Keyboard Based Password Generation Strategies

Ben Harsha, Jeremiah Blocki
Purdue University

The issue of password reuse

- Password reuse is a well-known problem e.g.[1]
- Users pick the same or similar passwords for multiple services
- If one service is compromised then an attacker can use information from one breach to break into other accounts
- Question: How can we solve this problem?

[1] The domino effect of password reuse, Blake Ives, Kenneth R. Walsh, and Helmut Schneider

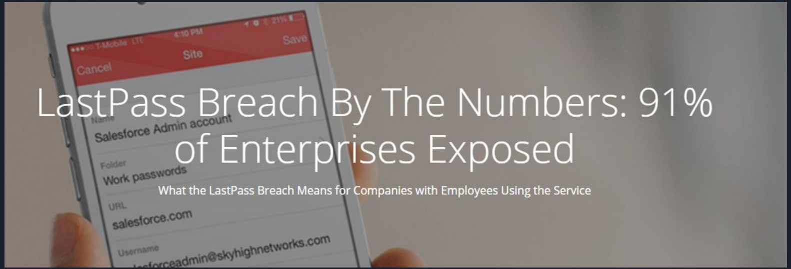
Existing solutions

- Password managers e.g. lastpass, keepass

LastPass •••|

KeePass

- Automatic, but not always portable, single point of failure, and breaches have occurred



LastPass Breach By The Numbers: 91% of Enterprises Exposed

What the LastPass Breach Means for Companies with Employees Using the Service

Human Computable Passwords

- Instead of memorizing passwords, learn a method to generate multiple distinct passwords

- Simple example - take a website name and append the first three letters to the end of a password e.g. for aardvark.com password becomes passwordaar
- Competing Goals:
  - Usability - easy to (re)generate passwords
  - Security - attacker cannot predict passwords

Existing HCP Strategies

- [BBDV14] High security at the cost of expensive memorization phase + auth time[2]
- [BV15] Simple mental calculations [3]

- Why not just use these strategies?

- We would like better security and usability

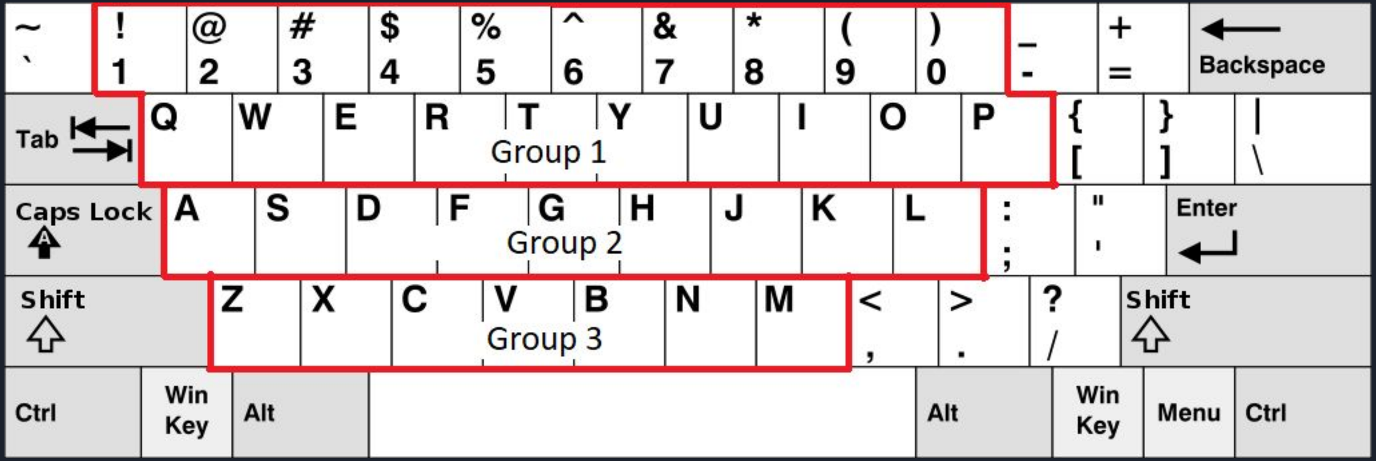
[2] Towards Human Computable Passwords. Blocki, Blum, Datta, Vempala
[3] Publishable Humanly Usable Secure Password Creation Schemas. Blum, Vempala

Keyboard-based schemes

- Idea: Have users use a tool at hand as an aid in computation
- Users will generate passwords based on where letters physically fall on a keyboard

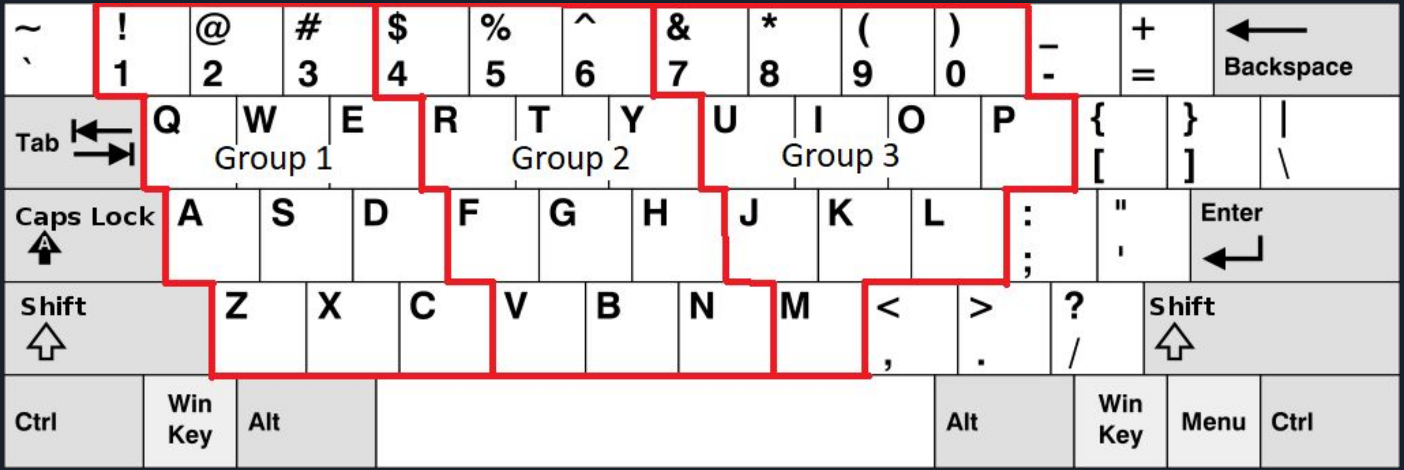
Fancy colors optional, but recommended for style

Row based



~ `
! 1
@ 2
# 3
$ 4
% 5
^ 6
& 7
* 8
(9
) 0
_ -
+ =
Backspace
Tab
Q
W
E
R
T
Y
U
I
O
P
{ [
}]
| \
Group 1
Caps Lock
A
S
D
F
G
H
J
K
L
: ;
" '
Enter
Group 2
Shift
Z
X
C
V
B
N
M
< ,
> .
? /
Shift
Group 3
Ctrl
Win Key
Alt
Alt
Win Key
Menu
Ctrl

Section based



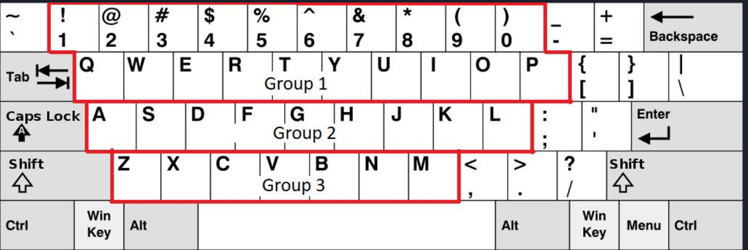
Word memorization

- Users memorize a set of nine secrets in one of two ways
  - Person - Action - Object stories (PAO)
  - Random words (words)
- PAO - memorize three three-word “stories”
  - E.g. TuringKickingDoor
- Random words - memorize a sequence of nine random words
- Both schemes divide the memorized secrets into three sets of three

Responding to challenges

- Challenges are short strings based on common website names i.e. Alexa Top 100 sites
- E.g. “wikipedia”

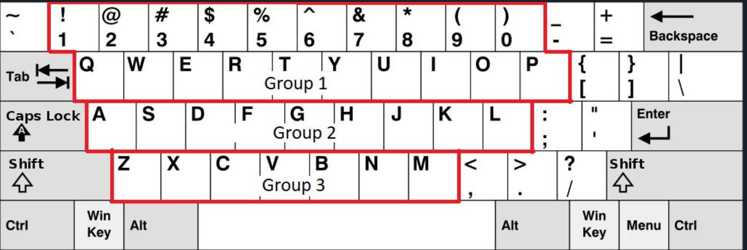
Turing	Kicking	Door
Einstein	Kissing	Piranha
Curie	Juggling	Frog



Responding to challenges

- Challenges are short strings based on common website names i.e. Alexa Top 100 sites
- E.g. “wikipedia”

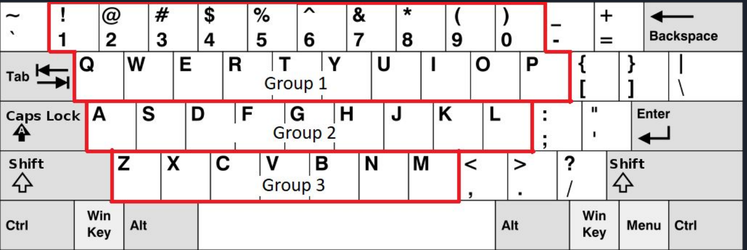
Turing	Kicking	Door
Einstein	Kissing	Piranha
Curie	Juggling	Frog



Responding to challenges

- Challenges are short strings based on common website names i.e. Alexa Top 100 sites
- E.g. “wikipedia”

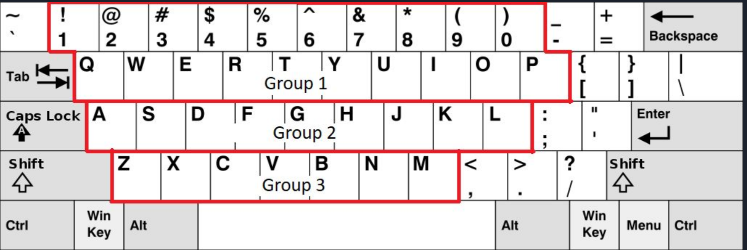
Turing	Kicking	Door
Einstein	Kissing	Piranha
Curie	Juggling	Frog



Responding to challenges

- Challenges are short strings based on common website names i.e. Alexa Top 100 sites
- E.g. “wikipedia”

Turing	Kicking	Door
Einstein	Kissing	Piranha
Curie	Juggling	Frog


~ ` ! 1 @ 2 # 3 $ 4 % 5 ^ 6 & 7 * 8 (9) 0 _ - + = Backspace
Tab Q W E R T Y U I O P { [}] | \
Group 1
Caps Lock A S D F G H J K L : ; " ' Enter
Group 2
Shift Z X C V B N M < , > . ? / Shift
Group 3
Ctrl Win Key Alt Alt Win Key Menu Ctrl

TuringKickingPiranha

User Study

- Longitudinal (50+ day) user study was run using MTurk
- Two studies
  - Pilot study - large number of groups
  - Main study - more users with small number of groups
- Studies involve a memorization training phase and a testing phase
  - Both are identical except for groups involved and number of return visits
- First study used as a “pilot” for the 2nd study. Best performing groups selected for second study

Study Conditions

1. Control - memorize a random string
2. Row divisions w/ PAO
3. Row divisions w/ words
4. Sections w/ PAO
5. Sections w/ words
6. Running sum method*

Initial Visit

- Users sorted into groups round-robin style
- Consent Form
- Instructions for their group
- Practice session
- Test session
- Return schedule shown

Testing phase

- Users are shown 5 challenges selected from Alexa Top 100

- Phase ends when all challenges are complete OR 10 mistakes (cumulative) are made

Return visits

- Users were asked to return several times in increasingly long intervals
  - Each interval 1.5 times the last, as has been found to be effective in previous studies [4]
  - First gap of 19 hours, ~2 week gap by the end

- 6 returns in the pilot study, 10 in the 2nd phase study

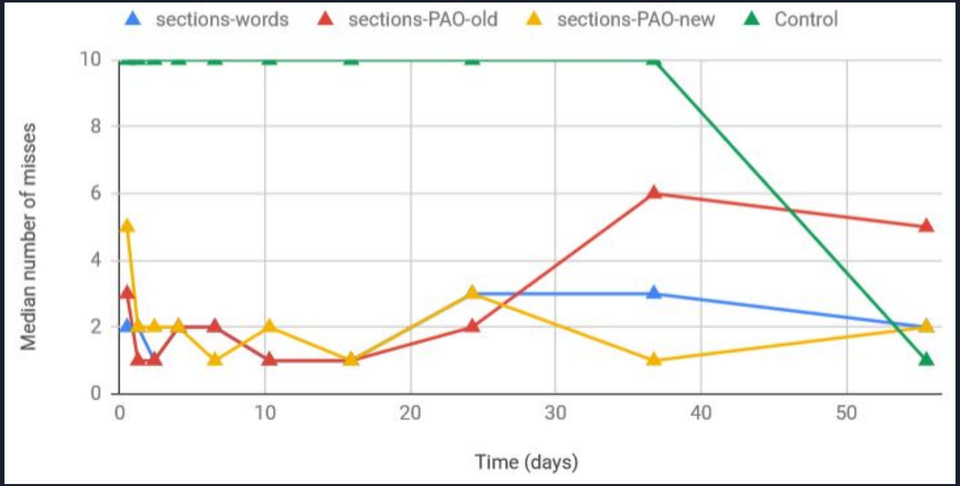
- Return visits were identical to the testing phase in the first visit

[4] Spaced repetition and mnemonics enable recall of multiple strong passwords. Blocki, Komanduri, Cranor, Datta

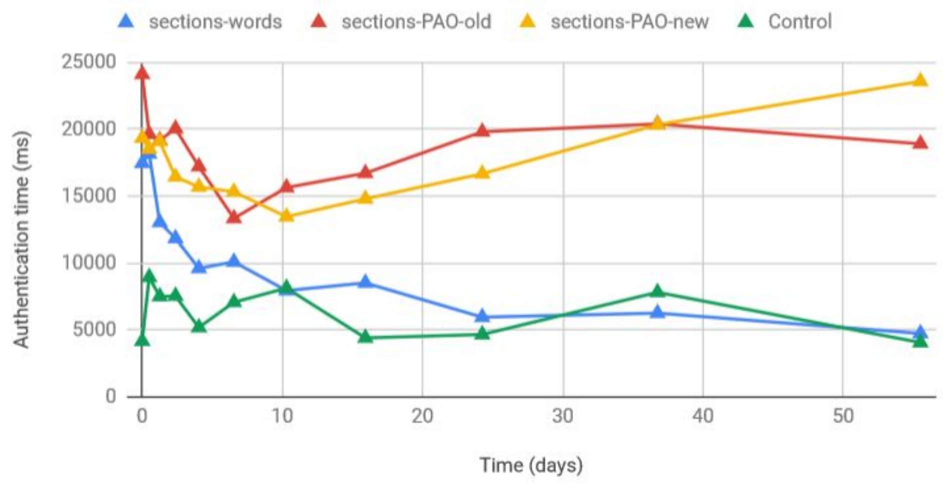
Debriefing

- On the final visit an optional demographic survey was shown
- Following this a NASA-Task Load Index form was shown
  - Suggested by local cognitive psychology group

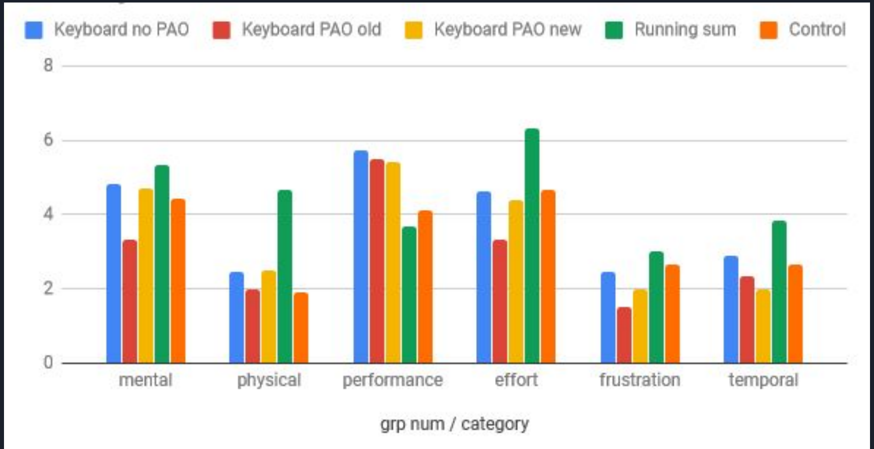
Mistake rates



Median successful authentication times



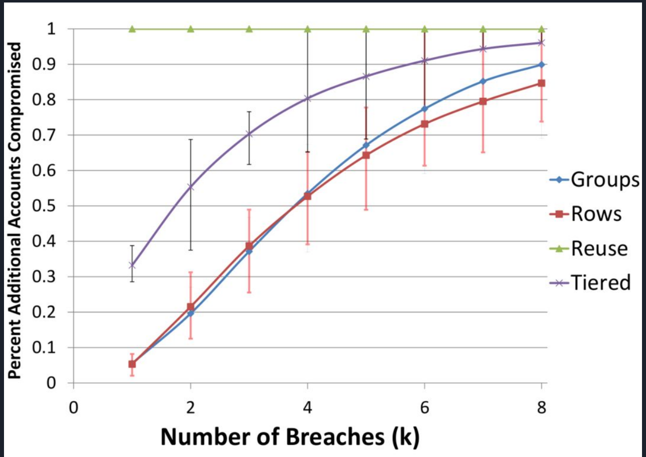
TLX results


Keyboard no PAO
Keyboard PAO old
Keyboard PAO new
Running sum
Control
8
6
4
2
0
mental
physical
performance
effort
frustration
temporal
grp num / category

Security of these strategies

- Question: As leaks happen and adversaries learn more passwords how well do these schemes hold up?

- Randomized experiment simulates leaks, chart shows estimated number of cracked accounts after k breaches



- Tiered - users select a weak, medium, or strong password based on self-perceived value of an account

Conclusions

- Users are able to successfully use keyboard based schemes!
- This scheme improves security over password reuse and tiered password security approaches

What’s next?

- What other schemes will work well?

- Can we improve these schemes to help users use them successfully?
    - Maybe differently worded instructions? More visual aids?

- In the end - can we design a human computable system that people are happy to use? What does it take to have people prefer these methods over password reuse?

Questions