Studying Passwords to Create Domain-Specific Blacklists

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

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?

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 user-created 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]).

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

Results & Discussion

• **9.4% of passwords created contain domain-specific information** (Figure 2)
• 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 by Panddar (7.3%) and HowYoDoin (6.1%).
• **33% of domain-specific passwords contained information about the recruitment platform** (Mechanical Turk).

Copyright is held by the author/owner. Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee. Poster presented at the 15th Symposium on Usable Privacy and Security (SOUPS 2019).

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

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

Figure 3: Guessability of passwords