RUB

Limiting Online Password-Guessing Financially

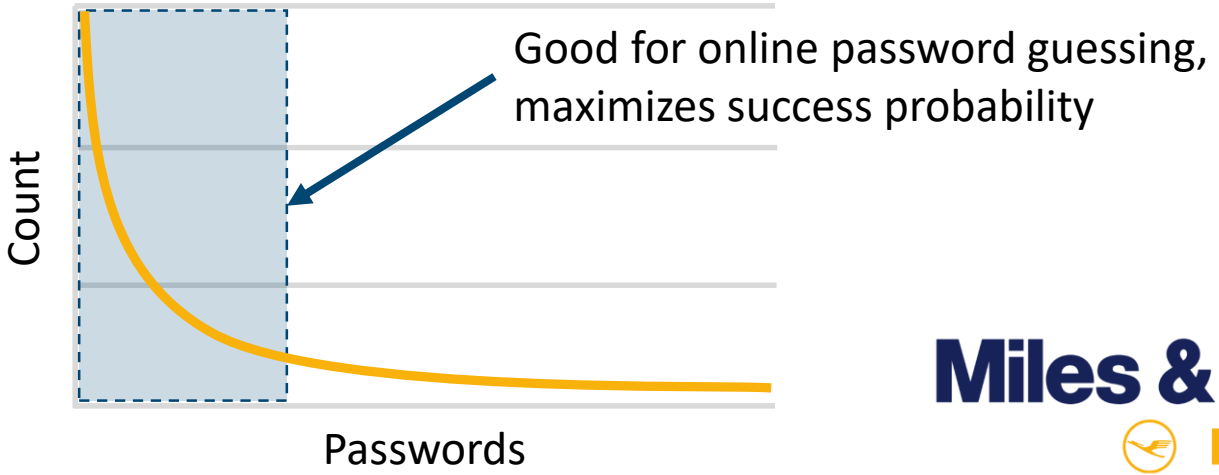
Maximilian Golla, Daniel V. Bailey, and Markus Dürmuth

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



Miles & More

Lufthansa

[Img. 1] Miles & More Lufthansa, wikipedia.org

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

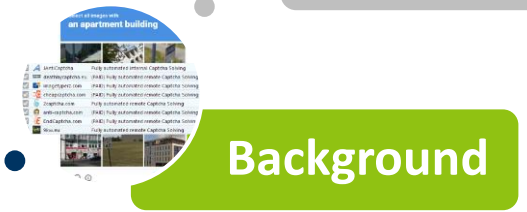
[Img. 1] Sarah Palin, politico.com; Mat Honan, wired.com

[Img. 2] Fishing trawler, pulse.ng

Outline


Evaluation


Approach


Background


Login
Username
Password
Motivation

Rate Limiting

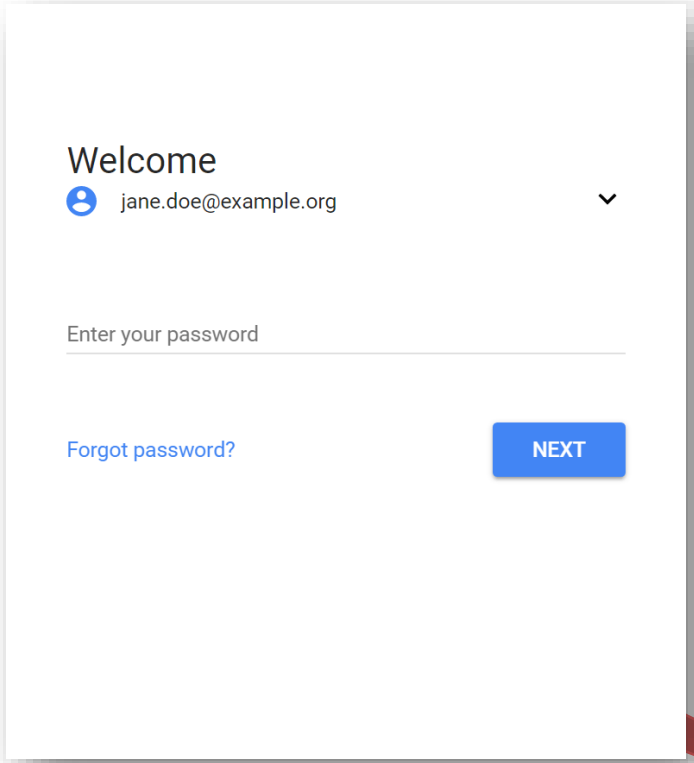
"... the verifier SHALL limit attempts on a single account to no more than 100."
NIST Special Publication 800-63B

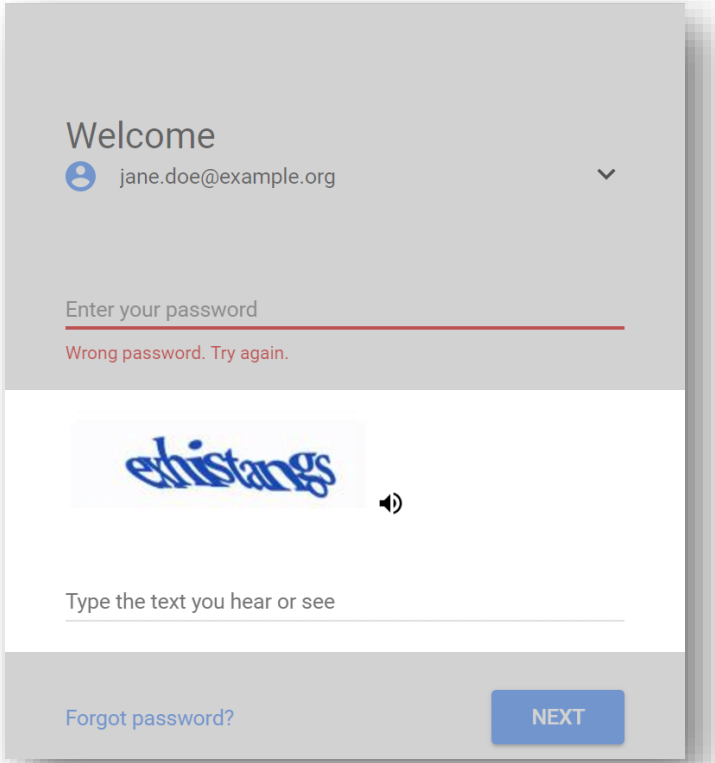
Techniques MAY be used:

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

 [Img. 1] Twitter's API limit, f5.com

Rate Limiting





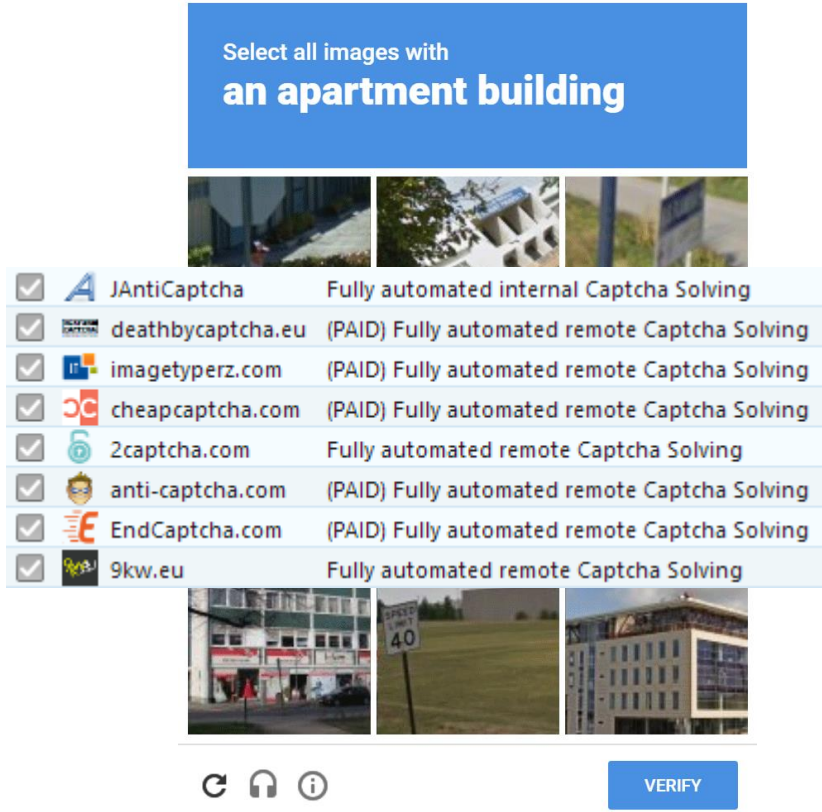
Try again, …

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.**”

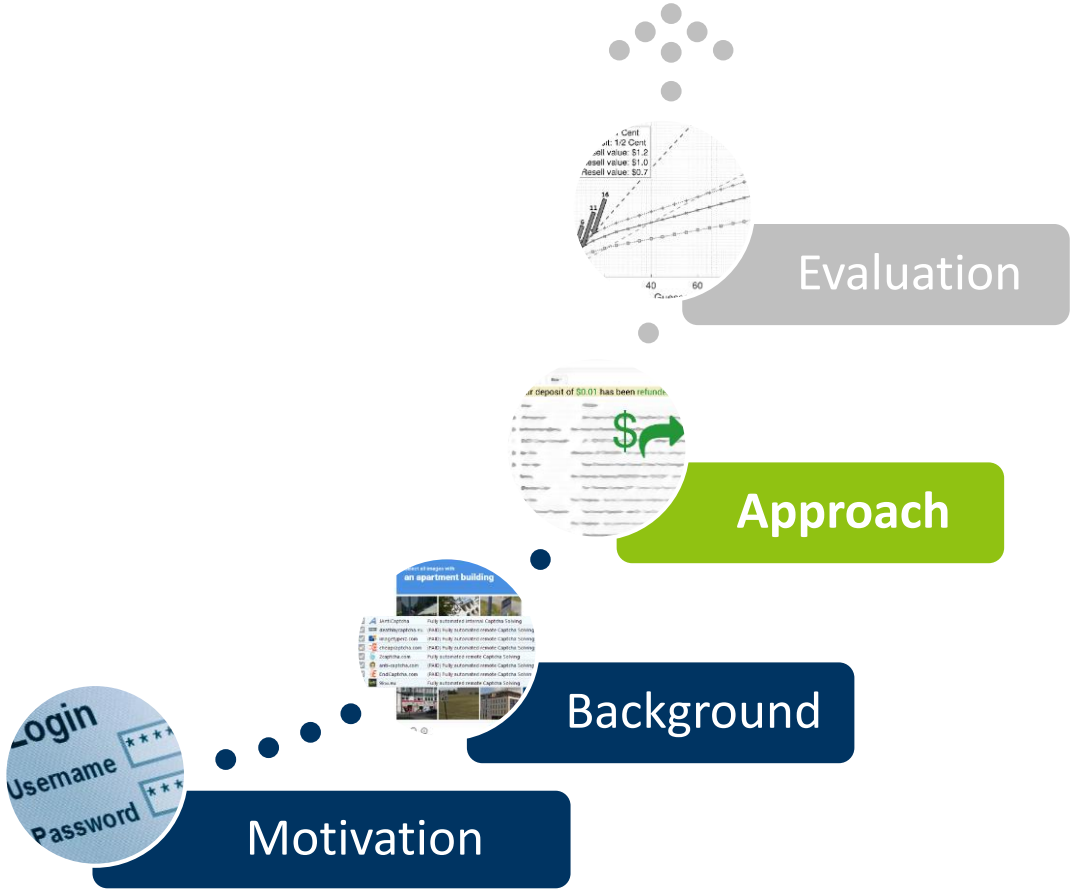


Audio CAPTCHAs?

- Low-Resource Attack (Speech2Text APIs) [1]

[Ref. 1] Kevin Bock et al.: unCaptcha: A Low-Resource Defeat of reCaptcha's Audio Challenge. (WOOT ’17)

Outline


Evaluation
Approach
Background
Motivation
Login
Username
Password

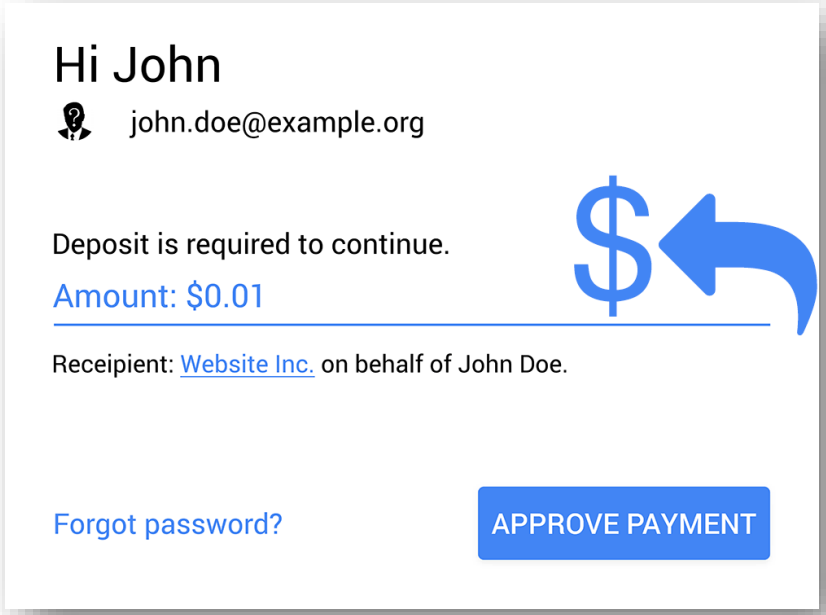
Deposit-based Rate Limiting

Demanding a small deposit for each login attempt

Immediately refunded
after a **successful login**

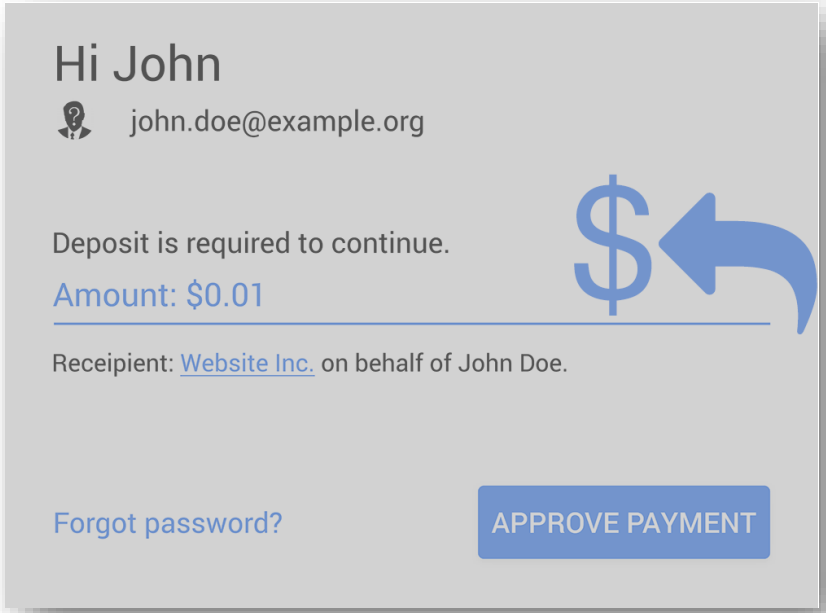
But, high costs for repeated
unsuccessful logins

Deposit-based Rate Limiting

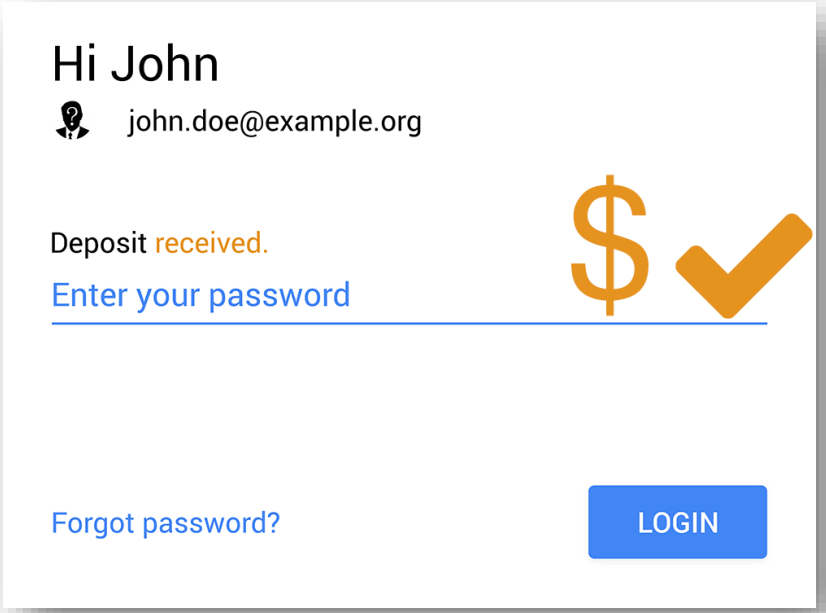


Step 1: Deposit Requested

Deposit-based Rate Limiting

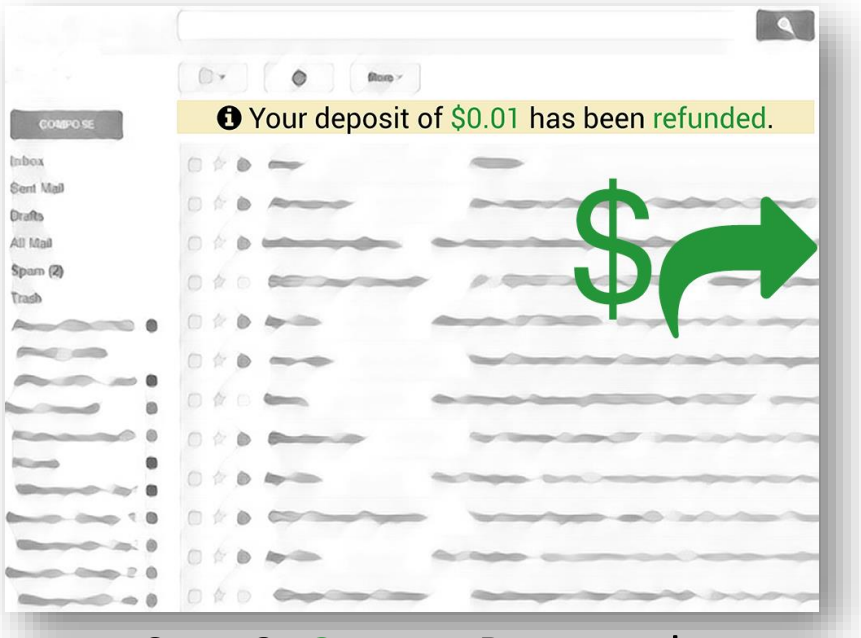


Step 1: Deposit Requested



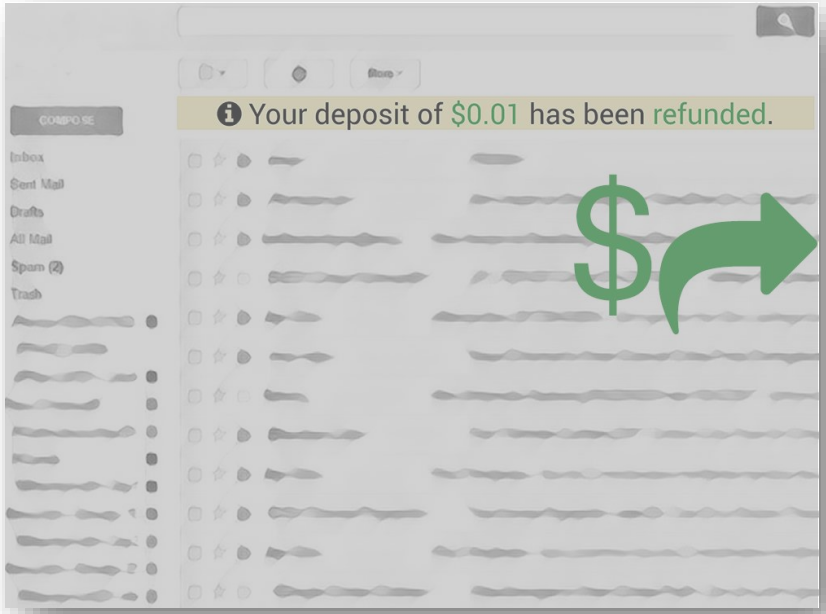
Step 2: Deposit Received

Deposit-based Rate Limiting

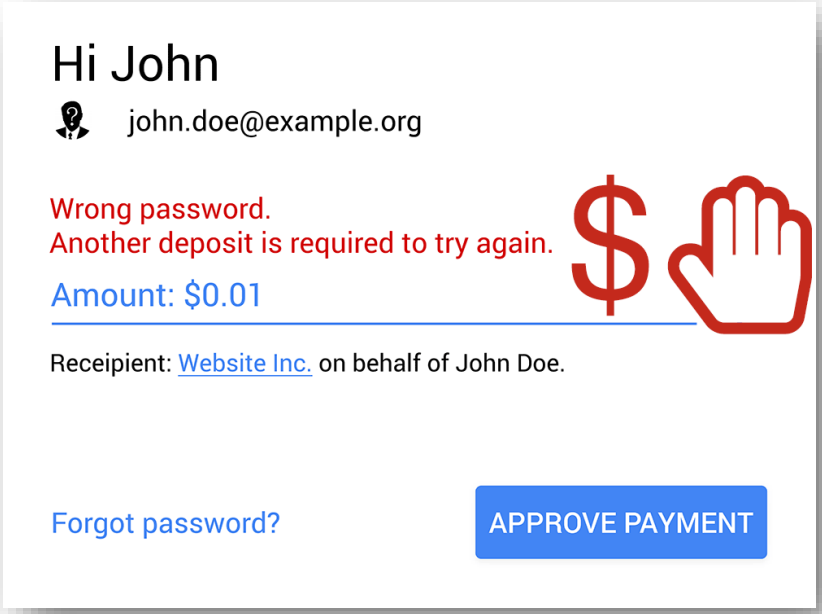


Step 3: Correct Password

Deposit-based Rate Limiting



Step 3: Correct Password



Step 3: Incorrect Password

Deposit-based Rate Limiting

Enrollment

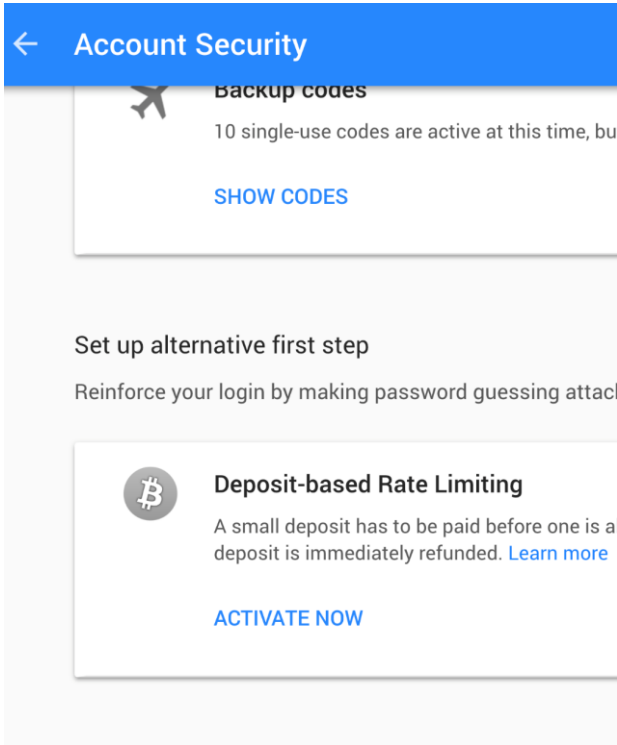
- No adaptations required
- 2FA-like, opt-in approach

Authentication

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

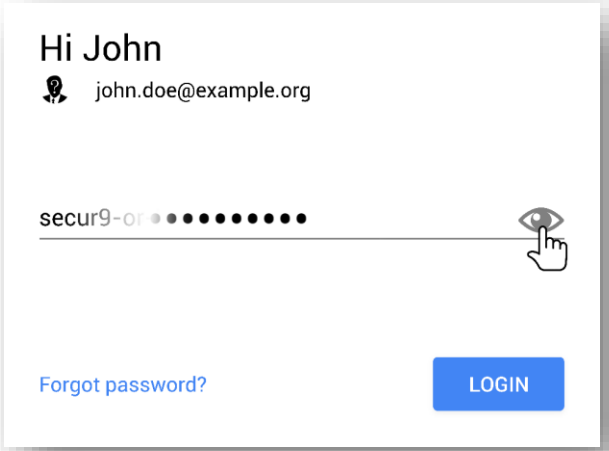
Fallback

- 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



[Ref. 1] Rahul Chatterjee et al.: pASSWORD tYPOS and How to Correct Them Securely. (SP '16)
[Ref. 2] William Melicher et al.: Usability and Security of Text Passwords on Mobile Devices. (CHI '16)

Payment System

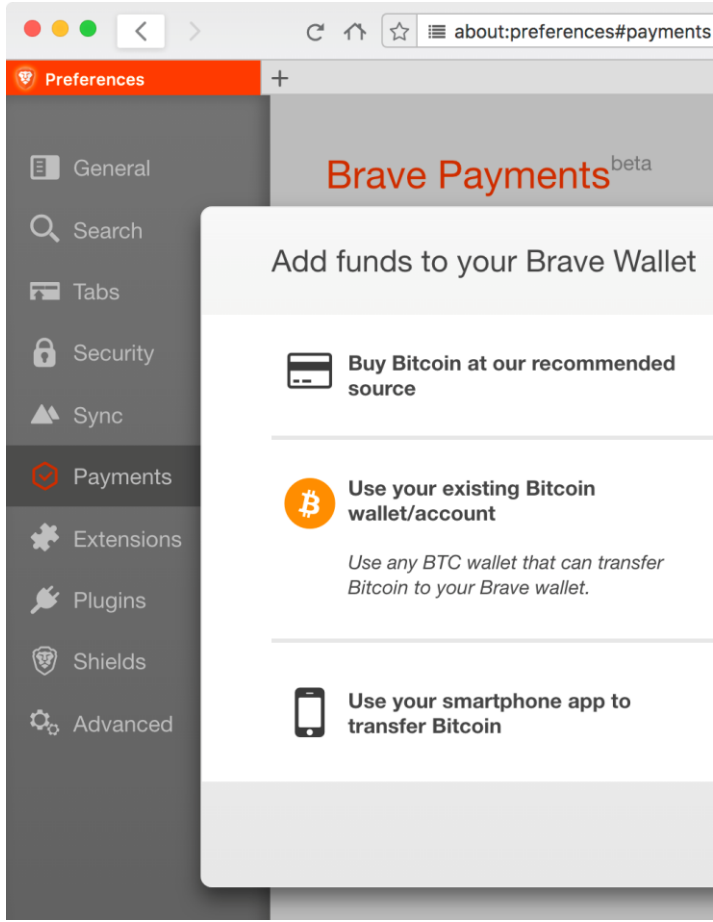
Requirements:

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

Proposals: [1,2,…]

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

Broad adoption remains a deployment challenge!



[Ref. 1] Joseph Poon et al.: The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments. (Technical Report)
[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

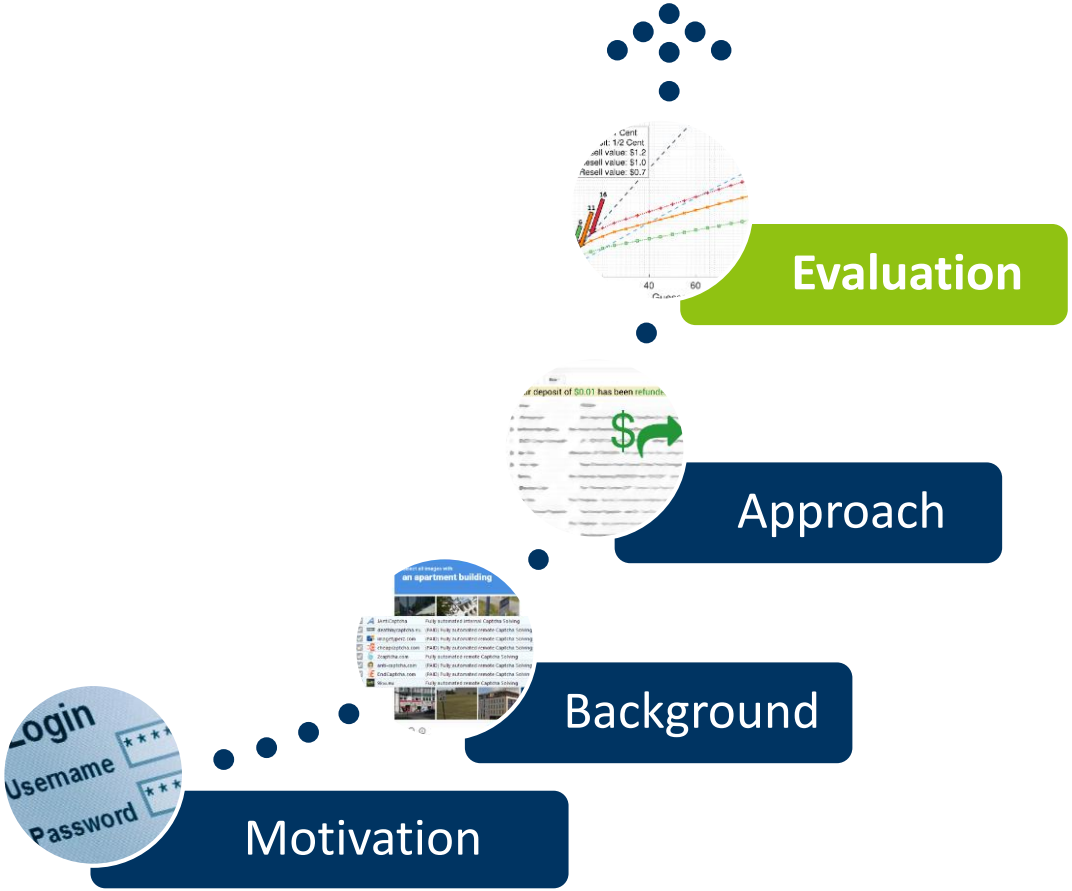
Refunding:

- 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

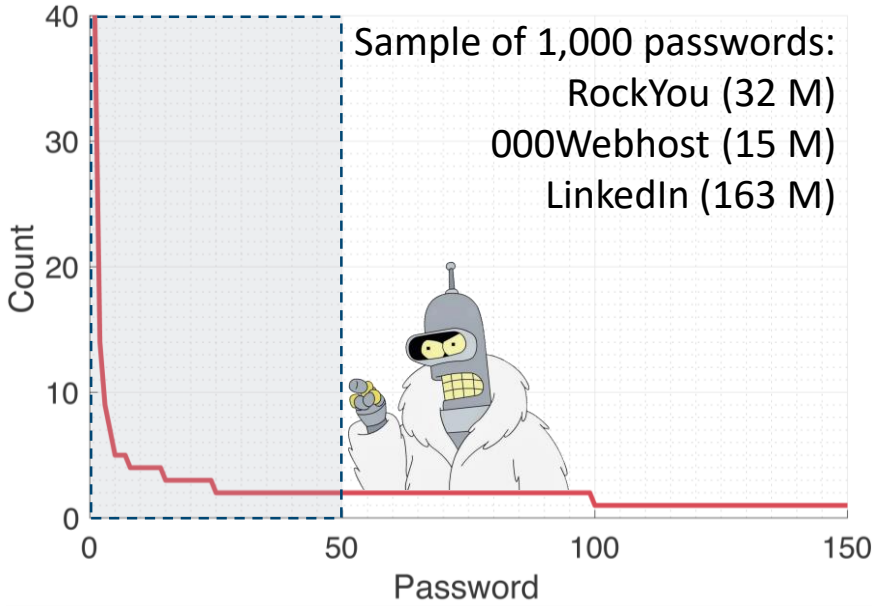
Outline


Evaluation
Approach
Background
Motivation
Login
Username
Password

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!

 [Img. 1] "Futurama" Put Your Head on My Shoulders, imdb.com

Attacker Profit

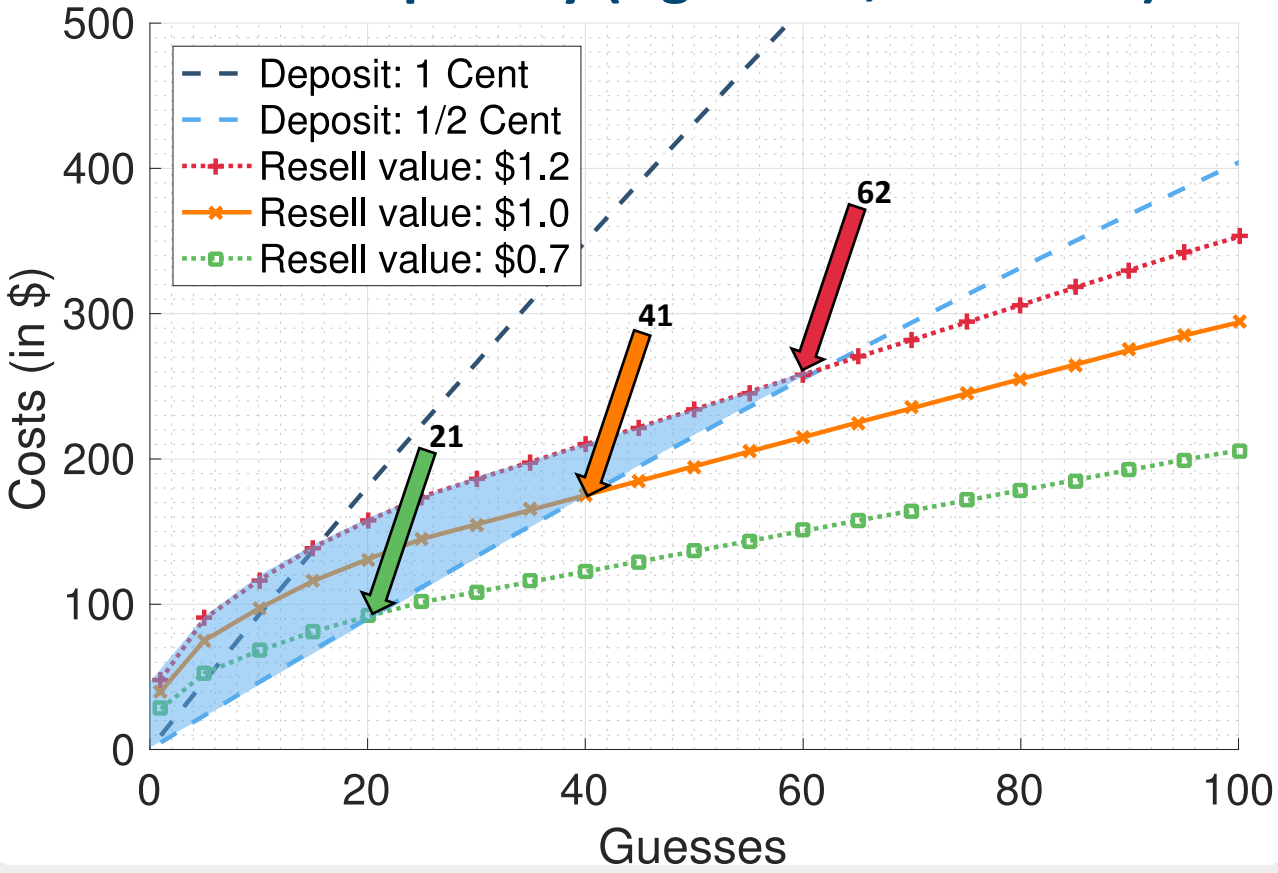
½ Cent per Try:

Against 1,000 Users

Resale Value	λ_1	λ_{10}	λ_{50}	λ_{100}
0.70$	23$	22$	-79$	-198$
1.00$	35$	51$	-21$	-110$
1.20$	43$	70$	18$	-51$

λ = #guesses

Attacker Profit – ½ Cent per Try (Against 1,000 Users)



Attacker Profit

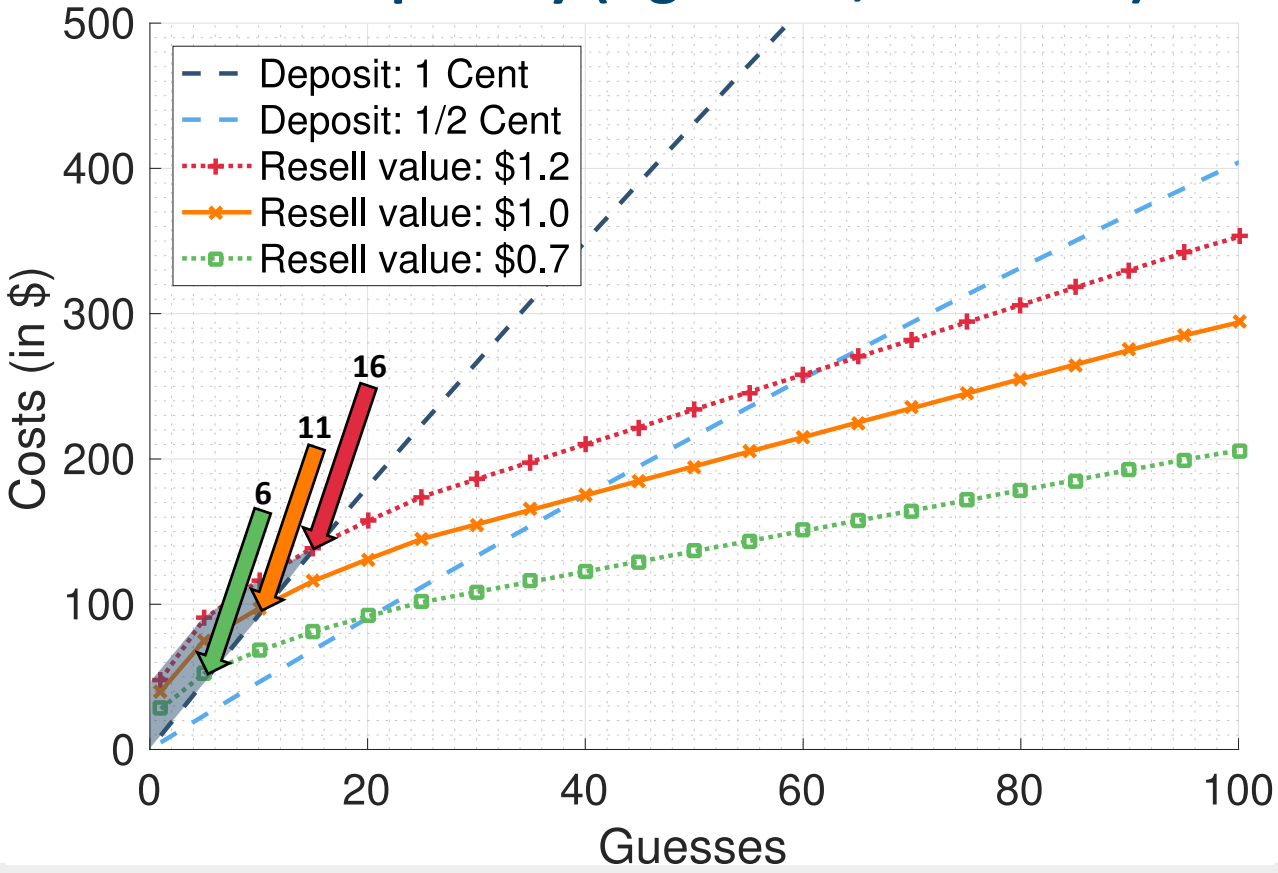
1 Cent per Try:

Against 1,000 Users

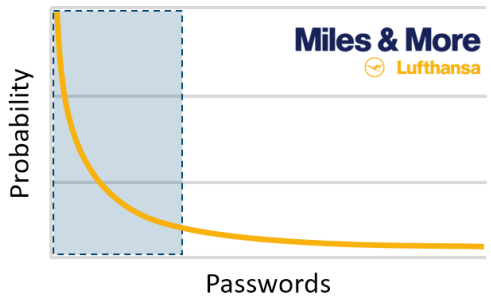
Resale Value	λ_1	λ_{10}	λ_{50}	λ_{100}
0.70$	18$	-25$	-295$	-602$
1.00$	30$	5$	-236$	-514$
1.20$	38$	24$	-197$	-455$

λ = #guesses

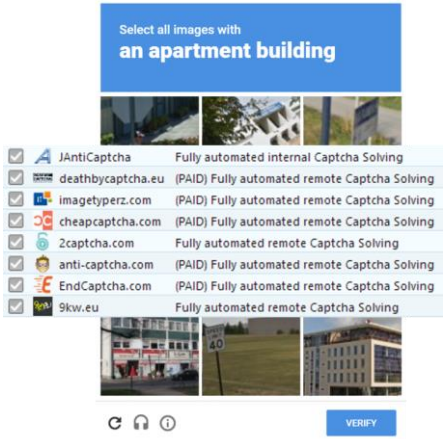
Attacker Profit – 1 Cent per Try (Against 1,000 Users)



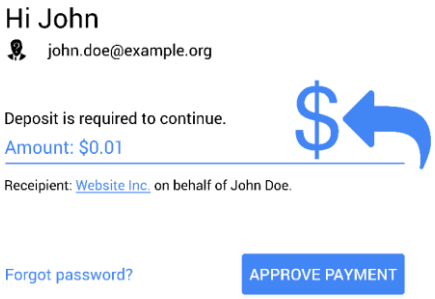
Takeaway



Online Password Guessing

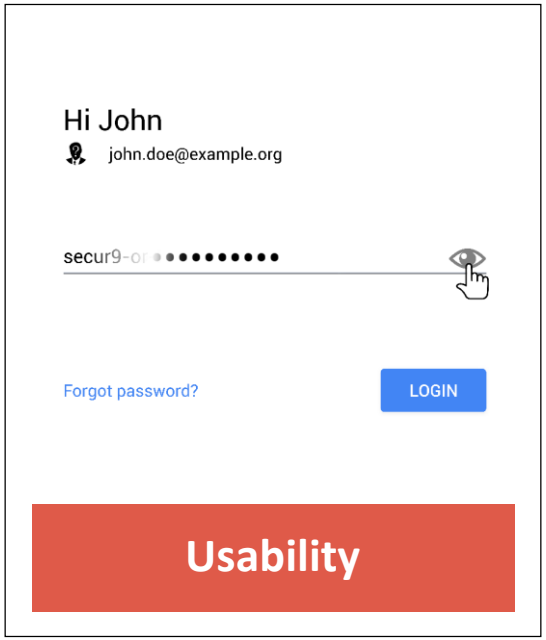


CAPTCHA Problem



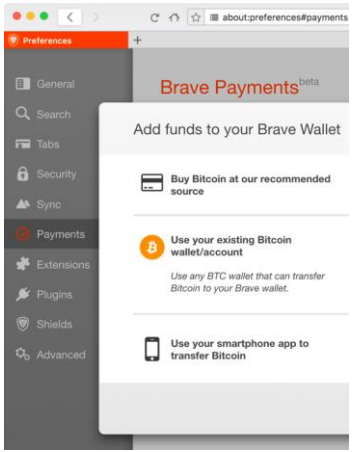
Deposit-based Rate Limiting

Discussion



Usability

Pricing



Payment System

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