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

1. 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
problems: the big 5

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

Small Business Banking

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

Commercial Banking

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

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
Secunia - Multiple Browsers IDN Spoofing Test

This window is serving content from Secunia.com, although the Address Bar says you are visiting: http://www.paypal.com/

This page could just as easily have been spoofed to look like a genuine PayPal page (or any other web site) asking you for e.g. usernames, passwords, credit card details, or contain malicious information convincing you to install programs.

Exploitation is only limited by the imagination of the attacker (phisher).

Close this window
Secunia - Multiple Browsers IDN Spoofing Test - Microsoft Internet Explorer

Address: http://www.paypal.com/

Google
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 name

site-specific password
master secret

site name

site-specific password
master secret

site name

⊕

site-specific password
solutions:

1. many passwords
2. dictionary attack
master secret

site name

⊕

site-specific password
site name

site-specific password
master secret

+ 

site name

site-specific password
master secret

+ 

site name

+ 

site-specific password
Password Multiplier (Halderman, 2005)

master secret

+ 

+ 

user name

site name

master secret

site-specific password
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: easy to guess? good (31 bits)

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

1 day 1 week 1 month 1 year 10 years 100 years 1000 years

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
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?

Firefox

Passpet

encrypted site labels

Passpet Server

encrypted site labels
practical matters:

What if you want to use existing websites?
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](http://www.pwdhash.com).
- Download the [Firefox extension](http://www.pwdhash.com/firefox) or the [Internet Explorer plugin](http://www.pwdhash.com/ie) (beta).
- Send us [feedback](mailto:feedback@pwdhash.com).
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/