The Bitcoin Brain Drain: A Short Paper on the Use and Abuse of Bitcoin Brain Wallets

Marie Vasek*, Joseph Bonneau°, Ryan Castellucci†, Cameron Keith¶ and Tyler Moore*

University of Tulsa*, Stanford University°, White Ops†, Southern Methodist University¶

Financial Cryptography
February 25, 2016
What is a Brain Wallet?
What is a Brain Wallet?

RANDOM??

[Diagram of a brain, a key, and a wallet]
... and why do we care?

Be careful with brain wallets, there are people sitting on the common ones! Lost 5 BTC.

I'm not sure how many of you use brain wallets, but PLEASE be very careful messing around with them. For those of you who don't know, they are a deterministic way of generating a Bitcoin keypair using a passphrase.

I read this post[^1] on Hacker News 3 weeks ago and started messing around with bitaddress.org[^2] to see if I could find any of the 1 BTC bounties. I found a few bitcoins at 13w4Hn1BJQM4bjZZgYTXyp4ciow29tK[^3] (I think the wallet passphrase was something simple like "satoshinakamoto" but I forget the exact phrase) and to see if it would actually work I tried adding it into blockchain.info's wallet.

Fast forward to today. I was moving some funds around[^4] and I just sent 5 BTC to the last address on my blockchain.info wallet (why on earth didn't I generate a new one?). I sent 0.1 BTC to SatoshiDICE for the hell of it and went about my business. A few minutes later, I went back to check the result of my bet and BAM. Someone had swept my funds[^5] less than 10 minutes after I put them in there.

So yes, I was an idiot and it was a very (very) expensive lesson in being careful with what addresses you send to and what brain wallet passphrases to use :(. Hopefully some of you can read this and avoid a similar fate.
Roadmap

• Generating Candidate Brain Wallet Passwords
• Brain Wallet Usage
• Brain Wallet Draining
# Password Corpora: 300 Billion Candidate Passwords

<table>
<thead>
<tr>
<th>Source</th>
<th># Wallets</th>
<th>(non-empty)</th>
<th>Unique</th>
<th>90% # drains</th>
<th>Total BTC</th>
<th>Total USD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Urban Dictionary</td>
<td>296</td>
<td>3</td>
<td>2</td>
<td>3.00</td>
<td>561.95</td>
<td>43 120.77</td>
</tr>
<tr>
<td>Two Words</td>
<td>13</td>
<td>3</td>
<td>0</td>
<td>4.00</td>
<td>0.79</td>
<td>92.65</td>
</tr>
<tr>
<td>Eng/Slang Urban Dict.</td>
<td>63</td>
<td>14</td>
<td>28</td>
<td>2.00</td>
<td>0.90</td>
<td>124.96</td>
</tr>
<tr>
<td>Eng. Wikipedia</td>
<td>250</td>
<td>0</td>
<td>0</td>
<td>2.00</td>
<td>505.77</td>
<td>38 833.16</td>
</tr>
<tr>
<td>WikiQuotes</td>
<td>35</td>
<td>0</td>
<td>0</td>
<td>12.00</td>
<td>60.96</td>
<td>17 620.50</td>
</tr>
<tr>
<td>Phrases</td>
<td>283</td>
<td>0</td>
<td>0</td>
<td>3.00</td>
<td>578.69</td>
<td>57 376.80</td>
</tr>
<tr>
<td>xkcd</td>
<td>90</td>
<td>3</td>
<td>3</td>
<td>13.00</td>
<td>97.66</td>
<td>29 140.44</td>
</tr>
<tr>
<td>Lyrics</td>
<td>329</td>
<td>4</td>
<td>16</td>
<td>3.00</td>
<td>230.45</td>
<td>26 788.97</td>
</tr>
<tr>
<td>Blockchain.info tags</td>
<td>112</td>
<td>0</td>
<td>10</td>
<td>7.00</td>
<td>577.93</td>
<td>31 683.29</td>
</tr>
<tr>
<td>Rootkit</td>
<td>123</td>
<td>2</td>
<td>0</td>
<td>6.00</td>
<td>4.50</td>
<td>570.78</td>
</tr>
<tr>
<td>MySpace</td>
<td>59</td>
<td>0</td>
<td>0</td>
<td>3.00</td>
<td>1.14</td>
<td>210.44</td>
</tr>
<tr>
<td>RockYou</td>
<td>415</td>
<td>3</td>
<td>2</td>
<td>3.00</td>
<td>113.82</td>
<td>33 807.17</td>
</tr>
<tr>
<td>LinkedIn</td>
<td>213</td>
<td>0</td>
<td>0</td>
<td>2.00</td>
<td>10.11</td>
<td>738.52</td>
</tr>
<tr>
<td>LEET MRL</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>1.00</td>
<td>0.01</td>
<td>1.49</td>
</tr>
<tr>
<td>Prince MRL</td>
<td>295</td>
<td>4</td>
<td>7</td>
<td>3.00</td>
<td>88.93</td>
<td>21 028.02</td>
</tr>
<tr>
<td>CrackStation</td>
<td>640</td>
<td>3</td>
<td>37</td>
<td>2.00</td>
<td>396.09</td>
<td>41 326.80</td>
</tr>
<tr>
<td>Naxxatoe</td>
<td>388</td>
<td>0</td>
<td>2</td>
<td>2.00</td>
<td>41.56</td>
<td>3 389.31</td>
</tr>
<tr>
<td>Skull Security</td>
<td>414</td>
<td>3</td>
<td>3</td>
<td>2.00</td>
<td>71.73</td>
<td>20 756.32</td>
</tr>
<tr>
<td>Uniqpass</td>
<td>490</td>
<td>3</td>
<td>0</td>
<td>2.00</td>
<td>134.95</td>
<td>35 266.27</td>
</tr>
</tbody>
</table>
## Password Corpora: 300 Billion Candidate Passwords

<table>
<thead>
<tr>
<th>Source</th>
<th># Wallets</th>
<th>(non-empty)</th>
<th>Unique</th>
<th>90% # drains</th>
<th>Total BTC</th>
<th>Total USD</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Non-word lists</em></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reddit User Challenge</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1.00</td>
<td>0.01</td>
<td>2.62</td>
</tr>
<tr>
<td>Brute Force</td>
<td>200</td>
<td>3</td>
<td>3</td>
<td>3.00</td>
<td>22.47</td>
<td>3895.99</td>
</tr>
<tr>
<td>Modified BW Passwords</td>
<td>74</td>
<td>1</td>
<td>9</td>
<td>2.00</td>
<td>2.25</td>
<td>209.98</td>
</tr>
<tr>
<td><strong>Overall</strong></td>
<td><strong>884</strong></td>
<td><strong>21</strong></td>
<td><strong>139</strong></td>
<td><strong>2.00</strong></td>
<td><strong>1806.22</strong></td>
<td><strong>103,472.13</strong></td>
</tr>
</tbody>
</table>
Brain Wallet Usage

- 884 distinct brain wallets
- 845 different passwords
- 1,806 BTC (approx. 103,000 USD)
- 798 uncompressed and 71 compressed

Notable Passwords
- one two three four five six seven
- ""
- how much wood could a woodchuck chuck if a woodchuck could chuck wood
Value Stored in Brain Wallets

CDF: Wallet Value (USD)

P(total USD) <= x

Total USD in Wallet

Rank-Order: Total Value (USD)

% Total USD

# Largest Wallets
Drainers

• 1895 drains on 884 wallets
  ○ 98% drained at least once
  ○ 69% of wallets are drained exactly once
  ○ 1.9% are drained more than ten times.

• 14 drainers (at least) targeting multiple brain wallets
  ○ Top 4 drainers netted $35 000 between them

• $1 – median value of drain among successful drainers
Brain Drain Time

CDF: Time-to-Drain by Wallet Value

- $100
- <$0.10

Overall

P(TTD) <= x hours

Graph showing the cumulative distribution function (CDF) for time-to-drain by wallet value, with three curves for different value ranges.
Brain Wallet Drains over Time
Conclusion

- Tested 300 billion passwords through BrainFlayer
- Found only 884 used brain wallets worth 1,806.22 BTC or 103,472.13 USD
- 98% drained at least once
  - Most within minutes
Conclusion

“DO NOT USE BRAINWALLETS”

https://en.bitcoin.it/wiki/Brainwallet
Conclusion

“DO NOT USE BRAINWALLETS”
https://en.bitcoin.it/wiki/Brainwallet

Now... with Science!
Questions?