Password Management Strategies for Online Accounts

Shirley Gaw & Edward W. Felten

SOUPS '06: Proceedings of the Second Symposium on Usable Privacy and Security, pp 44-55, 2006

Presented by: Wang Ying

Summary

- Paper used part laboratory exercise and part survey to study password practices on users' online accounts, focusing on password reuse, password management strategies, user model of attacker and password strength.

- Paper discuss how current technology support poor password practices.

- Paper also present potential changes in website authentication system and browser password manager.

Appreciation

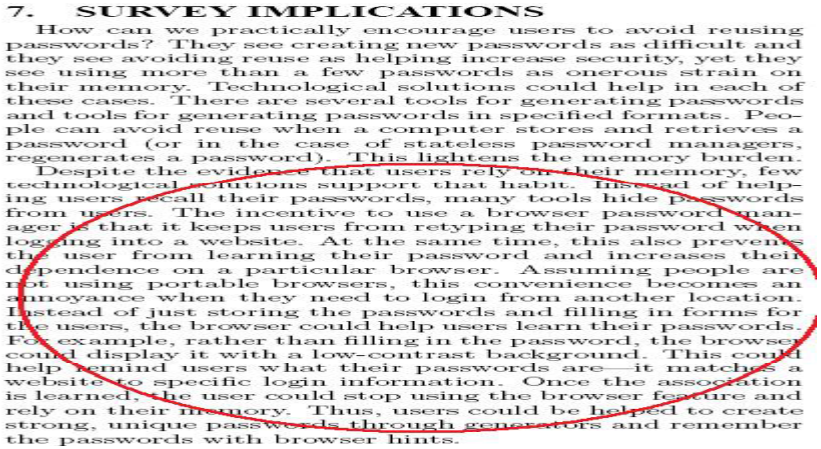
- **User-Centric Technology**

Study incorporate the needs of users. With the background on what users do, paper develop supportive technologies for password management.

These technologies are at the application level or at the browser level ,which can improve practice and change users' behavior.

- **Browser Password Manager**
- ✓ **User's characteristic I:**

  Users mostly rely on their memory.



7. SURVEY IMPLICATIONS

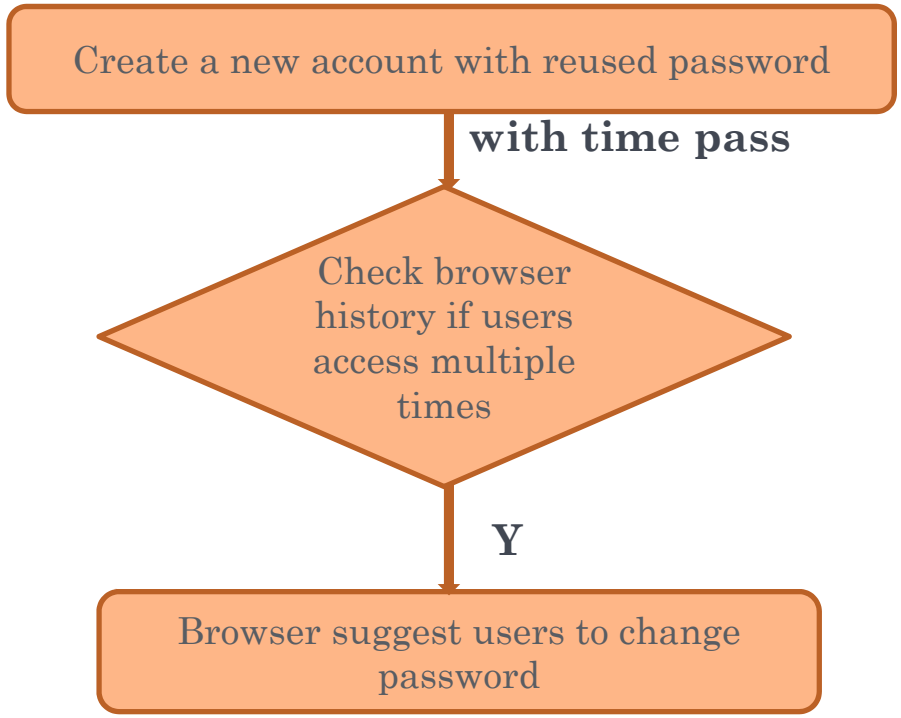
How can we practically encourage users to avoid reusing passwords? They see creating new passwords as difficult and they see avoiding reuse as helping increase security, yet they see using more than a few passwords as onerous strain on their memory. Technological solutions could help in each of these cases. There are several tools for generating passwords and tools for generating passwords in specified formats. People can avoid reuse when a computer stores and retrieves a password (or in the case of stateless password managers, regenerates a password). This lightens the memory burden.

Despite the evidence that users rely on their memory, few technological solutions support that habit. Instead of helping users recall their passwords, many tools hide passwords from users. The incentive to use a browser password manager is that it keeps users from retyping their password when logging into a website. At the same time, this also prevents the user from learning their password and increases their dependence on a particular browser. Assuming people are not using portable browsers, this convenience becomes an annoyance when they need to login from another location. Instead of just storing the passwords and filling in forms for the users, the browser could help users learn their passwords. For example, rather than filling in the password, the browser could display it with a low-contrast background. This could help remind users what their passwords are—it matches a website to specific login information. Once the association is learned, the user could stop using the browser feature and rely on their memory. Thus, users could be helped to create strong, unique passwords through generators and remember the passwords with browser hints.

Traditional Browser	User Model Browser
▪ Hide passwords from users ▪ Store passwords and fill in	Display password with low-contrast background
Prevent users from learning password	Help users learn their password
Increase dependence on browser	• Help to remind users • stop using browser feature • rely on their memory

- **User's characteristic II:**

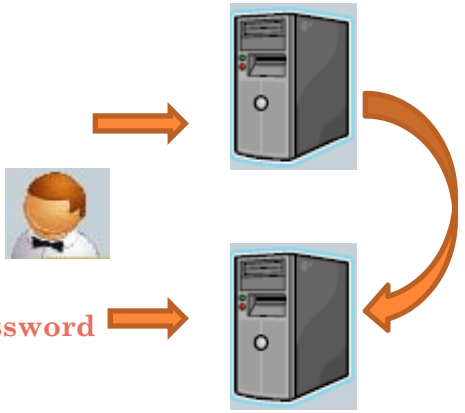
Users have the habit of reusing password when they create a new account. Also once chosen, there is little incentive to change it.



Website Authentication System

Traditional System:

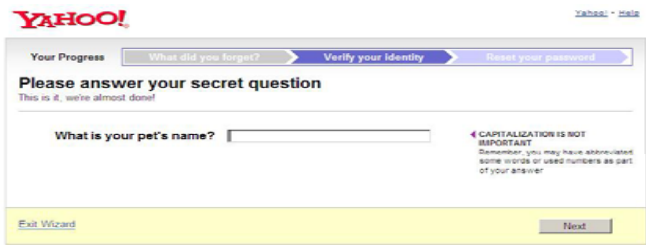
An e-mail is sent to the users' registered address, which sends the password or resetting the password.



- distribute information across multiple websites
- increase the chance for the hacker to crack their password

User Model System:

System check users' registration data for match, which includes some private information only known by users themselves. Then users could be directed to a page that not only log them in ,but also installs a cookie that identifies the user.



- rely on single password that the user places on a single server.

➢ Careful Experiment Design

- **Based on login attempts**

  Study measured results with actual login attempts rather than relying on participants to recall website.

  To avoid miscounting

- **Two pass method to quantify password reuse**

  First Pass : with pre-made lists

  Second Pass : with open-ended lists

  (any websites overlooked in first pass)

  To avoid missing

Criticism

➢ Inadequate explanation for method

❑ User Model of Attack Method

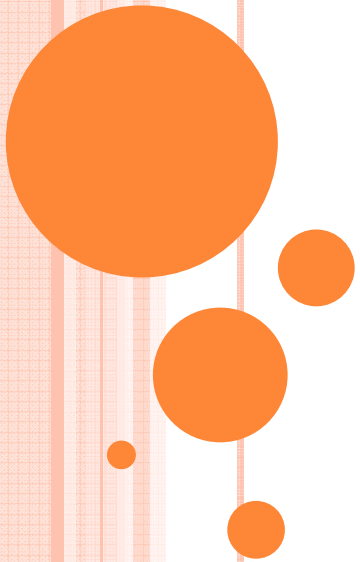
- ✓ Three Rankings to rate users' attack model:
  - Ability Ranking (ignore motivation)
  - Motivation Ranking (ignore ability)
  - Likelihood of attack (consider both motivation and ability)

❑ Problem

- ✓ Why we need Ability Ranking and Motivation Ranking?
  - They are extremely cases of the rankings.
  - In reality, a attacker always has both motivation and ability to crack users' password.

Question

What do you think is good user-centric browser password manager or user-centric website authentication system?



Thank you for your time