black hat EUROPE 2018

DECEMBER 3-6, 2018

EXCEL LONDON / UNITED KINGDOM

Thermanator:

Thermal Residue Attacks

Tyler Kaczmarek
Ercan Ozturk
Gene Tsudik

University of California, Irvine

A Common Scenario:

1. You arrive at work (shared workspace)
2. Go to your desk & workstation
3. Enter password (userid is often implied)
4. Get bored waiting for login process to finish
5. Look at screen, maybe click the mouse a few times

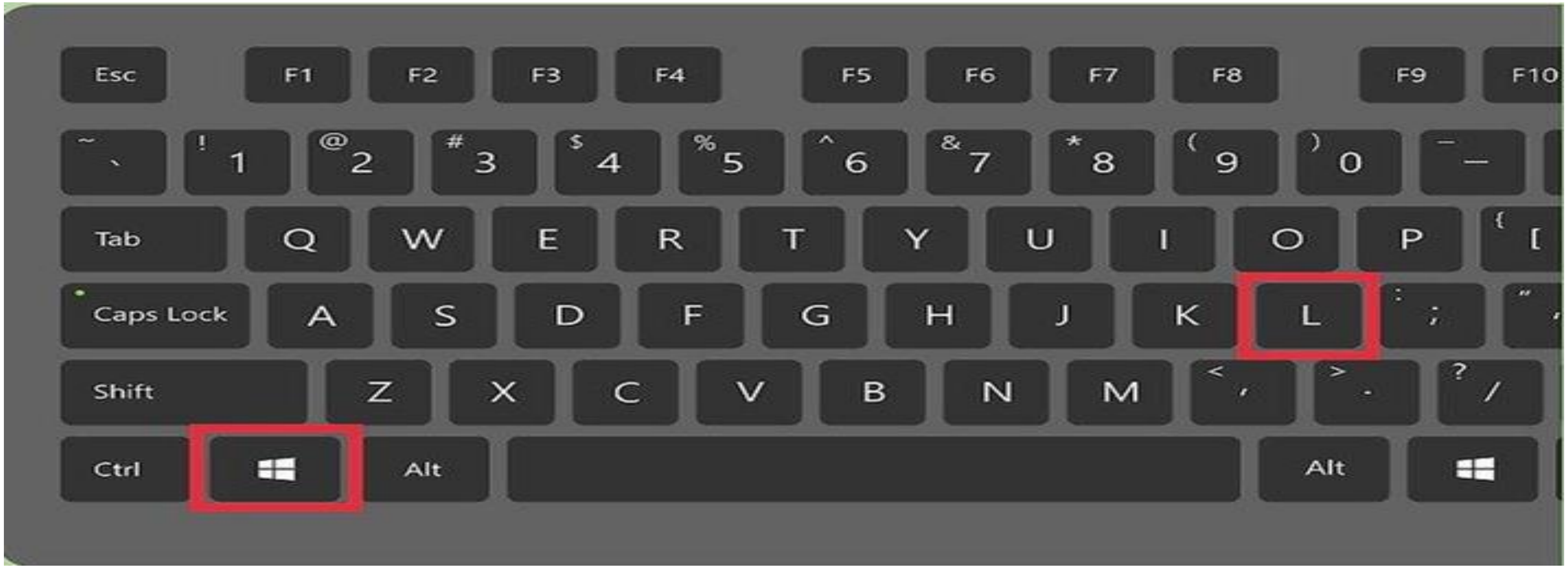
6a. A colleague calls you to a meeting or for coffee

OR

6b. You step away on your own (to bathroom, coffee, etc.)

7. Being security conscious, you might even lock the screen

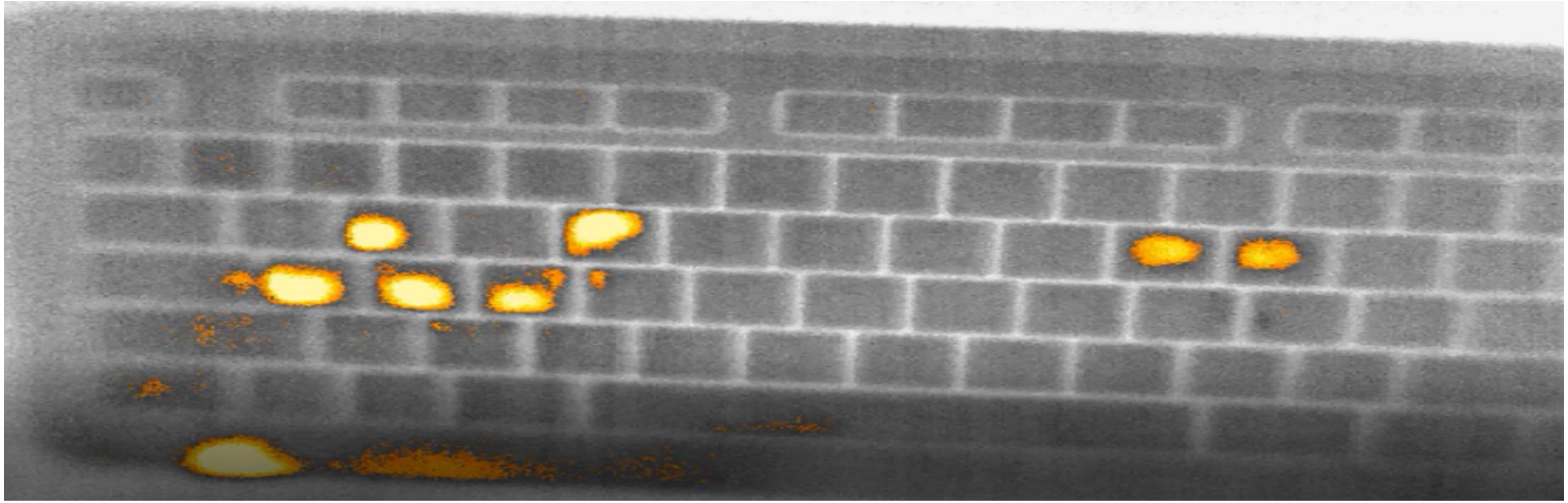
Any Problems?


Esc F1 F2 F3 F4 F5 F6 F7 F8 F9 F10
~ ` ! 1 @ 2 # 3 $ 4 % 5 ^ 6 & 7 * 8 (9) 0 _ –
Tab Q W E R T Y U I O P { [
Caps Lock A S D F G H J K L : ; "
Shift Z X C V B N M < , > . ? /
Ctrl Alt Alt

You didn’t wear oven mitts!

Why wear oven mitts?

(or any other thermal-insulator)



- ◆ Most modern external keyboards are made of plastic
- ◆ Poor conductor ➔ retains heat for a while…

Related Work

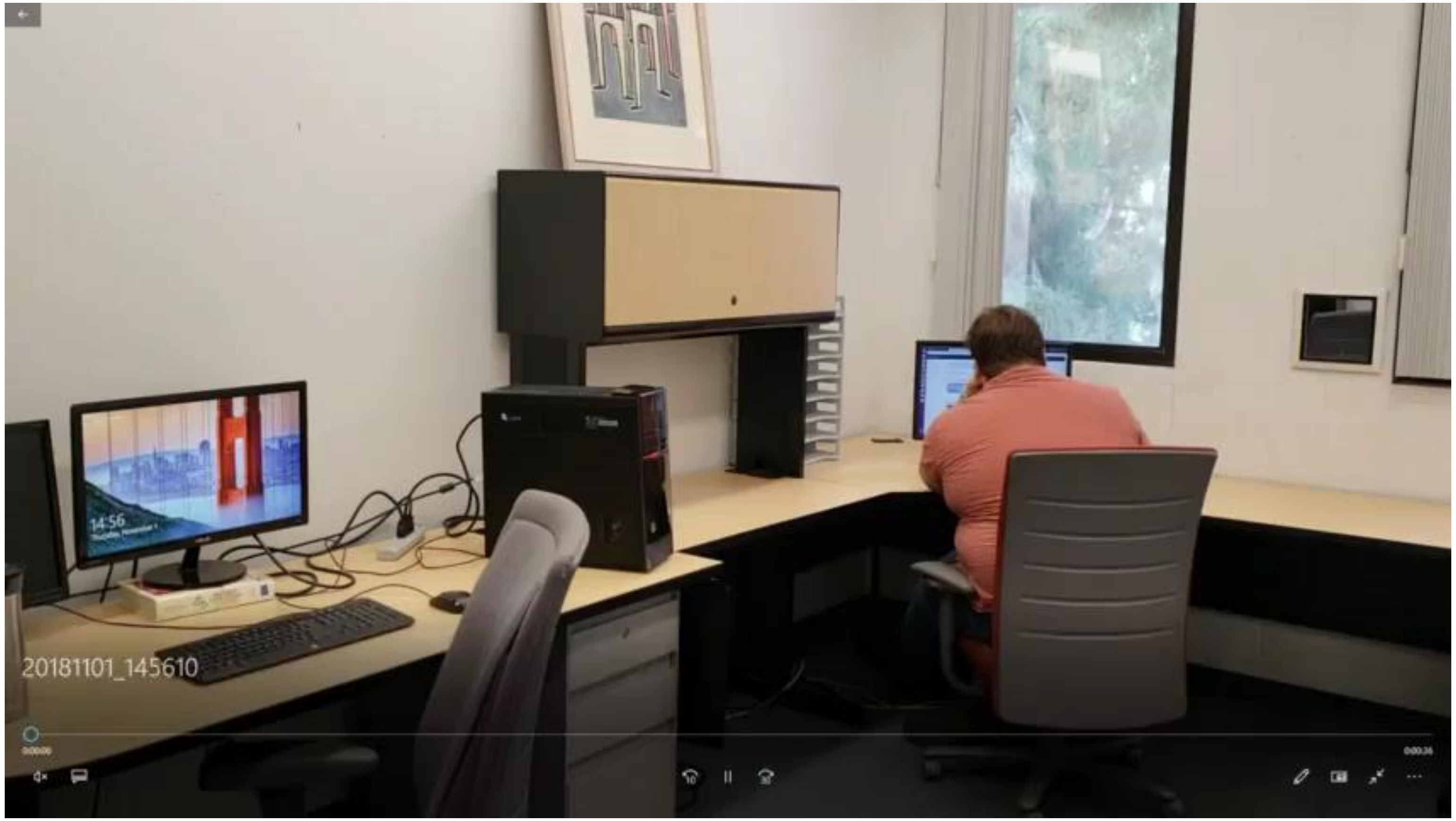
- Mainly focused on recovering PINs
- First work by Zalewski on cracking safes (2005)
    - Mowery, et al. (2011)
    - Wodo and Hanzlik (2016)
- Mobile devices (screen-lock patterns)
    - Androitis, et al. (2013)
    - Abdelrahman, et al. (2017)
- No systematic investigation of thermal residues on external keyboards

Thermanator aka “Coffee-Break” Attack

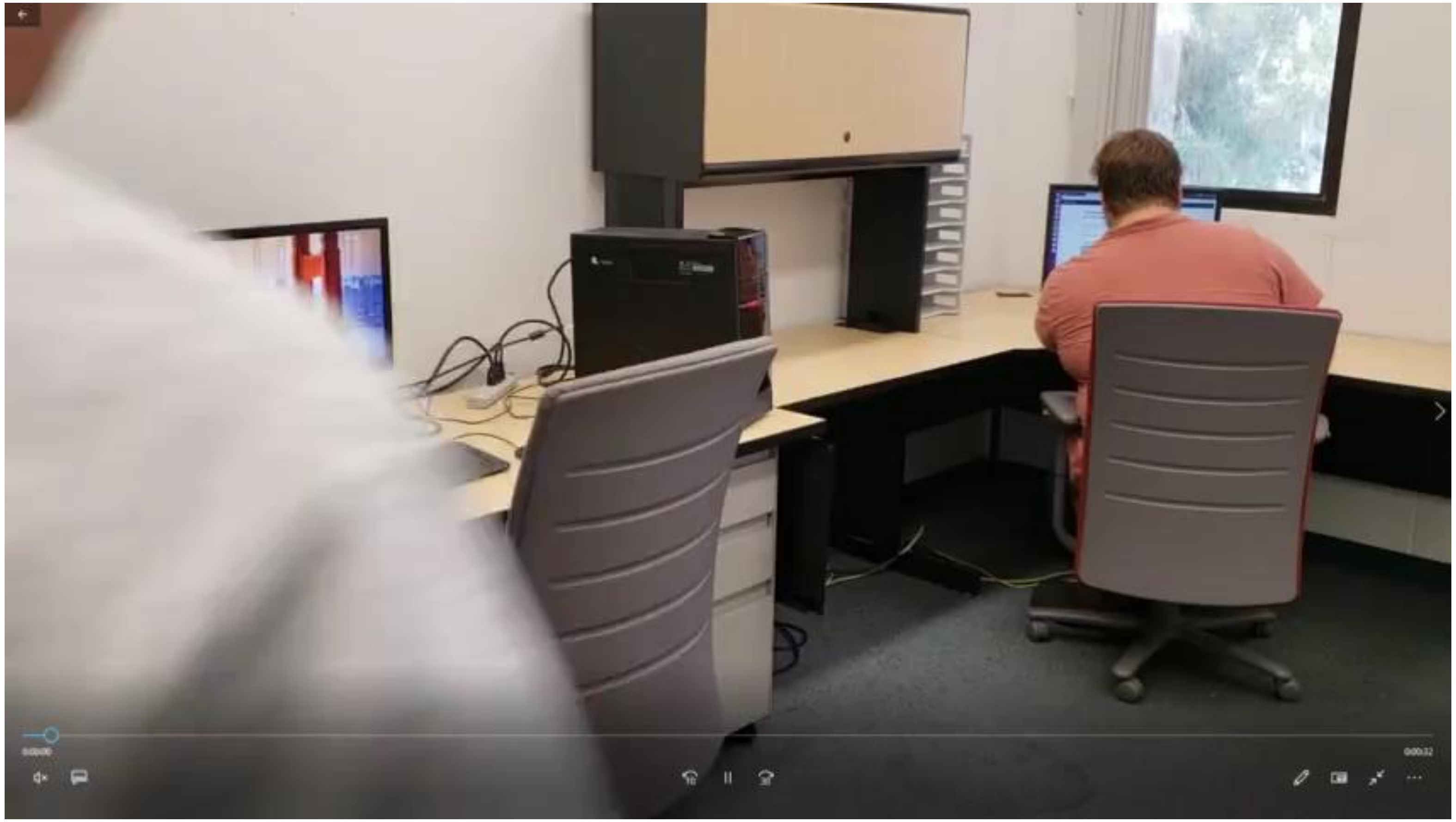
Two Flavors:

- **Opportunistic:** victim steps away on own accord
- **Orchestrated:** accomplice distracts and/or lures away

Opportunistic Thermanator Attack



Orchestrated Thermanator Attack



Questions:

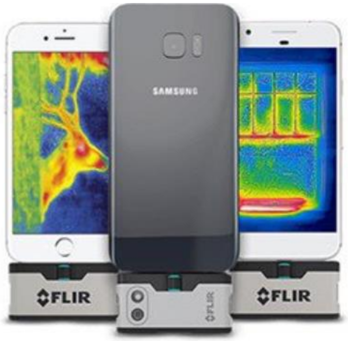
- How dangerous are **thermal** side-channel-based attacks?
- What is the realistic attack window?
- What does attack’s success require?
  - User physical attributes (e.g., fingertip size/shape)
  - Password strength (weak or strong)
  - Typing style (hunt-and-peck vs. touch typing)
  - Keyboard type (brand and model)

When in doubt, experiment!

Attacker Equipment:

- Mid-range thermal camera (FLIR SC620)
- Cost around $1,500 (used)
- Thermal imaging frequency: **1 Hz**

<u>Note:</u> to “un-initiated”, looks like a regular video camcorder.



FLIR One

SC620

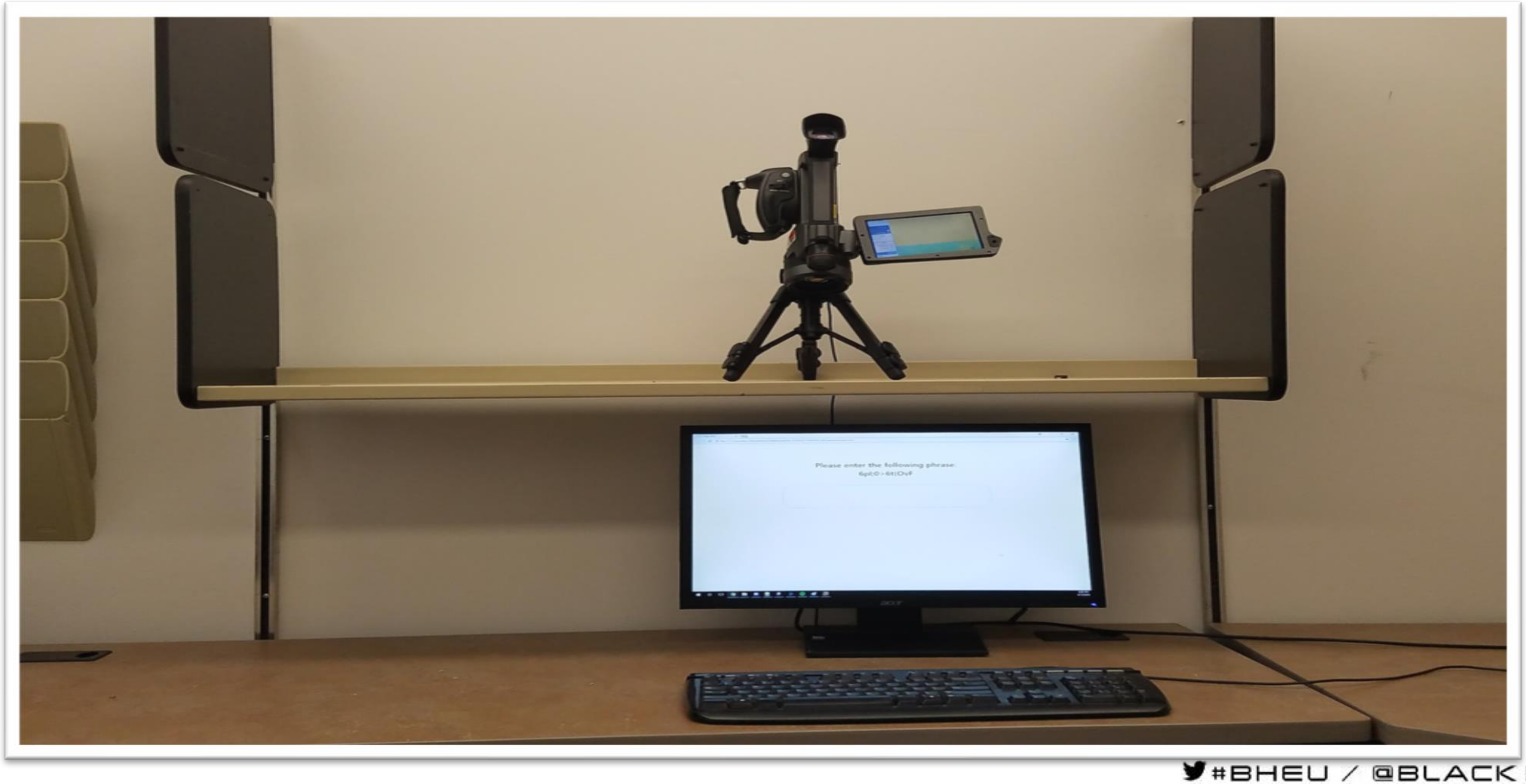
A6700sc

X8500sc

Model	Price	Capabilities
FLIR One	US$300	Sensitivity: 0.15K. Accuracy: ±1.5K or 1.5% of reading. Resolution: 50x80. Image Capture: Manual, 1 image at a time. Video Capture: None
SC620	US$1,500 (used)	Sensitivity: 0.04K Accuracy: ±2K or 2% of reading. Resolution: 640x480. Image Capture: Automatic, 1fps Video Capture: None.

Model	Price	Capabilities
A6700sc	US$25,000	Sensitivity: 0.018K Accuracy: ±2K or 2% of reading. Resolution: 640x512. Image Capture: Automatic, up to 100fps. Video Capture: Up to 100fps.
X8500sc	US$100,000	Sensitivity: 0.02K Accuracy: ±2K or 2% of reading. Resolution: 1280x1024 Image Capture: Automatic, up to 180fps. Video Capture: Up to 180fps.

Experimental Setting



Experiments: STAGE I

- ✓ Recruited 31 subjects, mixed gender, college-age

- ✓ Each entered 10 passwords:
  - ○ **Weak:** "password", "football", "iloveyou", "12345678", "12341234", "passw0rd", and "jordan23"
  - ○ **Strong:** "jxM#1CT[", "3xZFkMMv|Y", and "6pl;0>6t(OvF"

- ✓ Images taken every second, up to 1 minute **after** entry

Four Popular Keyboards (plastic)

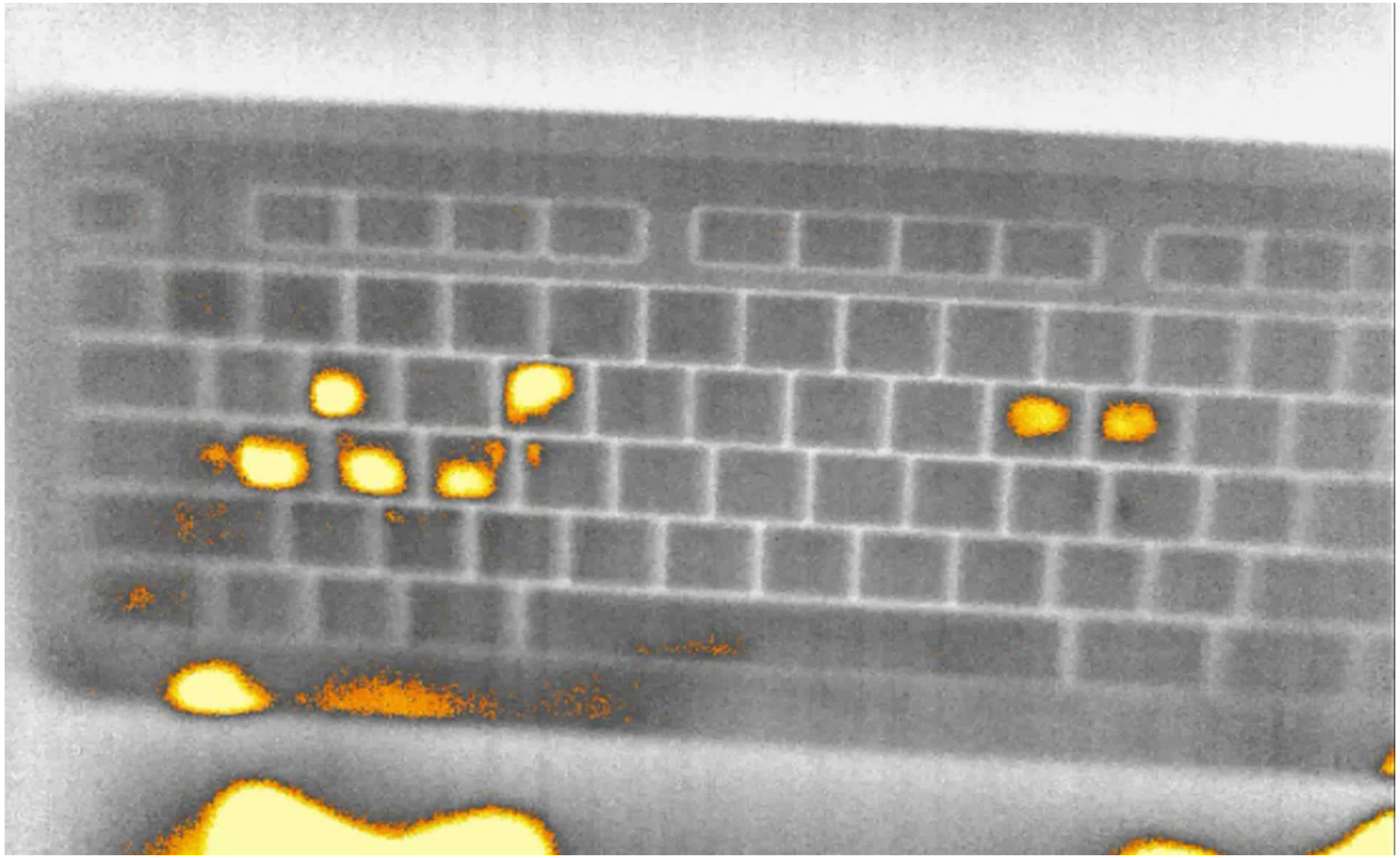
Dell SK-8115

HP SK-2023

Logitech Y-UM76A

AZiO Prism KB507

Sample “Video”



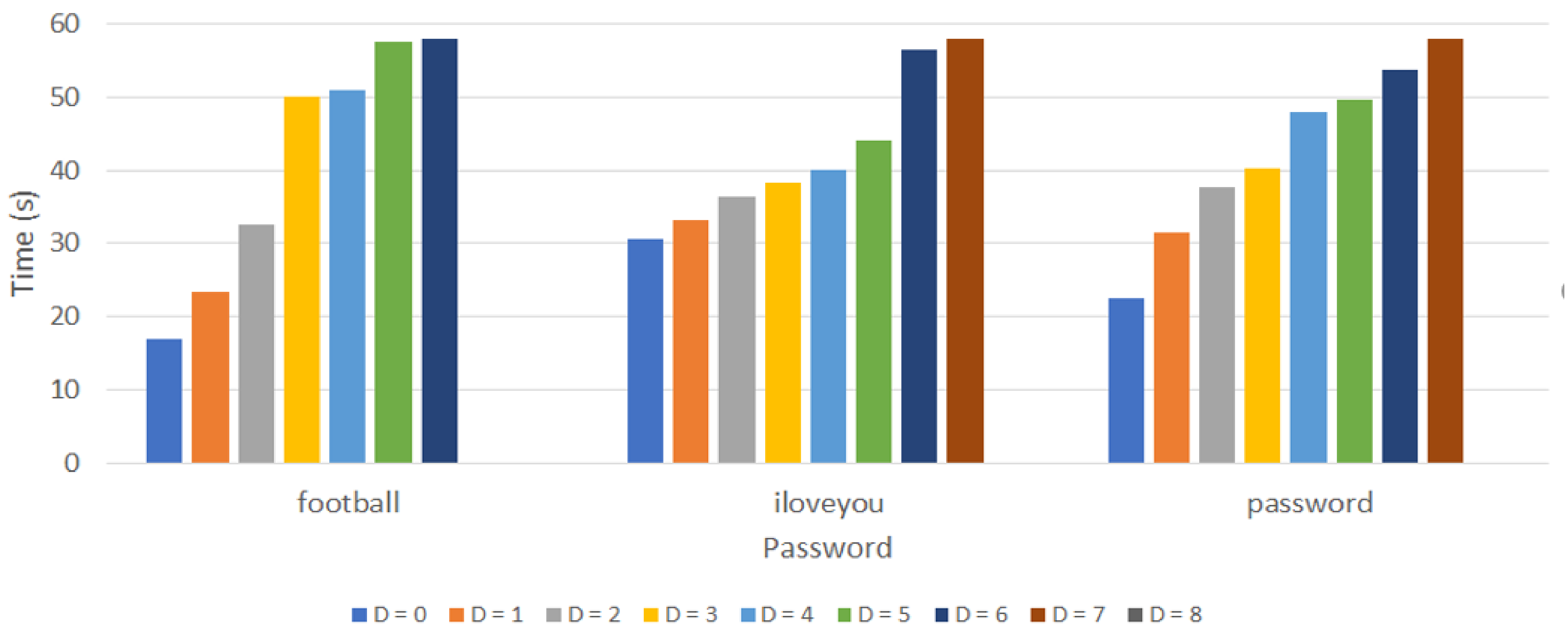
Experiments: STAGE II

- 8 non-expert subjects acted as adversaries

- Each shown 150 thermal recordings in random order

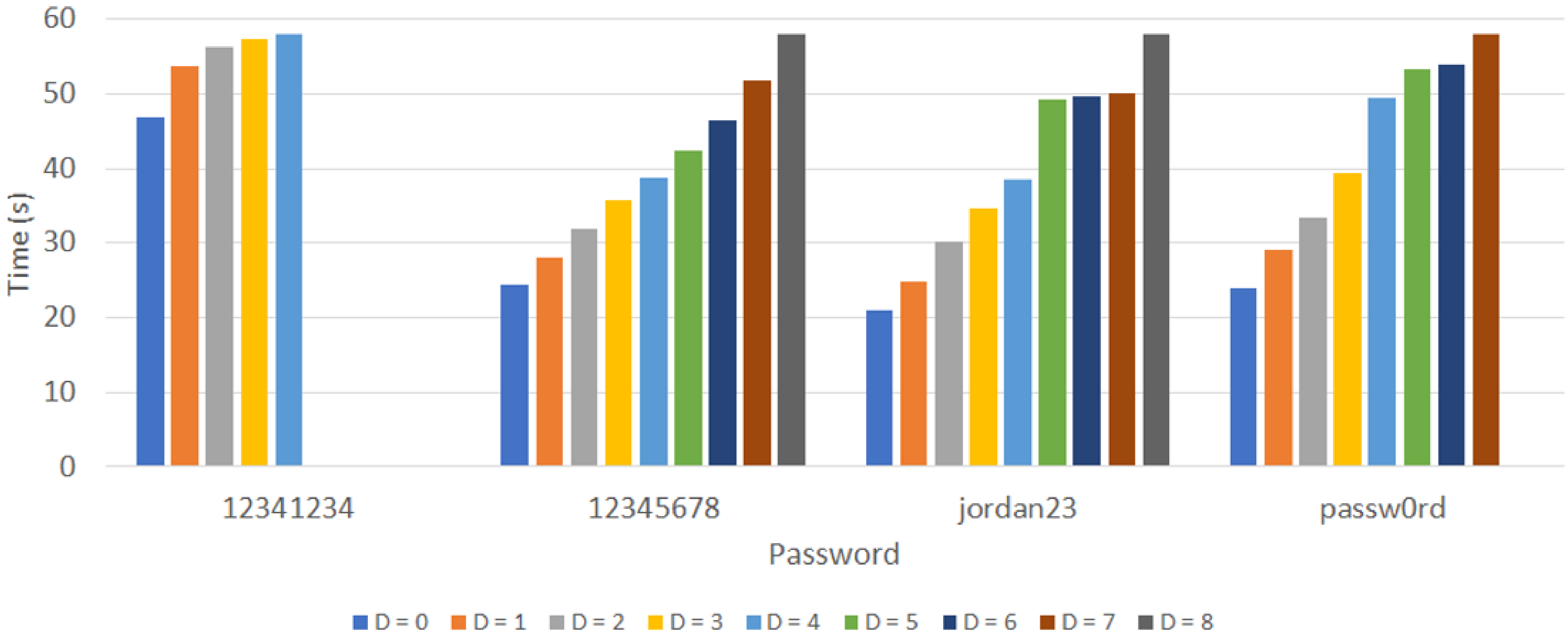
- Asked to identify “lit regions”
    - **NOT** asked to guess passwords

Results - Alphabetical “Insecure” Passwords

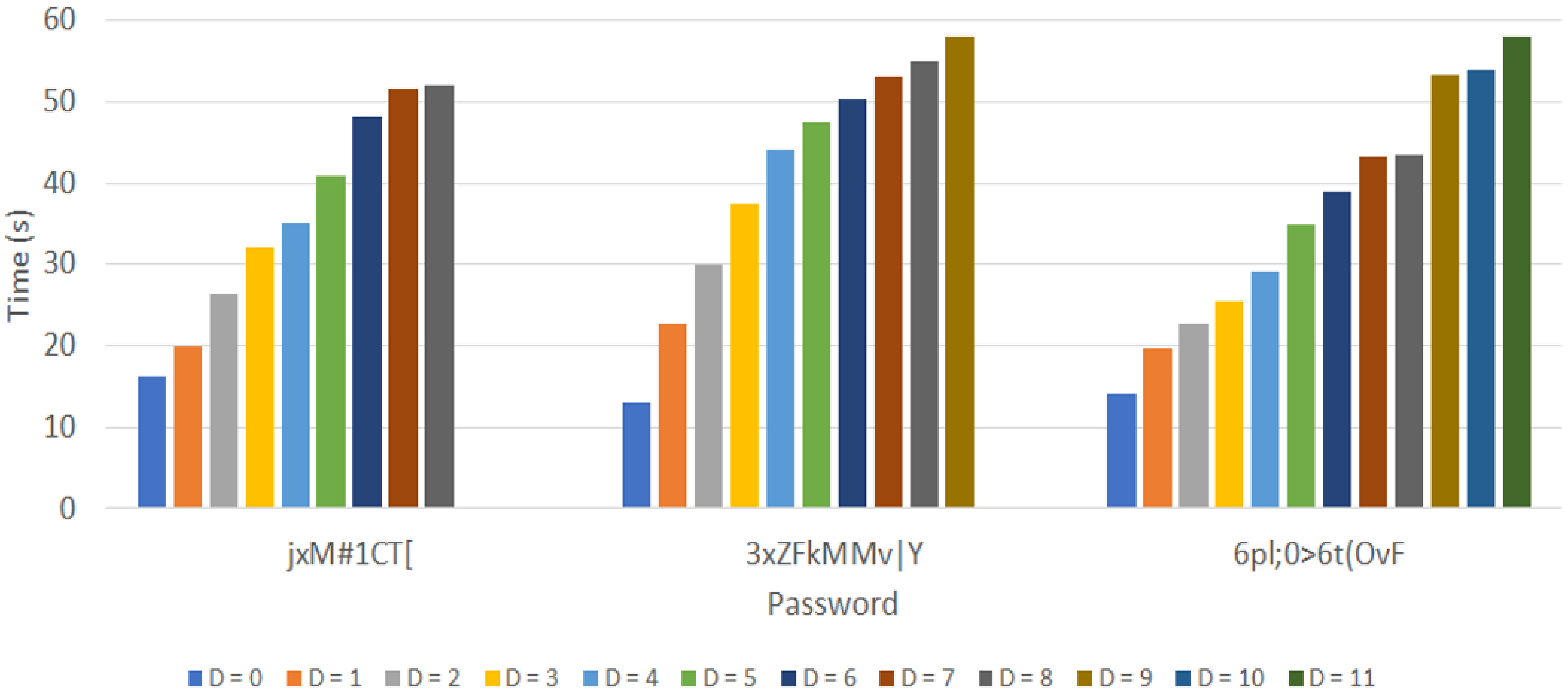


D = Number of missed + mis-identified keys

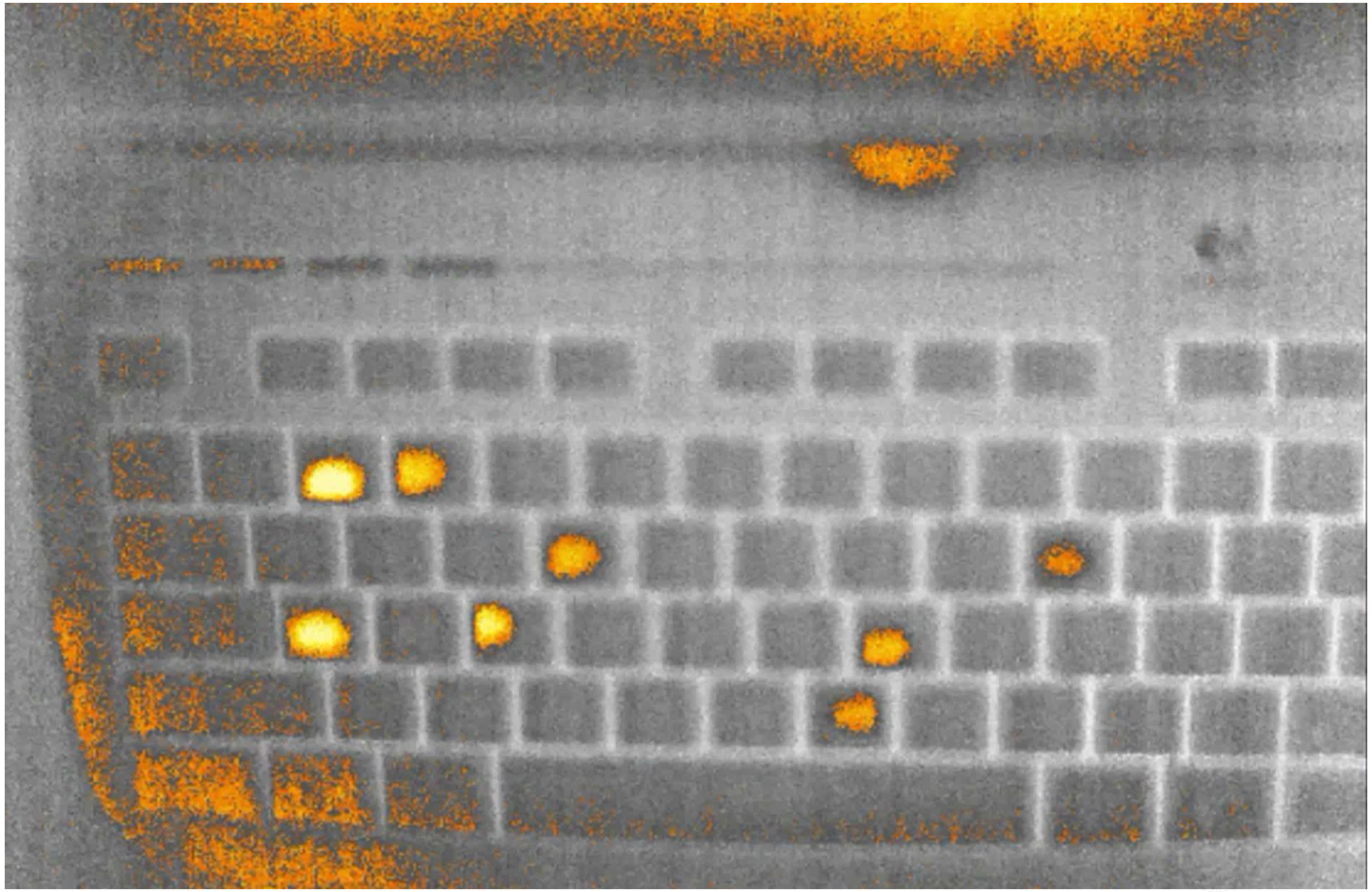
Results - Alphanumeric “Insecure” Passwords



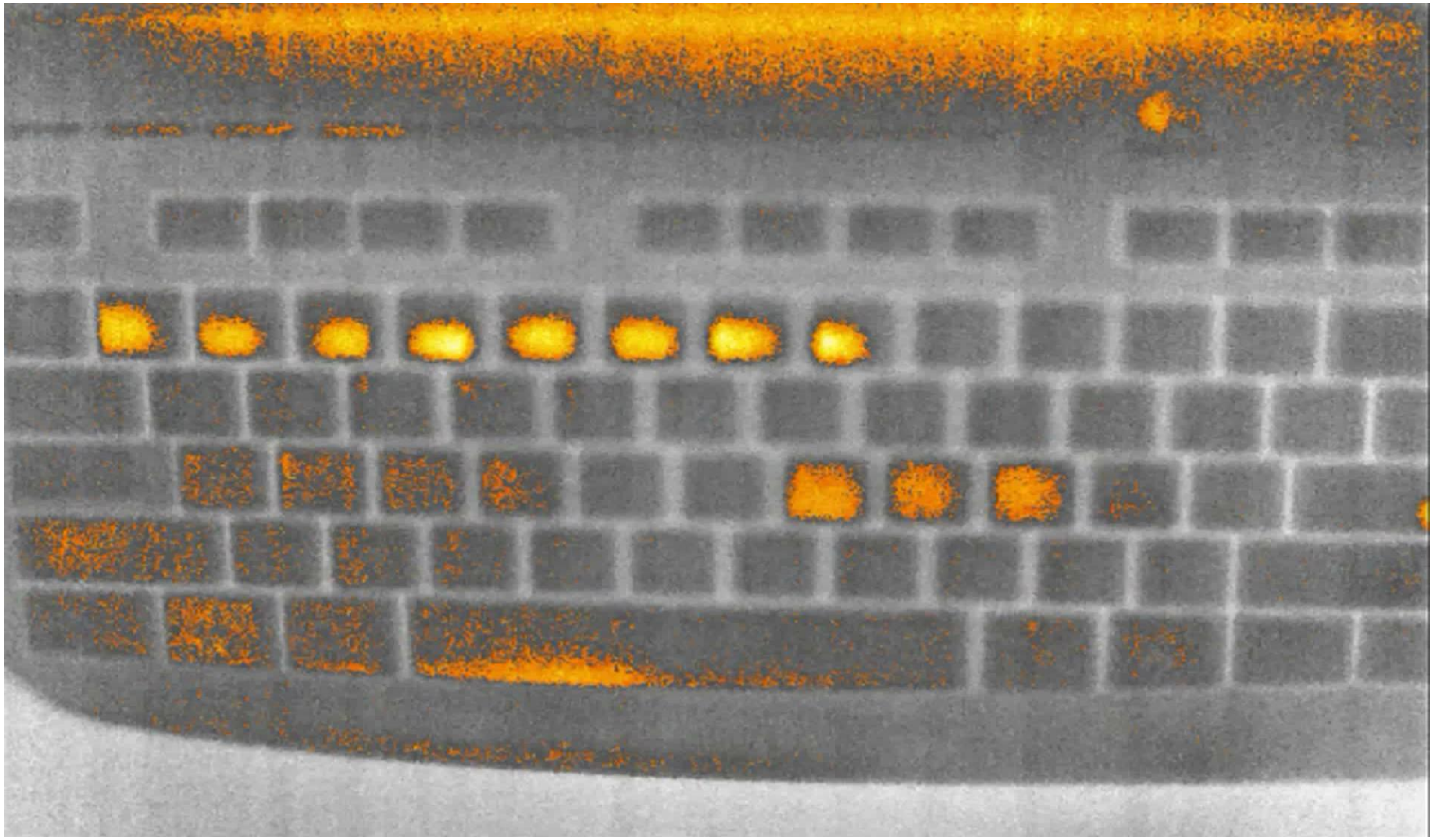
Results - “Secure” Passwords



Hunt-and-Peck Typists

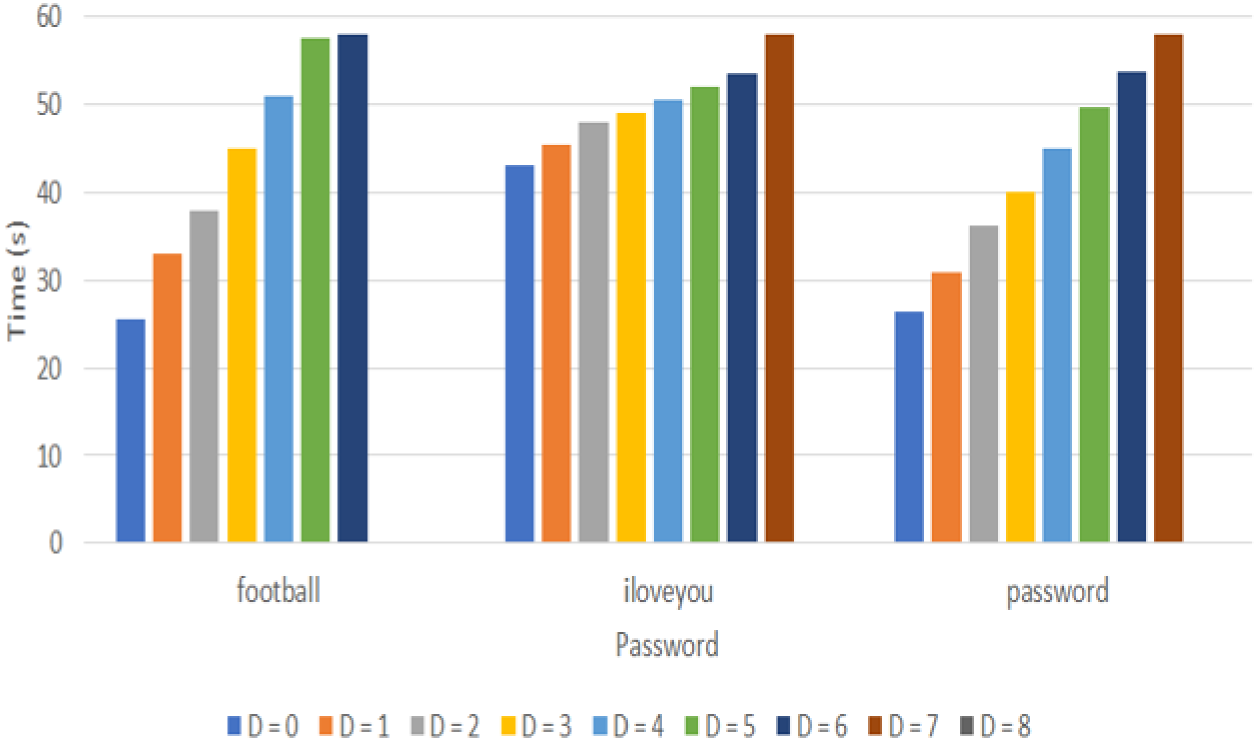


Touch Typists

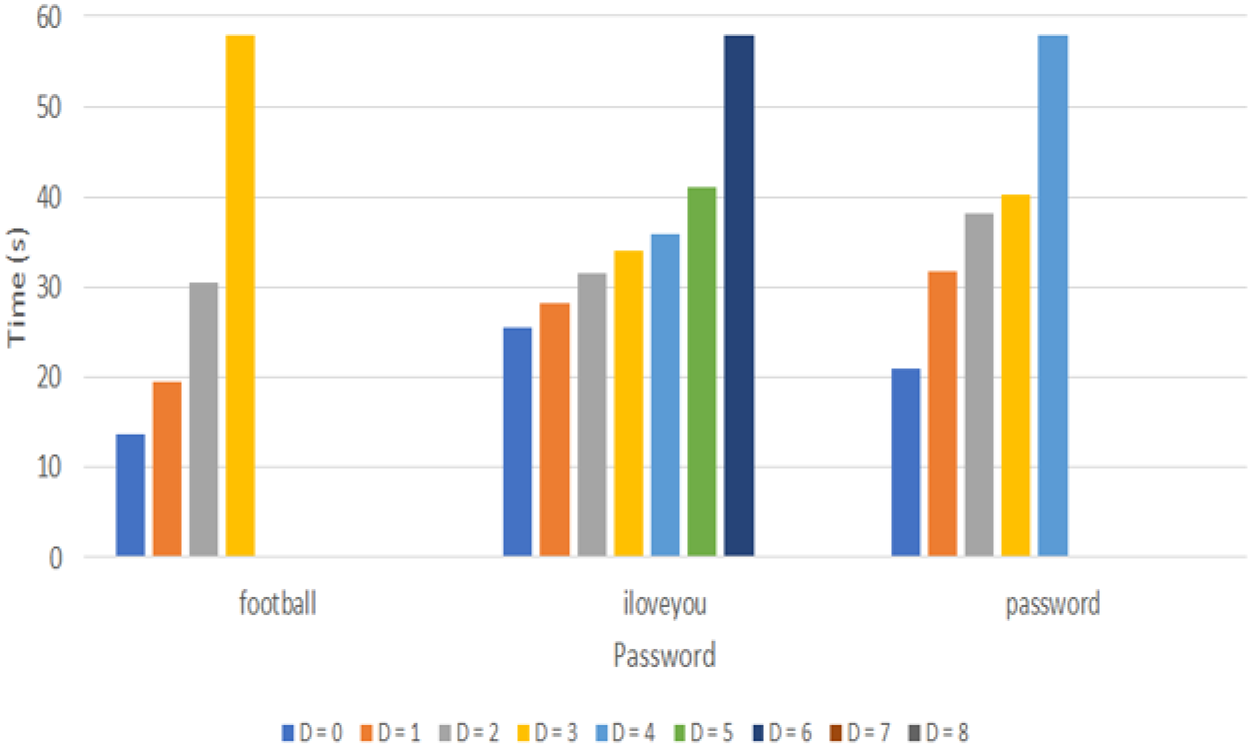


Results – Alphabetical “Insecure” Passwords

Hunt and Peck Typists

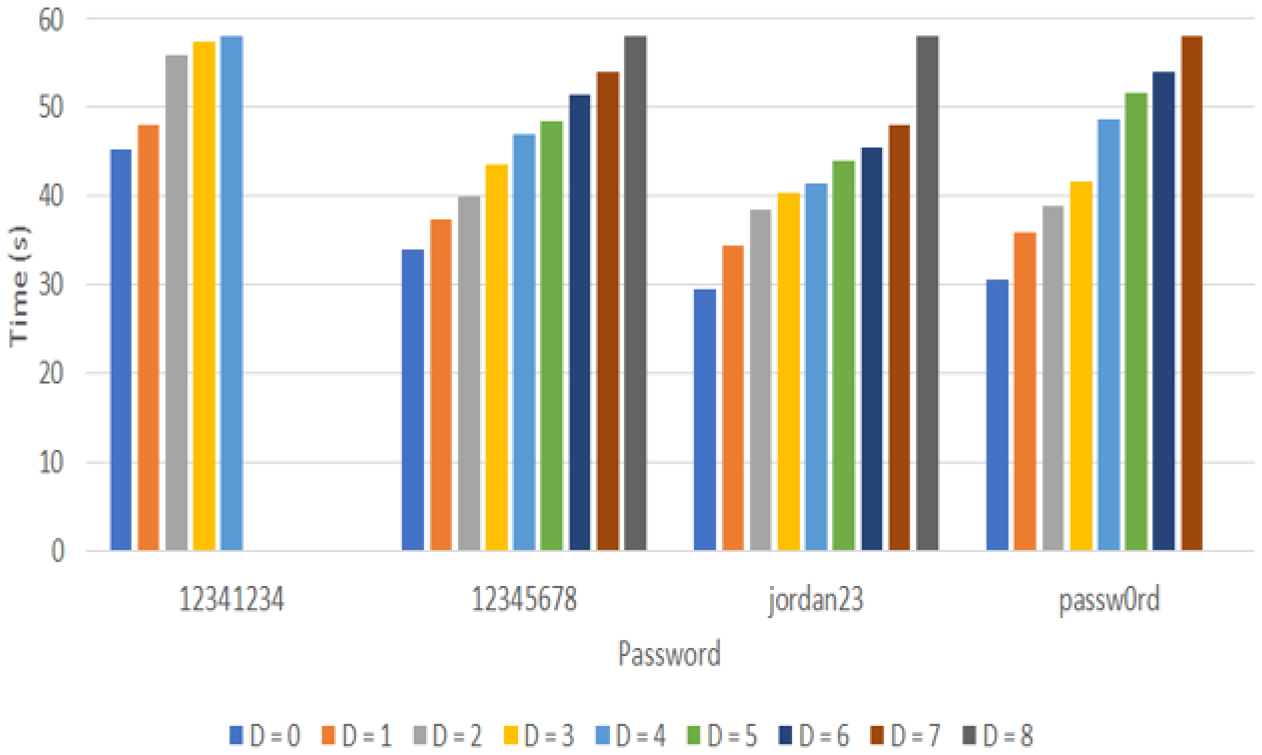


Touch Typists

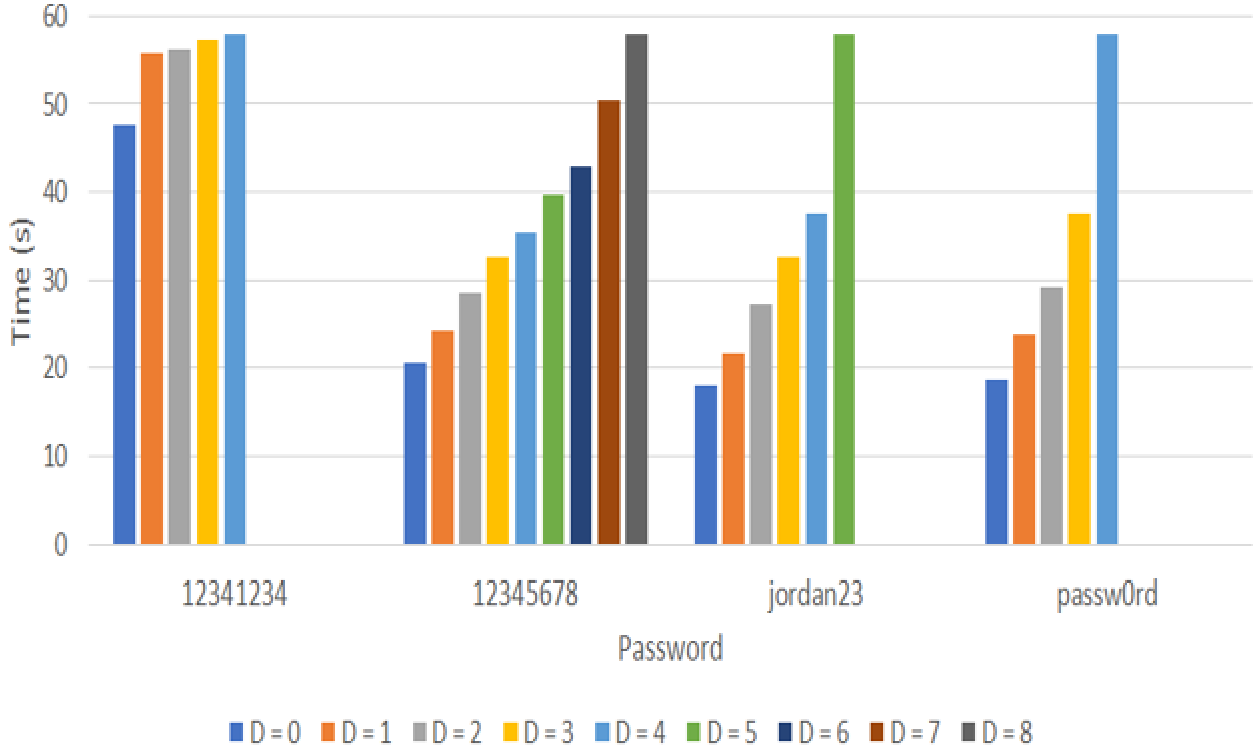


Results – Alphanumeric “Insecure” Passwords

Hunt and Peck Typists

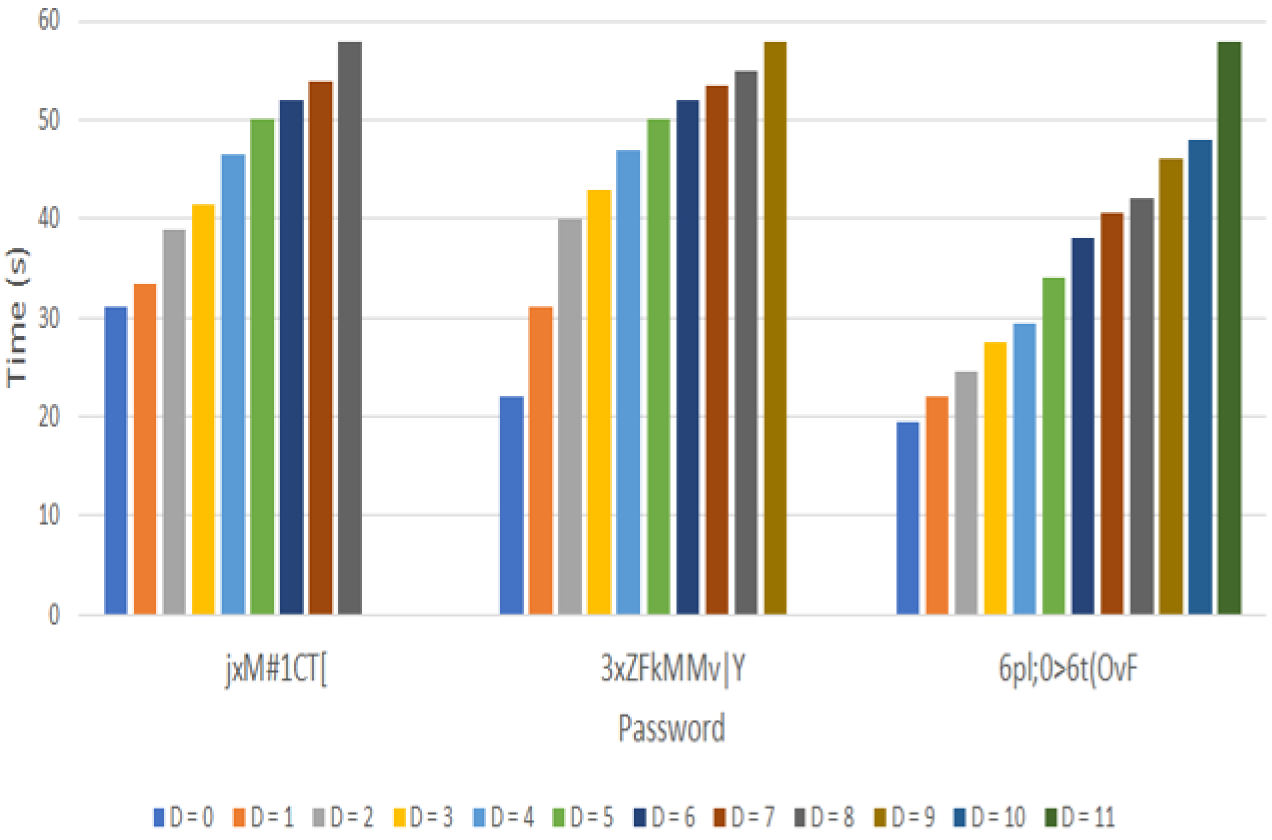


Touch Typists

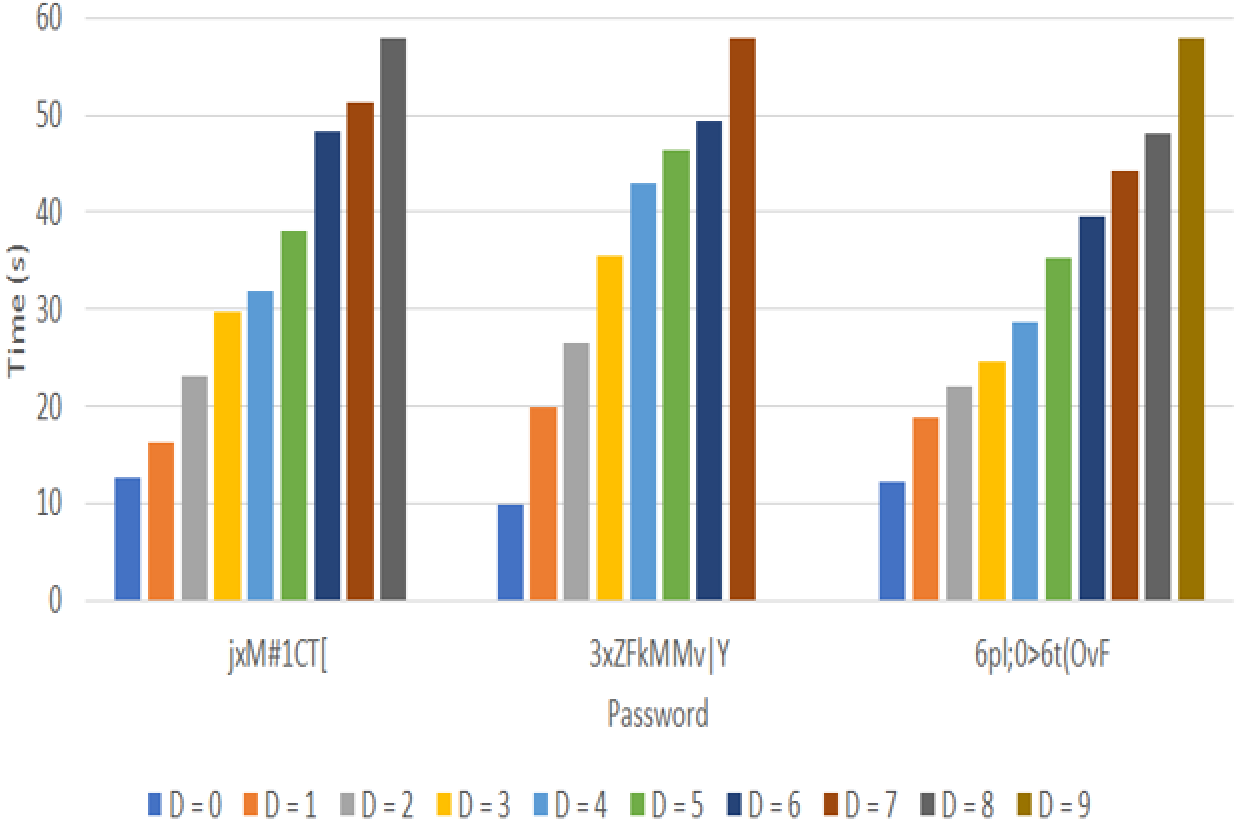


Results – “Secure” Passwords

Hunt and Peck Typists



Touch Typists



Results

Password recovery:

- Entire set of key-presses as late as **30 seconds**
- Partial sets up to **1 minute**

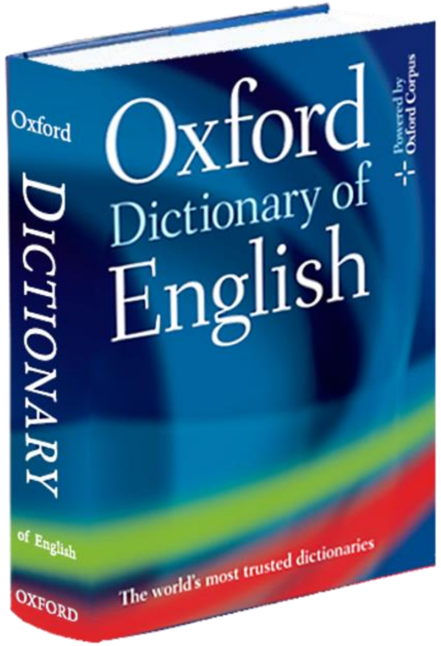
Typing style:

- Hunt-and-peck typists especially vulnerable

Results

Order:

- No reliable key-press ordering information
- Possible reasons: pressure, timing and area differences of fingers/presses
- Good news: We have dictionaries!!!


Oxford Dictionary of English
Oxford
DICTIONARY
of English
OXFORD
The world's most trusted dictionaries
Powered by Oxford Corpus

Mitigation

How to prevent or inhibit Thermanator attacks?

- ◆ Chaff typing (need dedicated on-screen scratchpad)
- ◆ Keyboard-less entry (touchscreen, mouse-based)
- ◆ Move away from passwords altogether
- ◆ Long acrylic nails, gloves or oven mitts ☺

Black Hat Sound Bytes

① Using (plastic) keyboards to enter passwords is even less secure than previously recognized

② Post factum thermal imaging attacks are realistic

③ We should either stop using keyboards for password entry or abandon passwords altogether.

Further Info:

- Website: SPROUT - Security and Privacy Research OUTfit
  sprout.ics.uci.edu/projects/thermanator/

- Full paper available on arxiv
  https://arxiv.org/abs/1806.10189