VISUAL PASSWORD CHECKER (VPC)

Kyriakos Kafas¹, <u>Nouf Aljaffan², Shujun Li²</u>

¹University of Cambridge, UK



²University of Surrey, UK

Users should be aware on how to construct **STRONGER PASSWORDS** which are more resistant to many attacks.

If static passwords are kept;



- 1. Generating random passwords.
- 2. Enforcing strong password policies.

This poster focuses on the proactive password checker that can work with strong password policies and can be tailored to fit a specific password policy.

UNIVERSITY OF

SIRREY

The Current Proactive Password Checkers' Problems

3. Using proactive password checker (meters).

username and password, all backed up le, time and easy to find at (you

Password strength: Weak

Use at least 8 characters. Don't use a password from another site or something

too obvious like your pet's name. Why?

Create a password
Confirm your password

The set of the second

Our Contributions

- □ 1-D password meter to 2-D space.
- Supports multiple threats at the same time.
- Provides detailed information about all threats.
- Reconfigurable and extensible.
- Pure HTML5/CSS/JavaScript based solution.
- □ Fairly fast; work even on mobile devices.
- Uses NIST password guessing entropy estimator [1].

Inadequate feedback \rightarrow users' difficulties of defining strong passwords.

Inconsistency in password strength estimator used

Hidden detail and inappropriate estimator algorithm \rightarrow misleading [2].



Four types of threats



Brute force attacks

Personalized dictionary attacks (e.g. Facebook)

Current password

Supports naive and rule-based dictionary attacks.

Supports personalized dictionary attacks (e.g. Facebook).

Design

Targeted users: normal end users.



- The whole radar screen is colored differently to estimate the overall level of risk to mimic coloring of 1-D password checkers.
- Each visualized threat is associated with a tooltip control showing more information about the threat.
- The Levenshtein distance is used to measure the edit distance (ED) between the current password and dictionary-based threats.
 - (For the password guessing entropy the edit distance is virtual -- ED=3 correspond to 80 bits)

ED = 1

We used the radar concept for reducing users' learning curve and showing different threats in a more structural & user-friendly way.

3. Implementation

Programming Languages: HTML5, CSS and JavaScript.
 Because of the screen limitation, the prototype shows up to 3 edit distance.



isual Password Checker 🗄 🗙 🔪	
C C vpc.cs.surrey.ac.uk/sampleRegistration.html	Q 🐷 🖒
Registration Form Please fill out the following details in order to complete your registration. All information will be kept confidential and used only for necessary purposes. Name: * Enter your name	apples apply append
Surname: *	apple apps app Overall Strength appal appall
Username: * Enter your username	
Password: *	appels
app * indicates a required field Submit	Dictionary Used: English Attack Type: Dictionary Search Attack Description: This method of attack uses a
	dictionary of words. Dictionaries can include lists with anything meaningful to a human. Some popular lists are places, countries, things, celebrities names etc.

Result of four different password entries.



□ Adding Support on more password composition rules.

- □ Adding more accurate password guessing entropy estimator.
- □ Adding strength estimated by password crackers.
- □ Adding password strength based on peer pressure.

□ Improving the coloring scheme.

□ A user study on the actual performance of VPC on real users.

A snapshot of the VPC prototype in use on a registration page. The prototype is available for testing at http://vpc.cs.surrey.ac.uk.

lution: Do not use words or parts of word



[1] W E Burr, D F Dodson, E M Newton, R A Perlner, W T Polk, S Gupta, and E A Nabbus. Electronic authentication guidelines. NIST SP 800-63-1, 2011.
[2] Intel Corporation. "How strong is your password?" https://wwwssl.intel.com/content/www/us/en/forms/passwordwi n.html.

SOUPS 2013 – The 9th Symposium on Usable Privacy and Security, Newcastle, UK, July 23-26, 2013