COMPUTER SECURITY

User Authentication and Password Management

(Phishing Attack)

Lecture 5-2

4th stage – (2020-2021)

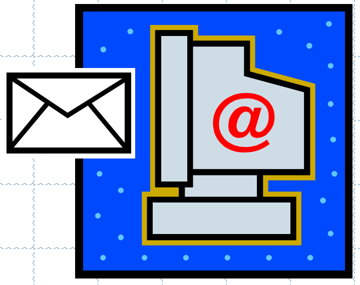
Dr. Moceheb Lazam Shuwandy

OUTLINE

- Phishing and online ID Theft
  - Phishing pages, server auth, transaction generators, secure attention sequence
- Two-factor authentication
  - Biometrics, one-time pwd tokens
- Server-side password functions
  - Ruby-on-Rails, pwd registration, email confirmation, OpenID

PHISHING ATTACK

Sends email: "There is a problem with your eBuy account"



Password sent to bad guy

User clicks on email link to www.ebuj.com.

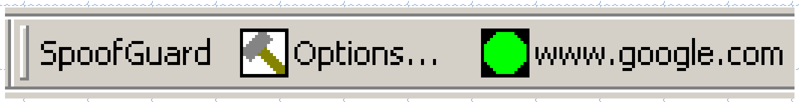
User thinks it is ebuy.com, enters eBuy username and password.

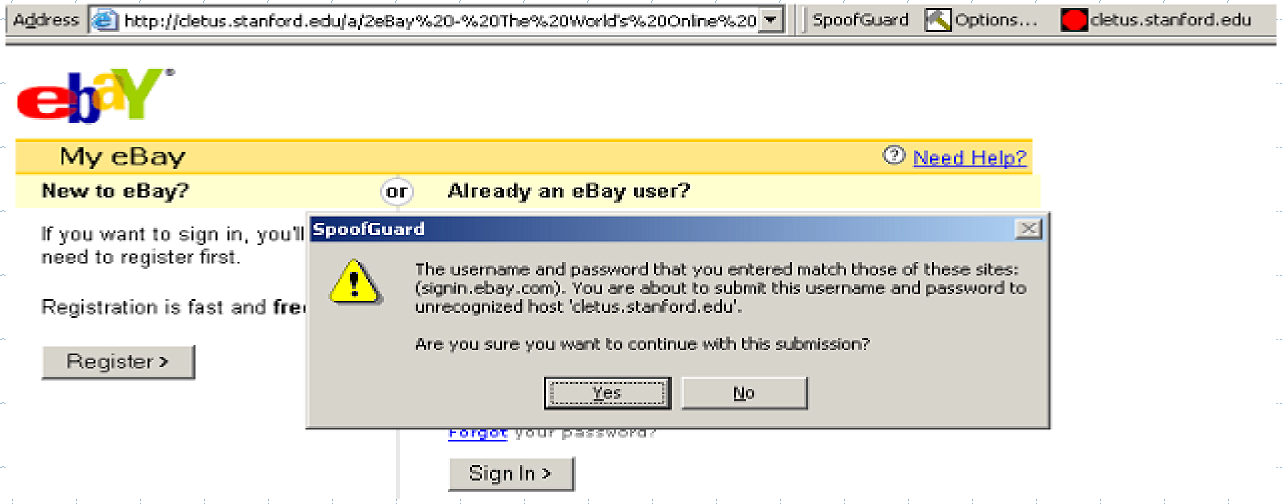
TYPICAL PROPERTIES OF SPOOF SITES

- Show logos found on the honest site
  - Copied jpg/gif file, or link to honest site
- Have suspicious URLs
- Ask for user input
  - Some ask for CCN, SSN, mother's maiden name, …
- HTML copied from honest site
  - May contain links to the honest site
  - May contain revealing mistakes
- Short lived
  - Cannot effectively blacklist spoof sites
- HTTPS uncommon

SPOOFGUARD BROWSER EXTENSION

- SpoofGuard is added to IE tool bar
  - User configuration
  - Pop-up notification as method of last resort





If you want to sign in, you'll need to register first.

Registration is fast and fre

SpoofGuard

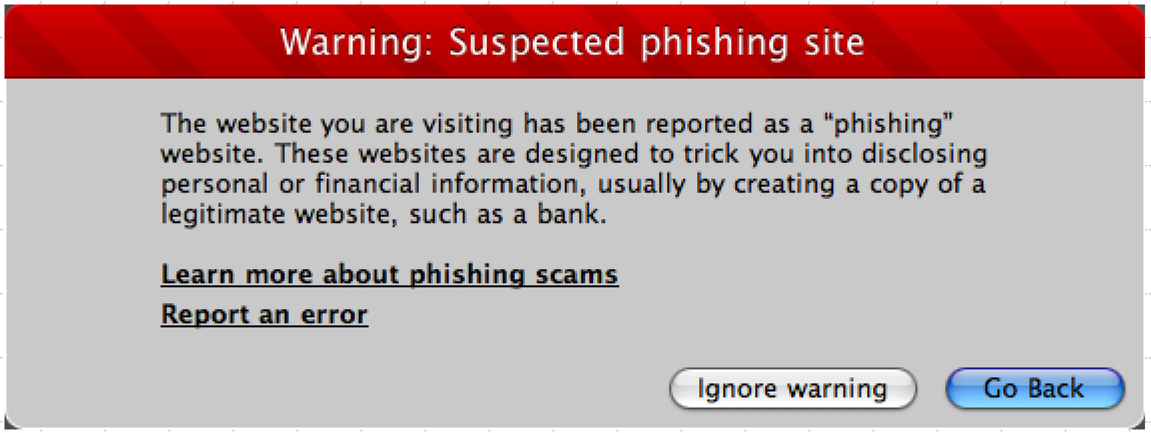
The username and password that you entered match those of these sites: (signin.ebay.com). You are about to submit this username and password to unrecognized host 'cletus.stanford.edu'.

Are you sure you want to continue with this submission?

Yes No

BROWSER ANTI-PHISHING FILTERS

- Major browsers use antiphishing measures
  - Microsoft antiphishing and anti-malware tool for IE
  - Firefox – combination of tools, including Google
  - Opera uses Haute Secure to provide bogus site warnings to end users
  - Google – own antiphishing technology in Chrome
  - Apple added antiphishing to Safari 3.2 (Nov '08)


Warning: Suspected phishing site

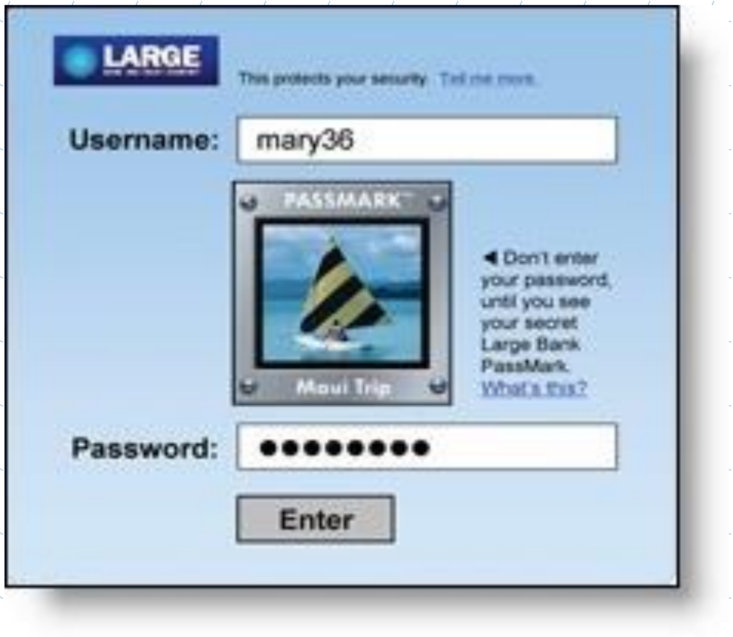
The website you are visiting has been reported as a "phishing" website. These websites are designed to trick you into disclosing personal or financial information, usually by creating a copy of a legitimate website, such as a bank.

Learn more about phishing scams

Report an error

PassMark™

Two-Factor Two-Way Authentication™



LARGE

This protects your security. Tell me more.

Username: mary36

PASSMARK

Maui Trip

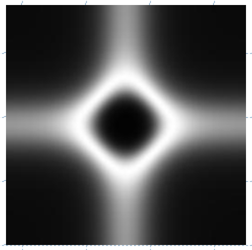
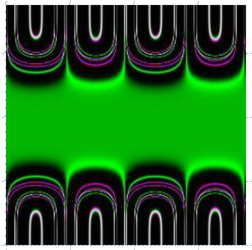
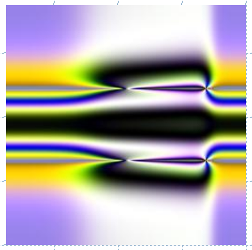
◀ Don't enter your password, until you see your secret Large Bank PassMark. What's this?

Password: ●●●●●●●●

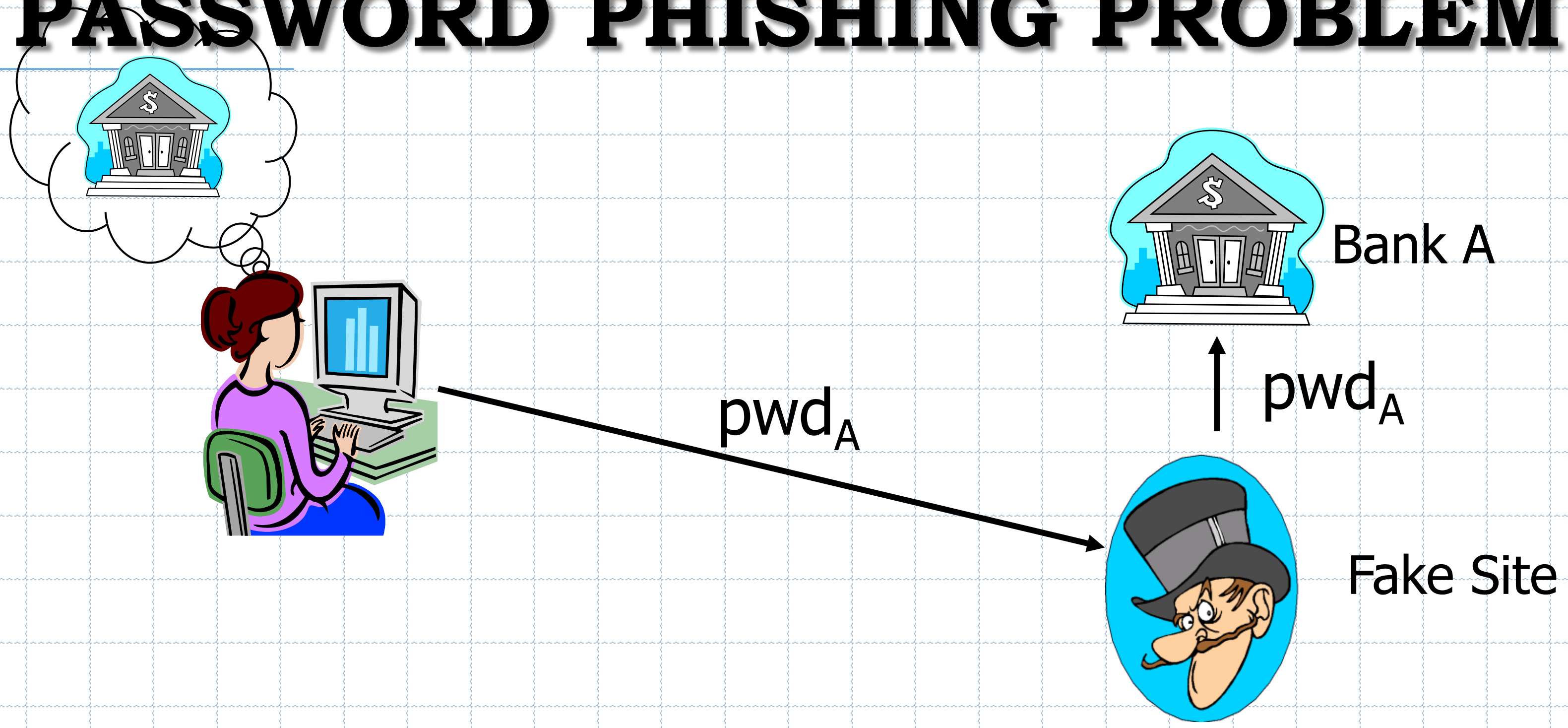
Enter

BERKELEY: DYNAMIC SECURITY SKINS

- Automatically customize secure windows
- Visual hashes
  - Random Art - visual hash algorithm
  - Generate unique abstract image for each authentication
  - Use the image to "skin" windows or web content
  - Browser generated or server generated

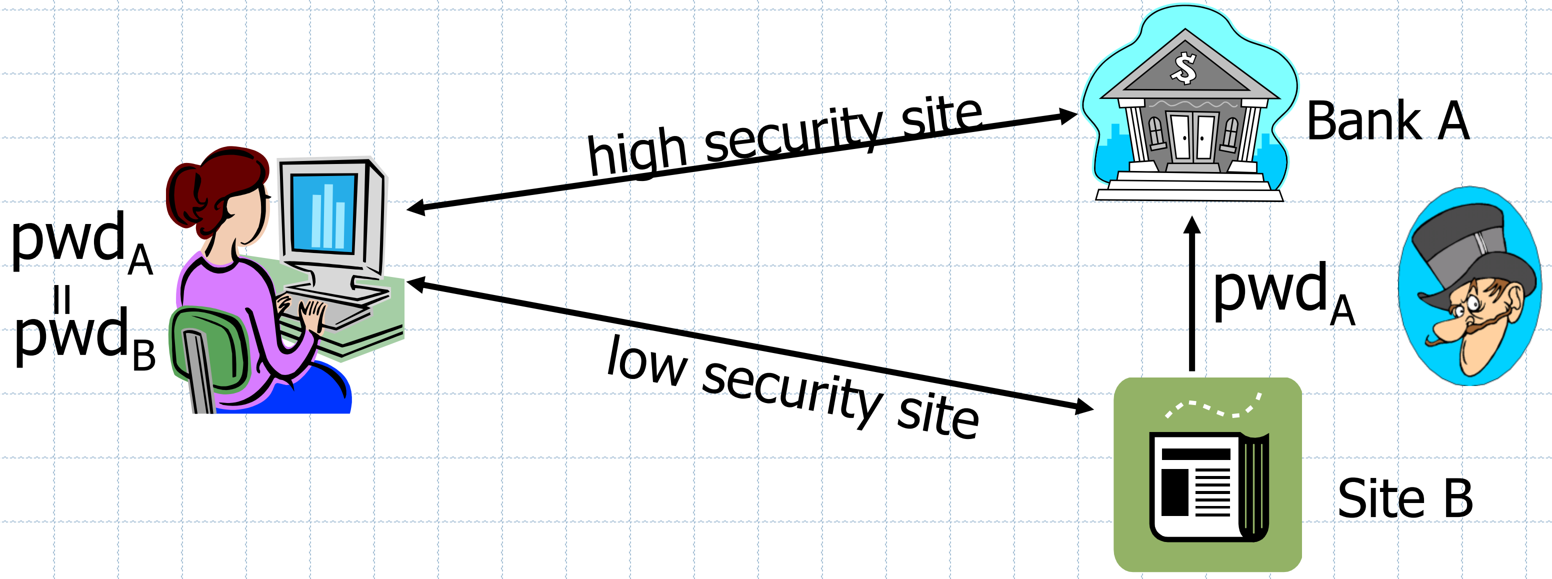




PASSWORD PHISHING PROBLEM



- User cannot reliably identify fake sites
- Captured password can be used at target site

COMMON PASSWORD PROBLEM

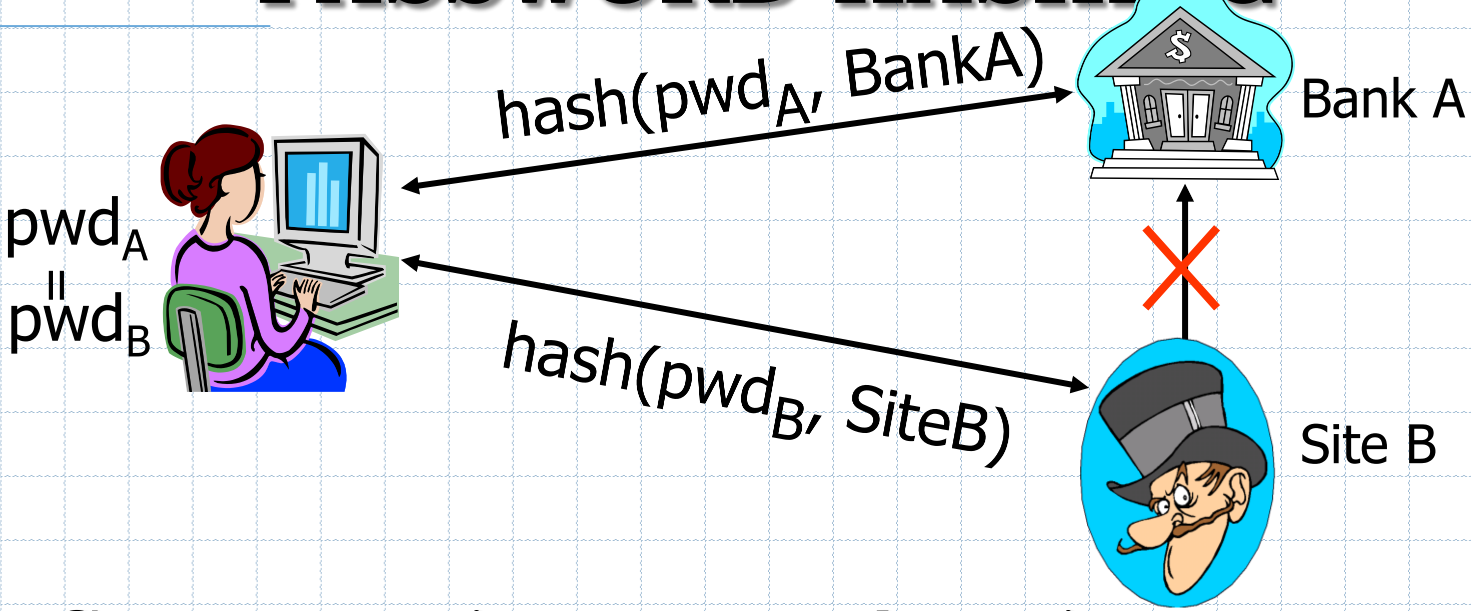


- Phishing attack or break-in at site B reveals pwd at A
  - Server-side solutions will not keep pwd safe
  - Solution: Strengthen with client-side support

STANFORD PWDHASH

- Lightweight browser extension
- Impedes password theft
- Invisible to server
    - Compute site-specific password that appears "ordinary" to server that received is
- Invisible to user
    - User indicates password to be hashed by alert sequence (@@) at beginning of pwd

PASSWORD HASHING

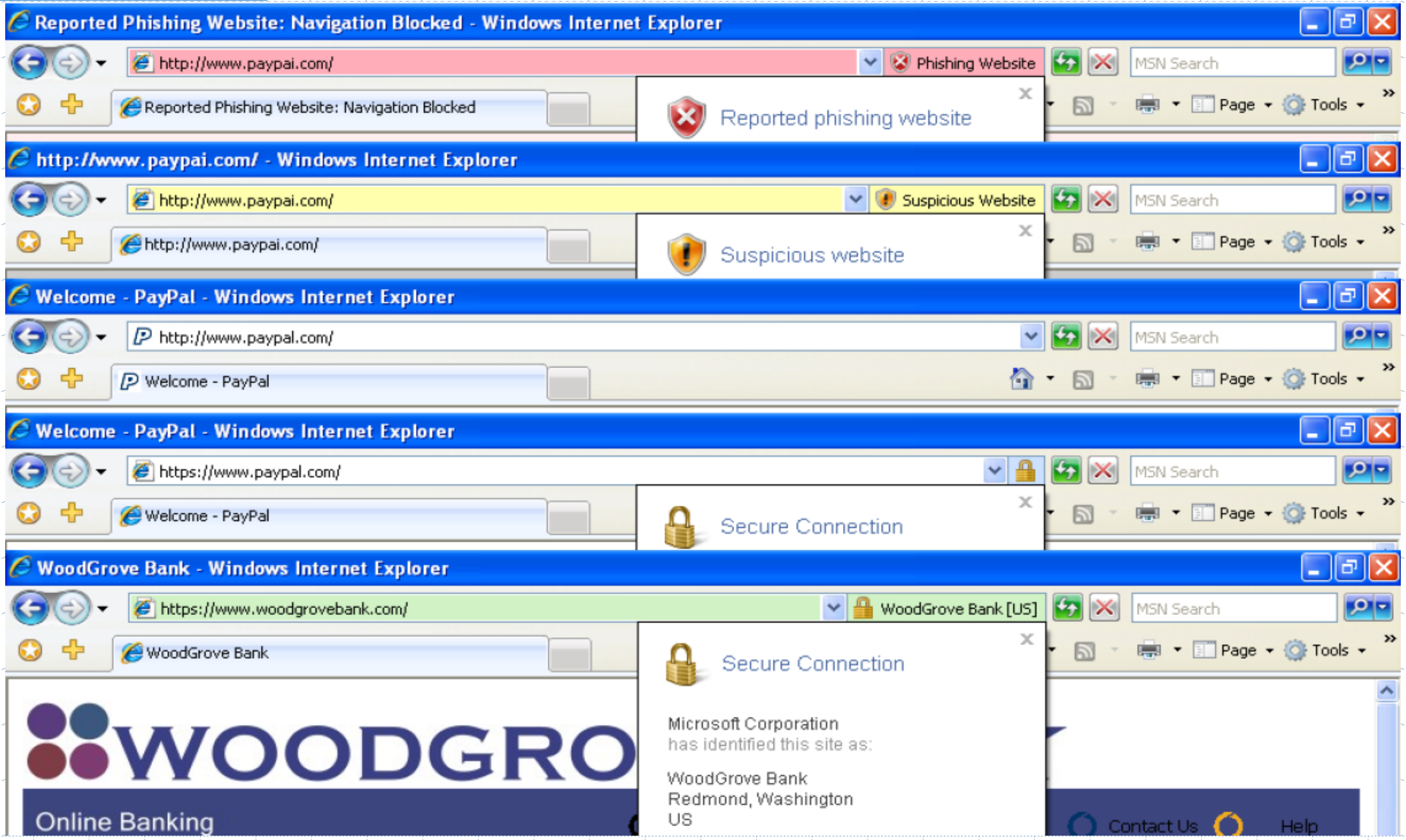


- Generate a unique password per site
  - $HMAC_{fido:123}$(banka.com) ⇒ Q7a+0ekEXb
  - $HMAC_{fido:123}$(siteb.com) ⇒ OzX2+ICiqc
- Hashed password is not usable at any other site
  - Protects against password phishing
  - Protects against common password problem

MANY TRICKY ISSUES

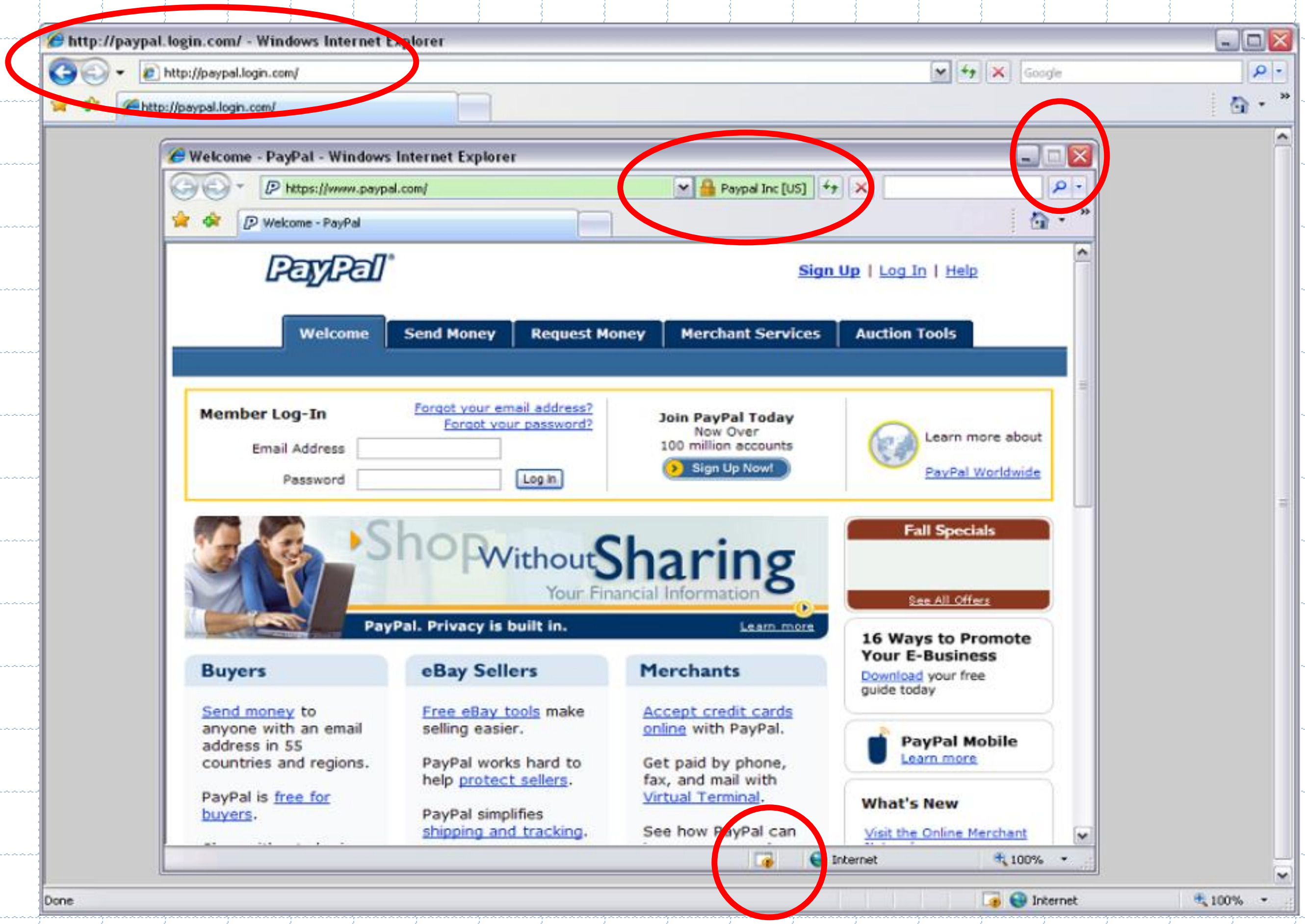
- Malicious javascript in browser
  - Implement keystroke logger, keep scripts from reading user password entry
- Password reset problem
- Internet café
- Dictionary attacks (defense: added salt)

ANTI-PHISHING FEATURES IN IE7



Reported Phishing Website: Navigation Blocked - Windows Internet Explorer
http://www.paypai.com/
Phishing Website
MSN Search
Reported Phishing Website: Navigation Blocked
Reported phishing website
Page
Tools
http://www.paypai.com/ - Windows Internet Explorer
http://www.paypai.com/
Suspicious Website
Suspicious website
Welcome - PayPal - Windows Internet Explorer
http://www.paypal.com/
Welcome - PayPal
Welcome - PayPal - Windows Internet Explorer
https://www.paypal.com/
Welcome - PayPal
Secure Connection
WoodGrove Bank - Windows Internet Explorer
https://www.woodgrovebank.com/
WoodGrove Bank [US]
WoodGrove Bank
Secure Connection
Microsoft Corporation
has identified this site as:
WoodGrove Bank
Redmond, Washington
US
WOODGRO
Online Banking
Contact Us
Help

PICTURE-IN-PICTURE ATTACK



http://paypal.login.com/ - Windows Internet Explorer

http://paypal.login.com/

Welcome - PayPal - Windows Internet Explorer

https://www.paypal.com/ — Paypal Inc [US]

Welcome - PayPal

PayPal

Sign Up | Log In | Help

Welcome | Send Money | Request Money | Merchant Services | Auction Tools

Member Log-In

Forgot your email address?
Forgot your password?

Email Address

Password

Log In

Join PayPal Today
Now Over
100 million accounts

Sign Up Now!

Learn more about PayPal Worldwide

Shop Without Sharing Your Financial Information

PayPal. Privacy is built in. Learn more

Fall Specials

See All Offers

16 Ways to Promote Your E-Business
Download your free guide today

PayPal Mobile
Learn more

What's New

Visit the Online Merchant

Buyers

Send money to anyone with an email address in 55 countries and regions.

PayPal is free for buyers.

eBay Sellers

Free eBay tools make selling easier.

PayPal works hard to help protect sellers.

PayPal simplifies shipping and tracking.

Merchants

Accept credit cards online with PayPal.

Get paid by phone, fax, and mail with Virtual Terminal.

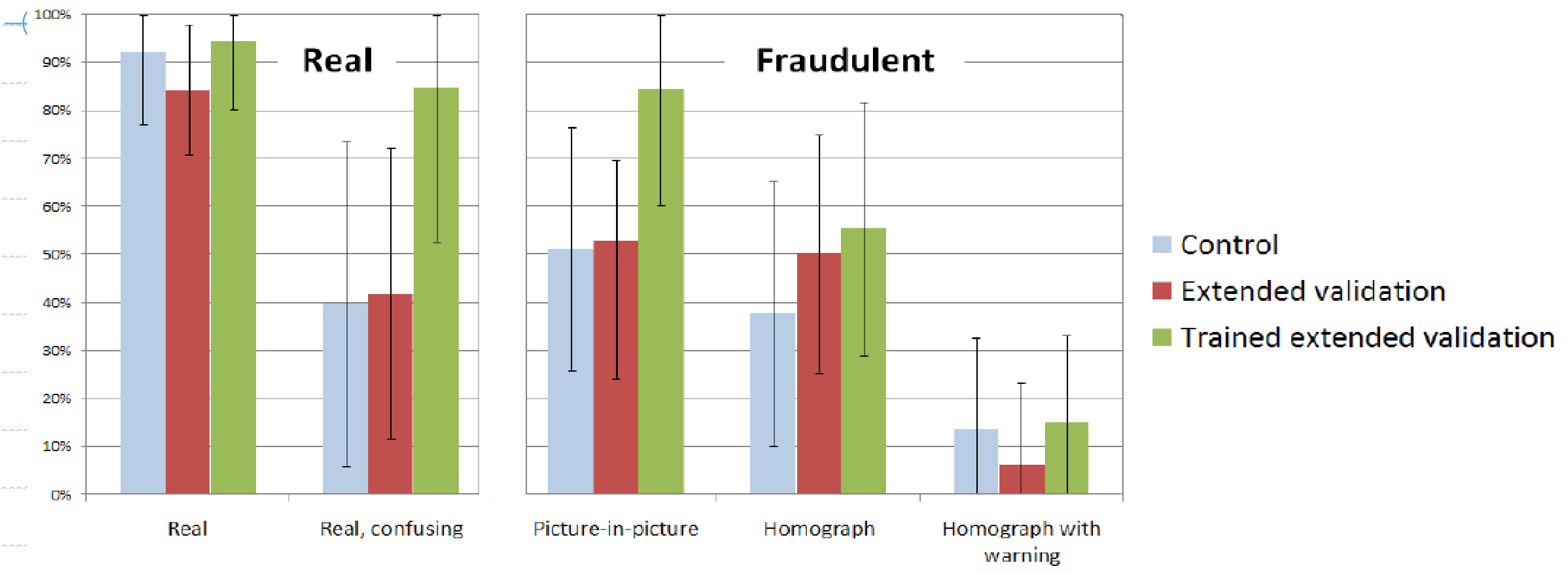
See how PayPal can

Internet 100%

Done

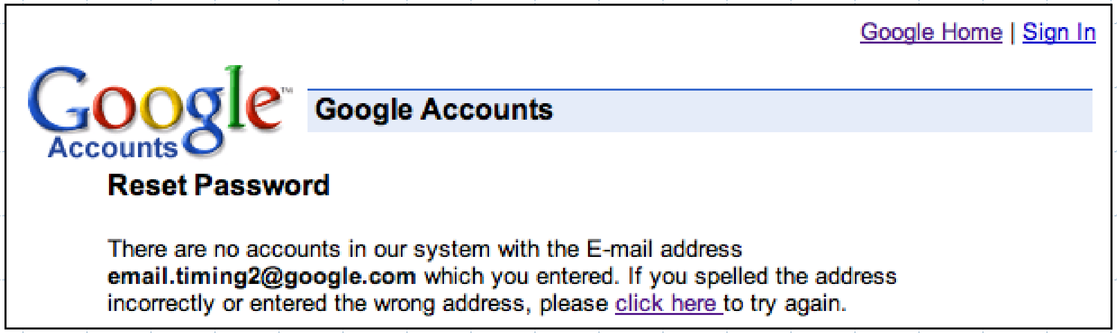
Internet 100%

RESULTS: IS THIS SITE LEGITIMATE?



WEB TIMING ATTACKS

- Most sites have "Forgot my password" pages



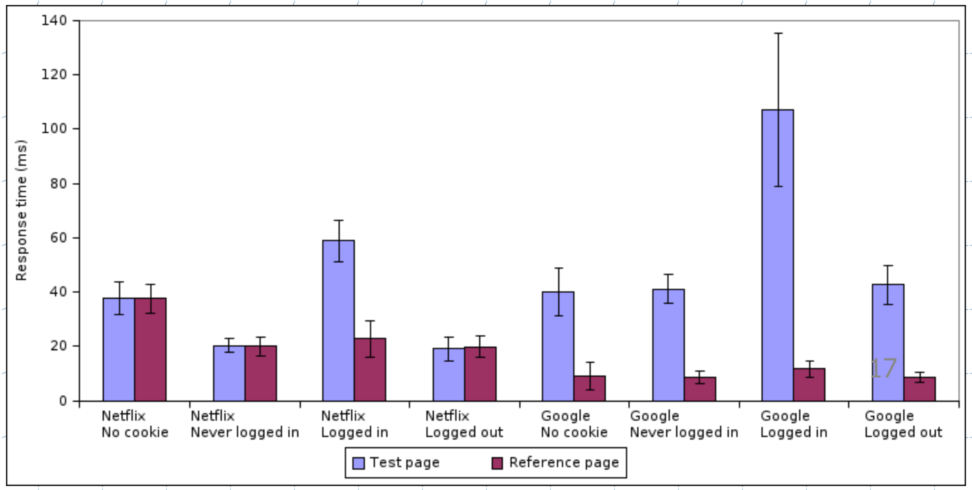
Google Home | Sign In

Google Accounts

Reset Password

There are no accounts in our system with the E-mail address **email.timing2@google.com** which you entered. If you spelled the address incorrectly or entered the wrong address, please click here to try again.

- These pages may leak whether an email is valid at that site
  - Identified through outreach to financial infrastructure company
  - Vulnerability found on virtually every site we tested
  - Communicated results, repair adopted



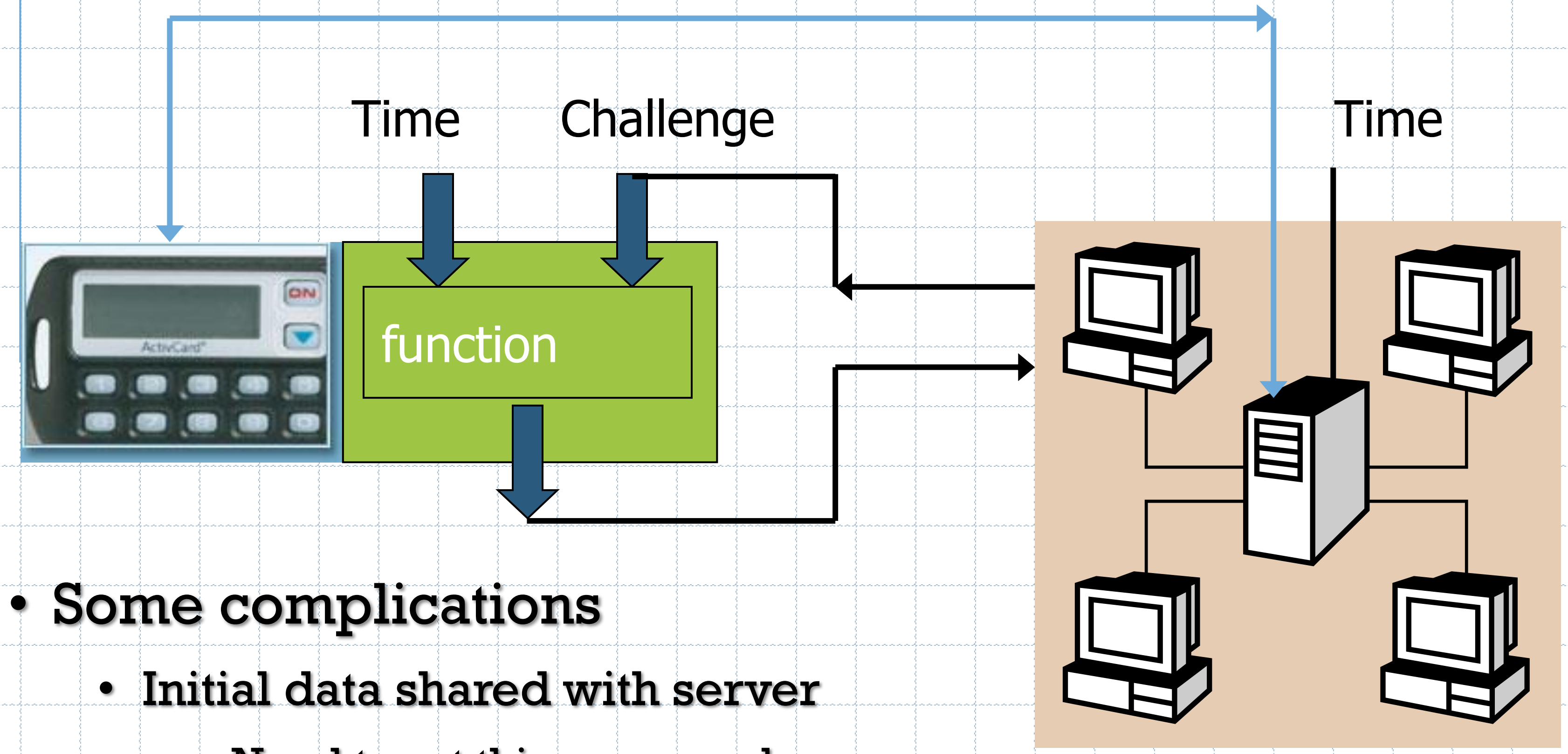
BIOMETRICS

- Use a person's physical characteristics
  - fingerprint, voice, face, keyboard timing, …
- Advantages
  - Cannot be disclosed, lost, forgotten
- Disadvantages
  - Cost, installation, maintenance
  - Reliability of comparison algorithms
    - False positive: Allow access to unauthorized person
    - False negative: Disallow access to authorized person
  - Privacy?
  - If forged, how do you revoke?

TOKEN-BASED AUTHENTICATION

- Several configurations and modes of use
  - Device produces password, user types into system
  - User unlocks device using PIN
  - User unlocks device, enters challenge
- Example: S/Key
  - User enters string, devices computes sequence
    - p_0 = hash(string|rand); p_{i+1} = hash(p_i)
    - p_n placed on server; set counter k = n
  - Device can be used n times before reinitializing
    - Send p_{k-1} = to server, set k = k-1
    - Sever checks hash(p_{k-1}) = p_k , stores p_{k-1}

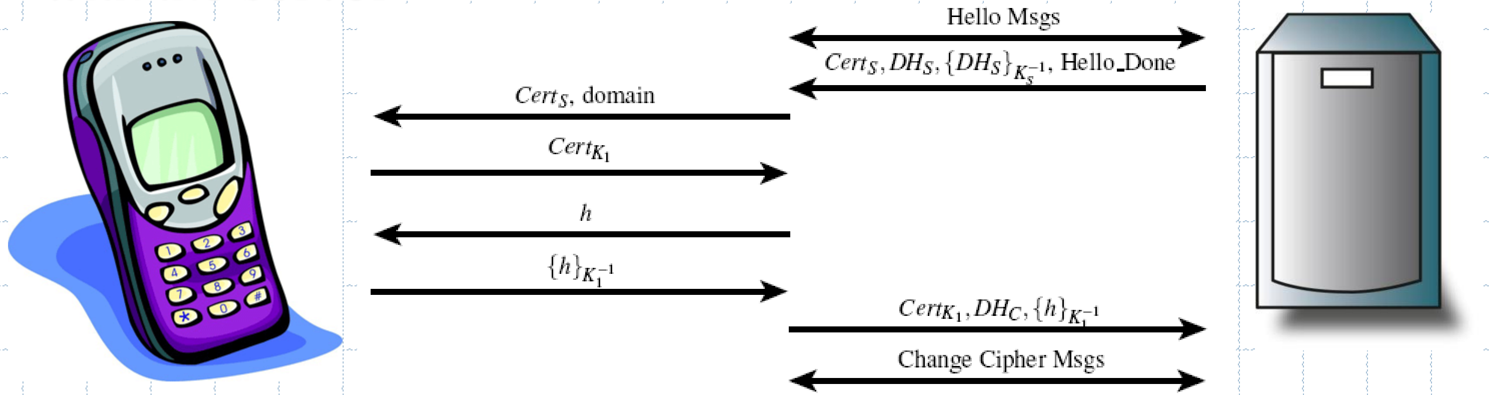
OTHER METHODS (SEVERAL VENDORS)



- Some complications
  - Initial data shared with server
    - Need to set this up securely
    - Shared database for many sites
  - Clock skew

CMU PHOOLPROOF PREVENTION

- Eliminates reliance on perfect user behavior
- Protects against keyloggers, spyware.
- Uses a trusted mobile device to perform mutual authentication with the server


Hello Msgs
$Cert_S, DH_S, \{DH_S\}_{K_S^{-1}}$, Hello_Done
$Cert_S$, domain
$Cert_{K_1}$
h
$\{h\}_{K_1^{-1}}$
$Cert_{K_1}, DH_C, \{h\}_{K_1^{-1}}$
Change Cipher Msgs

RUBY-ON-RAILS

- No built-in authentication framework
  - restful-authentication, Authlogic, Clearance
- Basic features
  - Registration of new users; validation by email address (optional)
  - Login – session creation
  - Logout – session destruction
  - Password recovery or reset
- Additional considerations
  - Hashing and/or encryption of user passwords
  - One-time or persistent tokens for cookies and validation emails
  - Multiple session support
  - Administrative controls
  - IP & login logging and other miscellaneous record keeping
  - Support for authentication platforms such as OpenID

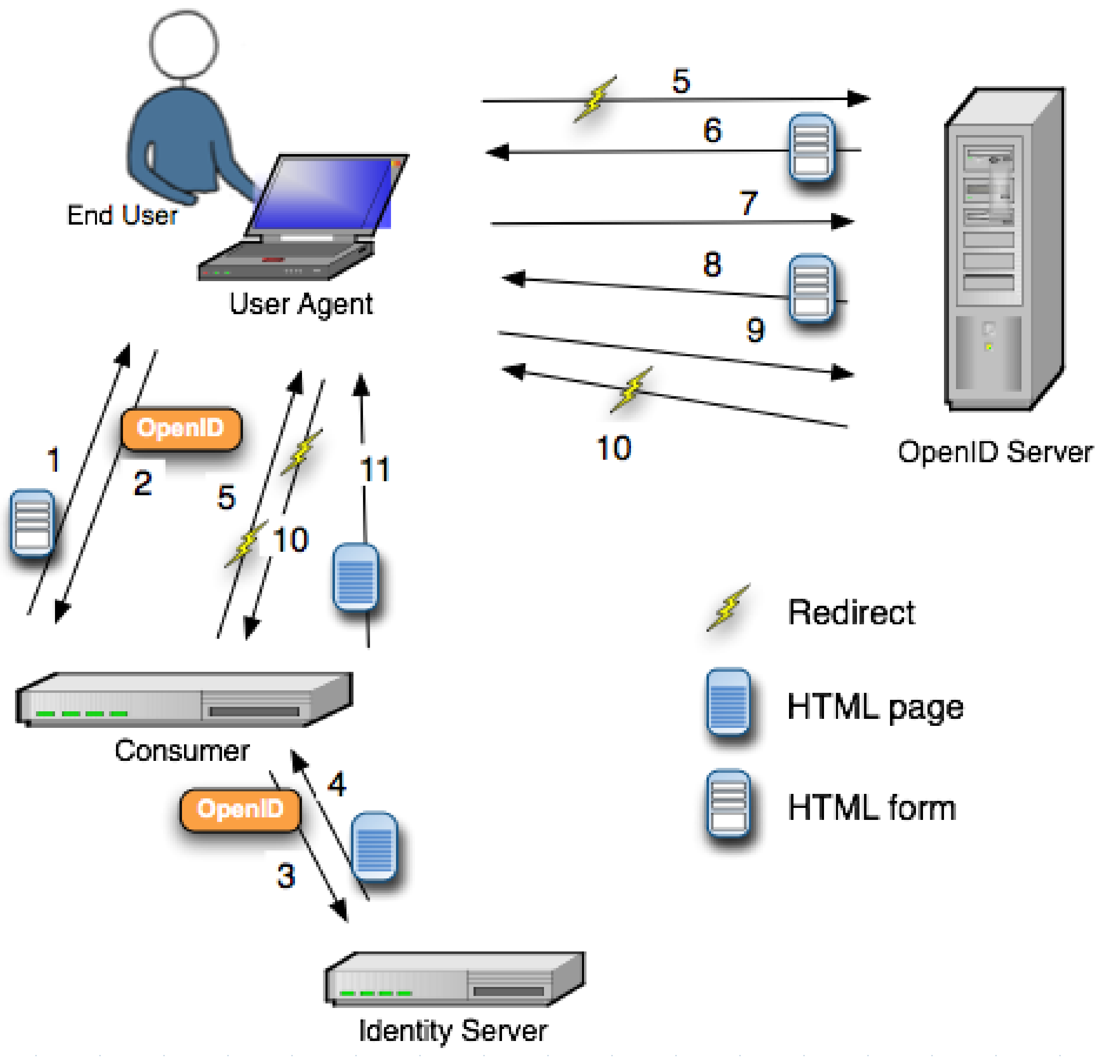
RESTFUL AUTHENTICATION

- Basic features
  - Login and logout
  - Secure password handling
  - Account activation by validating email
  - Account approval and disabling by email
  - Rudimentary hooks for authorization and access control
- Implementation
  - Uses Salt and SHA1 hash function

AUTHLOGIC

- May have some advantages
  - AuthLogic may do a better job of expiring sessions on the server side if the user's password changes or a time span elapses
  - Limits consequences of so an XSS exploit, other attacks

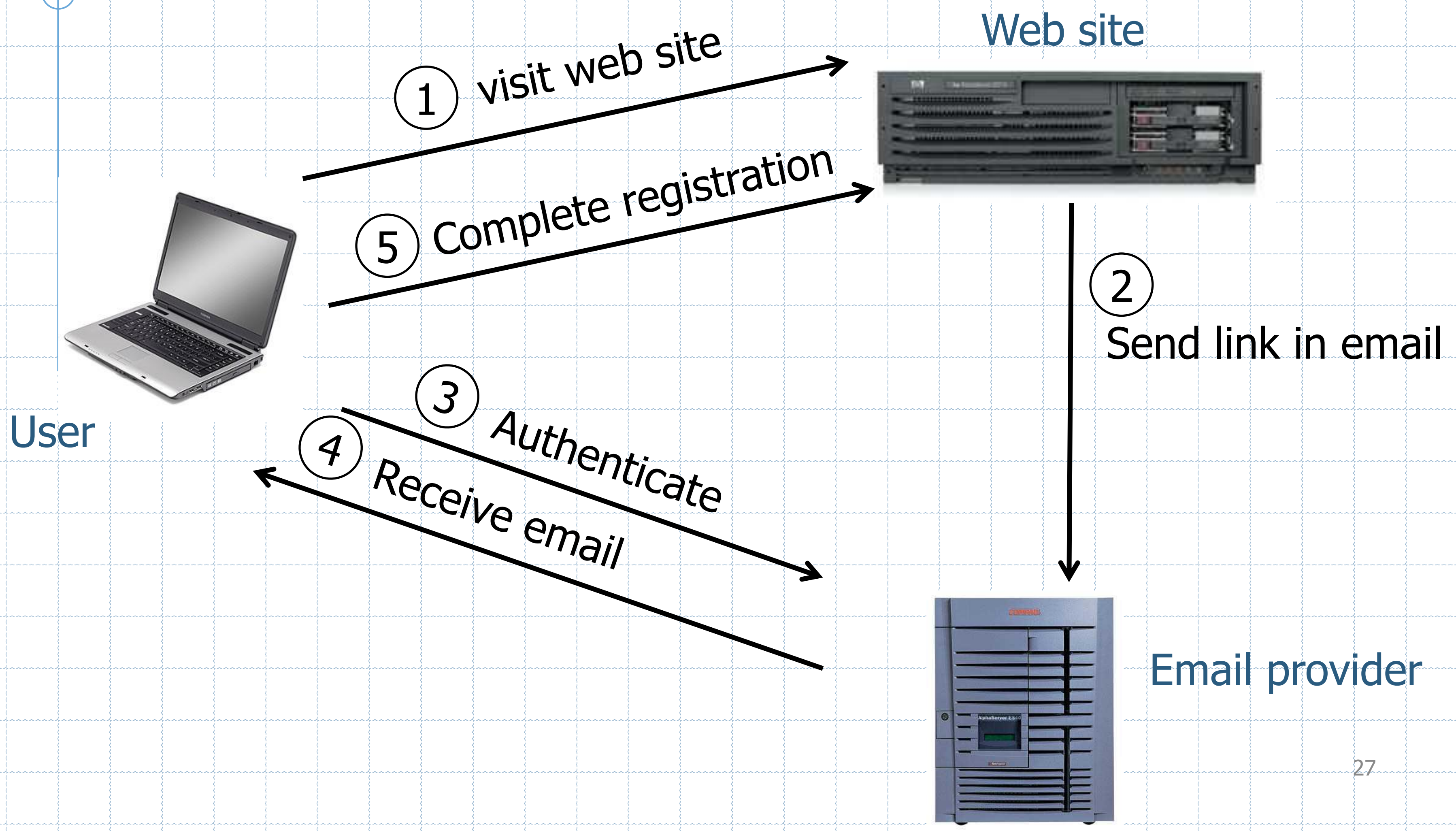
OPENID


End User
User Agent
OpenID Server
Consumer
Identity Server
OpenID
OpenID
1
2
3
4
5
5
6
7
8
9
10
10
11
Redirect
HTML page
HTML form

OPENID STEPS

1. User is presented with OpenID login form by the Consumer
2. User responds with the URL that represents their OpenID
3. Consumer canonicalizes the OpenID URL and uses the canonical version to request (GET) a document from the Identity Server.
4. Identity Server returns the HTML document named by the OpenID URL
5. Consumer inspects the HTML document header for <link/> tags with the attribute rel set to openid.server and, optionally, openid.delegate. The Consumer uses the values in these tags to construct a URL with mode checkid_setup for the Identity Server and redirects the User Agent. This checkid_setup URL encodes, among other things, a URL to return to in case of success and one to return to in the case of failure or cancellation of the request
6. The OpenID Server returns a login screen.
7. User sends (POST) a login ID and password to OpenID Server.
8. OpenID Server returns a trust form asking the User if they want to trust Consumer (identified by URL) with their Identity
9. User POSTs response to OpenID Server.
10. User is redirected to either the success URL or the failure URL returned in (5) depending on the User response
11. Consumer returns appropriate page to User depending on the action encoded in the URL in (10)

COMMON PWD REGISTRATION PROCEDURE



Q&A