VISUAL PASSWORD CHECKER (VPC)

Kyriakos Kafas[1], Nouf Aljaffan[2], Shujun Li[2]

[1]University of Cambridge, UK

[2]University of Surrey, UK

1. Introduction

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

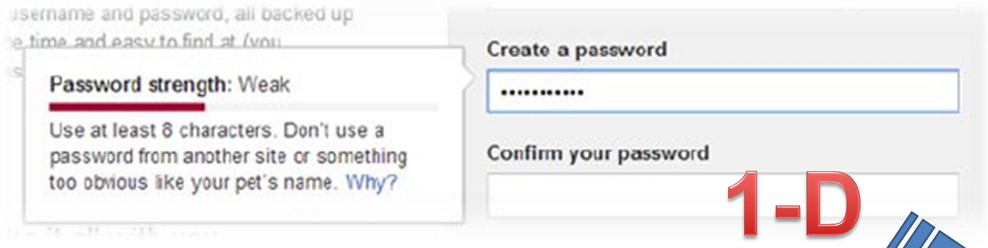
If static passwords are kept;

1. Generating random passwords.
2. Enforcing strong password policies.
3. Using proactive password checker (meters).

Current Solutions ➔ **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.**

The Current Proactive Password Checkers' Problems

Inadequate feedback ➔users' difficulties of defining strong passwords.
Inconsistency in password strength estimator used
Hidden detail and inappropriate estimator algorithm ➔ misleading [2].



1-D

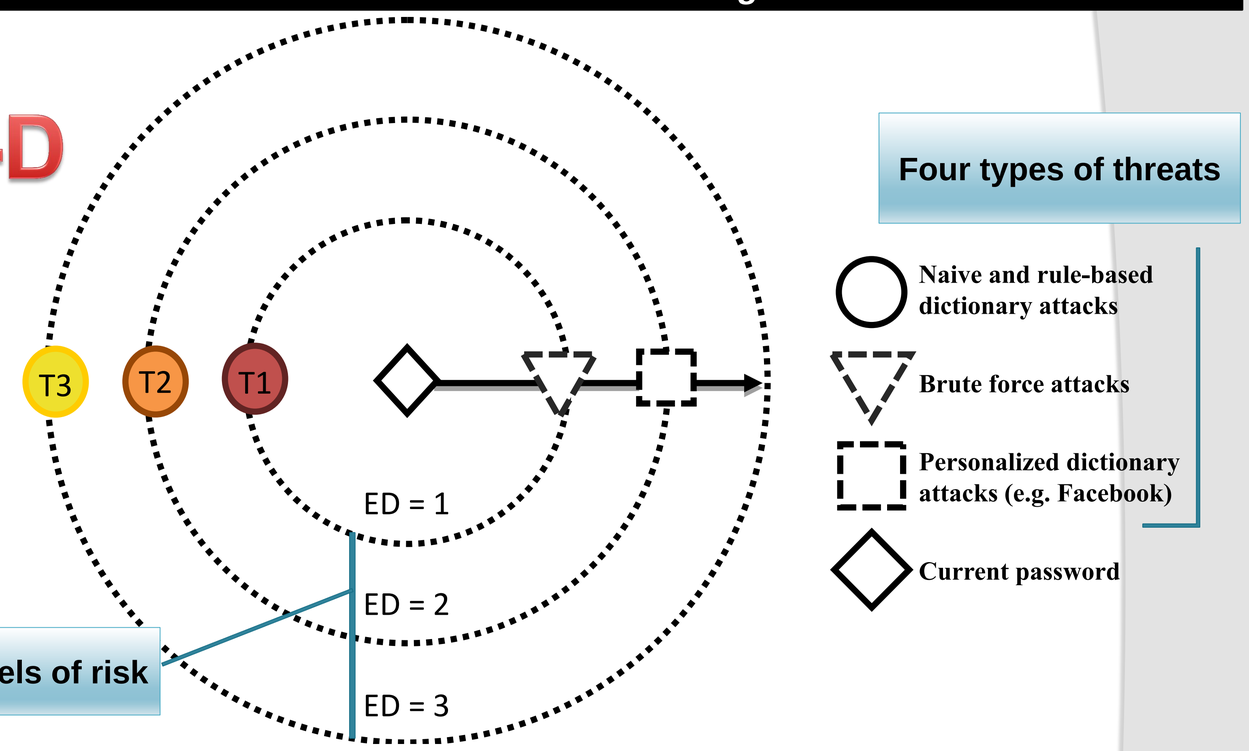
2. Contributions & User Interface Design

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].
- ❑ Supports naive and rule-based dictionary attacks.
- ❑ Supports personalized dictionary attacks (e.g. Facebook).

2-D

The visual user interface design of VPC.



- ❖ 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)

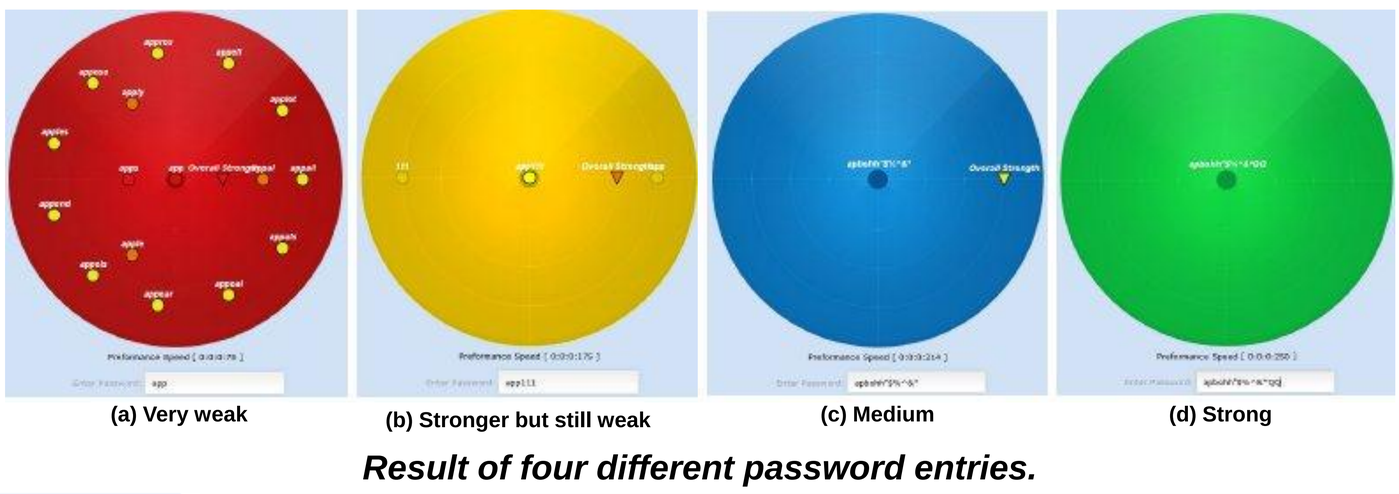
Design

Targeted users: normal end users.

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

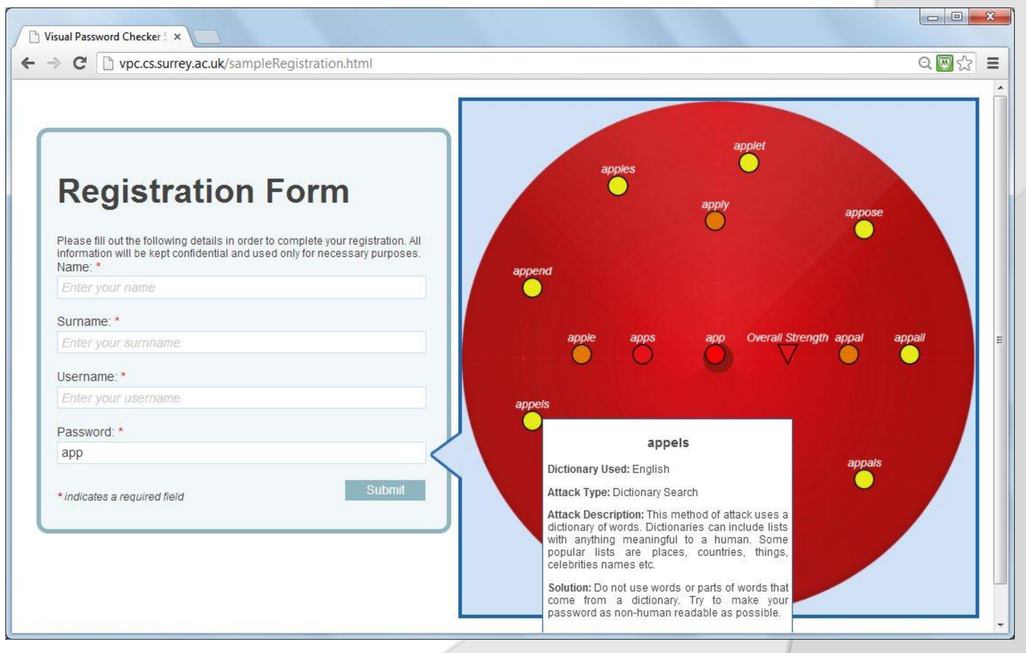
3. Implementation

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



(a) Very weak (b) Stronger but still weak (c) Medium (d) Strong

Result of four different password entries.



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.

5. Future Work

- ❑ **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.**

References

[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://www-ssl.intel.com/content/www/us/en/forms/passwordwin.html.

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