How Users Enter Generated Passwords on Non-Desktop Devices

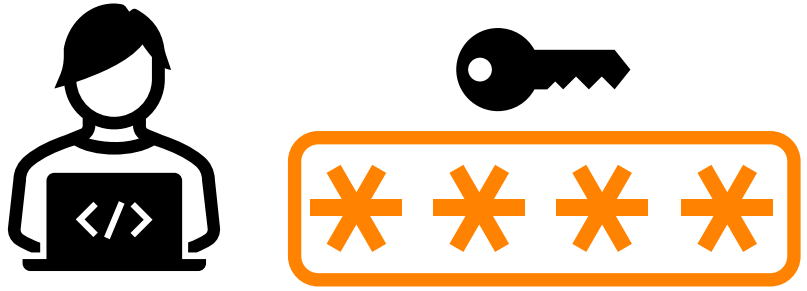
John Sadik, Joshoua Rodriguez,
Hector Santos Villalobos, Scott Ruoti



THE UNIVERSITY OF
TENNESSEE
KNOXVILLE

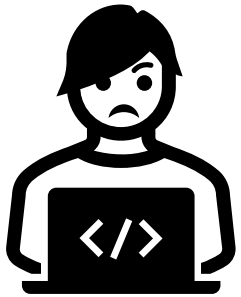
Password Pain Points

- Passwords are ubiquitous and problematic
  - Even with password-less authentication, passwords remain relevant
  - Reuse, user-created passwords are weak, can be forgotten
- Password managers can help with these issues
  - Can create, store, and autofill passwords
  - However, convenience has outweighed security
  - Generated passwords have been left behind



Generated Password Pain Points

- Historically, adoption has been low
  - Prior work suggests reason is manual entry
  - Entering randomly generated passwords can be slow
    - Especially on non-desktop devices

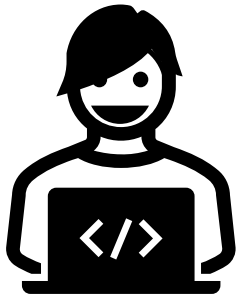




THE UNIVERSITY OF TENNESSEE KNOXVILLE

Generated Password Pain Points

- Historically, adoption has been low
  - Prior work suggests reason is manual entry
  - Entering randomly generated passwords can be slow
    - Especially on non-desktop devices
  - Solution: Improve generated passwords

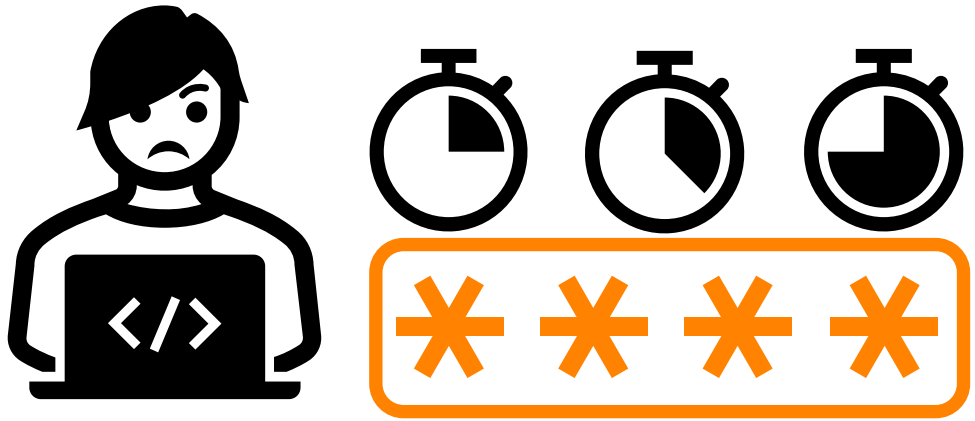




d56g@U2vxZwtnum<he[9

Entry Speed is Key

- Prior work: autofill isn't always available
  - Prior work: users care most about authentication speed
- Therefore, we propose **device-aware password generation**
  - The gap: need data and no publicly available data



Contribution 1

A publicly available dataset of fine-grained password entry events on various devices.

Contribution 1

A publicly available dataset of fine-grained password entry events on various devices.

Contribution 2

Empirical analysis identifying what drives entry time and errors.

Contribution 1

A publicly available dataset of fine-grained password entry events on various devices.

Contribution 2

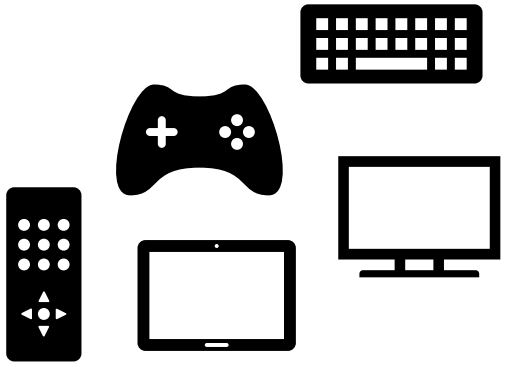
Empirical analysis identifying what drives entry time and errors.

Contribution 3

Two novel device-aware generation algorithms, validated via ML models trained on the dataset.

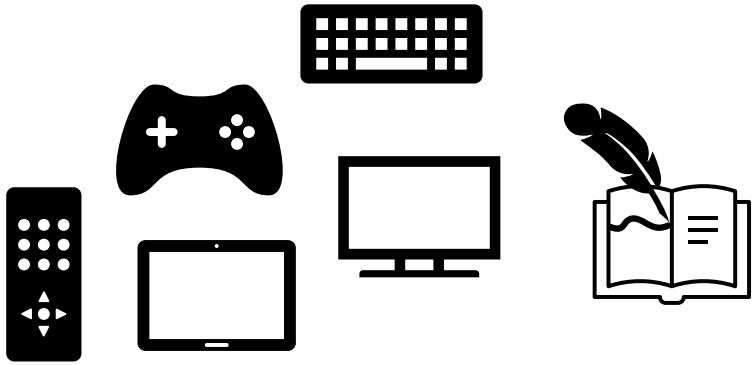
Study Design + Dataset

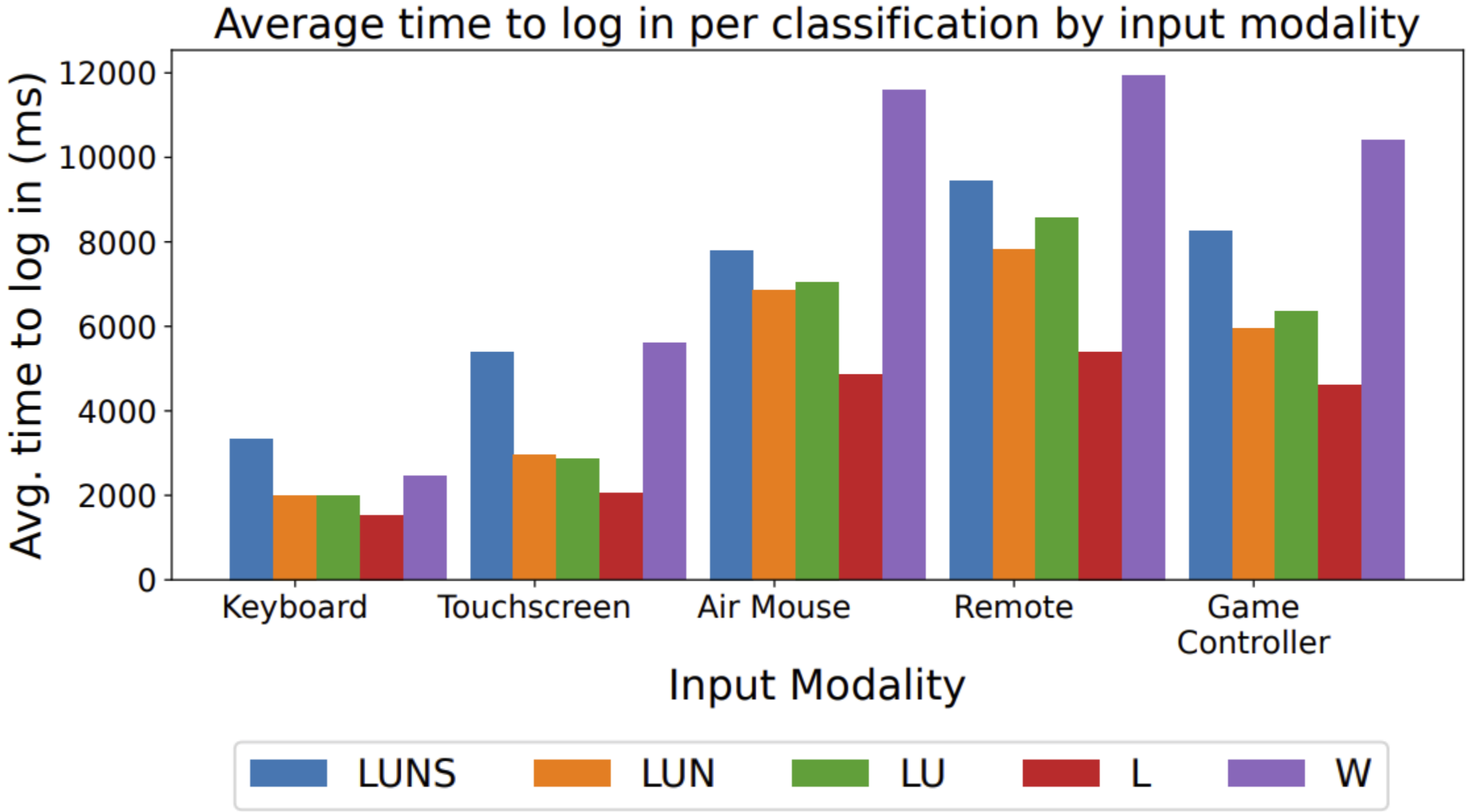
- In-person user study with 5 input modalities and 5 compositions
  - Keyboard, touchscreen, air mouse, TV remote, and game controller
  - L, LU, LUN, LUNS, W (passphrases)
- Collected nearly 5,000 password entries (~80,000 entry events)
  - We record everything the user did, including viewing the password, not just total entry time



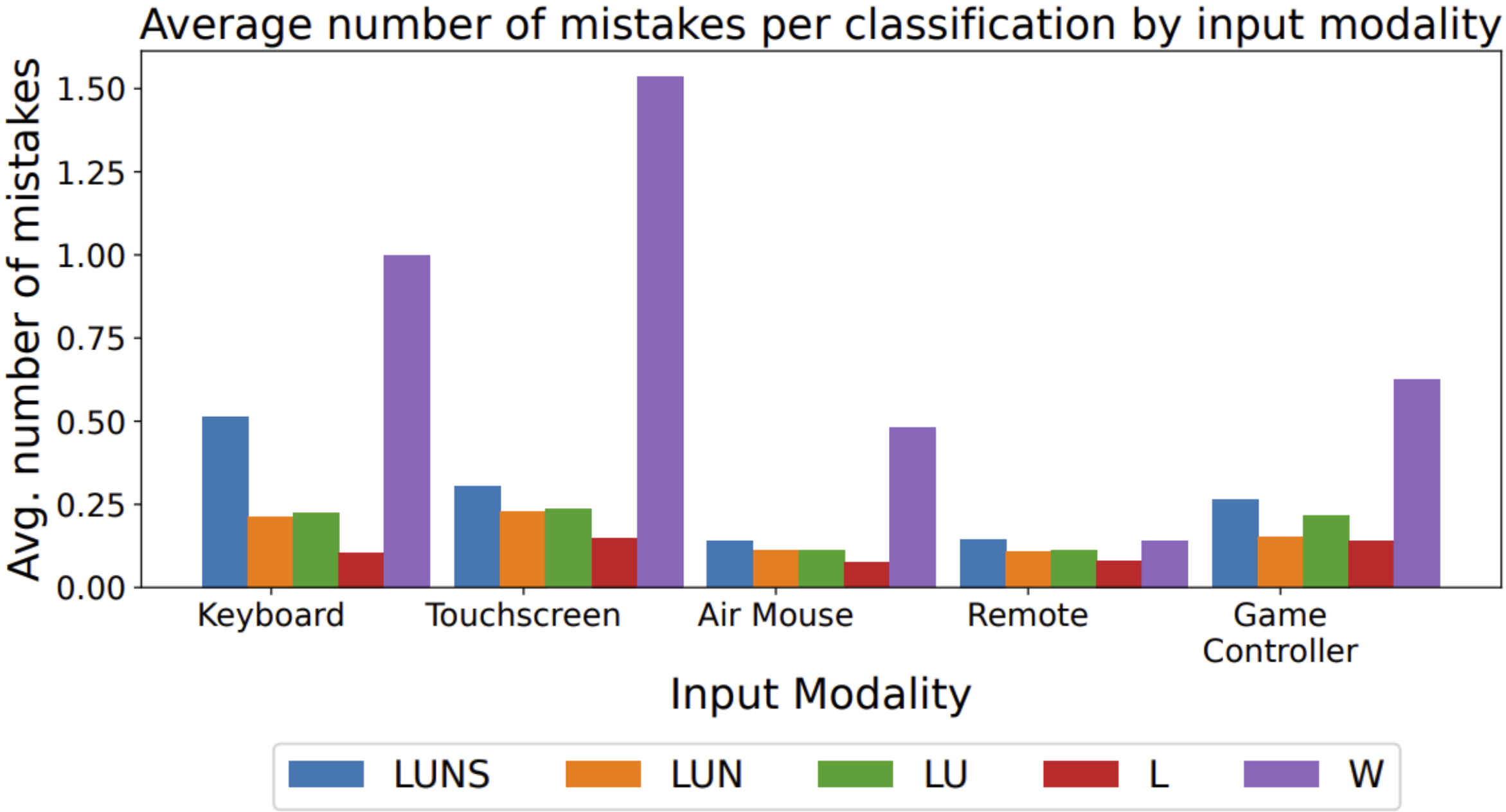
Analysis

- Within-subject (device x composition), between-subject (interface treatments)
- Two laws guide analysis
  - **Fitts' Law:** time to reach a target
  - **Hick's Law:** decision time increases with number/complexity of choices





THE UNIVERSITY OF TENNESSEE KNOXVILLE



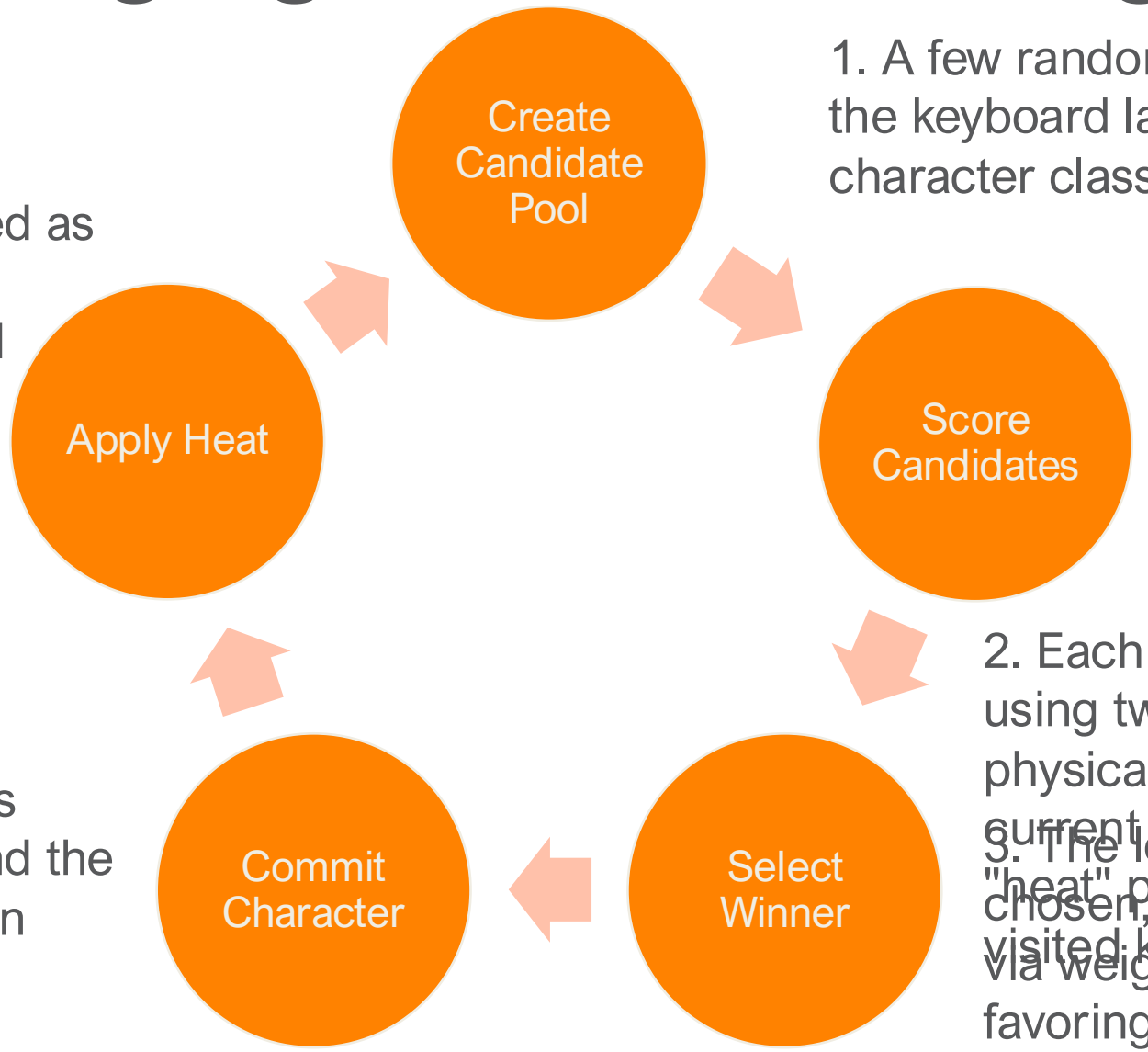
THE UNIVERSITY OF TENNESSEE KNOXVILLE

Predicted time (seconds) to enter passwords of the same security strength

Input Modality	LUNS (10 chars)	LUN (11 chars)	LU (12 chars)	L (14 chars)	W (6 words)
Keyboard	3.35	2.41	2.38	2.29	4.91
Touchscreen	5.39	3.54	3.44	3.06	11.21
Gamepad	8.25	7.14	7.62	6.90	20.80
Air-mouse	7.80	8.22	8.47	7.29	23.19
Remote	9.44	9.37	10.28	8.11	23.88

THE UNIVERSITY OF TENNESSEE KNOXVILLE

Physics “Foraging” Generation Algorithm



1. A few random keys are picked from the keyboard layout for the current character classes needed

2. Each candidate is scored using two combined factors: physical distance from the current cursor position, and a "heat" penalty for recently visited keys.

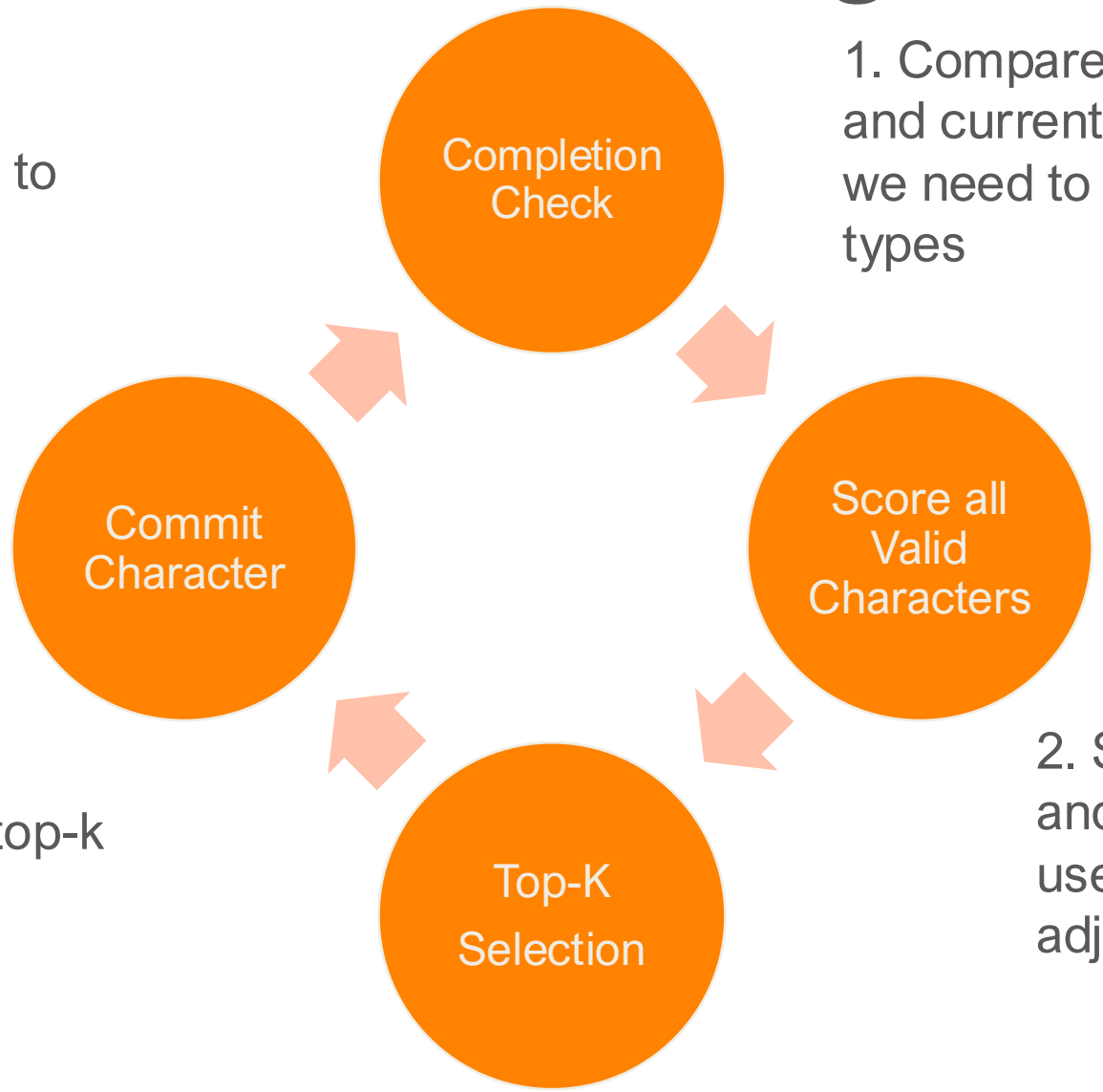
3. The lowest-cost candidate is chosen, with classes competing via weighted random selection favoring cheaper moves

4. The winning character is added to the password, and the cursor moves to its position

5. The chosen key and its neighboring keys are marked as "hot," making them less attractive for the next round

Kinetic Chain Generation Algorithm

1. Compare required character classes and current password to see how much we need to coerce certain character types



2. Score based on their distance and time cost, if it was recently used, and required classes adjustment

3. Select winner based on top-k sampling

4. Commit chosen character to password

Algorithm	Mean (Median) Time (s)	Improvement
Baseline (Random LUNS)	31.71 (34.90)	-
Physics-Constrained	22.97 (27.42)	27.56%
Kinetic Chain	21.79 (26.03)	31.28%

A Path Forward

- With a dataset in hand, we can now build and quickly test new password generation algorithms
  - Less-promising candidates can be identified early before committing time and money
- We hope the community will continue working on improving generated passwords and welcome any collaboration in this area

Contact: John Sadik (JohnS@utk.edu)

Dataset: zenodo.org/records/18711498

THE UNIVERSITY OF TENNESSEE KNOXVILLE