Telepathwords

Preventing Weak Passwords by
Reading Users' Minds


password
123456
12345678
1234
12345
qwerty
dragon
letmein
football
baseball
pussy
michael
mustang
abc123
monkey
master
jennifer
superman
shadow
jordan
696969
111111
2000
ranger
654321
asshole
access
jessica
freedom
soccer
computer
666666
killer
michelle
nicole
buster
george
hockey
robert
orange
taylor
fucker
123123
hunter
andrew
charlie
heather
batman
thomas
amanda
yankees
daniel
maggie
sexy
william
trustno1
hello
merlin
1234567
starwars
test
ashley
corvette
pepper
austin
love
harley
hammer
sunshine
1111
joshua
matthew
fuck
fuckyou
fuckme
123456789
thunder
tigger
silver
6969
biteme
ginger
summer
pass
dallas

Authentication ecosystem

System administrators

Users

Adversaries

Defending users

- System administrators set password policies
  - ——Constraints on passwords

Character requirements

- Common component of policies
  - ——Length
  - ——Uppercase, digit, symbol
- Couldn't prevent weak passwords:
  - ——Qwerty!123456
  - ——Thisismypassword!

Character requirements

- Default policies often use only character requirements

- In Microsoft Active Directory (**3class8**)
  - — 3 of the following :uppercase, lowercase, digit, symbol
  - — 8 character minimum

- **These requirements don't improve security and they make passwords harder to type.**

Goal

- Focus on weakest passwords
  - — Threat model: online attack of an organization
  - — Policies should make the weakest passwords harder to guess

Contributions

- Show that character requirements don't prevent weak passwords
- Introduce Telepathwords
  - — Detects weak passwords while providing real-time feedback
- Show that real-time feedback coupled with prevention of common patterns works well


"对不起，您的密码必须包括一个大写字母，两个数字，一个符号，一段激励人心的讯息，一句咒语，一个黑帮符号，一个埃及象形字符，以及一滴处女的血"
LOLINDIAN.COM
汉化：Revolucion@Guokr

Framework

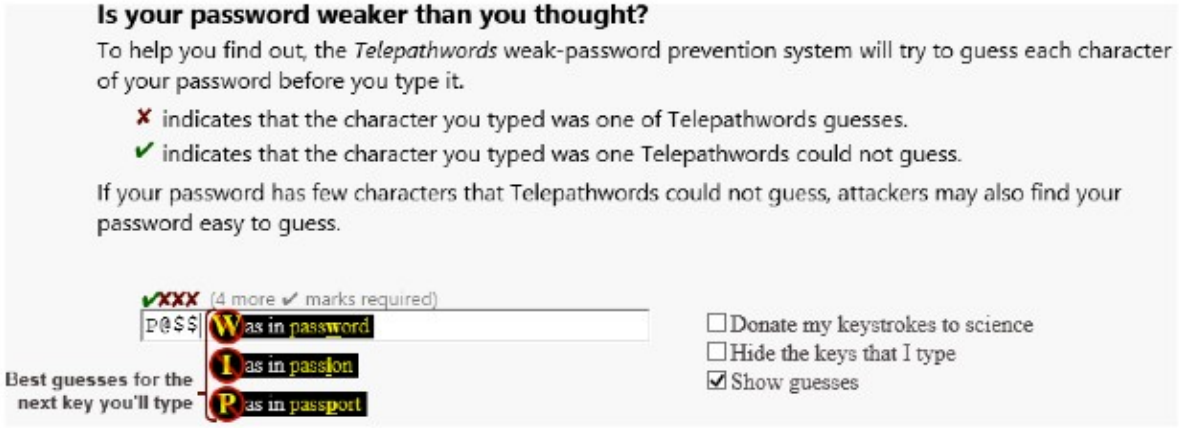
1. What is Telepathwords?
    1. Show website
2. Prediction algorithms
    1. Common character sequence
    2. Keyboard movements
    3. Repeated strings
    4. Interleaved strings
3. Testing
    1. Users response
    2. Security
4. Limitations
5. Conclusion

Framework

1. What is Telepathwords?
    1. Show website
2. Prediction algorithms
    1. Common character sequence
    2. Keyboard movements
    3. Repeated strings
    4. Interleaved strings
3. Testing
    1. Users response
    2. Security
4. Limitations
5. Conclusion

What is Telepathwords?

- weak-password-prevention system
- real-time prediction of next typed character
- how it looks



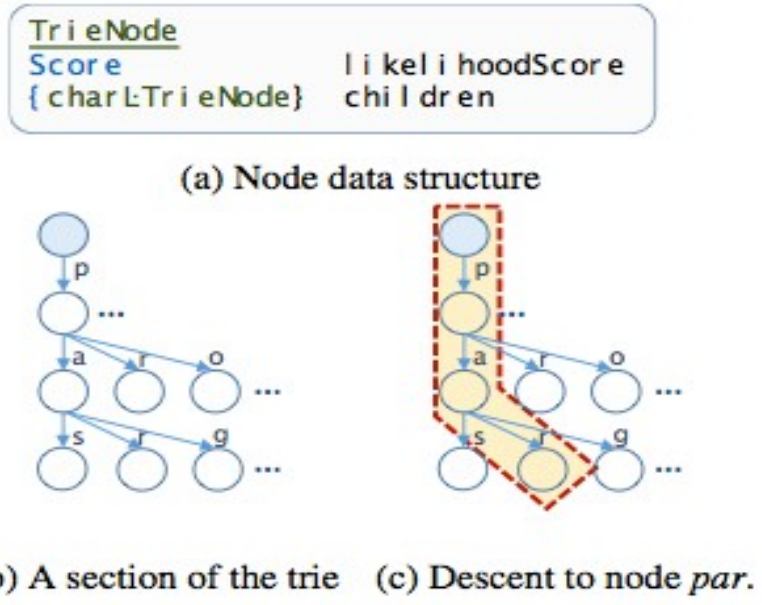
- https://telepathwords.research.microsoft.com/

Framework

1. What is Telepathwords?
    1. Show website
2. Prediction algorithms
    1. Common character sequence
    2. Keyboard movements
    3. Repeated strings
    4. Interleaved strings
3. Testing
    1. Users response
    2. Security
4. Limitations
5. Conclusion

Prediction Algorithms - Common character sequences

- each predictor uses a trie
- what is a trie?



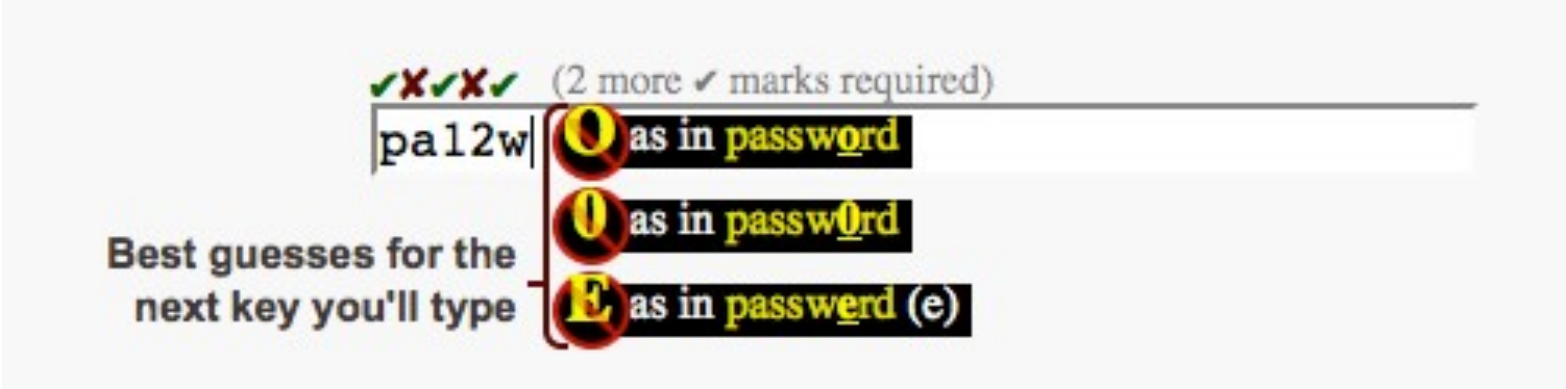
(a) Node data structure

(b) A section of the trie (c) Descent to node *par*.

- like binary trees
- walk from node to node
- common character sequences come from language models and databases of common passwords
- the most probable letter to come next is stored in the leftmost node

Prediction Algorithms - Common character sequences

- table for common character substitutions (e.g. $ for s, 3 for e, 0 for o)
- different windows for each prefix (note: cost of analysis increases)
    - detect words broken by distractor characters



Prediction Algorithms - Keyboard Movements

- maps characters to x and y coordinates
- counts consecutive moves that are to adjacent keys

Prediction Algorithms - Repeated Strings

- if repetitions are adjacent guesses next character in repetition
  e.g. xyabcabcabc

- if repetitions not adjacent assumes whatever is between the repetitions is part of repetition as well
  e.g. abcdefabcdef

(blue: user typed; red: guessed by program)

Prediction Algorithms - Interleaved Strings

- splits in odd and even
- runs two analyses, one for odds, one for even

e.g. phaeslslwooyrodu

password

helloyou

Framework

1. What is Telepathwords?
    1. Show website
2. Prediction algorithms
    1. Common character sequence
    2. Keyboard movements
    3. Repeated strings
    4. Interleaved strings
3. Testing
    1. Users response
    2. Security
4. Limitations
5. Conclusion

Testing

- 2 versions of Telepathwords-based policy:
  - telepath: at least 6 char unpredicted by system
  - telepath-v: same as telepath but password shown by default

- compared to:
  - basic8: at least 8 char long
  - 3class8: 8 char length, include 3 of 4 char classes
  - 3class12: 12 char length, include 3 of 4 char classes
  - 3class8-d: 8 char length, 3 of 4 char classes, doesn't match any of the 3M words in Openwall cracking dictionary

Testing - User Response

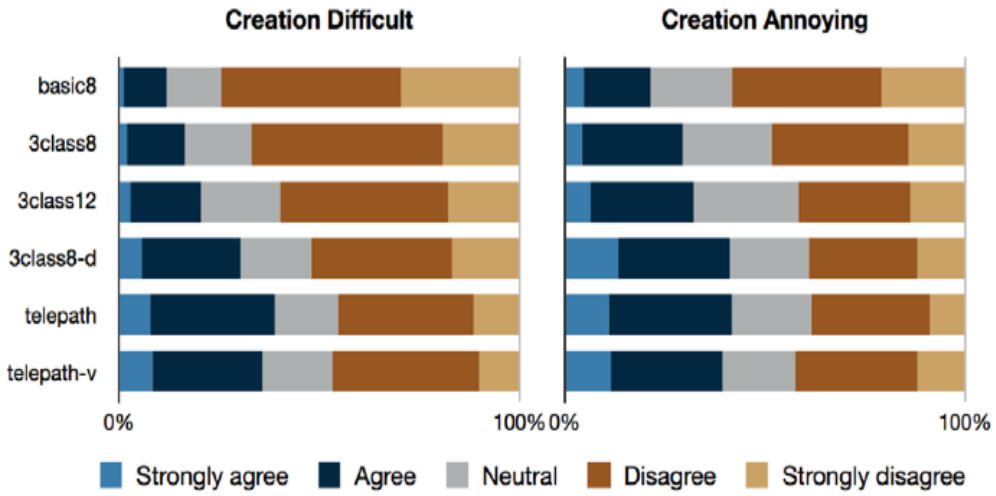


Figure 13: "Creating my password was difficult" and "Creating my password was annoying."

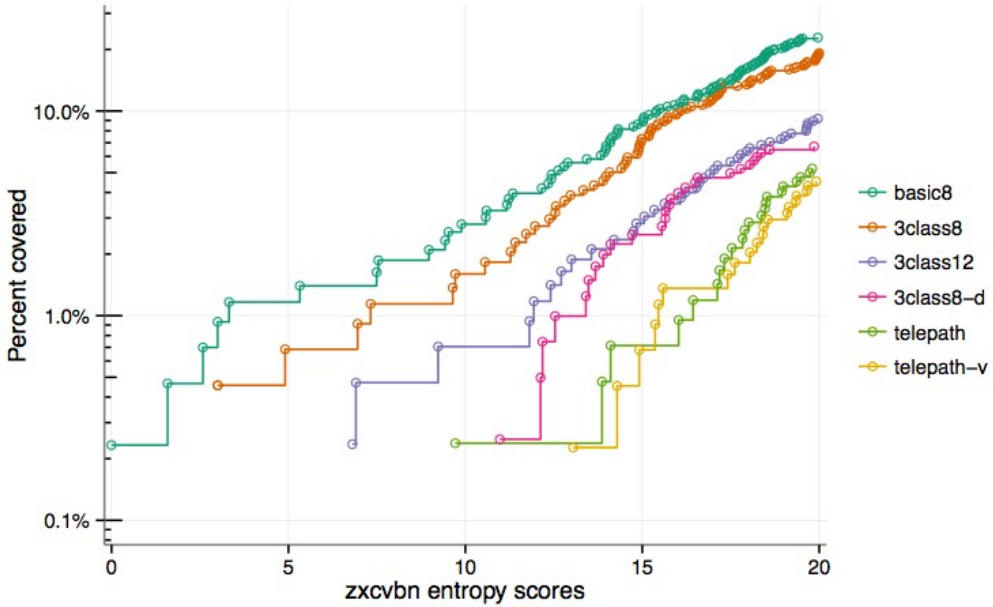
- More people annoyed by telepath than pure composition ones
- Users believed Telepath feedback provided more insight than others
- Both telepath among the treatments users considered more secure than previous password

Testing - Password Security

- Only considered weakest passwords
- Used three metrics to score passwords:
  - zxcvbn-entropy score: randomness score
  - Weir+ guess number: number of guesses to crack it
  - Telepathwords: number of hard to guess characters

Testing - Password Security

- All three metrics showed telepath and telepath-v were substantially more secure
- Telepath and telepath-v had the lowest percentages of passwords with zxcvbn-entropy scores of 20 or less



Testing - Password Security

- Security principle: psychological acceptability
- Tested user recall of passwords a few days later

	basic8	3class8	3class12	3class8-d	telepath	telepath-v
Password Recall in 5 tries without reminder						
during part one	423/431 (98%)	434/440 (99%)	414/425 (97%)	391/402 (97%)	407/420 (97%)	429/442 (97%)
part two did not store or re-use	83/135 (61%)	97/149 (65%)	86/140 (61%)	73/118 (62%)	84/138 (61%)	69/112 (62%)

Framework

1. What is Telepathwords?
    1. Show website
2. Prediction algorithms
    1. Common character sequence
    2. Keyboard movements
    3. Repeated strings
    4. Interleaved strings
3. Testing
    1. Users response
    2. Security
4. Limitations
5. Conclusion

Limitations

System limitations:

- US-centered language corpus (somewhat dated too)
- can't detect reversed sequences characters
- privacy policy prevents growth of language corpus

Testing limitations:

- role-play scenario might not reflect reality
- user recall tested after a short period

Conclusion

- Telepathwords provides users with significantly more insight into quality of their passwords
- Results in passwords stronger than approaches that do not use dictionaries
- To crack 1% of Telepathwords passwords, need 1000+ more guesses than default password policies passwords