iPass Framework to Create Secure and Usable Passwords

DHANANJAY KULKARNI **FREDRICK C. SELLS**
BOSTON UNIVERSITY – METROPOLITAN COLLEGE
DEPARTMENT OF COMPUTER SCEICNE

CCS 2009

Motivation

Password Security is Not Funny!
What is average number passwords an Internet user has to manage?
What are the top 10 commonly used passwords?
Does a user know how strong the password is, or when to update it?

And, by the way…
Already too many passwords
Password should be easy to remember
Login process must be easy, quick
Password maybe weak

Examples (from top 10 common password)
"password"
"123456"
"qwerty"

I have see this before

NOTE TO MYSELF
Passwords are the fist line of defense!

Possible Attacks include:
Dictionary Attack
Guessing
Social Engineering
Brute Force

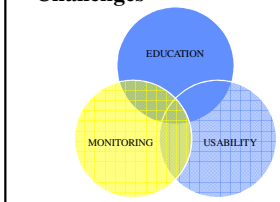
So, what is a strong password?
So, is my password weak?

Google
Indicates password strength, but no feedback

eBay
Provides additional information, but not the strength

Microsoft Password Checker
To help gauge strength, only for reference

Challenges



I am the organization. I decide the policy. Ha ha!

Why Organizations Prefer that Users Use a Strong Password?
Well…
- Organizations provide online services to users Banking, Stock Trading, Credit Card Payment, etc
- Information accessible online needs to be protected from unauthorized access
-The system is only as strong as the 'weakest link'

Example
8-15 chars (2 special chars, 2 digits, 2 upper case)

Not fair!
Why have a password policy?
These are hard! I want something simple.

Can I use my own pet's name? Humm. Do I have one?

Is it Really a Challenge?

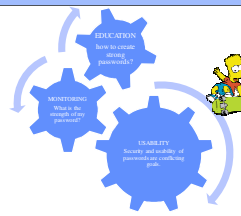
OK, listen everyone. This is really a big challenge for all of us.

Ask me why?

Loser! Do you even know why password policies exist??

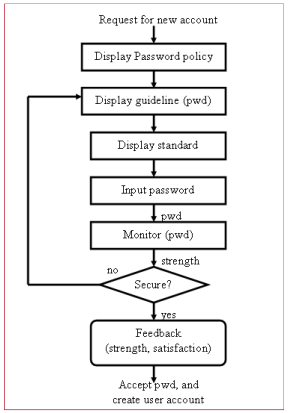
Why?

Problem statement:
Given a password policy, how can we balance security and the usability of the system, where security is measured in terms of the password strength, and usability is measured in terms of customer satisfaction during the password creation process



Dad, I am going to take my chances and go to a different web-site and buy stuff. I don't want to be educated, monitored or be useful. Please.

Our Approach



Yes, my friend..Do you want Krusty to tell you all about it?

Is this iPass? "The" iPass?

OVERVIEW: We have implemented iPass framework as a web-based interface
Novel techniques include:
- Educating the user about password creation
- Monitoring strength and potential vulnerabilities
- Usability-aware enforcement to update passwords

EDUCATION: We show the standard and guidelines to the user on the same HTML page
Standard
- 8-15 characters
- At least 1 special character from @, #, $, %, &
- Cannot have 3 or more consecutive numbers
- No white spaces
Guidelines:
Examples on how to create secure password
Current password can be modified to provide choices

VALIDATION AND MONITORING TOOLS: The password MUST pass the standard. Monitoring tools also determines the password strength.
- Point based technique (1-10)
- Check for dictionary words, popularity of words
- Check for use of personal information
- Check for repetitions
- Output of tools is used to assist in estimating the password update interval

USABILITY-AWARE ENFORCEMENT: Customer satisfaction depends on the 'experience' of the process. Users specify rating (satisfaction level) between 1-10.
- Satisfied clients can be reminded frequently
- Weaker passwords need to be updated frequently
- We make use of user-specified rating to calculate the update interval (U)

How to Create a Secure Password?

It is kinda tricky initially – but all worth it in the end!

You mean to say, I'll be reminded for password updated based on MY satisfaction? That's neat.

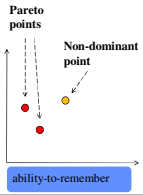
PASSWORD SUGGESTIONS

1. You can start with a password.
2. If the password is strong enough, then you are fine
3. If the password is not strong, then the .computer will assist you and suggest new passwords that you can choose from.
4. Only passwords that meet the standard and are stronger than the threshold are suggested, so you can choose any 1 of them
5. Viola! That wan't too bad, was it?
6. Example: You type "Elephant", and the computer suggests
   - "e1eph@nt"
   - "ElePH@nT1"

WHAT ARE PARETO PASSWORDS?

1. You can start with a password.
2. You can optimize the choice of passwords by participating in the password selection process.
3. First – you close your eyes, and think how difficult it is to remember the suggested passwords.
4. You give a rating 1-10 for each.
5. Based on the password strength, and the difficult-to-remember, the computer picks the ones that are pareto-optimal and shows it to you.
6. You can choose any 1 of the pareto-optimal passwords.

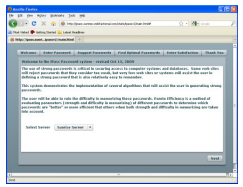
I have heard about pareto-optimality. Isn't that the best way to do 2 things at the same time?

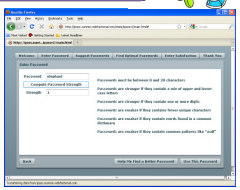


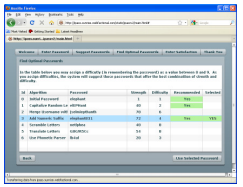
Implementation

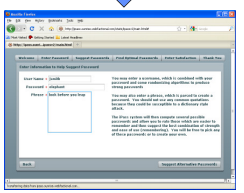
Oh yes, we went a lot of trouble to make sure that this actually works! iPass is a web-based tool built using **Python** and **TurboGears** framework on Windows.

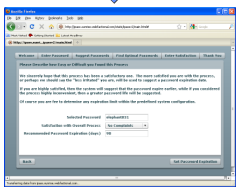
Mom?







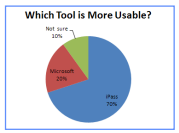


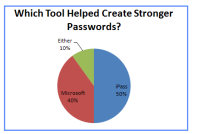


This tool is actually good..now I can create a password that I can remember + I don't have to change it too often! …which means I can spend more time with family…aham, and do some shopping too.

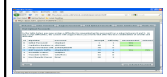
Experiments

Apart from this test, we conducted experiments to test the usability of 2 tools.

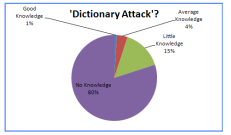


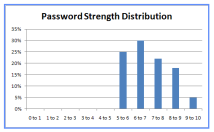


Microsoft Password Checker



iPass Framework





Conclusions and Future Work

- **Our tool can balance security and usability requirements**
- **Users participate in the password selection process**
- **Password reminders are based on the password strength and user satisfaction**

Adios! But I still need to improve that password strength, and password suggestion logic.