On the Security of Cracking-Resistant Password Vaults

Maximilian Golla, Benedict Beuscher, and Markus Dürmuth

Horst Görtz Institute for IT-Security
Ruhr-University Bochum
Password Vaults

LastPass Password Mgr” by LastPass, “iCloud Keychain iOS 9” by 9to5mac.com
Password-based Encryption (PBE)

- Master Password \texttt{mpw}
- Salt \texttt{salt}
- Domain Password \texttt{pwd}
- Key Derivation Function
- Encryption / Decryption
- Ciphertext \texttt{c}
Normal Password Vault

Correct Master Password

Incorrect Master Password

Try again, ...
Cracking-Resistant Password Vault

Correct Master Password

Incorrect Master Password

Decoy!\[1\]

Password-based Encryption (PBE)

If MPW is incorrect

DEL34<(ä/!°$901 + #õNUL(°x+#. ,0= @<^SOHzę4!õ°$)!õ? =$°%($ − 4^ACKf Σ3d4
PBE + ?

"I think you should be more explicit here."
**PBE + Honey Encryption**[2]

[Ref. 2] Ari Juels and Thomas Ristenpart.  
Honey Encryption: Security Beyond the Brute-Force Bound. (EUROCRYPT '14)
PBE + Honey Encryption\textsuperscript{[2]} $\rightarrow$ NoCrack\textsuperscript{[3]}

NoCrack (Cracking-Resistant Password Vault)

Honey Encryption (HE)

- Domain Password $pwd$
- Natural Language Encoder
- Encode ($pwd$) $\rightarrow$ $\hat{s}$

- $pwd \leftarrow$ Decode ($\hat{s}$)

Password-based Encryption (PBE)

- Master Password $mpw$
- Salt $salt$
- Key Derivation Function SHA-256
- Encryption / Decryption AES-CTR
- Ciphertext $c$

Cracking-Resistant vault based on Honey Encryption. PCFG-based NLE.

[Ref. 3] Rahul Chatterjee, Joseph Bonneau, Ari Juels, and Thomas Ristenpart. Cracking-Resistant Password Vaults using Natural Language Encoders. (SP ‘15)
Benefits of Cracking-Resistant Vaults

Attacker needs to **verify every guessed master password by trying to login with some alleged credentials.**

Via Honey Encryption we can generate decoys **on the fly!**
Outline

1. Password Vaults
2. Attack
3. Results
4. Adaptive NLEs
How to Crack a Cracking-Resistant Vault?

Correct Master Password

Bit String $s$ → Natural Language Encoder → Domain Password $pwd$

A „real“ Password Distribution
How to Crack a Cracking-Resistant Vault?

Incorrect Master Password

Bit String \( S \) → Natural Language Encoder → Domain Password \( pwd \)

Incorrect Password Distribution

Decoy
Attack Idea

• A realistic adversary doesn’t know the “real” password distribution\(^4\)

• but, can approximate NoCrack’s distribution!

• If we observe outliers (not following NoCrack’s distribution), we can use them for ranking.

Attack Overview

1. Approximate Decoy Distribution

2. Trial-Decryption

3. Ranking of Vault Candidates

4. Online Verification
1. Approximate Distribution of Decoy Vaults

Repeatedly sample passwords from the distribution by evaluating the KDF and trial-decrypting the vault.
2. Trial-Decryption

Decrypt vault with candidate master passwords. (Assume the correct master password is in this list.)
3. Ranking of Vault Candidates

**Rank candidates** so that the real vault is (hopefully) near the top of the list.
4. Online Verification

Go **online** and **verify** the correctness, starting with the highest ranked vault.

1. melissa88
2. RosesAreRed
3. qwerty
4. bond007
Outline

Adaptive NLEs

Results

Attack

Password Vaults
Experimental Setup

- Dataset from previous work\textsuperscript{[3]}. (Org. gathered by malware)

<table>
<thead>
<tr>
<th>Vault Size:</th>
<th>2-3</th>
<th>4-8</th>
<th>9-50</th>
</tr>
</thead>
<tbody>
<tr>
<td>Samples</td>
<td>100</td>
<td>89</td>
<td>87</td>
</tr>
</tbody>
</table>

- Ranking with 1,000 vaults (relative ranking)
  - 999 decoy vaults, 1 real vault

\textsuperscript{[Ref. 3]} Rahul Chatterjee, Joseph Bonneau, Ari Juels, and Thomas Ristenpart. Cracking-Resistant Password Vaults using Natural Language Encoders. (SP ‘15)
Experimental Setup

• Kullback–Leibler (KL) divergence
  – to measure the difference between the distributions.

\[ D_{KL}(P \parallel Q) = \sum_{z \in \text{supp}(P)} P[z] \cdot \log \frac{P[z]}{Q[z]} \]

• Tested influence of approx. precision (1.000 - 30.000.000 vaults)

• Tested different vault sizes (2-50 passwords)
## Results

<table>
<thead>
<tr>
<th>Attack</th>
<th>Perfect NLE</th>
<th>Prev. Work [^{[3]}]</th>
<th>Our Classifier</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Guessing</td>
<td>ML</td>
<td></td>
</tr>
<tr>
<td>Attack</td>
<td>Mean Rank</td>
<td>Median Rank</td>
<td></td>
</tr>
<tr>
<td></td>
<td>50.0%</td>
<td>37.8%</td>
<td>6.2%</td>
</tr>
<tr>
<td></td>
<td>50.0%</td>
<td>/</td>
<td>2.0%</td>
</tr>
</tbody>
</table>

[^{[3]}]: Rahul Chatterjee, Joseph Bonneau, Ari Juels, and Thomas Ristenpart. Cracking-Resistant Password Vaults using Natural Language Encoders. (SP '15)
Influence of Approximation Precision

![Graph showing the relationship between training size and ranking failure rate.](image)

- **KL Divergence**

The graph illustrates how the ranking failure rate decreases as the training size increases. The x-axis represents the training size (in thousands), and the y-axis represents the ranking failure rate (in %). The data points show a clear downward trend, indicating improved precision with larger training sets.
## Difference in Vault Size

<table>
<thead>
<tr>
<th>Vault Size:</th>
<th>2-3</th>
<th>4-8</th>
<th>9-50</th>
<th>All (2-50)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mean Rank</strong></td>
<td>9.6%</td>
<td>6.0%</td>
<td>3.1%</td>
<td>6.2%</td>
</tr>
<tr>
<td><strong>Median Rank</strong></td>
<td>2.1%</td>
<td>1.9%</td>
<td>1.7%</td>
<td>2.0%</td>
</tr>
</tbody>
</table>
Correlation,

Correlation

Name
Maximilian  Golla

Choose your username
maximilian.golla.1337  @gmail.com

Create a password
madmax1337
Correlation

Name
Maximilian
Golla

Choose your username
maximilian.golla.1337
@gmail.com

Create a password
madmax1337

Reuse

My Passwords:

Yahoo: madmax1337
Gmail: madmax1337
Facebook: Madmax2016
Tumblr: madmax1337!
Grillshop24: master
Correlation, Reuse, and Policies Issues

**Correlation**

- **Name**
  - Maximilian
  - Golla

- **Choose your username**
  - maximilian.golla.1337 @gmail.com

- **Create a password**
  - madmax1337

**Reuse**

- **My Passwords:**
  - Yahoo: madmax1337
  - Gmail: madmax1337
  - Facebook: Madmax2016
  - Tumblr: madmax1337!
  - Grillshop24: master

**Policies**

- **Password strength:** Strong
  - Use at least 8 characters. Don’t use a password from another site, or something too obvious like your pet’s name. *Why?*

- **Create a password**
  - Password to be entered

- **Confirm your password**
  - Password to be confirmed
## Results

<table>
<thead>
<tr>
<th>Attack</th>
<th>Perfect NLE</th>
<th>Prev. Work</th>
<th>Correlation</th>
<th>Reuse</th>
<th>Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mean Rank</td>
<td>Guessing</td>
<td>ML</td>
<td>KL</td>
<td>6.4%</td>
<td>6.2%</td>
</tr>
<tr>
<td></td>
<td>50.0%</td>
<td>37.8%</td>
<td>6.2%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Median Rank</td>
<td></td>
<td>/</td>
<td>2.0%</td>
<td>2.1%</td>
<td>2.0%</td>
</tr>
<tr>
<td></td>
<td>50.0%</td>
<td>/</td>
<td>2.0%</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

→ **KL**: Reduction of required online queries by a factor of **8**.

→ **KL + background info**: Reduction by a factor of **20**.
The Flaw

Improbable password are a strong signal for the real vault.

<table>
<thead>
<tr>
<th>The Real Vault</th>
<th>A Decoy Vault (No. 23)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>Q:</td>
</tr>
<tr>
<td>kamaria</td>
<td>1.00E-14</td>
</tr>
<tr>
<td>khalilah</td>
<td>1.00E-14</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>pinkrose13</td>
<td>1.00E-14</td>
</tr>
<tr>
<td></td>
<td>password</td>
</tr>
<tr>
<td></td>
<td>1.74E-02</td>
</tr>
<tr>
<td></td>
<td>JOHNCENA</td>
</tr>
<tr>
<td></td>
<td>4.02E-06</td>
</tr>
<tr>
<td></td>
<td>...</td>
</tr>
<tr>
<td></td>
<td>p4ssw0rd</td>
</tr>
<tr>
<td></td>
<td>8.05E-06</td>
</tr>
</tbody>
</table>

→ Change NoCrack’s NLE to simulate the correct aka “the real” password distribution!
Static NLEs
Static NLEs

There is no „the real“ password distribution!
Dist. differs by service and time → We can’t predict it

→ Do not assign low probabilities to passwords that appear in the real vault!
Adaptive NLEs

Boost their probabilities by a constant value

Select a fraction of ALL $n$-grams (real and decoy)

Re-normalize

Paper gives a bound on the amount of information that is leaked.
Limitations / Future Work

• **Lack of sample data**

• Are master passwords guessable?
  • Is a master password related to the domain passwords inside the vault?

• Improve **adaptive NLEs**
  • Improve attack
Takeaway

1. Honey Encryption → Cracking-Resistant Password Vaults

2. Building an NLE is challenging! (Distribution, Reuse, Correlation, Policies, ...)

3. Adaptive NLE can solve the distribution problem.
### Step 3: Ranking Example

**The Real Vault**

<table>
<thead>
<tr>
<th>Password</th>
<th>P:</th>
<th>Q:</th>
<th>Sum:</th>
</tr>
</thead>
<tbody>
<tr>
<td>kamaria</td>
<td>0.1</td>
<td>1.00E-14</td>
<td>4.651</td>
</tr>
<tr>
<td>khalilah</td>
<td>0.1</td>
<td>1.00E-14</td>
<td>9.302</td>
</tr>
<tr>
<td>kamaria1</td>
<td>0.3</td>
<td>1.00E-14</td>
<td>13.952</td>
</tr>
<tr>
<td>kamaria1</td>
<td>0.3</td>
<td>1.00E-14</td>
<td>18.603</td>
</tr>
<tr>
<td>kamaria1</td>
<td>0.3</td>
<td>1.00E-14</td>
<td>23.254</td>
</tr>
<tr>
<td>pinkrose13</td>
<td>0.4</td>
<td>1.00E-14</td>
<td>27.904</td>
</tr>
<tr>
<td>pinkrose13</td>
<td>0.4</td>
<td>1.00E-14</td>
<td>32.555</td>
</tr>
<tr>
<td>pinkrose13</td>
<td>0.4</td>
<td>1.00E-14</td>
<td>37.206</td>
</tr>
<tr>
<td>pinkrose13</td>
<td>0.4</td>
<td>1.00E-14</td>
<td>41.856</td>
</tr>
<tr>
<td>pinkrose14</td>
<td>0.1</td>
<td>1.00E-14</td>
<td>46.507</td>
</tr>
</tbody>
</table>

**A Decoy Vault (No. 23)**

<table>
<thead>
<tr>
<th>Password</th>
<th>P:</th>
<th>Q:</th>
<th>Sum:</th>
</tr>
</thead>
<tbody>
<tr>
<td>password</td>
<td>0.4</td>
<td>1.74E-02</td>
<td>0.181</td>
</tr>
<tr>
<td>password</td>
<td>0.4</td>
<td>1.74E-02</td>
<td>0.362</td>
</tr>
<tr>
<td>password</td>
<td>0.4</td>
<td>1.74E-02</td>
<td>0.543</td>
</tr>
<tr>
<td>password</td>
<td>0.4</td>
<td>1.74E-02</td>
<td>0.724</td>
</tr>
<tr>
<td>malinda</td>
<td>0.4</td>
<td>1.00E-14</td>
<td>5.374</td>
</tr>
<tr>
<td>malinda</td>
<td>0.4</td>
<td>1.00E-14</td>
<td>10.025</td>
</tr>
<tr>
<td>malinda</td>
<td>0.4</td>
<td>1.00E-14</td>
<td>14.676</td>
</tr>
<tr>
<td>malinda</td>
<td>0.4</td>
<td>1.00E-14</td>
<td>19.326</td>
</tr>
<tr>
<td>p4ssw0rd</td>
<td>0.1</td>
<td>8.05E-06</td>
<td>19.462</td>
</tr>
<tr>
<td>JOHNCENA</td>
<td>0.1</td>
<td>4.02E-06</td>
<td>19.608</td>
</tr>
</tbody>
</table>

**Final Ranking**

<table>
<thead>
<tr>
<th>Rank</th>
<th>Vault</th>
<th>KL-Div:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DECOY 12</td>
<td>49.829</td>
</tr>
<tr>
<td>2</td>
<td>REAL</td>
<td>46.507</td>
</tr>
<tr>
<td>3</td>
<td>DECOY 78</td>
<td>42.683</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>712</td>
<td>DECOY 23</td>
<td>19.608</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>999</td>
<td>DECOY 16</td>
<td>4.805</td>
</tr>
<tr>
<td>1000</td>
<td>DECOY 14</td>
<td>0.966</td>
</tr>
</tbody>
</table>

**KL-Div: 46.507**

**KL-Div: 19.608**