



# Bars, Badges, and High Scores: On the Impact of Password Strength Visualizations

Maximilian Golla, Björn Hahn, Karsten Meyer zu Selhausen, Henry Hosseini, and Markus Dürmuth

Horst Görtz Institute for IT-Security  
Ruhr University Bochum

# Password Strength Meters (PSMs)

Nudge users toward secure password

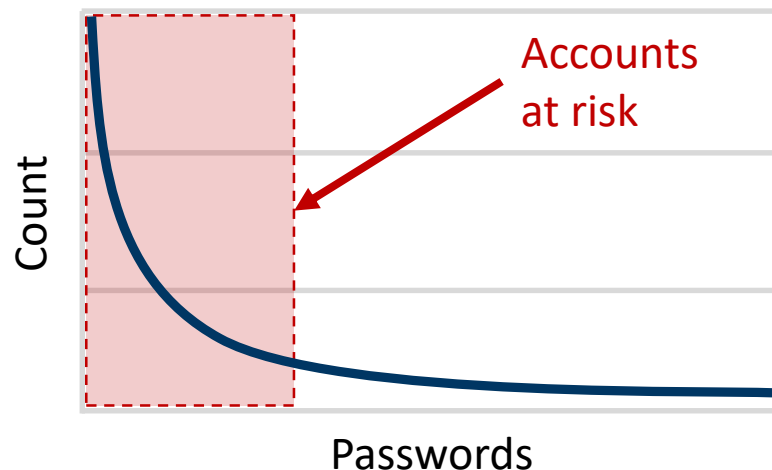
## Academic Proposals:

Markov models, PCFGs, RNNs

In this study: **zxcvbn** [1]

## Reality (deployed):

Home-brewed (LUDS) 🙈



**Common:** Bar-based meters

Strong ■■■■■■■■

→ Explore alternative visualizations and motivators!

[1] Daniel Lowe Wheeler. **zxcvbn: Low-Budget Password Strength Estimation**. USENIX Security '16

<sup>2</sup> [Image 1] See-No-Evil Monkey - Twemoji by Twitter Inc. - CC-BY 4.0

# Research Goals

Explore gamification and peer-pressure in PSMs

Baseline: Classic bar meter + control group without any meter



Peer-Pressure



Gamification

[Image 2] Peer Pressure - [vapanthepress.com](http://vapanthepress.com); [Image 3] DRAGON by Mauricio Herrera - [deviantart.com](http://deviantart.com);

3 [Image 4] Fantasy Icon Pack by Krzysztof Dycha - [opengameart.org](http://opengameart.org)

Baltimore, August 12, 2018 | WAY '18

# Study Design and Demographics

We tested 5 different conditions

Central coffee lounge on campus

302 participants, no passwords were stored

Participants believed to evaluate new university portal “smartRUB”



58% Male



38% Female

**Age**  
**18-30** 93%

**CS** 19%

## Condition 1: High Score Meter

Peer-Pressure:

- “X of Y users have chosen stronger passwords than you!”
- List contains 522 decoy entries (RockYou)
- Feedback:
  - Unintentionally leak of sensitive info
  - Change highlighting color based on strength

### Password-Highscore

| Rank | Score |
|------|-------|
| 1.   | 1600  |
| 2.   | 1452  |
| 3.   | 1332  |
| 10.  | 1132  |
| 25.  | 982   |
| 50.  | 848   |
| 100. | 732   |
| 150. | 675   |
| 200. | 612   |
| 290. | 524   |
| 300. | 520   |
| 400. | 405   |
| 520. | 78    |

289 of 522 users have chosen stronger passwords than you!

## Condition 2: Badges Meter

Fantasy Theme

3 Categories:

- Length 6-10
- Strength (33%, 66%, 100%)
- Blacklist (1k, 10k, 100k RockYou)

### Password-Badges

Length



6+



8+



10+

Strength



Level 1



Level 2



Level 3

Not in a dictionary



Small



Medium

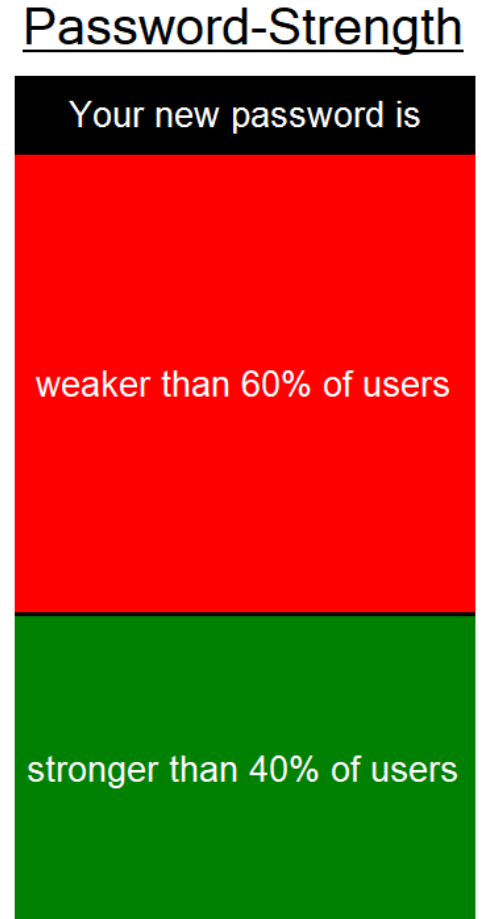


Large

## Condition 3: Peer-Pressure Meter

Proposal by Egelman et al. [2]

- Peer-Pressure approach:  
“You password is weaker than X% of users stronger than Y% of users”
- Increasing/decreasing red/green areas



## Condition 4: Bar Meter

Based on Egelman et al.'s bar meter

- 10% steps
- Color:
  - Red (0-30%)
  - Yellow (40-60%)
  - Green (70-100%)
- Text:
  - Weak
  - Medium
  - Strong

Email address:

[How to make strong passwords](#)

Use at least 6 characters

Password:  

Password-Strength: 

Medium

Confirm password:  

## Condition 5: No Meter

- Control group
- No strength meter was displayed

Email address:

[How to make strong passwords](#)

Use at least 6 characters

Password:



Confirm password:



## Results – Interaction

| Meter               | Median Strength | Mean Strength | Median Time | Usage on Website           | Median Edits |
|---------------------|-----------------|---------------|-------------|----------------------------|--------------|
| High Score Meter    | 7.94            | 8.12          | 47.5        | Very satisfied (52%)       | 11           |
| Badges Meter        | 8.00            | 8.35          | 42.0        | Slightly satisfied (26%)   | 11           |
| Peer-Pressure Meter | 8.00            | 7.83          | 38.0        | Moderately satisfied (28%) | 11           |
| Bar Meter           | 8.00            | 8.35          | 38.0        | Moderately satisfied (33%) | 11           |
| No Meter            | 7.81            | 7.39          | 38.0        | -                          | 10           |

$\text{Log}_{10}(\text{zxcvbn's guess number})$ ; Time in seconds

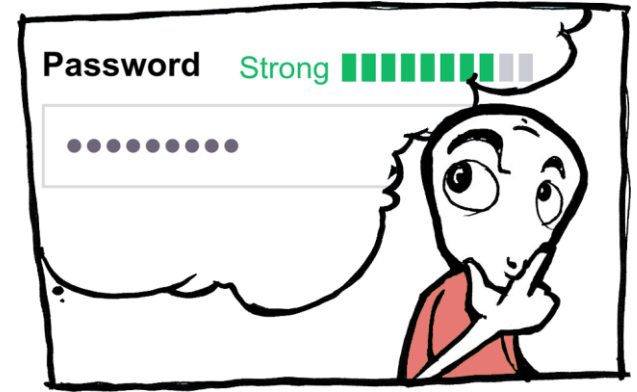
We found no significant difference in password strength across conditions!

# Lessons Learned

## Measuring the influence of PSMs is difficult!

- Realistic scenario?
  - Convincing scenario
  - Quiet in-lab study
  - Stricter meters
- Accurate strength estimation?

“Meters led users to create longer passwords. ... the resulting passwords were only marginally more resistant to password cracking attacks.” [3]



# Thank You!



(Faster) **Dancing Bunny** PSM  
Ur et al. [SSYM '12]



# Future Directions: Provide Additional Guidance

Username

Password

☐ Show Password & Detailed Feedback

Confirm Password

Your password could be better.

- Don't use words used on Wikipedia [\(Why?\)](#)
- Avoid using very common passwords as part of your own password [\(Why?\)](#)
- Consider inserting digits into the middle [\(Why?\)](#)

[How to make strong passwords](#)

Password  
usenix1234

☐ Show Password & Detailed Feedback

Your password could be better.

- Don't use words used on Wikipedia (seni) [\(Why?\)](#)
- Avoid using very common passwords like 1234 as part of your own password [\(Why?\)](#)
- Consider inserting digits into the middle, not just at the end [\(Why?\)](#)

A better choice: usef12 4n4ix

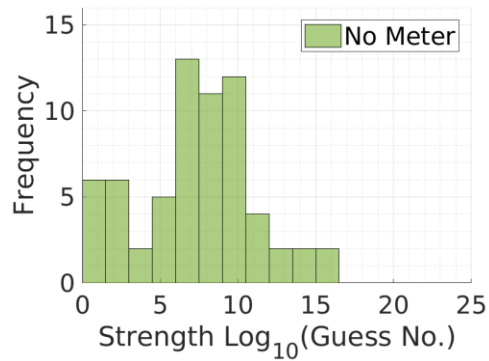
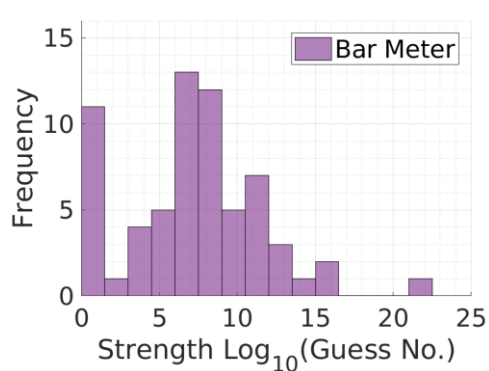
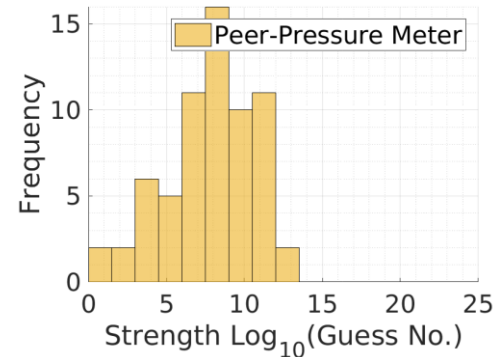
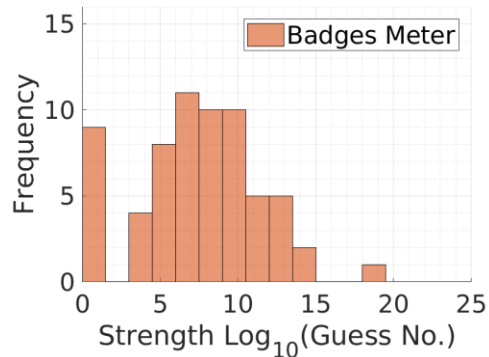
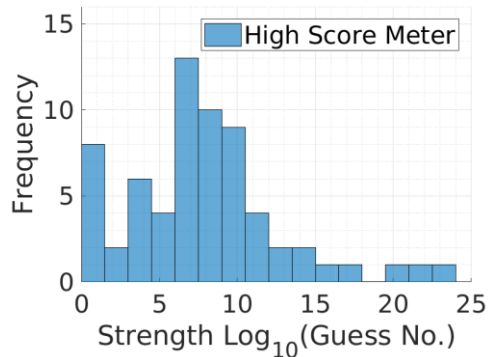
[How to make strong passwords](#)

## “Design and Evaluation of a Data-Driven Password Meter”

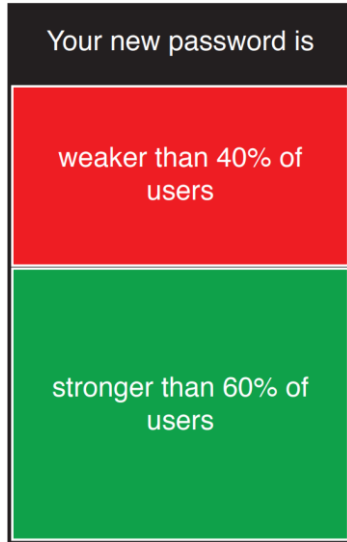
RNN-based approach + 21 advanced heuristics

Ur et al. [CHI '17]

# Strength Distributions



# Alternative Motivators



## “Peer-Pressure”

Egelman et al. [CHI ‘13]



## “Social Influence”

Ohyama and Kanaoka [SOUPS ‘15]



The password you entered is very **insecure** and may take a hacker **1 day** to guess.



Having your password guessed means a hacker would be able to access other accounts that use a similar password.

## “Interactive Fear Appeals”

Vance et al. [HICSS ‘13]

# Alternative Visualizations



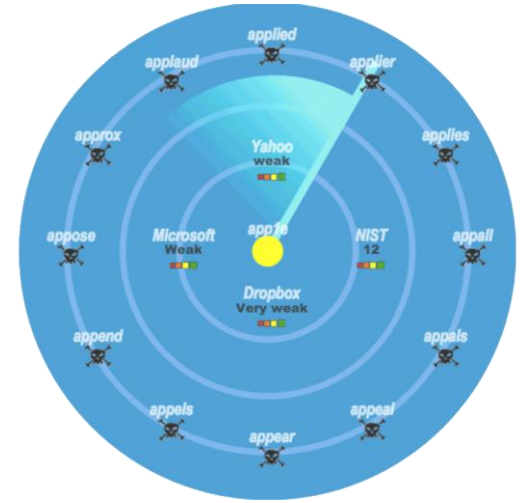
**Tachometer**

Ohyama and Kanaoka [SOUPS '15]



**(Faster) Dancing Bunny**

Ur et al. [SSYM '12]



**Password Security Visualizer**

Aljaffan et al. [SOUPS '13, HAS '17]