Limiting Online Password-Guessing Financially

Maximilian Golla, Daniel V. Bailey, and Markus Dürmuth

Horst Görtz Institute for IT-Security
Ruhr-University Bochum
Online Password Guessing

“The hackers used lists to try to match usernames and passwords - when one matched, they made purchases using the miles on the frequent flyer's account.”

Reuters, 2015

Good for online password guessing, maximizes success probability
Online Password Guessing

Targeted Attacker: (Specific user)
Exploiting personal information
• Politician Sarah Palin, 2008
• WIRED author Mat Honan, 2012

Trawling Attacker: (Any user)
Guesses answers based on population-wide statistics
Simultaneously attacks many accounts
Outline

Motivation

Background

Approach

Evaluation
Rate Limiting

“... the verifier SHALL limit attempts on a single account to no more than 100.”
NIST Special Publication 800-63B

Techniques MAY be used:

• CAPTCHA
• Requiring to wait (30s to 1h)
• IP white lists
• Risk-based authentication (Fingerprinting)
Rate Limiting

Welcome

Enter your password

Forgot password?

Next

Wrong password. Try again.

Type the text you hear or see

Forgot password?

Next

Try again, ...
CAPTCHA Security Problem

Automatic Solving Services:

• $0.0014 per CAPTCHA
• Average solving time: 6 sec
• Average accuracy rate: 97%
• API available: Python, Perl, PHP, C, ...
• Customer reviews:
  “Great service, and gets the job done.”

Audio CAPTCHAs?

• Low-Resource Attack (Speech2Text APIs) \(^1\)
Outline

- Motivation
- Background
- Approach
- Evaluation
Deposit-based Rate Limiting

Demanding a small deposit for each login attempt

Immediately refunded after a **successful login**

But, high costs for repeated **unsuccessful logins**
Deposit-based Rate Limiting

Hi John
john.doe@example.org

Deposit is required to continue.
Amount: $0.01

Recipient: Website Inc. on behalf of John Doe.

Forgot password?

Step 1: Deposit Requested
Deposit-based Rate Limiting

Hi John
john.doe@example.org

Deposit is required to continue.
Amount: $0.01

Recipient: Website Inc. on behalf of John Doe.

Forgot password?
APPROVE PAYMENT

Step 1: Deposit Requested

Hi John
john.doe@example.org

Deposit received.
Enter your password

Forgot password?
LOGIN

Step 2: Deposit Received
Deposit-based Rate Limiting

Step 3: Correct Password
Deposit-based Rate Limiting

Step 3: Correct Password
Step 3: Incorrect Password

Hi John
john.doe@example.org

Wrong password. Another deposit is required to try again.
Amount: $0.01

Recipient: Website Inc. on behalf of John Doe.

Forgot password?
APPROVE PAYMENT
Deposit-based Rate Limiting

Enrollment
- No adaptations required
- 2FA-like, opt-in approach

Authentication
- User authorizes payment of deposit
- Deposit received? -> Allow to authenticate

Fallback
- PW reset without a deposit
- No disadvantage for the user
Avoid Unsuccessful Logins!

- Securely correct common typographical errors \(^1\)
- Option: Display password in plain text \(^2\)
- Disable CAPTCHA solving for opted-in accounts
- Password reset without deposit

\(^1\) Rahul Chatterjee et al.: pASSWORD TYPOS and How to Correct Them Securely. (SP ’16)
Payment System

Requirements:

• Real-time
• No transaction fees
• Anonymity
• Widely-accepted

Proposals: [1,2,...]

• Off-blockchain transactions.
• On-blockchain enforceability.

Broad adoption remains a deployment challenge!

[Ref. 2] Ranjit Kumaresan et al.: How to Use Bitcoin to Play Decentralized Poker. (CCS ’15)
Pricing Options

**Static**: system-wide deposit price
- E.g., black market value

**Dynamic**: based on the value/risk of the individual account
- E.g., number of previous failed attempts
- May incentivize phishing attacks / denial of service attacks

**Refunding:**
- Deposit of the current login only
- The last 3–5 failed login attempts only
- All deposits for previous failed attempts

[Img. 1] Three Hundred Big Boys, imdb.com
[Img. 2] Dynamic IP or Static IP, bestreviews.net
Attacker

Simulation:

• Trawling attacker
• Top 1,000 passwords
• Account resale: $0.70, $1.00, $1.20
• Deposit: ½ cent, 1 cent per login

Assumptions:

• Perfect knowledge of the password distribution (guessing only correct passwords in the perfect order)

We provide a lower bound on the security offered!
## Attacker Profit

### ½ Cent per Try:
Against 1,000 Users

<table>
<thead>
<tr>
<th>Resale Value</th>
<th>$\lambda_1$</th>
<th>$\lambda_{10}$</th>
<th>$\lambda_{50}$</th>
<th>$\lambda_{100}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.70$</td>
<td>23$</td>
<td>22$</td>
<td>-79$</td>
<td>-198$</td>
</tr>
<tr>
<td>1.00$</td>
<td>35$</td>
<td>51$</td>
<td>-21$</td>
<td>-110$</td>
</tr>
<tr>
<td>1.20$</td>
<td>43$</td>
<td>70$</td>
<td>18$</td>
<td>-51$</td>
</tr>
</tbody>
</table>

$\lambda = \#\text{guesses}$
Attacker Profit – ½ Cent per Try (Against 1,000 Users)
## Attacker Profit

### 1 Cent per Try:
Against 1,000 Users

<table>
<thead>
<tr>
<th>Resale Value</th>
<th>$λ_1$</th>
<th>$λ_{10}$</th>
<th>$λ_{50}$</th>
<th>$λ_{100}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.70$</td>
<td>18$</td>
<td>-25$</td>
<td>-295$</td>
<td>-602$</td>
</tr>
<tr>
<td>1.00$</td>
<td>30$</td>
<td>5$</td>
<td>-236$</td>
<td>-514$</td>
</tr>
<tr>
<td>1.20$</td>
<td>38$</td>
<td>24$</td>
<td>-197$</td>
<td>-455$</td>
</tr>
</tbody>
</table>

$λ$ = #guesses
Attacker Profit – 1 Cent per Try (Against 1,000 Users)
Takeaway

Online Password Guessing

CAPTCHA Problem

Deposit-based Rate Limiting
Discussion

Hi John
john.doe@example.org

Forgot password?
LOGIN

Usability

Pricing

Payment System

[Img. 1] Dynamic IP or Static IP, bestreviews.net