Passworld: A Serious Game to Promote Password Awareness and Diversity in an Enterprise

USENIX SOUPS 2020

Gokul Chettoor Jayakrishnan  |  Gangadhara Reddy Sirigireddy  |  Sukanya Vaddepalli
Vijayanand Banahatti  |  Sachin Premsukh Lodha  |  Sankalp Suneel Pandit

TCS Research, Tata Consultancy Services Limited, Pune, India

August 2020

Contact: gokul.cj@tcs.com
Sneak Peek...

- Passwords: The solution, The problem
- How to Help Users Regarding Passwords?
- Our Research Questions
- Password Heuristics
- Passworld
- Game Design Principles
- Design Choices and Real World Analogy
- Passworld: The Flow of a Game Level
- Game Mechanics
- Game Data Analysis
- Answers to Our Research Questions
- Insights and Future Scope
- Limitations
- Conclusions
Passwords
The Solution, the Problem.
• Despite the available alternatives, password-based authentication still remains a widely used method to secure user’s important and valuable accounts.

• Weak passwords can be cracked easily, making the user’s account vulnerable to cyberattacks.

• An organizational password leak could bring in financial and reputational losses apart from legal consequences.
How to Help Users Regarding Passwords?

Tools

• Proactive password checking tools: Password strength meters \cite{1, 2}.

• However, many of these tools rate passwords inconsistently \cite{3}.

• Advanced Data Driven Password Strength Meter by Ur. Et al has shown compelling results by scoring user passwords using a set of password heuristics \cite{4}.

Awareness Training

• Various training methods in cybersecurity domain have found to be helpful \cite{6, 5, 7}.

• Some of the previous studies involving serious games include Anti-Phishing Phil \cite{5}, CyberCIEGE \cite{8}, Phishy \cite{6}, GAP \cite{9}, Cyberaware \cite{10}, PASDJO \cite{3} and Control-Alt-HACK \cite{11} to name a few.

Figure 1: Phishy Gameplay
Our Research Questions

- Can a game-based password awareness training teach participants about the various password heuristics?
- Can such a training improve the organizational password diversity?
Password Heuristics

- Heuristics: The techniques or practices that have to be satisfied to improve the overall password strength.

- From the previous study \cite{4}, we selected 16 heuristics based on organizational requirements and assigned them to two game levels.
## Password Heuristics (Level 1, 2)

<table>
<thead>
<tr>
<th>Heuristics</th>
<th>Description</th>
<th>Identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password Length</td>
<td>Password length must be more than 8 characters</td>
<td>H1</td>
</tr>
<tr>
<td>Presence of Lower case</td>
<td>At least 1 lower case character must be present</td>
<td>H2</td>
</tr>
<tr>
<td>Presence of Upper case</td>
<td>At least 1 upper case character must be present</td>
<td>H3</td>
</tr>
<tr>
<td>Presence of Digits</td>
<td>At least 1 digit must be present</td>
<td>H4</td>
</tr>
<tr>
<td>Presence of Symbols</td>
<td>At least 1 symbol must be present</td>
<td>H5</td>
</tr>
<tr>
<td>Repeated Characters</td>
<td>Not more than 3 consecutive repeated characters (Eg: honeeeey)</td>
<td>H6</td>
</tr>
<tr>
<td>Duplicated Characters</td>
<td>Duplicated characters not more than 50% of total length</td>
<td>H7</td>
</tr>
<tr>
<td>Repeated Sections</td>
<td>Not 3 or more than 3 repeated sections (Eg: abababba)</td>
<td>H8</td>
</tr>
<tr>
<td>Alphabetic Sequences</td>
<td>Not more than 3 consecutive sequences (Eg: 12345, abcde)</td>
<td>H9</td>
</tr>
</tbody>
</table>
Password Heuristics (Level 2)

<table>
<thead>
<tr>
<th>Heuristics</th>
<th>Description</th>
<th>Identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>Predictable positions of:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Symbols</td>
<td>Eg: password@ or password@123 have predictable positions</td>
<td>H11</td>
</tr>
<tr>
<td>Digits</td>
<td>Should not be present just at beginning, end or all characters</td>
<td>H12</td>
</tr>
<tr>
<td>Uppercase characters</td>
<td>Should not be present in the beginning or have all uppercase</td>
<td>H13</td>
</tr>
<tr>
<td>Predictable Structure</td>
<td>Should not be present in the list of common structures</td>
<td>H14</td>
</tr>
<tr>
<td>Keyboard Patterns</td>
<td>Eg: QWERTY (English Language keyboards)</td>
<td>H10</td>
</tr>
<tr>
<td>Date Formats</td>
<td>All date formats like DDMMYY, MMDDYY, having month names etc.</td>
<td>H15</td>
</tr>
<tr>
<td>Black lists</td>
<td>Should not be present in organizational blacklist of passwords</td>
<td>H16</td>
</tr>
</tbody>
</table>
Passworld: The Game
Design, Mechanics
Game Design Principles

1. Experiential Gaming model [15]
2. Bloom’s Taxonomy [12]
3. Six ‘I’s of Serious Game Design [13]
5. Our Design Choices
Design Choices and Real World Analogy

- Open Interconnected World: Jungle Environment
- Digital Assets need Protection: Securely store the artifact
- Know thy enemy: Learning the password heuristics
- Prepare to Defend: Resource Gathering
- Build a Strong Defense: Creation of Password Gate
Passworld: The Flow of a Game Level

Start → Pre-test → Gameplay → Password Creation stage → Post-test → End

- Distraction task: Mini activities
- Password Recall stage
- Animals attack to check password heuristics
- Resource Collection, Animals with heuristic lessons

Figure 2: Passworld Game Level Flow
Passworld: Level 1 Gameplay

- **Genre:** Platformer Game
- **Central character:** Soma
- **Objective:** Secure two ancient artifacts

**Figure 3: Passworld Gameplay**
Passworld: Level 1 Gameplay

- Oncoming animals provide hints on various password heuristics.

Figure 4: How animals provide instructions upon encounter
Passworld: Level 1 Password Creation Stage

Figure 5: Password Creation Stage Level 1

- The stage where the players test their password knowledge and learnings about heuristics.
- Players create passwords here, which is checked by oncoming animals.
Password: Level 2 Password Creation Stage

- How an animal checks a password, based on the heuristic it taught in the earlier level.
- If the heuristic is not satisfied, the animal breaks the fort and enter the camp.

Figure 6: Password Creation Stage Level 2, Animal comes to check the created password
Passworld: Level 1 Distraction Task (Drag and Drop)

- There are two distraction tasks (simple drag and drop activities).
- Intended to provide a brief distraction, to check if the players remember their created passwords even after completing this task.

Figure 7: Distraction Task
Passworld: Level Password Recall Stage

• Password Recall Stage where the player enters the same password that was created earlier.

Figure 8: Password Recall Stage
Passworld: Data Analysis
Answers to our Research Questions
Game Data

- Total participants: **4,906**
- Participants created **17,319** passwords, that fell in **11,286** different Password Structures\(^{[14]}\).

  Eg: \texttt{P@ssw0rd} => \texttt{USLLLDLL}

- We tried to answer our research questions based on the analysis of the participant data.
1. Can a game-based password awareness training teach participants about the various password heuristics?

- We checked the players' correct answer percentages in both pre- and post-tests and analyzed this to find out improvement in users' knowledge levels.

![Figure 9: Participants' correct answers in Level 1](chart)

Analysis based on participants' correct answers: **Level 1**
1. Can a game-based password awareness training teach participants about the various password heuristics?

- **Analysis based on participants’ correct answers:** Level 2

  ![Bar chart showing percentage of participants who gave correct answers in Level 2 Pre - Post tests](chart.png)

  **Heuristics**
  - Keyboard pattern (H10)
  - Symbol predictable (H11)
  - Digit predictable (H12)
  - Uppercase predictable (H13)
  - Date format (H15)

  **Increase in average correct answers:**
  - From 5.96 (SD = 2.3) in pre-test to 6.57 (SD = 2.69) in post-test
  - Significance by Two-tailed paired t-test: 
    \[ t(4905) = -19.35, p<0.001 \]

  **Figure 10:** Participants’ correct answers in Level 2
2. Can Such a Training on Heuristics Improve the Participants’ Password Diversity?

- We analyzed the changes in password structures created by participants in both levels and found that there is a visible spread in the common structures found.

<table>
<thead>
<tr>
<th>LEVEL 1</th>
<th>LEVEL 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>ULLLLSDDDD</td>
<td>LSLLLDLU</td>
</tr>
<tr>
<td>ULLLLSDDDD</td>
<td>LSLLDLULLU</td>
</tr>
<tr>
<td>ULLSDDDD</td>
<td>LLLUSDLLL</td>
</tr>
<tr>
<td>ULLLLLSDDDD</td>
<td>ULLSUDDL</td>
</tr>
<tr>
<td>ULLLLLSDDDD</td>
<td>LLLUSDDDUU</td>
</tr>
<tr>
<td>LLLLLLDLU</td>
<td>UUUUSDDDLL</td>
</tr>
<tr>
<td>ULLLLSDDD</td>
<td>ULSUSDLU</td>
</tr>
<tr>
<td>ULLLLLSSDD</td>
<td>SLLDLLLLU</td>
</tr>
<tr>
<td>ULLLLLSDD</td>
<td>LSLLSULLDDDL</td>
</tr>
<tr>
<td>ULLLLLSSDD</td>
<td>ULSULDDDDL</td>
</tr>
</tbody>
</table>

*Figure 11: Spread of password structures from Level 1 to Level 2*
Game Feedback Data

- Game feedback data was collected from the participants to get insights on how the game fared when it comes to entertainment and educational value.

![Participant Feedback Survey Responses](image)

- **Have you learned?** 94.24% (M = 4.48, SD = 0.68)
- **Is Passworld Educational?** 93.85% (M = 4.42, SD = 0.68)
- **Is Passworld Fun?** 93.50% (M = 4.42, SD = 0.69)

*Figure 12: Participants’ Feedback Data*
Insights and Future Scope

- Participants showed improvements in many complex heuristics like predictable positions of symbols, digits, date formats etc.

- Password Structures showed diversity after the game-based training, with over 90% of unique password structures created in Level 2.

- H6, H10 and H13 showed decrease in performance, showing that they will need further training.

- Gameplay time and heuristic overload will have to reduced in the future versions of the game.
Limitations

- Demographics had at least bare minimum knowledge on cybersecurity topics.
- Real-time effects of the game could not be tested, as it involves real-time password monitoring.
- Control condition was not followed for the present study.
- Long term password memorability not studied.
Conclusions

- Passworld is a game created to increase password awareness among enterprise users.
- From 4,906 participants’ data, there is a clear improvement in the number of correct answers given by participants in the post-test compared to pre-test.
- Participants have created very diverse set of password structures in Level 2 compared to Level 1.
- Participants found the game to be educational and entertaining.
References

Thank You

TCS Research, Tata Consultancy Services Limited, Pune, India

Contact: gokul.cj@tcs.com