

Passpet

Convenient Password Management
and Phishing Protection

Ka-Ping Yee
ping@zesty.ca

Kragen Sitaker
kragen@pobox.com

problems:

design:

solutions:

practical matters:

evaluation:

problems: the big 5

problems: the big 5

- I many passwords

problems: the big 5

- 1 many passwords
- 2 dictionary attack


problems: the big 5

- 1 many passwords
- 2 dictionary attack
- 3 password entry in webpages

Username:

Password:

☒ [Remember Me](#)

 SSL

Username:

Password:

☒ Remember me on this computer.

Email Address

Password

Username:

Password:

☐ Remember me

User Name:

Password:

Username:

Password:

Nickname

Password

(6-20 characters long)

☐ **Public Terminal**

problems: the big 5

- 1 many passwords
- 2 dictionary attack
- 3 password entry in webpages
- 4 site impersonation

Bank of the West |

←

→

↻

🏠


http://www.bankofthewest.com/BOW/home

Wednesday, July 12, 2006

中文 Chinese | Español | Locations | Employment | Contact Us | Search:

GO

BANK OF THE WEST



PERSONAL

SMALL BUSINESS

COMMERCIAL

ABOUT US

Online Banking

[Learn More](#) | [Enroll Online](#)

eTimeBanker® Sign In:

User Name:

Password:

SIGN IN

[Sign In Assistance](#)

Other Online Services:

Select...

GO

Apply Online

Select...

GO

Locations

State:

All


ZIP code:


LOCATE

SUSPICIOUS EMAIL

Protect yourself from fraud.
Report unusual email
regarding your accounts.
[READ MORE »](#)

**HOME EQUITY
LOCK IN A GREAT RATE**

Click here to find out more. 



Personal Banking

Welcome to your community bank.
First job. Last job. New home. College tuition.
We're here to help guide your finances through the
challenges of every life stage. Stop by a branch to
experience our hallmark service for yourself.

Checking

Savings & CDs

Debit & Credit Cards

Online Banking

Wealth & Trust

Consumer Loans

Mortgages

More ...

Industry Specialties

**We're not just bankers. We're business
advisors.**
From the dairy farmer to the commercial developer
to the church looking to expand, chances are good
we know what your business needs. Because

Small Business Banking

**Taking care of business. Across town. Around
the globe.**
As you navigate your business through all its cycles,
you're not on your own. We assign a dedicated
relationship manager to help you make the right
financial choices. Give us a call. We pick up the
phone!

Business Checking

Cash Management

Merchant Services

Loans & Lines

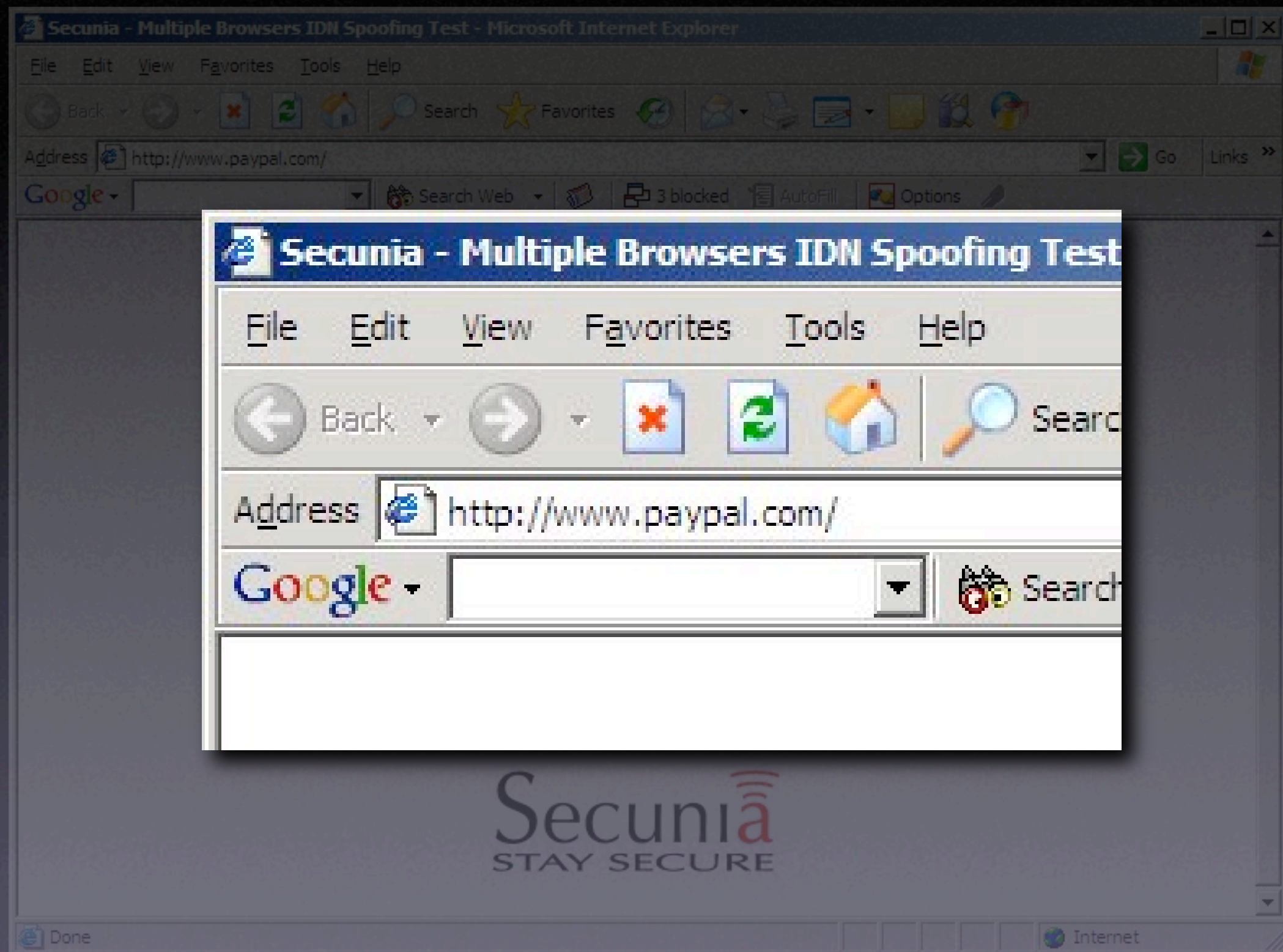
SBA Lending

More...

Commercial Banking

Your cornerstone of stability and growth.
Middle-market to multi-national, our corporate
clients give us high marks for flexible financing, fast





problems: the big 5

- 1 many passwords
- 2 dictionary attack
- 3 password entry in webpages
- 4 site impersonation
- 5 UI spoofing

Authenticate



Installer requires that you type your password.

Name: Ka-Ping Yee

Password:

► Details



Cancel

OK

problems: the big 5

- 1 many passwords
- 2 dictionary attack
- 3 password entry in webpages
- 4 site impersonation
- 5 UI spoofing

design:

design:

- logging in
- setting up a new password
- setting up Passpet

solutions:

solutions:

- | many passwords

master secret

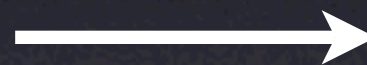


site-specific
password

site name



master secret



site-specific
password

site name



master secret



site-specific
password

site name



solutions:

- 1 many passwords
- 2 dictionary attack

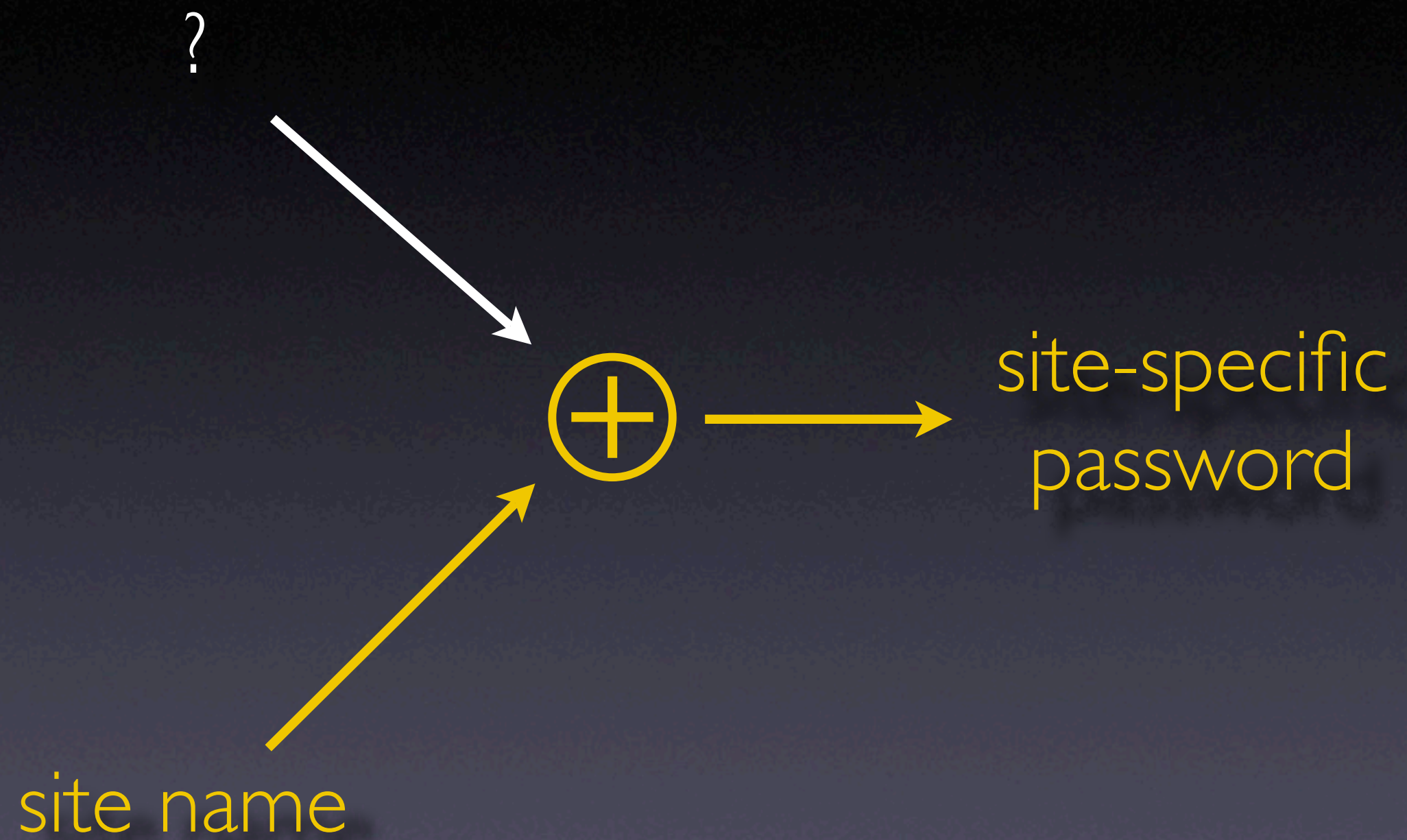
master secret

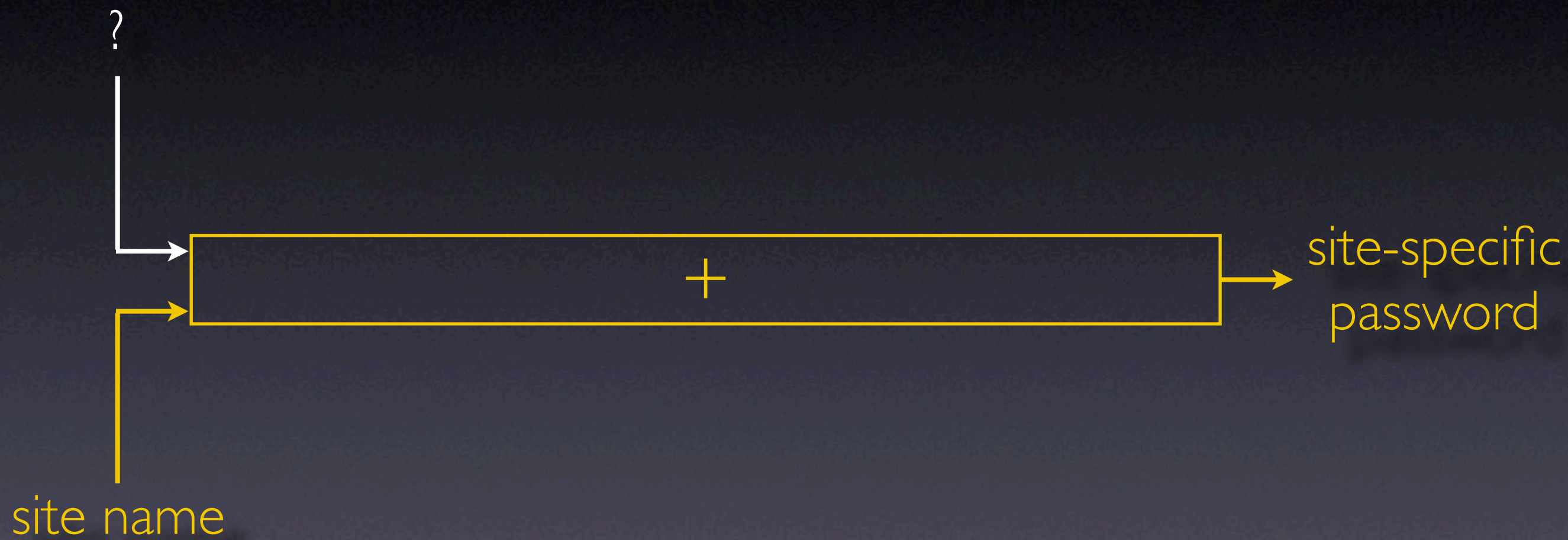


site-specific
password

site name







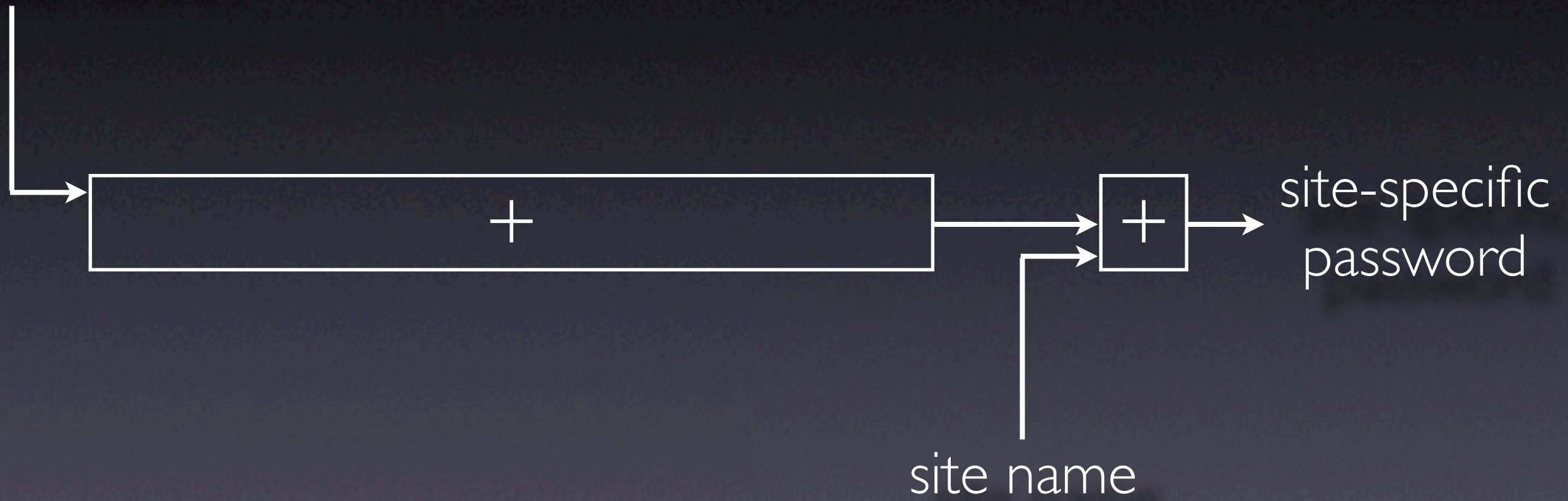
master secret

site name

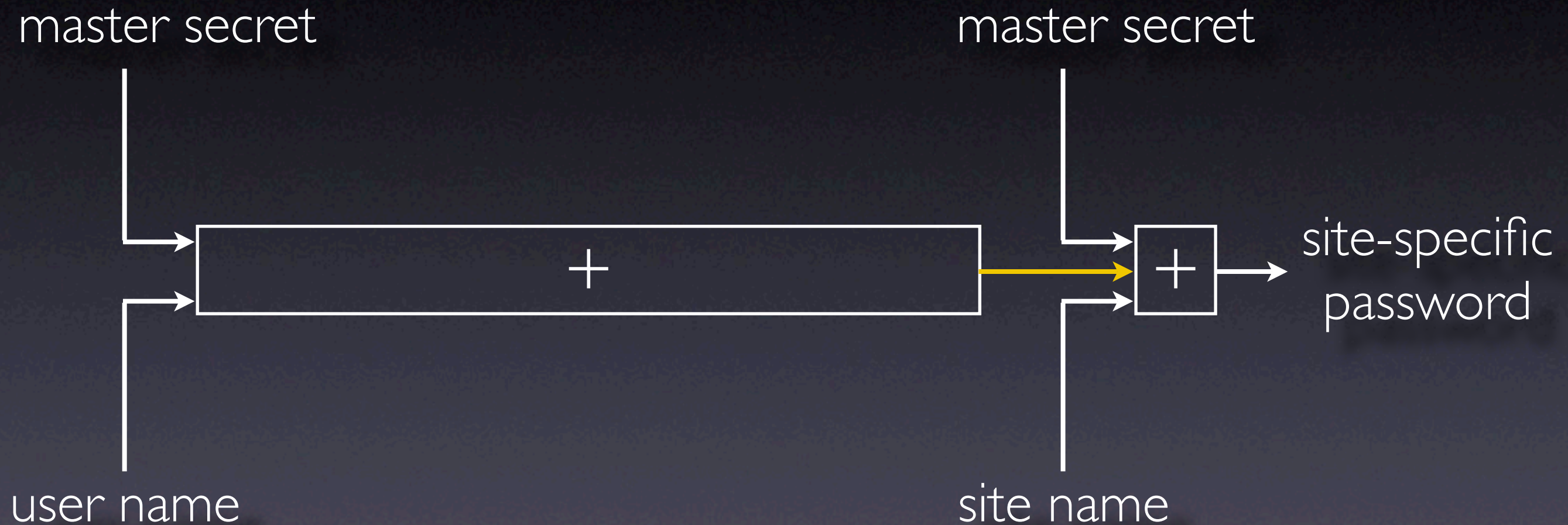


site-specific
password

master secret



Password Multiplier (Halderman, 2005)



Passpet: variable-strength password hash

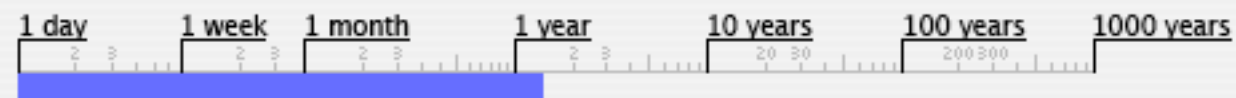
Choose your master secret.

You will only need to memorize one secret. All your passwords will be produced from this secret, so make up something hard to guess, write it down, and keep it in a safe place. For a better secret, avoid normal words and mix letters, numbers, and symbols.

Choose your master secret:

good (31 bits)

The longer you wait, the stronger your secret will get.



It would take about **1.3 years** for an attacker to guess your secret using a typical \$1000 computer made in 2006. When you are happy with it, enter it again below.

Confirm your master secret:

Cancel

Use this master secret

Give responsive feedback
on password strength.

solutions:

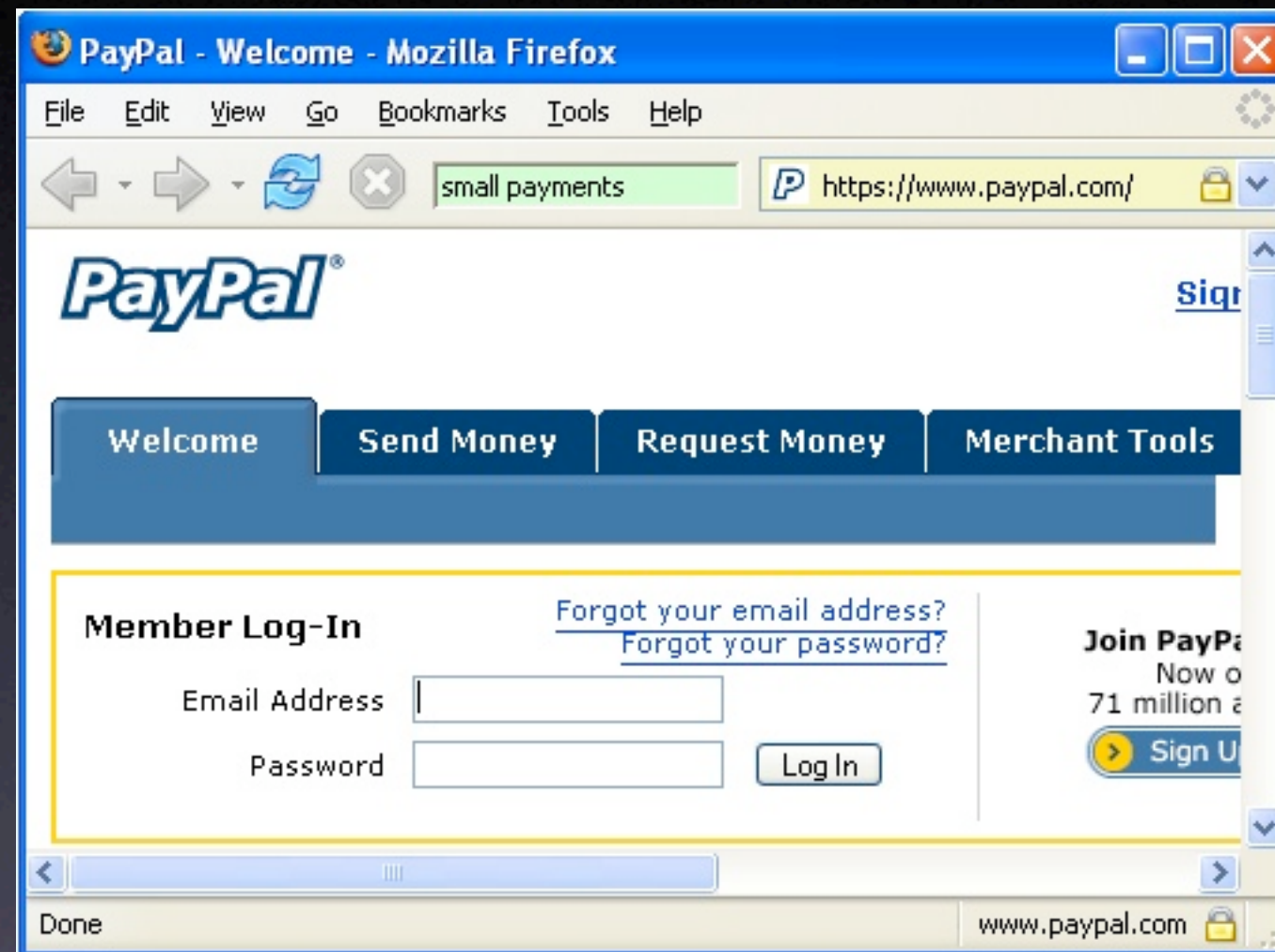
- 1 many passwords
- 2 dictionary attack
- 3 password entry in webpages



solutions:

- 1 many passwords
- 2 dictionary attack
- 3 password entry in webpages
- 4 site impersonation

Petname Tool (Close, 2005)



Passpet: use site label for hashing

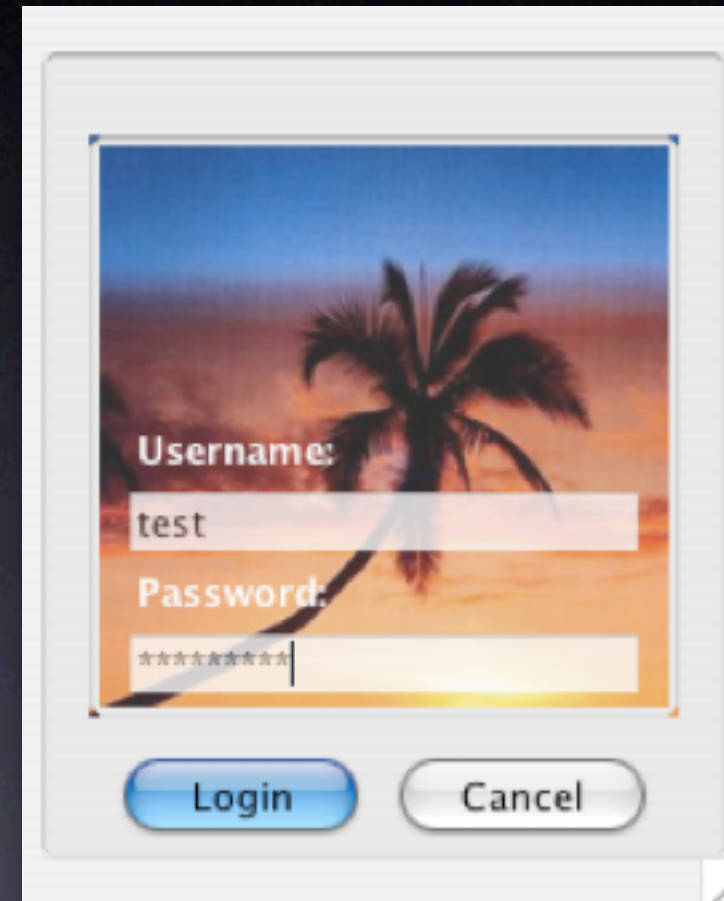
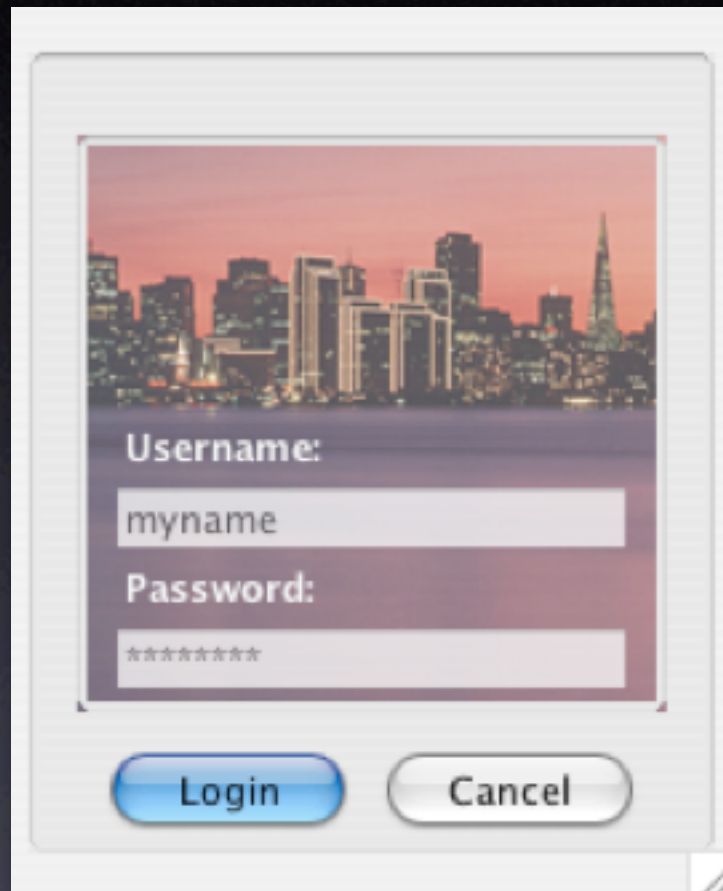


Help users rely on information
from the user, not an attacker.

solutions:

- 1 many passwords
- 2 dictionary attack
- 3 password entry in webpages
- 4 site impersonation
- 5 UI spoofing

Dynamic Security Skins (Dhamija, 2005)



Passpet: interact directly with custom icon



Passpet: interact directly with custom icon



Get the user to **interact**
with something personalized.

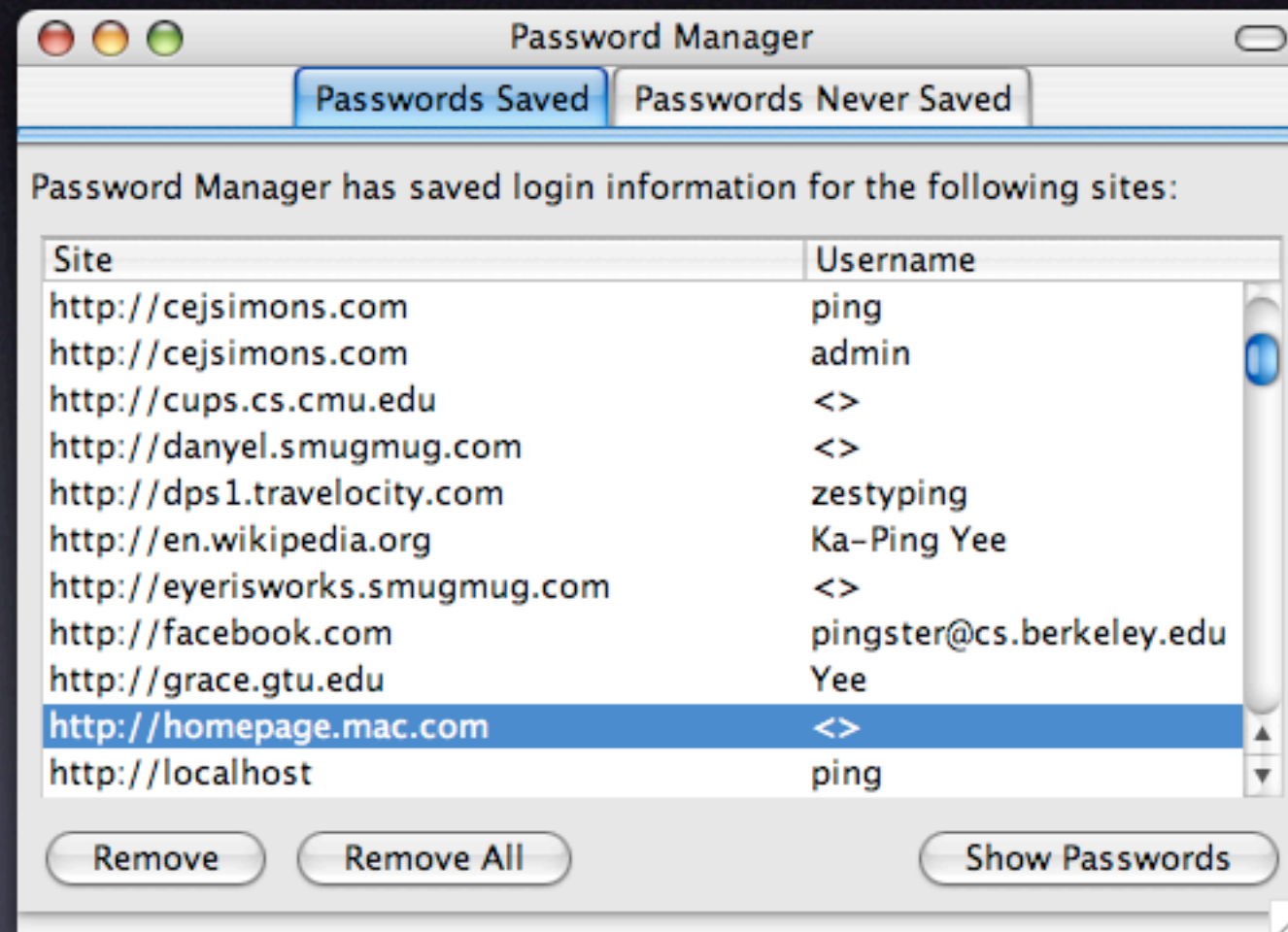
contributions:

- 1 variable-strength hashing
- 2 password strength feedback
- 3 use user-assigned labels for hashing
- 4 personalized security agent
- 5 direct interaction with customized UI

practical matters:

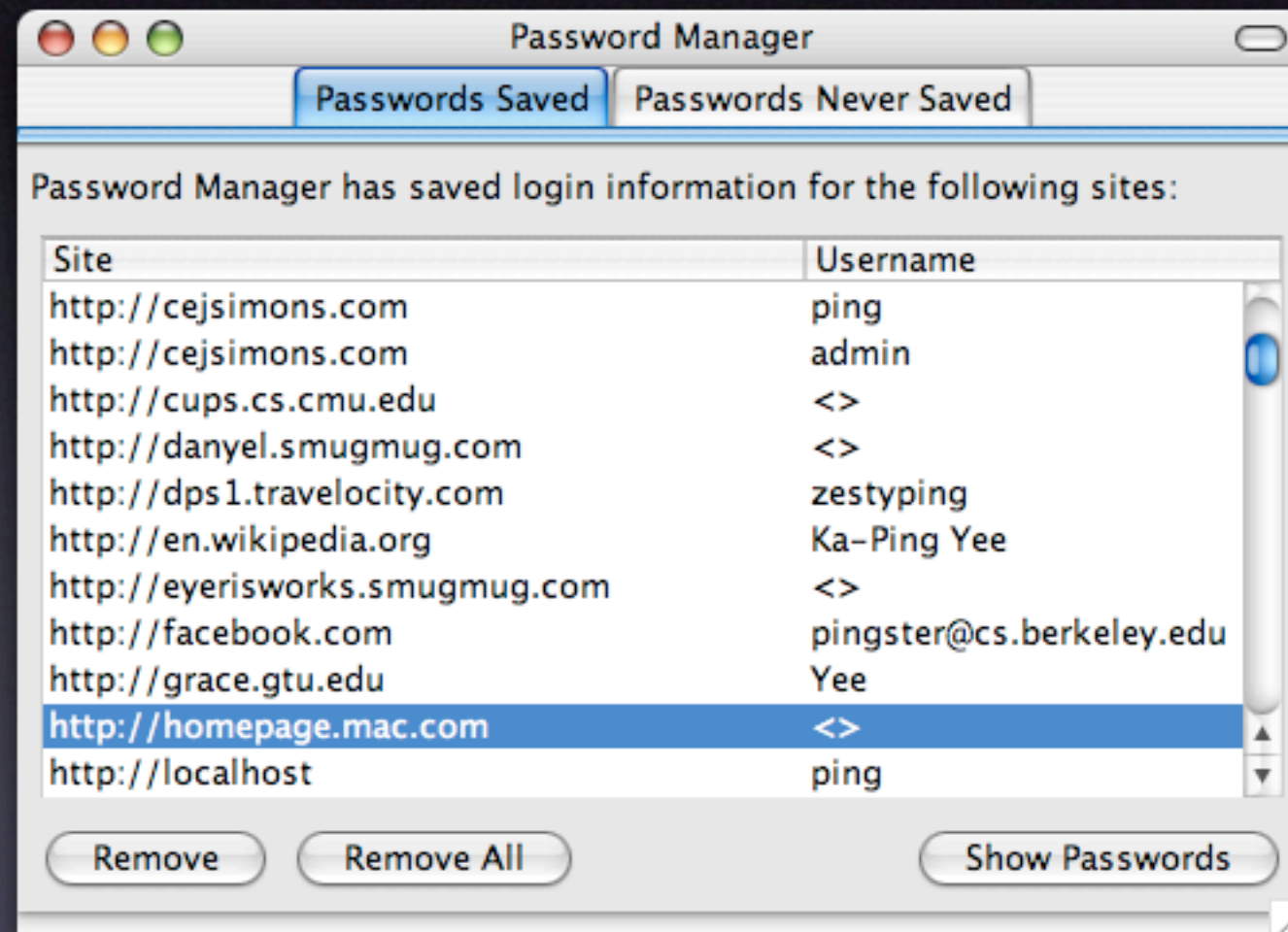
practical matters:

What if you want to use another computer?



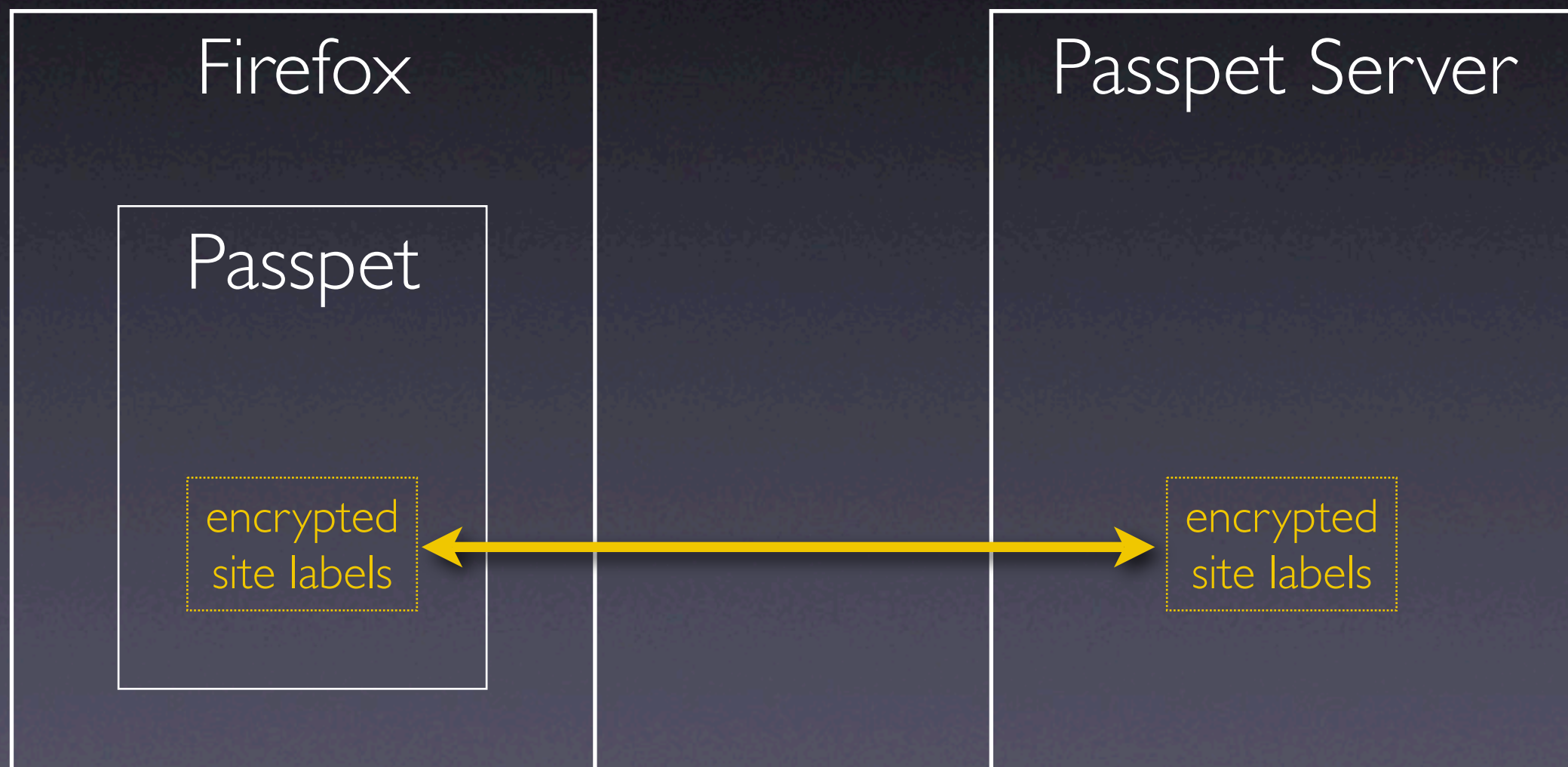
practical matters:

What if someone gets your password file?



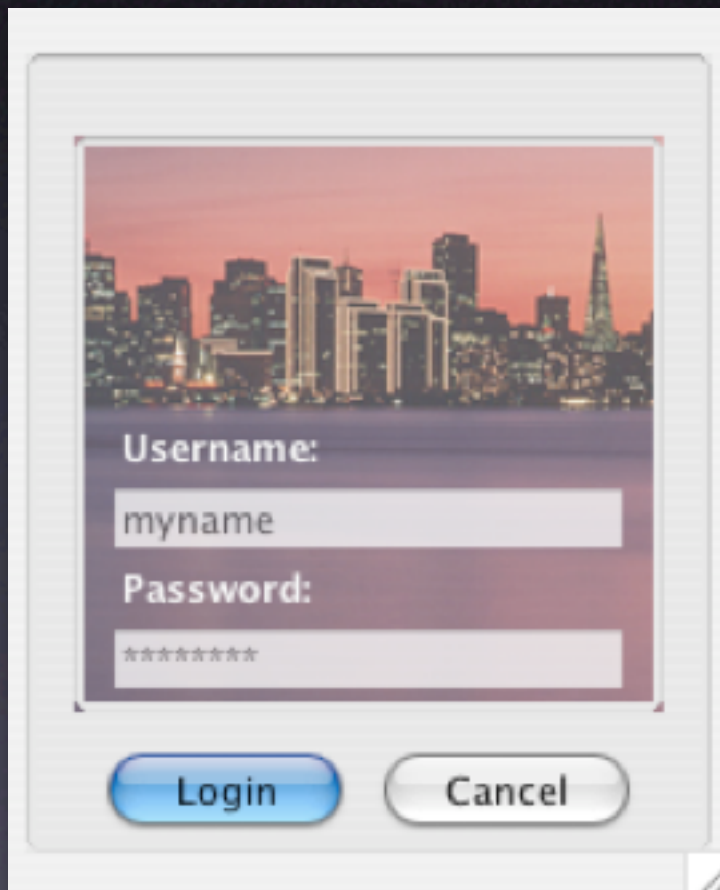
practical matters:

What if you want to use another computer?

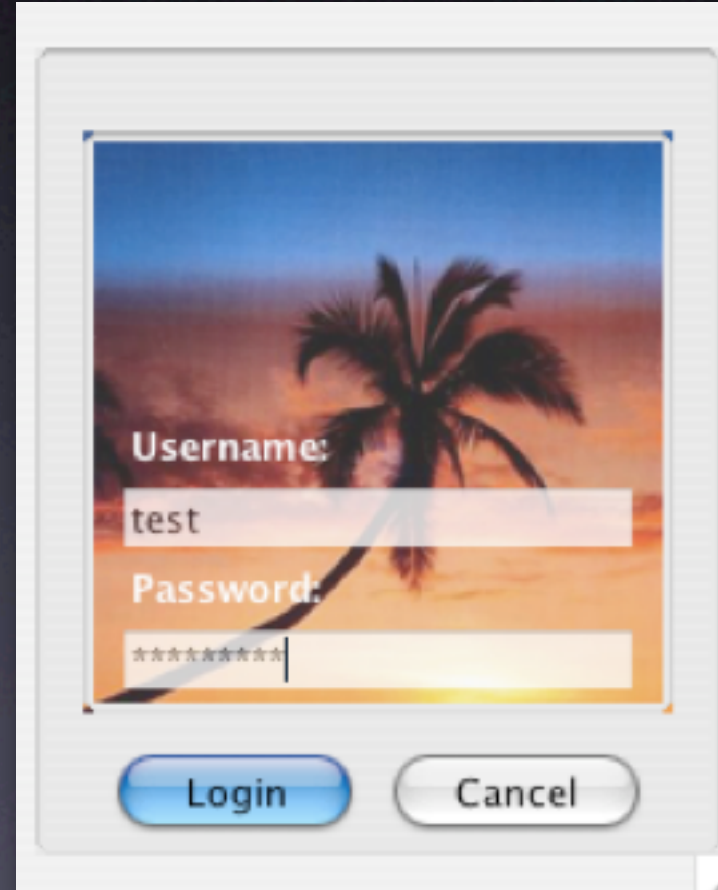


practical matters:

What if you want to use existing websites?



A login form with a background image of a city skyline at dusk. The form contains two input fields: "Username:" with the text "myname" and "Password:" with masked text "*****". Below the fields are two buttons: "Login" (blue) and "Cancel" (white).



A login form with a background image of a palm tree at sunset. The form contains two input fields: "Username:" with the text "test" and "Password:" with masked text "*****". Below the fields are two buttons: "Login" (blue) and "Cancel" (white).

practical matters:

What if you need to change a password?



Stanford PwdHash

PwdHash is a browser extension that invisibly generates theft-resistant passwords. You can activate this protection by pressing F2 before you type your password, or by choosing passwords that start with @@.

- Visit the [project website](#).
- Download the [Firefox extension](#) or the [Internet Explorer plugin](#) (beta).
- Read the [USENIX Security Symposium 2005 paper](#) (PDF).
- Send us [feedback](#).

Site Address

Site Password

Hashed Password

Version 0.8 ([more versions](#))

evaluation:

evaluation:

Passpet for Internet Explorer:

- tested at HP labs with 15 users

- main complaint: want to use other computers

Passpet for Firefox:

- not yet usability-tested

thanks:

Tyler Close (Petname Tool)

Alan Karp (Passpet user study)

David Wagner (design and cryptography)

J. Alex Halderman (Password Multiplier)

Rachna Dhamija (Dynamic Security Skins)

<http://passpet.org/>