# Motivating User Password Choice Through Peer Pressure

Andreas Sotirakopoulos, Ildar Muslukhov, Serge Egelman, Cormac Herley, Konstantin Beznosov

Why motivation is important in Usable Security?

- Security is boring for an average user
- In most of the cases Security is the secondary task, not the primary one

Compare: Games and Security

Motivation vs. Usability

Motivation

Usability

Undesirable Area

Desirable Area

Super undesirable area

Undesirable Area
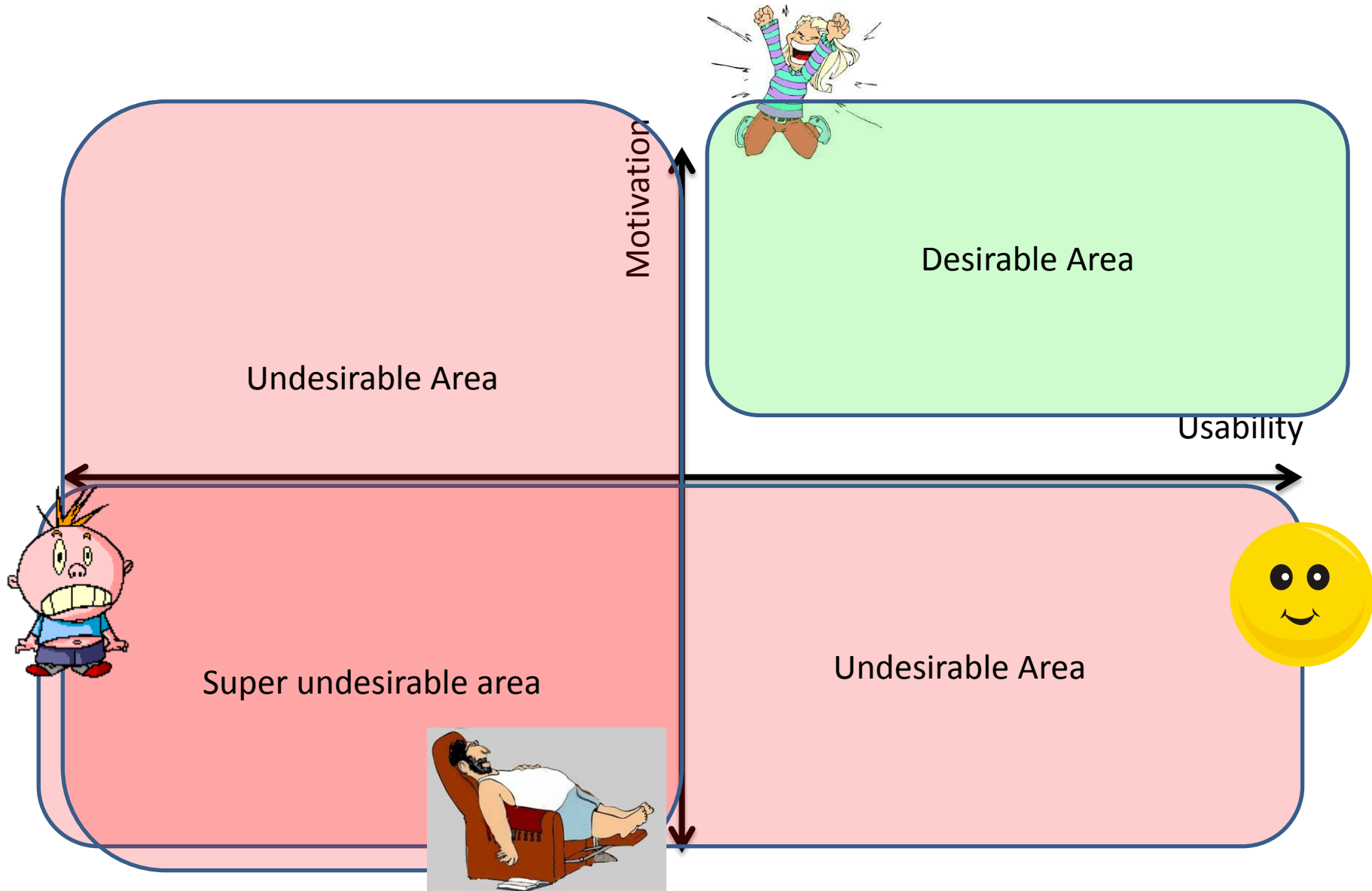
How are we doing to passwords?

Deployed Systems

- Users have two ways to judge password strength

  1. Policies and instructions
  2. Feedback while creating the password

Is it good or bad?

- Many users do not know about password best practices and do not read policies.

- Most instructions recommend a mixture of letters and digits and a length of 8 characters and more.

Feedback on password strength

- A way to prompt users choose good passwords is proactive checking (EM).
  - Series of rules that check against a password string and result in a strength assessment

So now users know, right?

Is "**p@ssw0rd**" a good password choice?
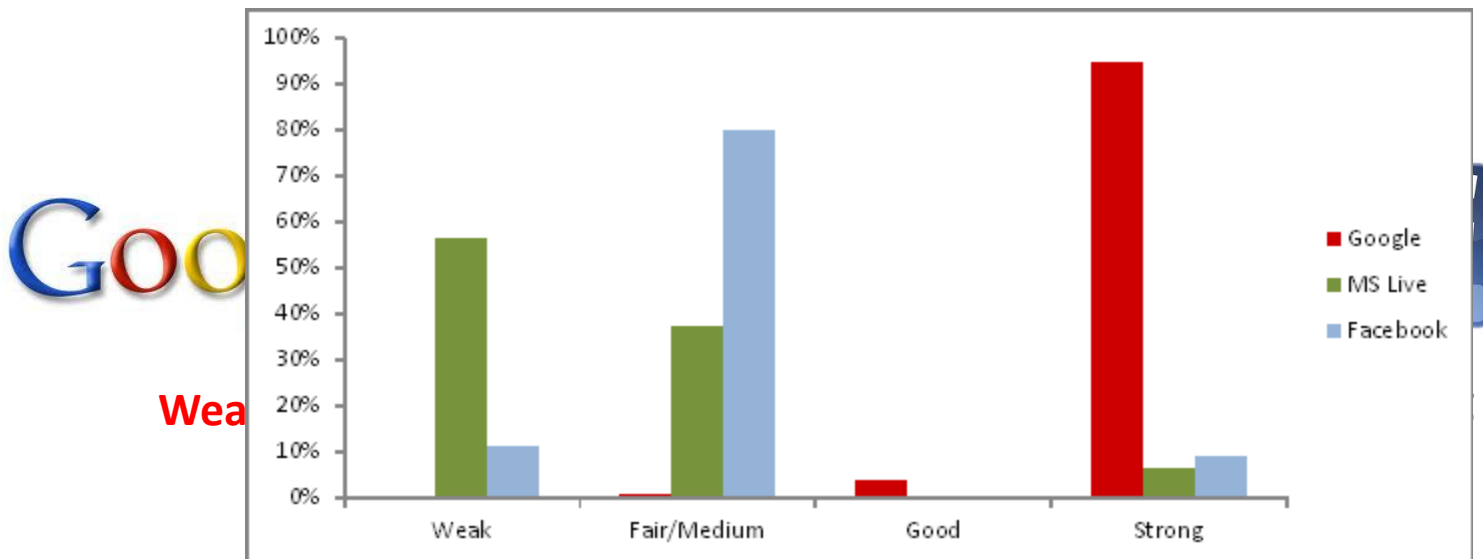
Is the user to blame for poor choices?

Another way to motivate users to pick stronger passwords

Peer Pressure

- Users receive feedback of relative password strength in form of peer pressure motivators (PPM)

- Each system has each own value to user

- They get to decide how strong is "enough"

Roots of peer pressure in research

- Was studied first by Solomon Asch in 1950 (Harvard University)
- In each participant group only one real participant, the rest are confederates
- In 2 cases out of 3 confederates give an incorrect answer

Results:

- In control group only one participant (out of 35) gave an incorrect answer
- In treatment group 75% of subjects gave at least one incorrect answer.
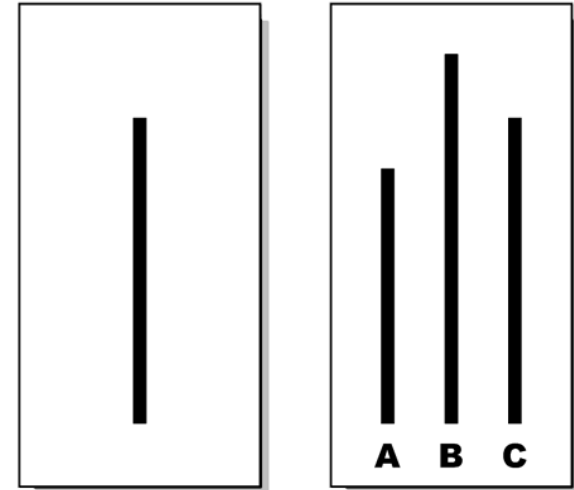
Asch, S. E. (1951). Effects of group pressure upon the modification and distortion of judgment. In H. Guetzkow (ed.) Groups, leadership and men. Pittsburgh, PA: Carnegie Press.

Research Questions

- To what extend, peer pressure motivators (PPM) stimulate users to create better in comparison to other types of existing (EM) and in the absence of any motivators?

- Does PPM have an impact in the memorability of passwords?

Methodology

- Between-subjects user study of 47 participants
  - 3 conditions: EM, PPM, Control (i.e., no feedback)
  - Asked to evaluate the MyUBC portal
  - Deploy prototypes on CWL web page and actually changed CWL password

Methodology

Change Password

You must first enter y[...] [...] [...]password
before changes will ta[...]

CWL New Policy: Change your password

Your password has expired. You have to change your Campus Wide Login password.

To secure the CWL network UBC Campus Wide Login has now to be changed on a regular basis to ensure system integrity.
The new policy is gradually rolled out for all CWL users in an effort to provide more secure IT services to UBC CWL users.

ℹ more info

Change Y[...]

Old Pas[...]

New Pa[...]

Confirn[...]

Proceed

Save

Results

Measured entropy for old and new passwords and their difference

Condition	N	Mean
Control	15	49.97
EM	16	49.18
PPM	16	49.9

Old password entropy

Condition	N	Mean
Control	15	49.37
EM	16	60.75
PPM	16	64.91

New password entropy

Results

Condition	N	Mean
Control	15	-0.66
EM	16	11.57
PPM	16	15.01

Difference between old and new password entropies

Statistical significant differences between EM vs. Control and PPM vs. Control

Question?