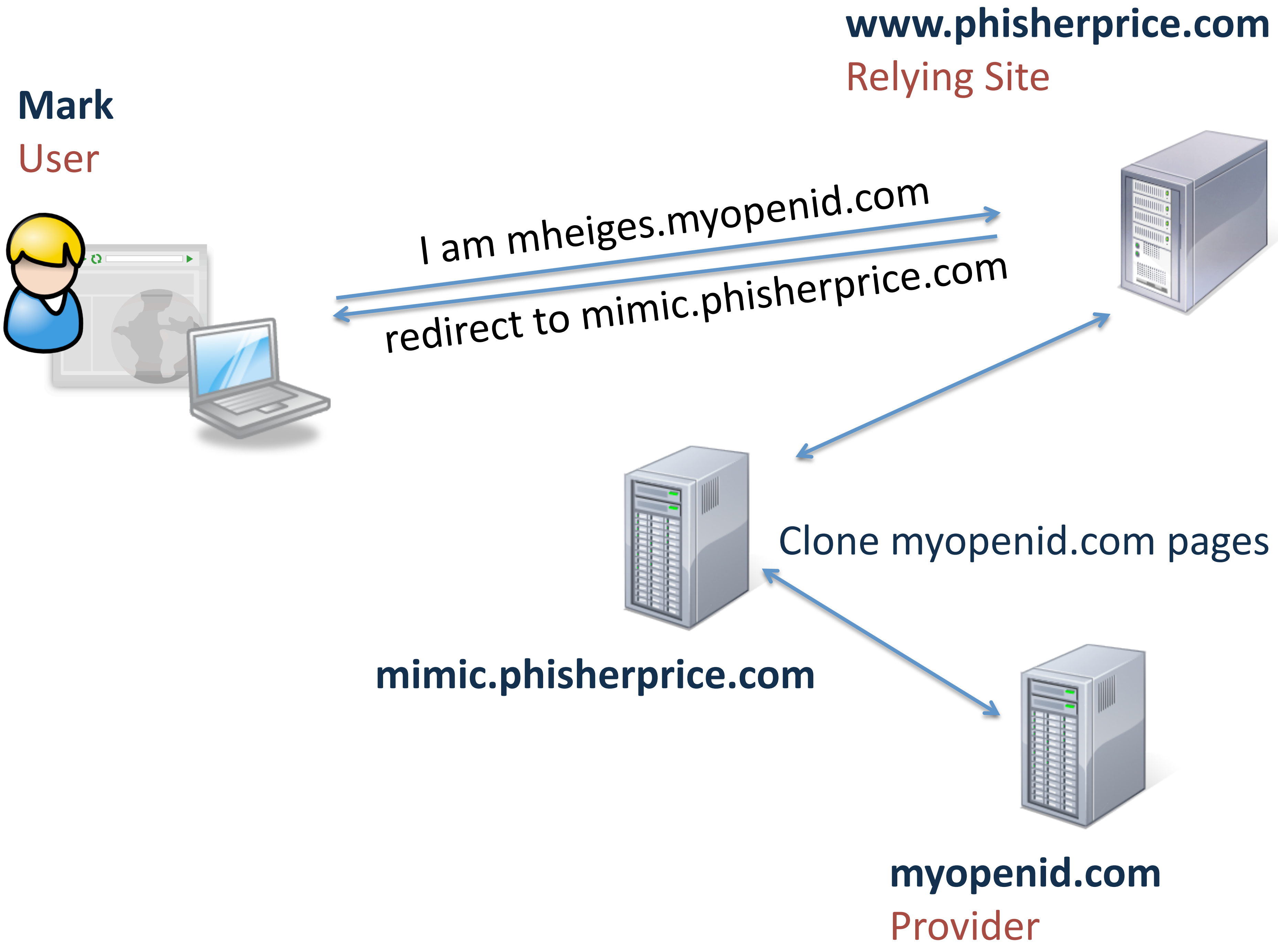
# One password == single point of compromise

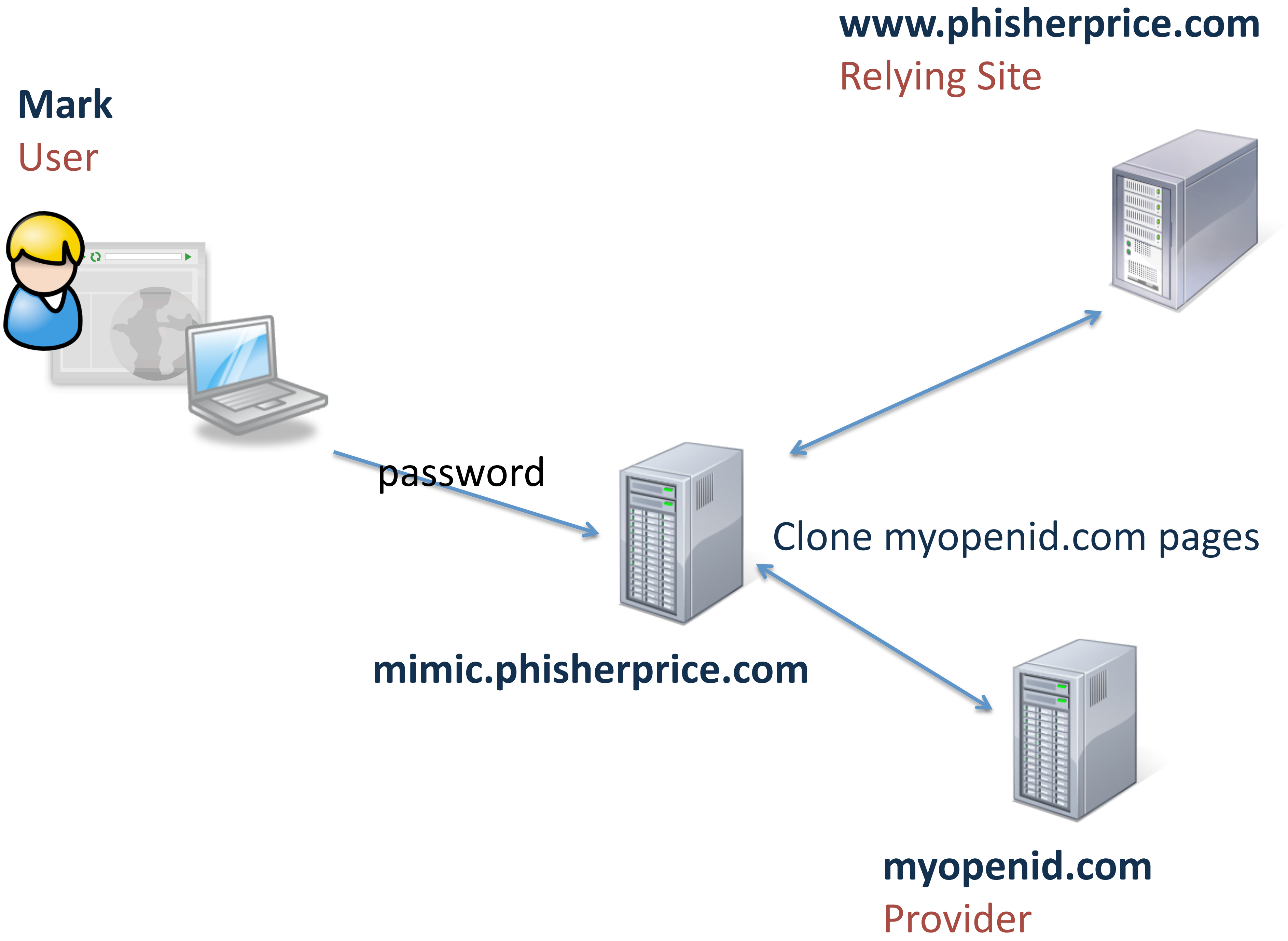
- counterpoint:
- you probably already have that problem
  - sites often allow you to reset password by email
  - if your email is compromised, so is everything else

# Phishing






www.phisherprice.com
Relying Site
Mark
User
I am mheiges.myopenid.com
redirect to mimic.phisherprice.com
Clone myopenid.com pages
mimic.phisherprice.com
myopenid.com
Provider



**www.phisherprice.com**
Relying Site

**Mark**
User

password

Clone myopenid.com pages

**mimic.phisherprice.com**

**myopenid.com**
Provider

# Phishing Mitigation

- Pre-authenticate only.
  - Verisign PIP
- Multi-factor authentication
  - Yubikey + clavid.com
- Client-side certificates
- Other standard anti-phish techniques
- User Education

# Lost Identity

- OP goes out of business
- Your domain is not renewed
- Now you are shut out of your accounts

# Profiling

- OP tracks the sites you log in to

# No Trust

- allows fake identities
- proposals for foaf, web of trust, + sreg

# More Info

- OpenID protocol
  - http://www.theserverside.com/news/1364125/Using-OpenID
  - http://openid.net/pres/protocolflow-1.1.png
- Books
  - OpenID: The Definitive Guide: Identity for the Social Web
- Critiques
  - http://www.untrusted.ca/cache/openid.html
    - response: http://daveman692.livejournal.com/310578.html
- Code
  - http://wiki.openid.net/w/page/12995176/Libraries