Beyond Credential Stuffing: Password Similarity Models using Neural Networks

Bijeeta Pal*, Tal Daniel+, Rahul Chatterjee*, and Thomas Ristenpart*

*Cornell Tech +Technion

Password Breaches

Millions of passwords leaked every year
First half of 2018 alone, about 4.5 billion records were exposed[1]

[1] "Data breaches compromised 4.5bn records in half year 2018 – Gemalto". The Citizen, October 17, 2018

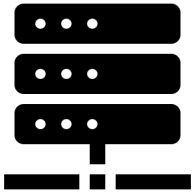
Implication of breaches

Username	Password
mark	jicDfba1
julia	password
tom	abc123
…	…

Leaked Dataset

Attacker

mark, jicDfba1



Server

Username	Password
mark	jicDfba1
charlie	123456
amelie	y567dty56
…	…

Authentication Database

Prior work: 40% users reuse passwords[2]

Credential Stuffing Attack

90% of login traffic and most prevalent form of account compromise![3]

[2] S. Pearman et al. “Let’s go in for a closer look:Observing passwords in their natural habitat,”.ACM CCS 2017, pp. 295–310.
[3]Shape Security, “2017 Credential spill report,” http://info.shapesecurity. com/rs/935-ZAM-778/images/Shape-2017-Credential-Spill-Report.pdf/, 2018.

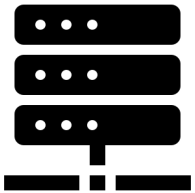
Countermeasures

Username	Password
mark	jicDfba1
julia	password
tom	abc123
…	…

Leaked Dataset

Attacker

mark, jicDfba1



Server

Username	Password
mark	jicDfba1
charlie	123456
amelie	y567dty56
…	…

Authentication Database

Breach Notification Service

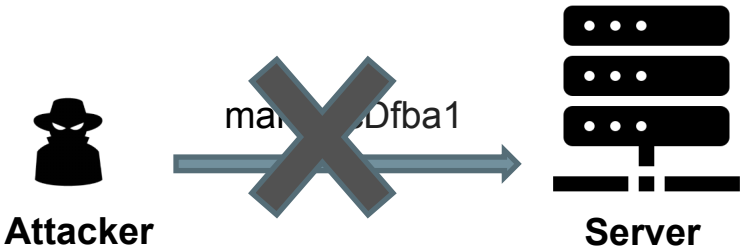
mark

Reset Password!

Countermeasures

Username	Password
mark	jicDfba1
julia	password
tom	abc123
…	…

Leaked Dataset



Username	Password
mark	jicDfba123
charlie	123456
amelie	y567dty56
…	…

Authentication Database

Credential tweaking attacks

Username	Password
mark	jicDfba1
julia	password
tom	abc123
…	…

Leaked Dataset

Username	Password
mark	jicDfba123
charlie	123456
amelie	y567dty56
…	…

Authentication Database

Our contributions

Attack

Most damaging credential tweaking attack to date

- Built using state of art deep learning framework
- **16%** of accounts compromised in less than **1000** guesses
- Evaluated on **real user accounts** of a large university

Defense

Personalized password strength meters (PPSM)

- Built using neural network based embedding models
- **Robust** against all known attacks
- **Fast** and **light-weight** (3MB)

Starting point: breach data

User	Password List
mark	jicDfba1, jicDfba123
julia	password, 123456, 1234567
tom	abcd123, abcd
…	…

Lots of similar passwords

First discovered by 4iQ on the Dark Web [4]

1.4 billion email, password pairs
1.1 billion unique emails
463 million unique passwords

More than **150 million** users with **2 or more passwords**

Around **10%** of distinct password pairs of same user are within **1 edit distance**

[4] J. Casal, "1.4 Billion Clear Text Credentials Discovered in a Single Database, " https://medium.com/4iqdelvedeep/1-4-billion-clear-textcredentials-discovered-in-a-single-database-3131d0a1ae14, Dec, 2017.

Prior work: manually chosen transformation rules

User	Password List
mark	jicDfba1, jicDfba123
julia	password, 123456, 1234567
tom	abcd123, abcd
…	…

Previous work[5][6]

- Can't generate new guesses once rules exhaust
- Might have missed similarity patterns

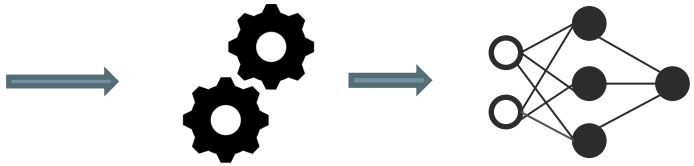
  markFacebook → mark@facebook

  markSuperman → marcSuperman

[5] A. Das et al., "The tangled web of password reuse." in NDSS, vol. 14, 2014, pp. 23–26.
[6] D. Wang et al., "Targeted online password guessing: An underestimated threat," in ACM CCS, 2016, pp. 1242–1254

Data-driven approach for learning similarity

User	Password List
mark	jicDfba1, jicDfba123
julia	password, 123456, 1234567
tom	abcd123, abcd
…	…



Machine learning

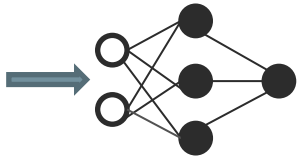
Similarity model

$P(w' \mid w)$

Models probability user selects w' given old password w

Goal: Build credential tweaking attacks using $P(w' \mid w)$

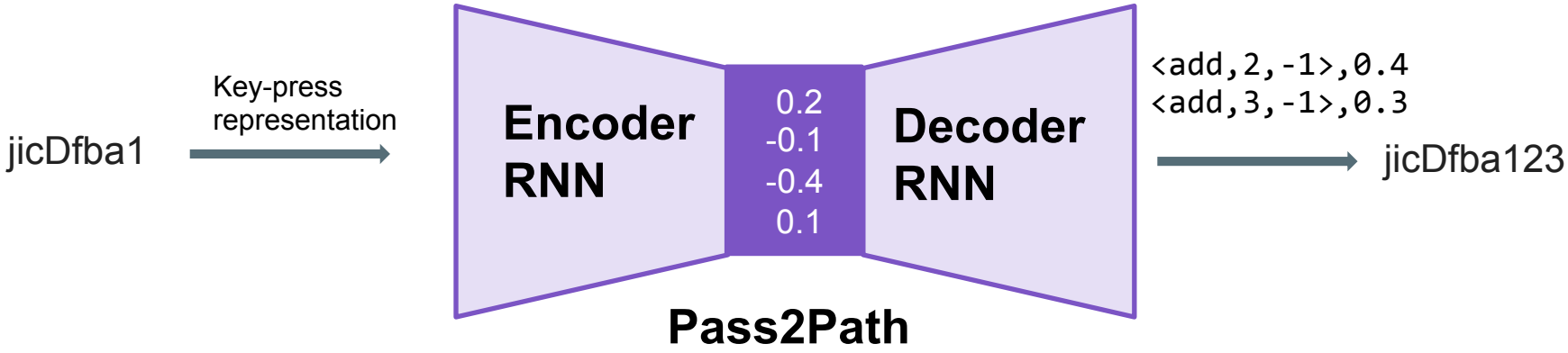
w = jicDfba1



Passwords	P($w' \mid w$)
jicDfba123	0.6
jicDfba	0.2
JicDfba1	0.1

Training generative similarity models

Encoder-decoder architecture built using character level recurrent neural network (RNN)

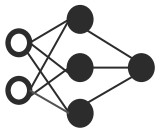


Trained on **144 million** of password pairs
Took 2 days on Nvidia GTX 1080 GPU and Intel Core i9 processor
Model has 2.4 million parameters, takes 60 MB space

Simulation-based evaluation

User	Password List
mark	jicDfba1, jicDfba123
julia	password, 123456, 1234567
tom	abc123, ftgKdu45
…	…

Training data
(144 mn w,w' pairs)



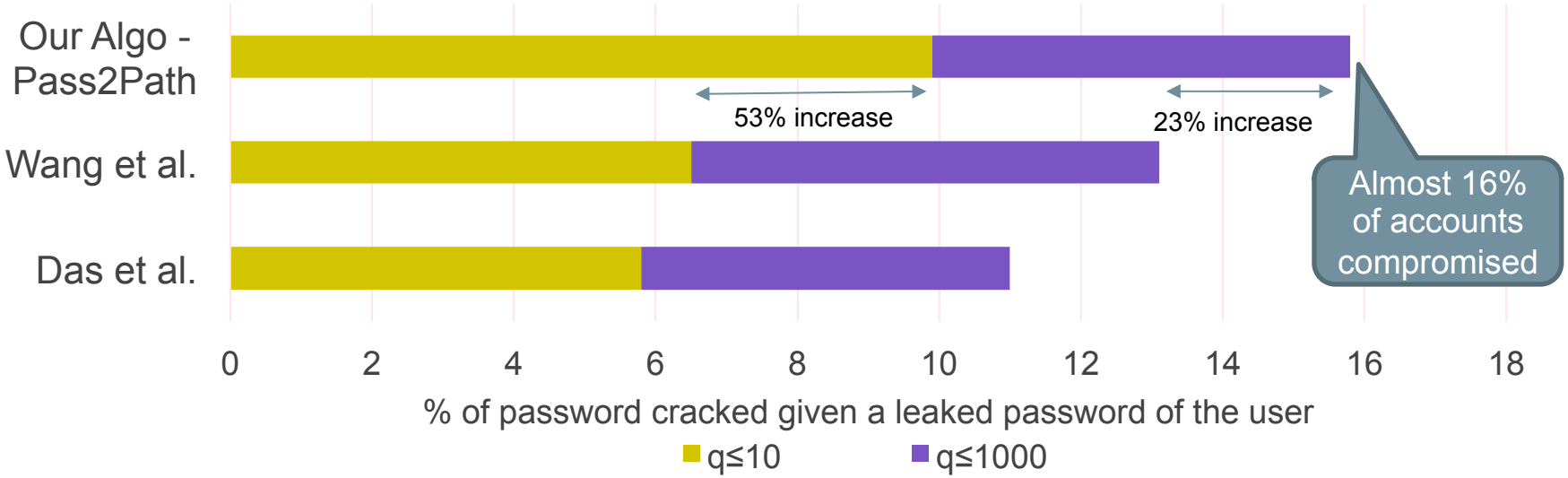
Pass2Path

Test data
(100,000
w',w pairs)

Online credential tweak attack setting:

- Given w, guess w' with q attempts
- $q \leq 1000$
- Report fraction of passwords guessed

Credential tweaking attacks



Using multiple leaked passwords: $P(w' \mid w1, w2, \ldots)$

Pass2path-based attack compromising **23%** of accounts (see paper)

Credential tweaking in practice

No real world evaluation of cred tweaking attacks

Partnered with Cornell University IT Security (ITSO)

Large-scale auth system
- ~500,000 accounts
- Use credential stuffing defenses
- Password rules

19,868 Cornell emails in leaked dataset

Ran our attack on these accounts to audit

Total 1,374 active accounts vulnerable

Vulnerable accounts put under watchlist by ITSO

Defense against these attacks

To date **no defenses** against credential tweaking attacks

- 71% vulnerable passwords considered strong by zxcvbn

only considers population wide pw distribution

Warn users when passwords are vulnerable to credential tweaking attacks

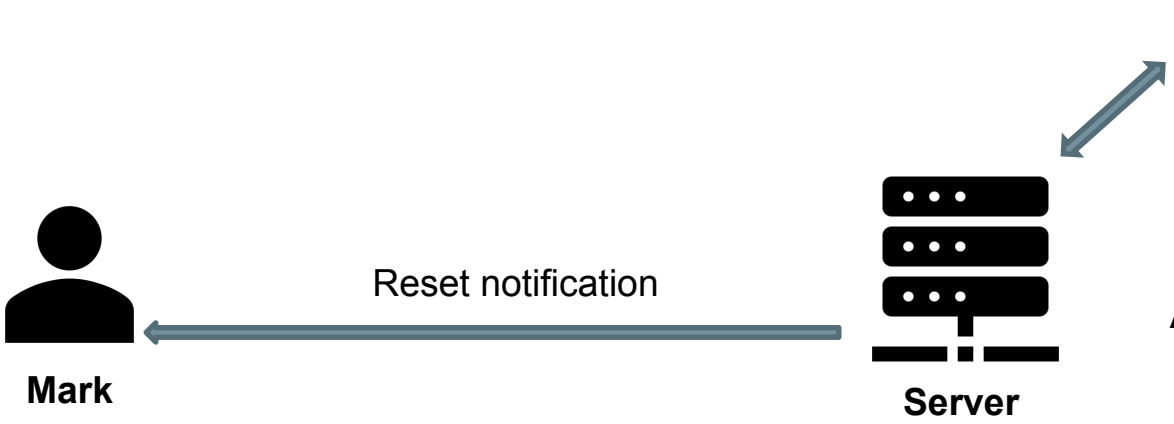
Expensive to run

Run audits using credential tweaking attacks

Our solution

Personalized password strength meter (PPSM)

Personalized password strength meter (PPSM)



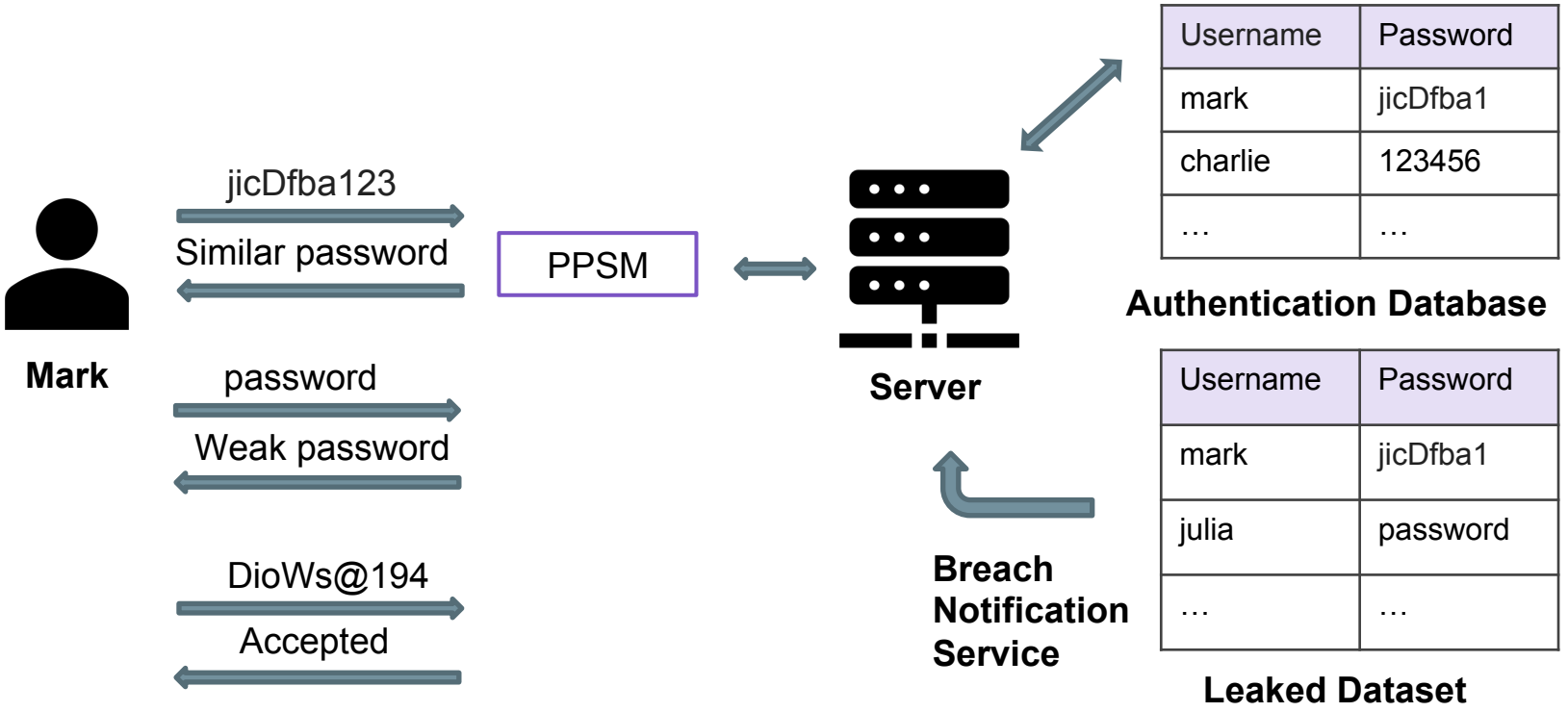
Username	Password
mark	jicDfba1
charlie	123456
…	…

Authentication Database

Username	Password
mark	jicDfba1
julia	password
…	…

Leaked Dataset

Personalized password strength meter (PPSM)

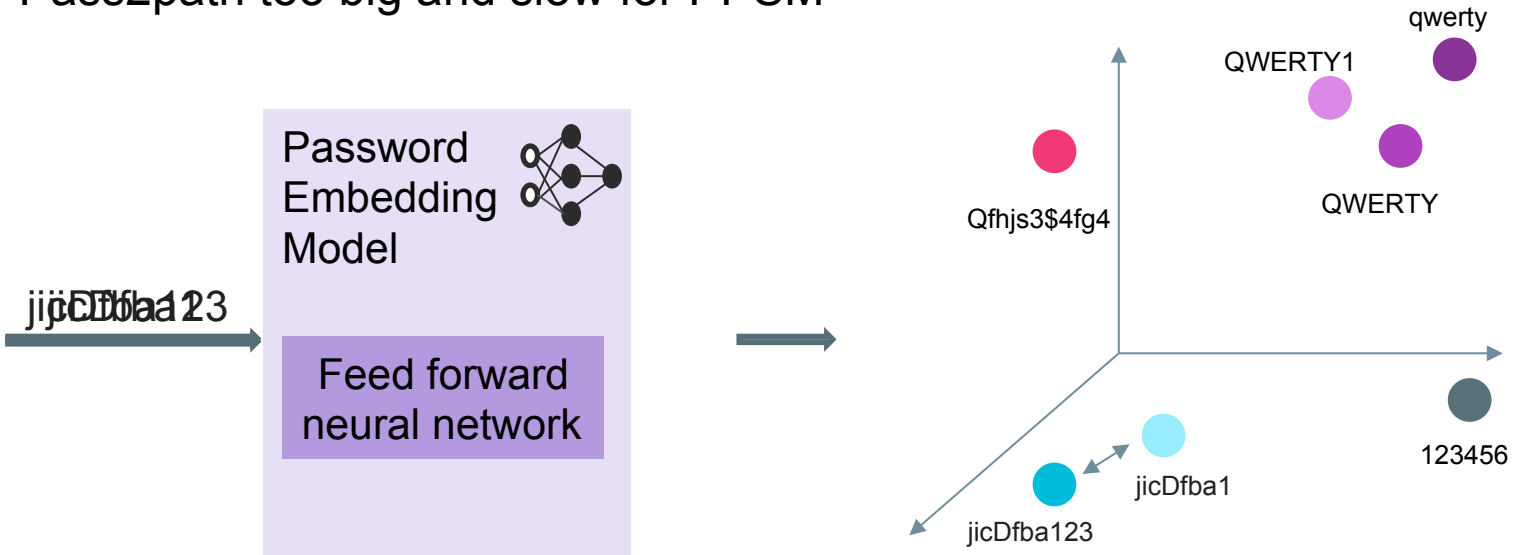


Username	Password
mark	jicDfba1
charlie	123456
…	…

Username	Password
mark	jicDfba1
julia	password
…	…

Building PPSMs

Pass2path too big and slow for PPSM



Compressed model detects 96% vulnerable passwords

Easy to deploy: 3 MB, Fast: 0.3 ms

Beyond credential stuffing

Modeling similarity of human chosen passwords
Build both damaging tweaking attack and first-ever defense against it

Attack

- Data-driven, state-of-the-art deep learning
- Outperforms the best previous attacks
- *1,374* active user accounts at Cornell University vulnerable

Defense

- PPSM using password embedding model
- Prevents credential tweaking attacks
- Fast and lean (3MB)

Email: bp397@cornell.edu
Website: cs.cornell.edu/~bijeeta/
Github: github.com/Bijeeta/credtweak

Thank you!