Studying Passwords to Create Domain-Specific Blacklists

Introduction

- **Passwords** remain the authentication method that best balances deployability, usability & security [1].
- **Blacklists** help users create stronger passwords [3].
- Motivation: What type of domain-specific information should be added to blacklists?



Figure 1: Torch is an imitation of Tinder's website.

Our Contribution

- We analyzed passwords newly created by online participants and obtained similar results as Wei et al [3]
- Observed the presence of website/service name as well as words/phrases related to the category/theme of the website/service.
- Also found that text and major visual elements on the presented website were also used in usercreated passwords.
- May indicate that the *content* of passwords created through crowdsourcing platforms may not be representative of real-life passwords (although they are similar in strength [4]).

Kentrell Owens, Mengchen Yong, Neha Sridhar, Ziheng Ni, Josh Tan, Lorrie Cranor

Methodology

- Made three imitation websites for password creation
- Twitter (Panddar), Tinder (Torch), and WhatsApp (HowYoDoin)
- Recruited 680 Amazon Mechanical Turk Users
 - 49% women, 49% men, 1% trans/non-binary
 - Average age is 36 years old
 - 75% do not have background in computer science
- \$0.55 for Part 1, \$0.70 bonus for Part 2
- Part 1: Make a password for one of the three imitation websites, take a survey about the password creation process
- Part 2 (48 hours later): Re-enter password, take a survey about how you stored the password



Figure 2: Number of Domain-Specific Passwords in Different Groups

- *IEEE Symposium on Security and Privacy*. IEEE, 553-567.
- Authentication Workshop (WAY) (2018). http://dx.doi.org/10.1145/2508859.2516726



Figure 3: Guessability of passwords

Results & Discussion

- **information** (Figure 2)
- by Panddar (7.3%) and HowYoDoin (6.1%).

1. Joseph Bonneau, Cormac Herley, Paul C Van Oorschot, and Frank Stajano. 2012. The quest to replace passwords: A framework for comparative evaluation of web authentication scheme. In 2012

2. Hana Habib, Jessica Colnago, William Melicher, Blase Ur, Sean Segreti, Lujo Bauer, Nicolas Christin, and Lorrie Cranor. 2017. Password creation in the presence of blacklists. Proc. USEC (2017), 50. 3. Miranda Wei, Maximilian Golla, and Blase Ur. 2018. The password doesn't fall far: How service influences password choice. Proceedings of the 5th SOUPS Who Are You?! Adventures in

4. Michelle L. Mazurek, Saranga Komanduri, Timothy Vidas, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Patrick Gage Kelley, Richard Shay, and Blase Ur. 2013. Measuring Password Guessability for an Entire University. In Proceedings of the 2013 ACM SIGSAC Conference on Computer and Communications Security (CCS '13). ACM, New York, NY, USA, 173–186. DOI:

9.4% of passwords created contain domain-specific

• No significant usability or security differences between domain-specific/non-domain specific passwords

> Usability metric: Number of attempts needed to recall password in Part 2 (average of 0.88/0.87 for domain-specific/non-domain specific passwords)

• Security metric: Guessability (Figure 3)

Torch was the website for which users created the highest percentage (14.5%) of domain-specific passwords, followed

33% of domain-specific passwords contained information about the recruitment platform (Mechanical Turk).