Is it too late for PAKE?

John Engler
(UC Berkeley)

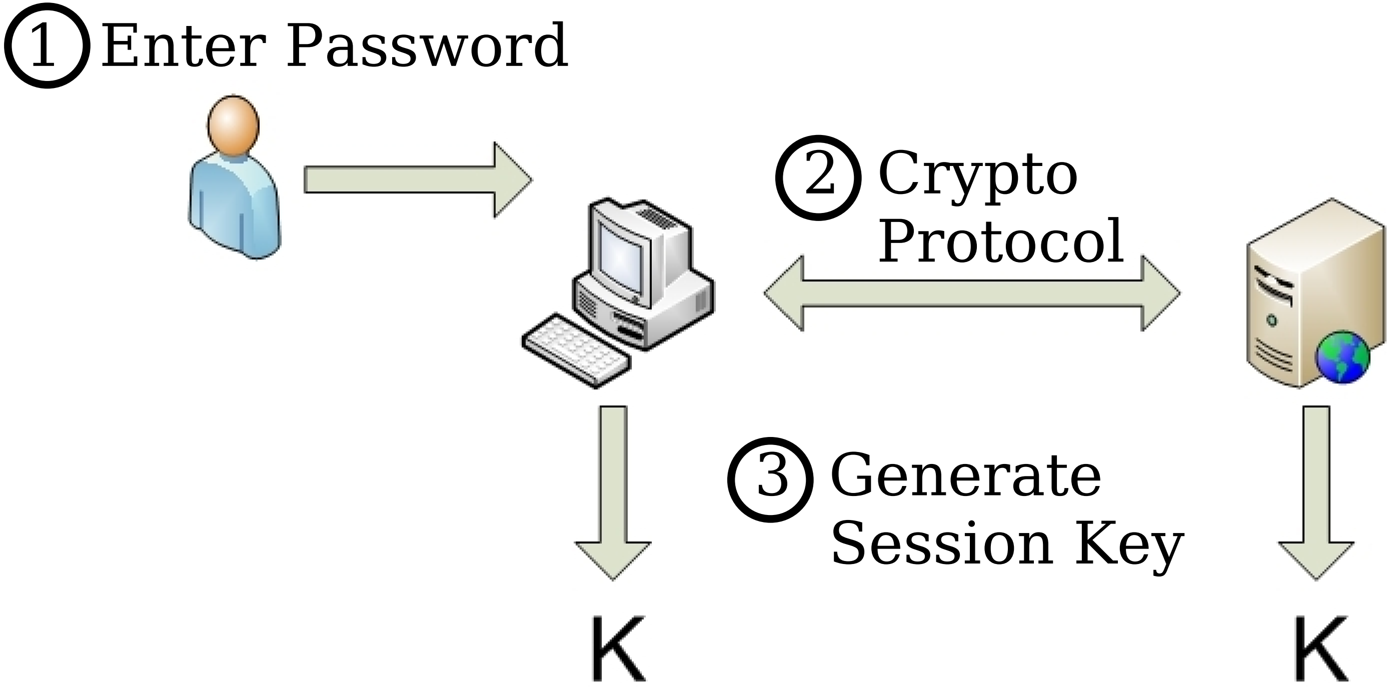
Chris Karlof
(Usable Security
Systems)

Elaine Shi
(PARC)

Dawn Song
(UC Berkeley)

What is PAKE?

- Password Authenticated Key Exchange



① Enter Password

② Crypto Protocol

③ Generate Session Key

Why PAKE?

- Password not transmitted

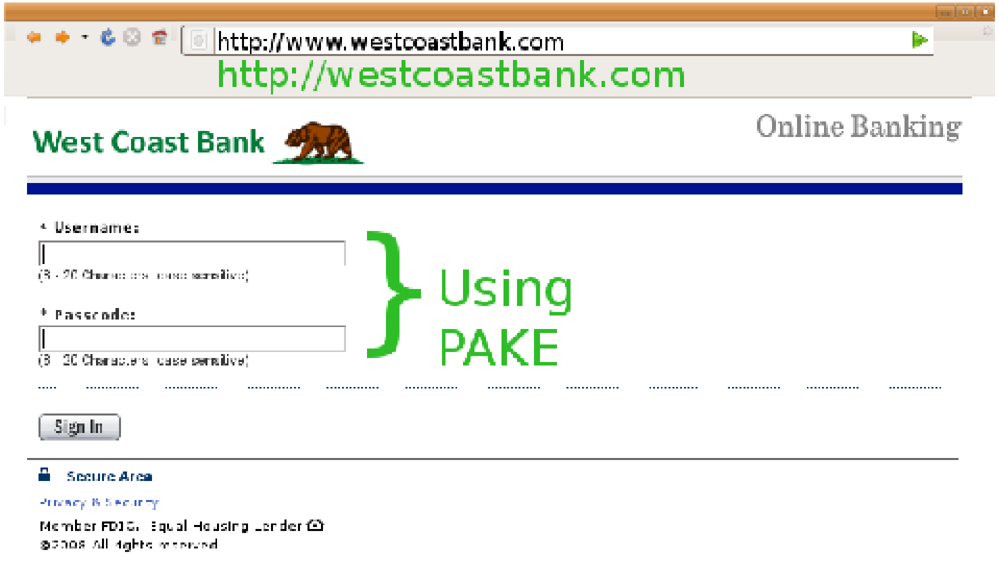
- Mutual Authentication

Two Hurdles

- Secure password entry

- Branding and message

Problem: Mimicry Attacks



http://www.westcoastbank.com

http://westcoastbank.com

West Coast Bank

Online Banking

* Username:

(3 - 20 Characters, case sensitive)

* Passcode:

(3 - 20 Characters, case sensitive)

Sign In

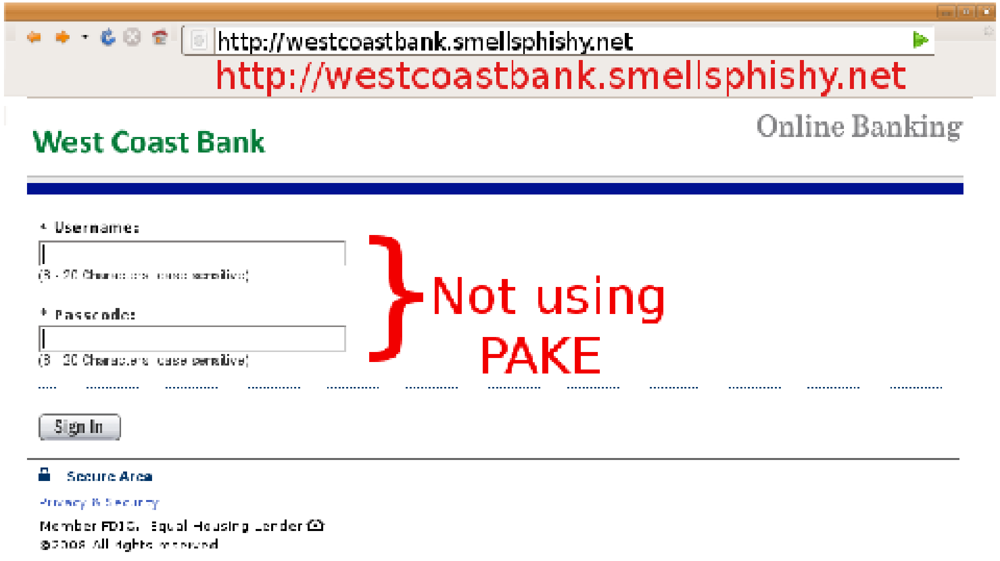
Secure Area

Privacy & Security

Member FDIC, Equal Housing Lender

©2008 All rights reserved

Using PAKE



http://westcoastbank.smellsphishy.net

http://westcoastbank.smellsphishy.net

West Coast Bank

Online Banking

* Username:

(3 - 20 Characters, case sensitive)

* Passcode:

(3 - 20 Characters, case sensitive)

Sign In

Secure Area

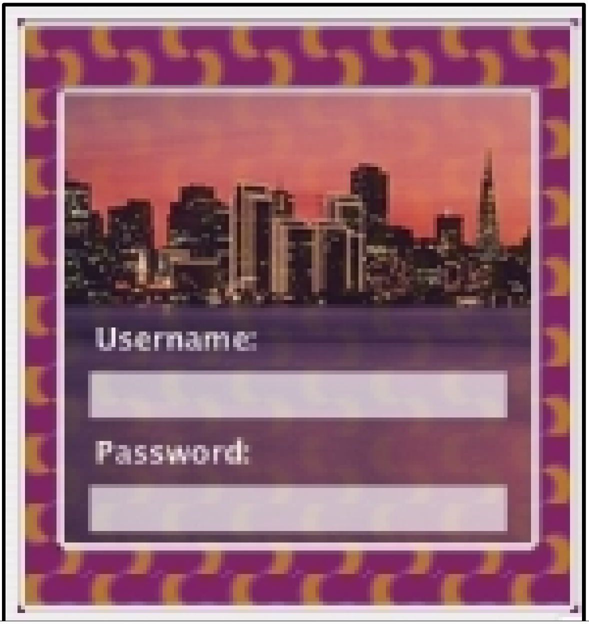
Privacy & Security

Member FDIC, Equal Housing Lender

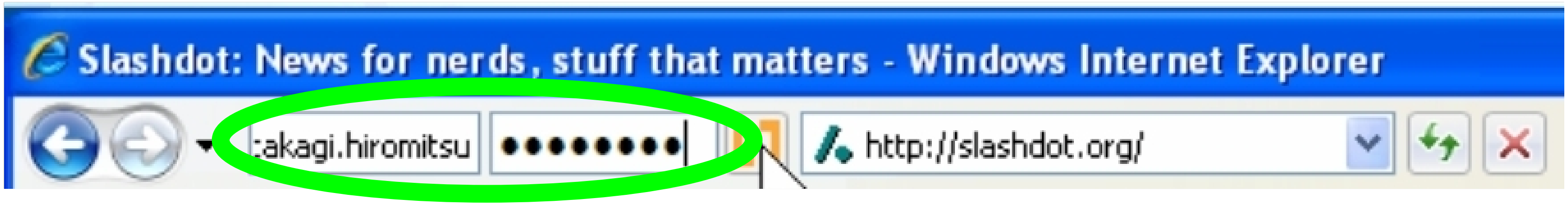
©2008 All rights reserved

Not using PAKE

Possible Solution: Secure UI



Rachna, et al. Dynamic Security Skin Login

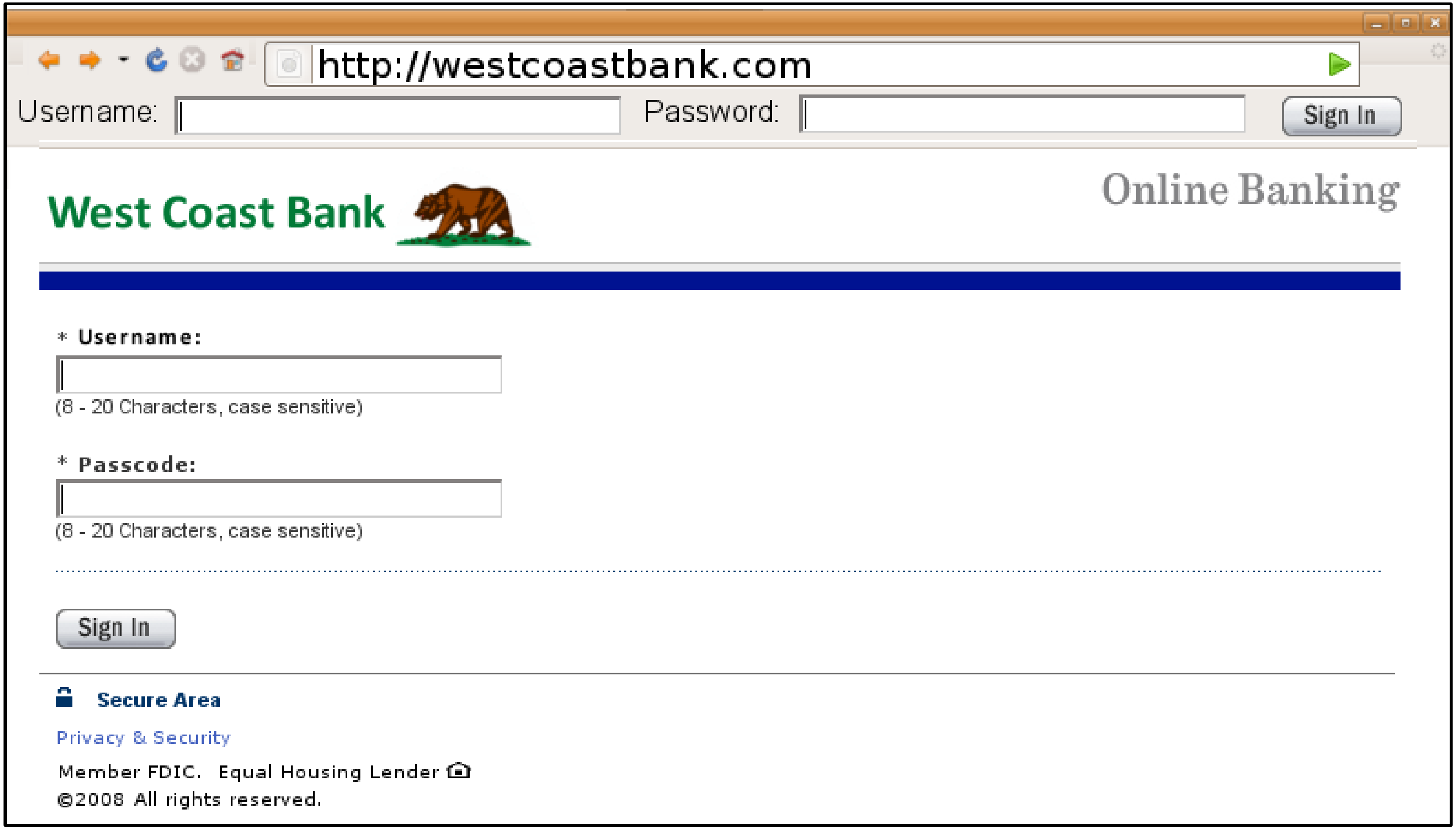

Slashdot: News for nerds, stuff that matters - Windows Internet Explorer

akagi.hiromitsu ●●●●●●●●●

http://slashdot.org/

Oiwa, et al. MAP-HTTP's In-chrome Login

Problem: Confusion Attacks



http://westcoastbank.com

Username: Password:

West Coast Bank

Online Banking

* Username:

(8 - 20 Characters, case sensitive)

* Passcode:

(8 - 20 Characters, case sensitive)

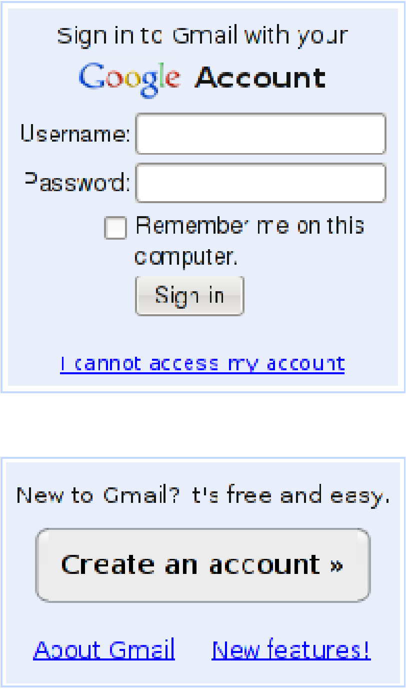
Secure Area

Privacy & Security

Member FDIC. Equal Housing Lender

©2008 All rights reserved.

Problem: Branding and Messaging



Sign in to Gmail with your

Google Account

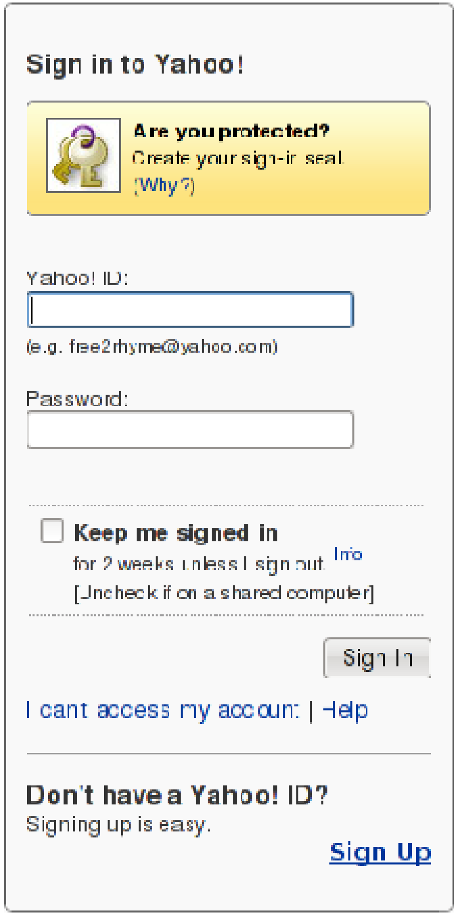
Username:

Password:

□ Remember me on this computer.

I cannot access my account

New to Gmail? It's free and easy.



Sign in to Yahoo!

Are you protected?
Create your sign-in seal.
(Why?)

Yahoo! ID:

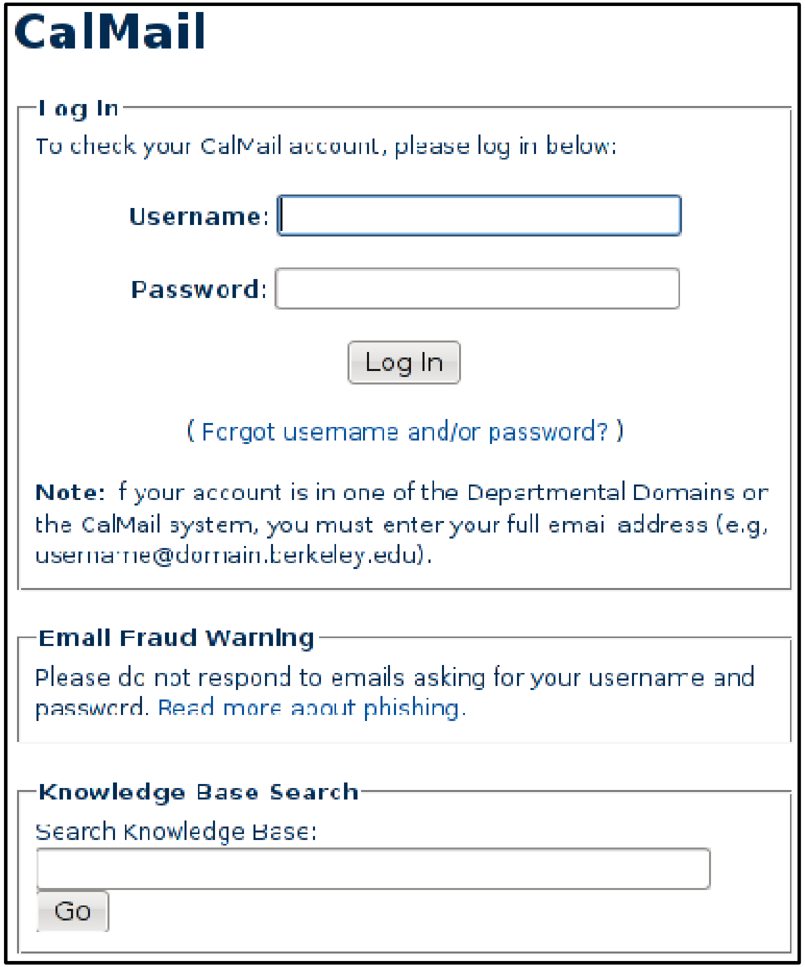
(e.g. free2rhyme@yahoo.com)

Password:

□ **Keep me signed in**
for 2 weeks unless I sign out. Info
[Uncheck if on a shared computer]

I can't access my account | Help

Don't have a Yahoo! ID?
Signing up is easy.



CalMail

Log In

To check your CalMail account, please log in below:

Username:

Password:

(Forgot username and/or password?)

Note: If your account is in one of the Departmental Domains or the CalMail system, you must enter your full email address (e.g. username@domain.berkeley.edu).

Email Fraud Warning

Please do not respond to emails asking for your username and password. Read more about phishing.

Knowledge Base Search

Search Knowledge Base:

Conclusion

- More issues remain:
  - User Training
  - Implementation
  - Deployment
- PAKE: Potential benefits but hurdles.
- Full Paper:Firefox implemenation: http://webblaze.cs.berkeley.edu/2009/pake/