DualStrike: Accurate, Real-time *Eavesdropping* and *Injection* of Keystrokes on Commodity Keyboards

Xiaomeng Chen†, Jike Wang†, Zhenyu Chen†, Qi Alfred Chen‡, Xinbing Wang†, Dongyao Chen†

†Shanghai Jiao Tong University, China

‡University of California, Irvine, USA

NDSS SYMPOSIUM/2026

Xiaomeng Chen

M.S student

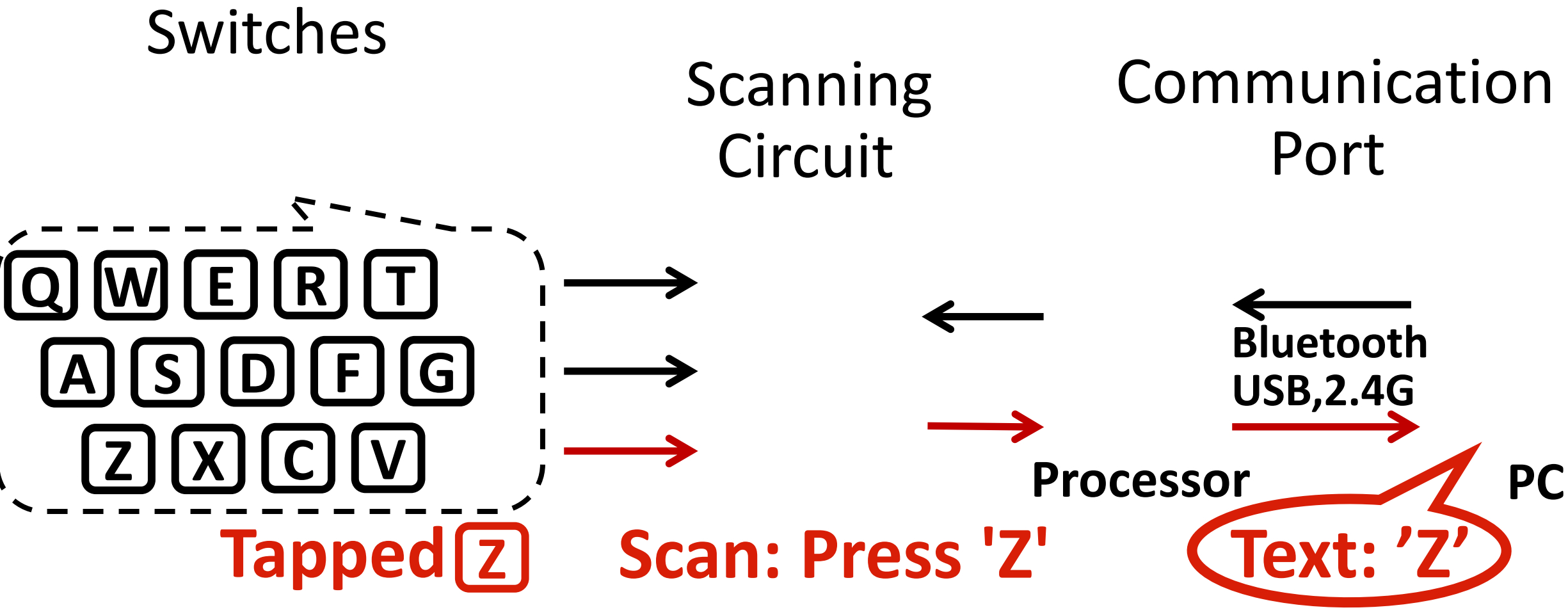
Shanghai Jiao Tong University, China

sjtu_chenxm@sjtu.edu.cn

A System builder,

Passionate in designing effective, efficient, and reliable human-machine collaborative systems.

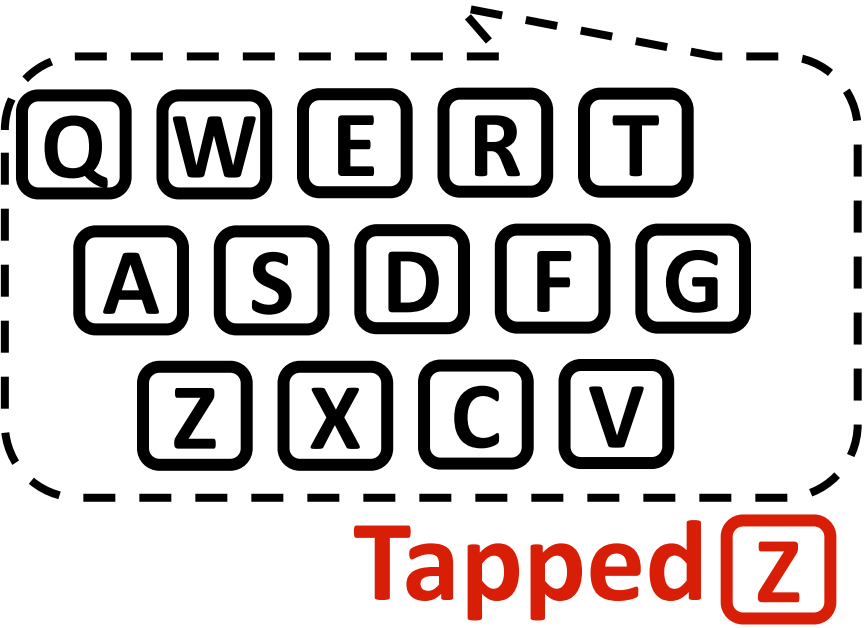
An Overview of Keyboard: Workflow



An Overview of Keyboard: Different Types

- Keyboards come in various types: Mechanical, Hall-Effect, Optical, and more.

Switches



Difference:

Keystroke sensing mechanism

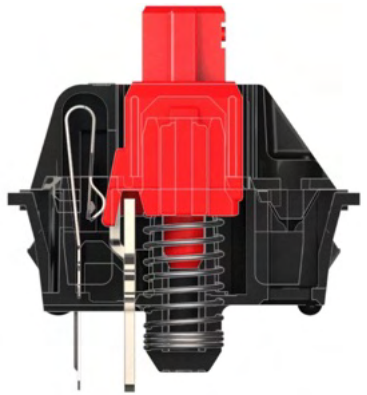
How is Z sensed?

Mechanical Keyboard vs *Hall-effect Keyboard*

Mechanical Switch

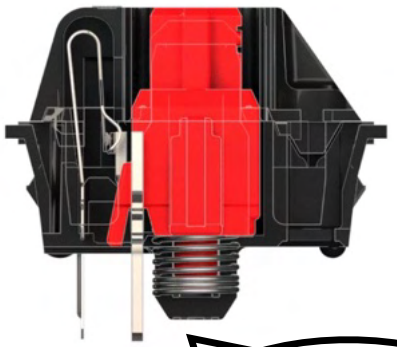
- Contacted-based
- Need fully pressed

Before pressing



Credit: https://www.keymouse.com/cherry-mx-switches

After pressing

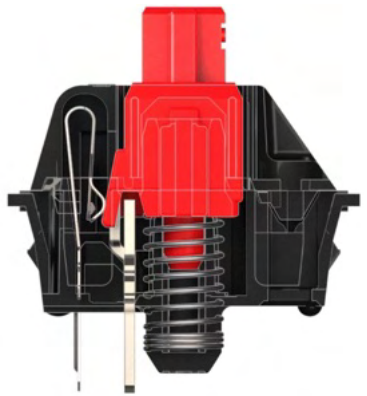


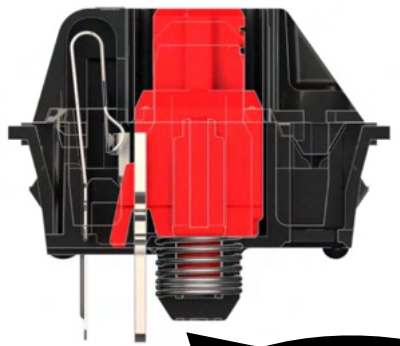
Mechanical Keyboard vs *Hall-effect Keyboard*

Mechanical Switch

- Contacted-based
- Need fully pressed

Before pressing After pressing



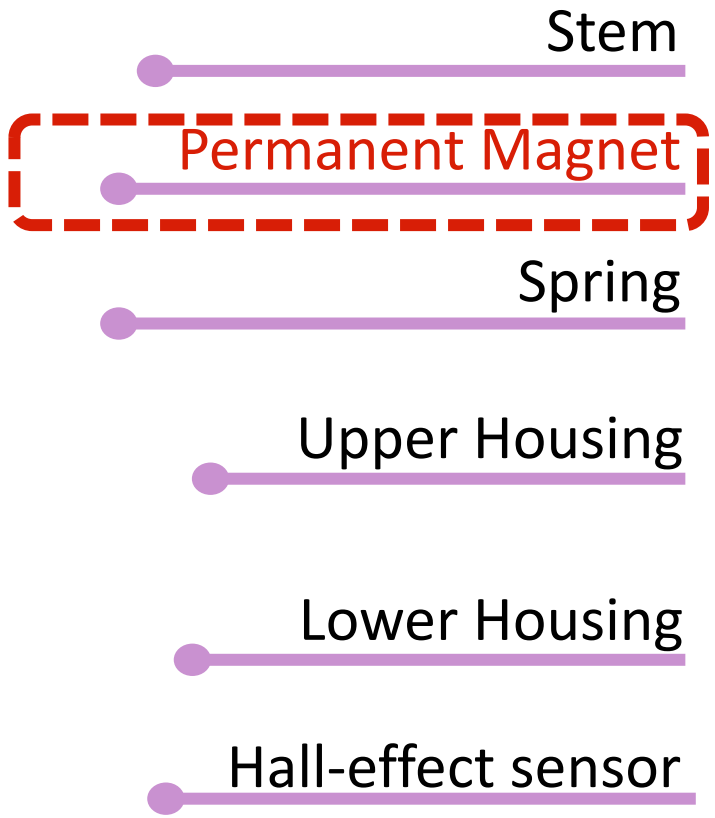


Credit: https://www.keymouse.com/cherry-mx-switches

Keystroke detected!

Hall-effect Switch

- Keystroke detection via Hall Effect



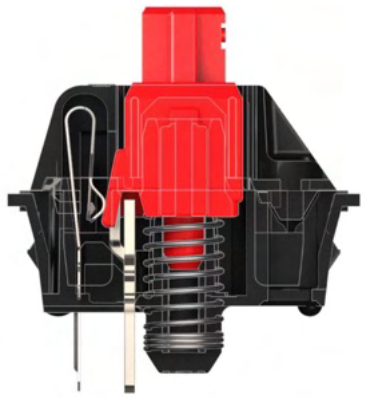
Credit: https://www.gateron.com/products/gateron-magic-jade-switch?VariantsId=11143

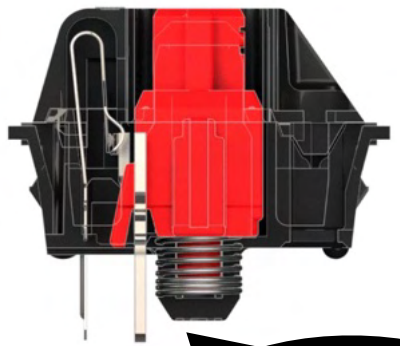
Mechanical Keyboard vs *Hall-effect Keyboard*

Mechanical Switch

- Contacted-based
- Need fully pressed

Before pressing After pressing





Credit: https://www.keymouse.com/cherry-mx-switches

Keystroke detected!

Hall-effect Switch

- Keystroke detection via Hall Effect

Permanent magnet

magnetic field

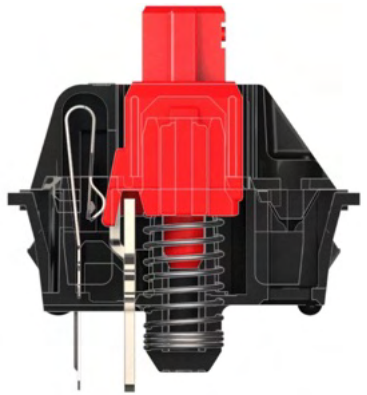
Credit: https://www.gateron.com/products/gateron-magic-jade-switch?VariantsId=11143

Mechanical Keyboard vs *Hall-effect Keyboard*

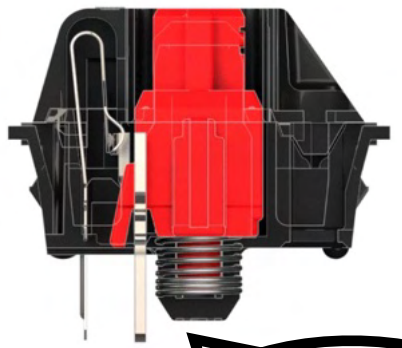
Mechanical Switch

- Contacted-based
- Need fully pressed

Before pressing



After pressing



Keystroke detected!

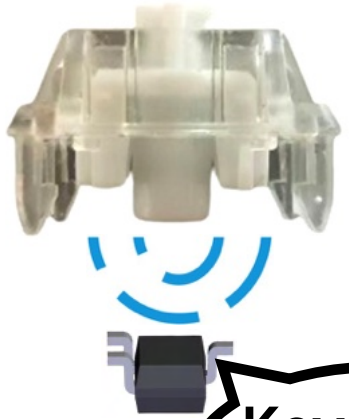
Credit: https://www.keymouse.com/cherry-mx-switches

Hall-effect Switch

- Contactless
- Press distance is adjustable

Before pressing

After pressing



Keystroke detected!

Credit: https://www.gateron.com/products/gateron-magic-jade-switch?VariantsId=11143

Hall-effect Keyboard Advantages

- **Customizable key travel**: e.g., SteelSeries Apex Pro Hall-effect keyboard key travel between 0.1 mm and 4 mm, granularity of 0.1 mm
- **Quicker response time:** favorable in high-performance applications
- **Longer lifespan**: Contactless -> more than **100 million** clicks

Credit: https://www.vecteezy.com/free-photos/individuals-pc-setup?page=3

Everyday Keyboard Users

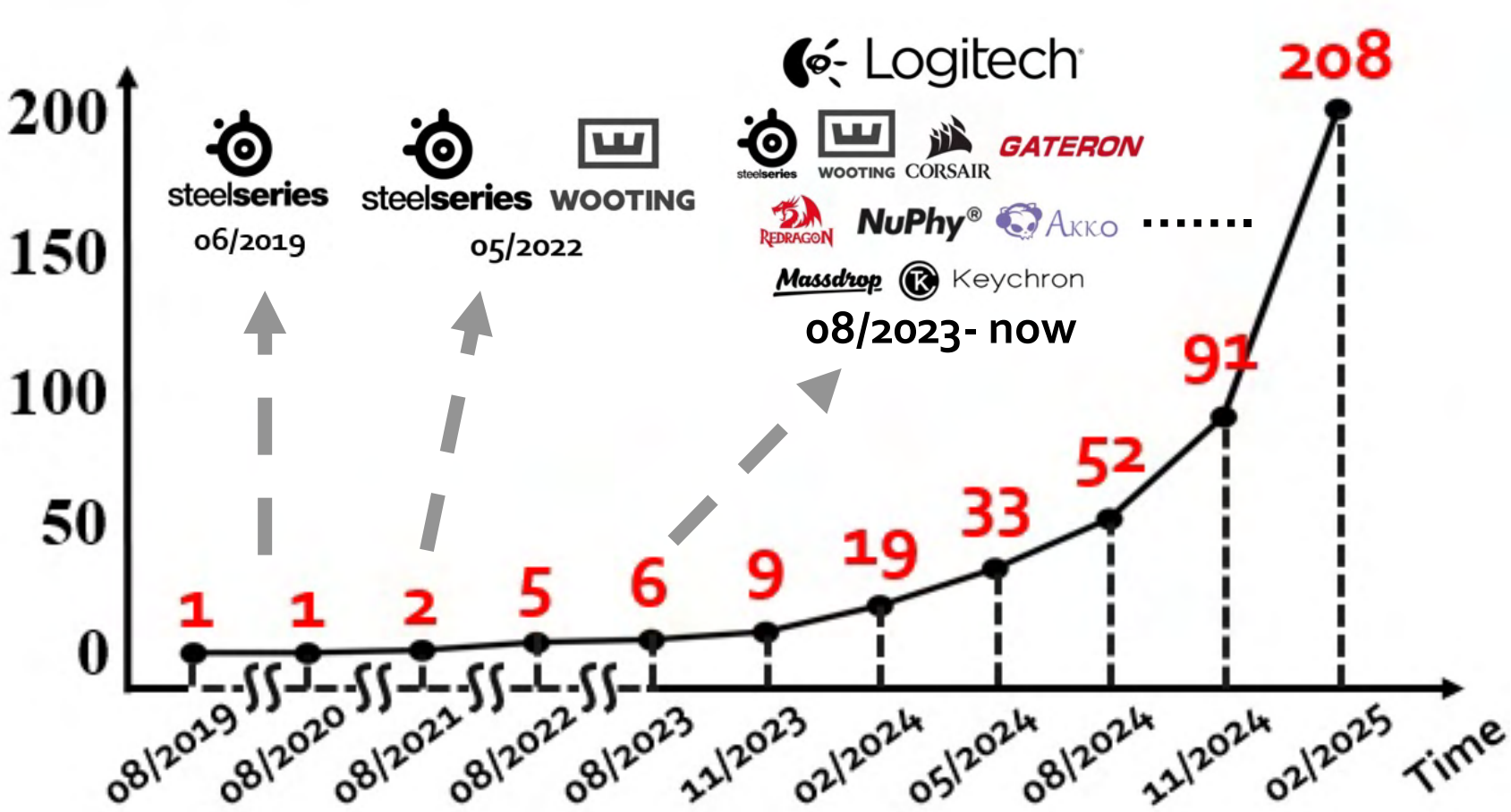
Credit: https://www.akiani.fr/en/realisations/improving-the-performance-of-esport-players/

Esports Players

Fast-emerging Hall-effect keyboard

- Hall-effect keyboard models recorded an average growth rate of **82.60% every three months.**
- Hall-effect keyboard market size exhibits a **CAGR of 18.7% since 2024.**

Num. of Hall-effect keyboard models

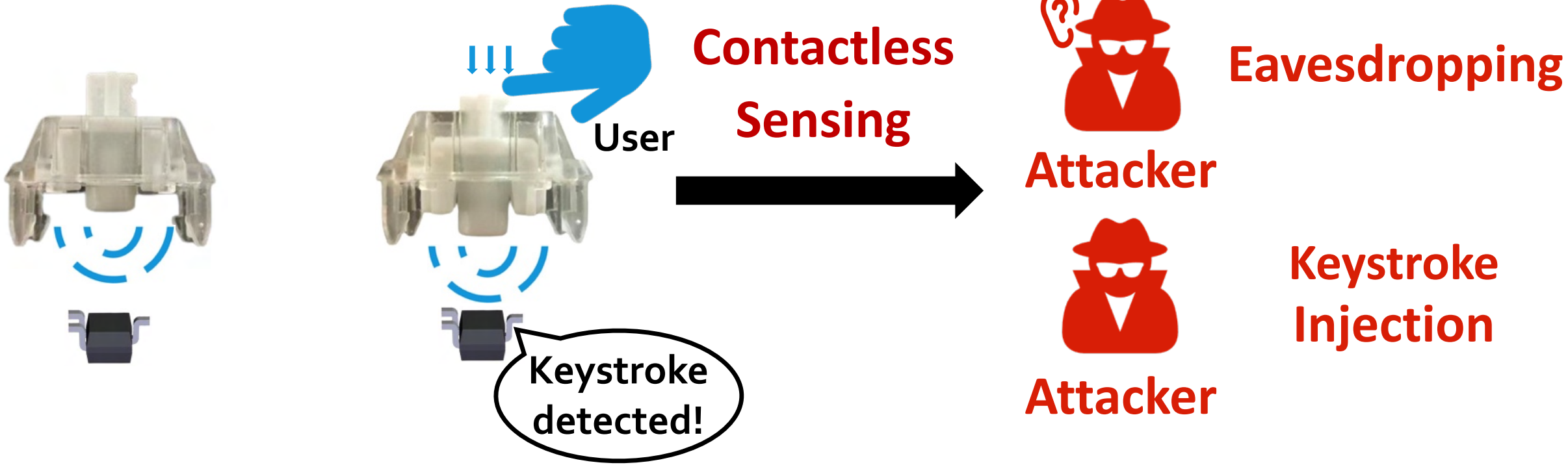


However, are Hall-effect keyboards truly trustworthy?

Vulnerability of Hall-effect Switches

During Normal Use

Before pressing After pressing

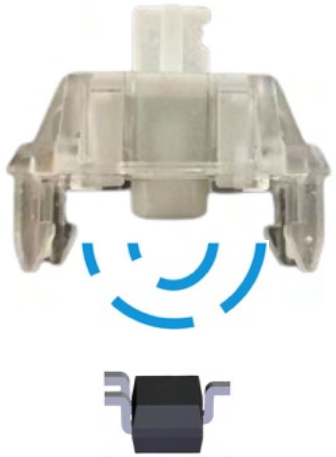


Vulnerability of Hall-effect Switches

- Magnetic field changes from keystrokes can leak as side-channel information, enabling keystroke monitoring.

During Normal Use

Before pressing

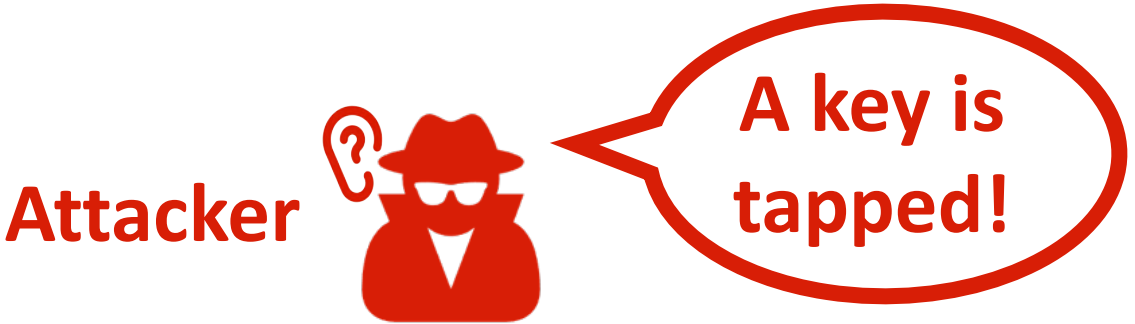


After pressing

User

Attacker Eavesdropping

User

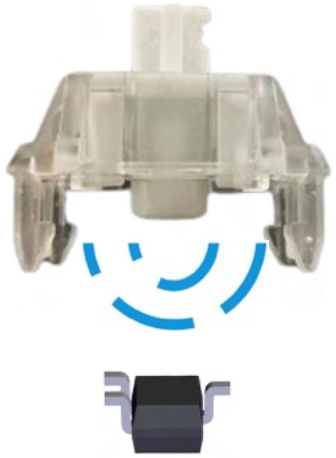


Vulnerability of Hall-effect Switches

- Similarly, external magnetic fields can mimic these variations, enabling keystroke injection.

During Normal Use

Before pressing

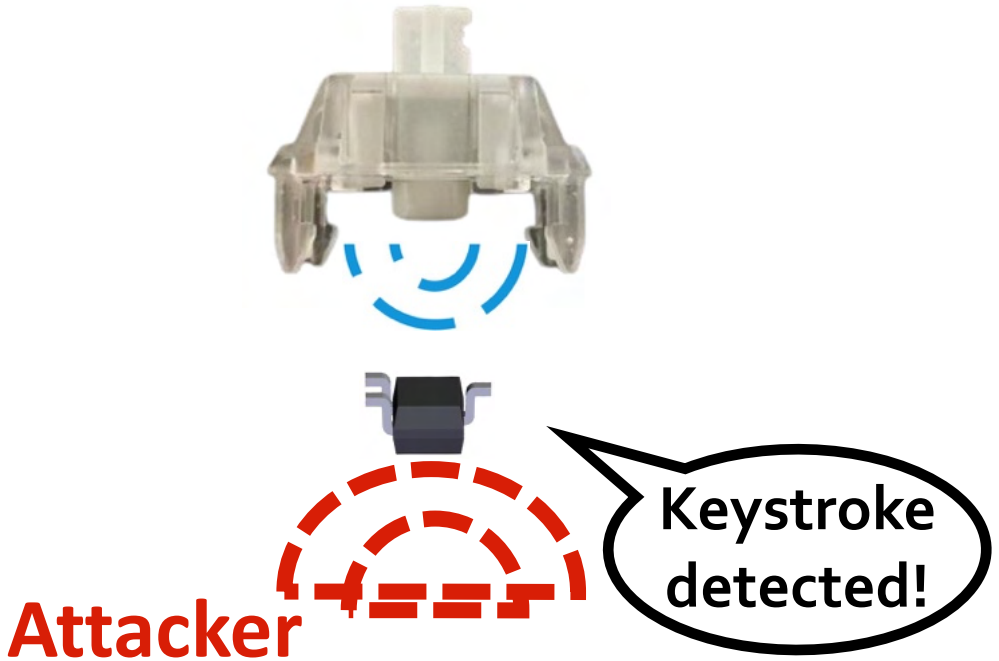


After pressing

User

Attacker Injecting Keystrokes

User not tapping



What attacks could these Hall-effect vulnerabilities enable?

Existing Keyboard Attacks

Only Eavesdropping

- Leveraging side-channel signals of keyboards to infer current keystrokes.

visual

acoustic

Existing Keyboard Attacks

Only Eavesdropping

- Leveraging side-channel signals of keyboards to infer current keystrokes.

visual

acoustic

Only Keystroke Injection

- BadUSB attack.

Credit: https://www.youtube.com/watch?v=1ZW-tZLm0jE

Now protected

- Authentication
- Windows + Kaspersky

Existing Keyboard Attacks

Only Eavesdropping

- Leveraging side-channel signals of keyboards to infer current keystrokes.

visual

acoustic

electromagnetic

Only Keystroke injection

- **GhostType**[1] enables contactless keystroke injection via electromagnetic interference **(EMI).**

However, GhostType:

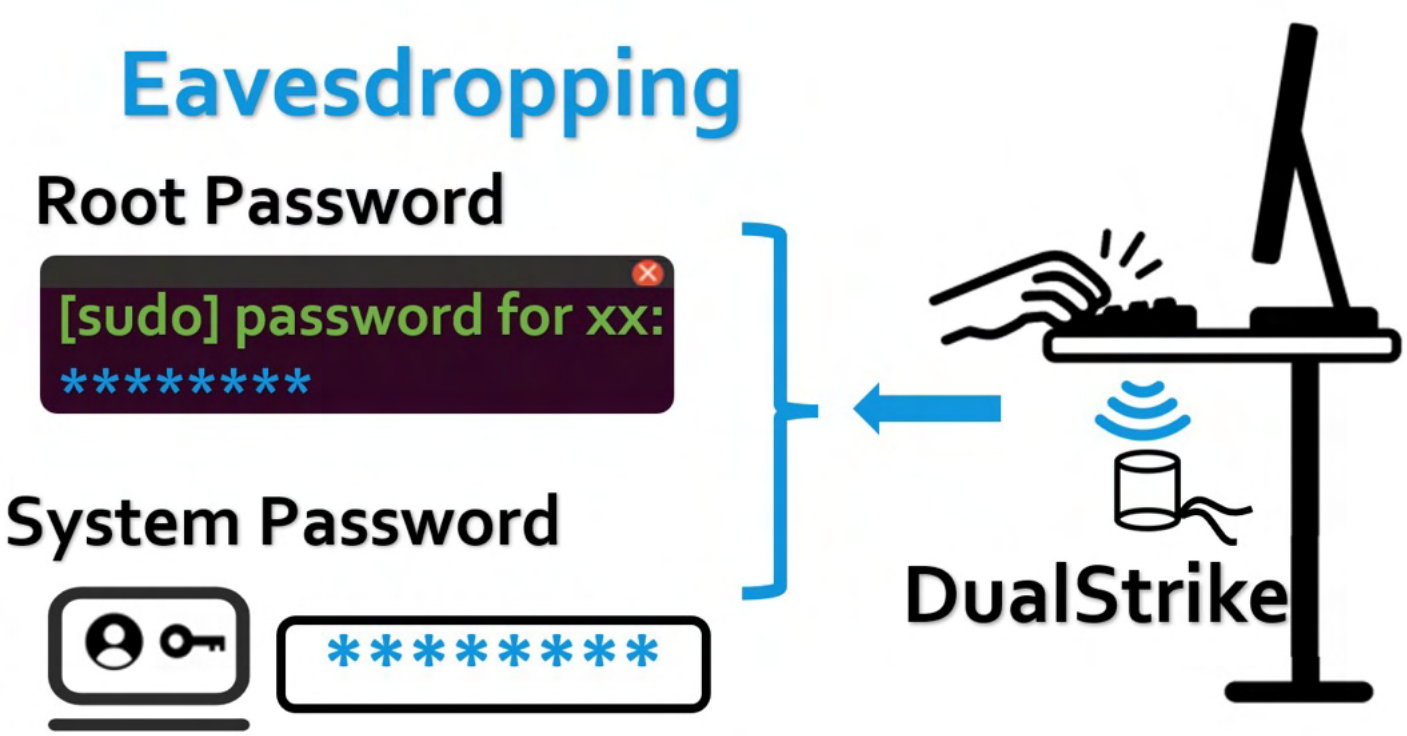
- Need EMI generation devices: signal generator, amplifier, etc.
- **Cannot achieve per-key injection**

A Practical Attack on Keyboard Should Be

- ❑ Achieve both Eavesdropping and Keystroke injection
  - ↓ Real-time eavesdropping
  - ↓ Non-invasive, per-key injection
- ❑ Robust against practical disturbances, e.g. displacement

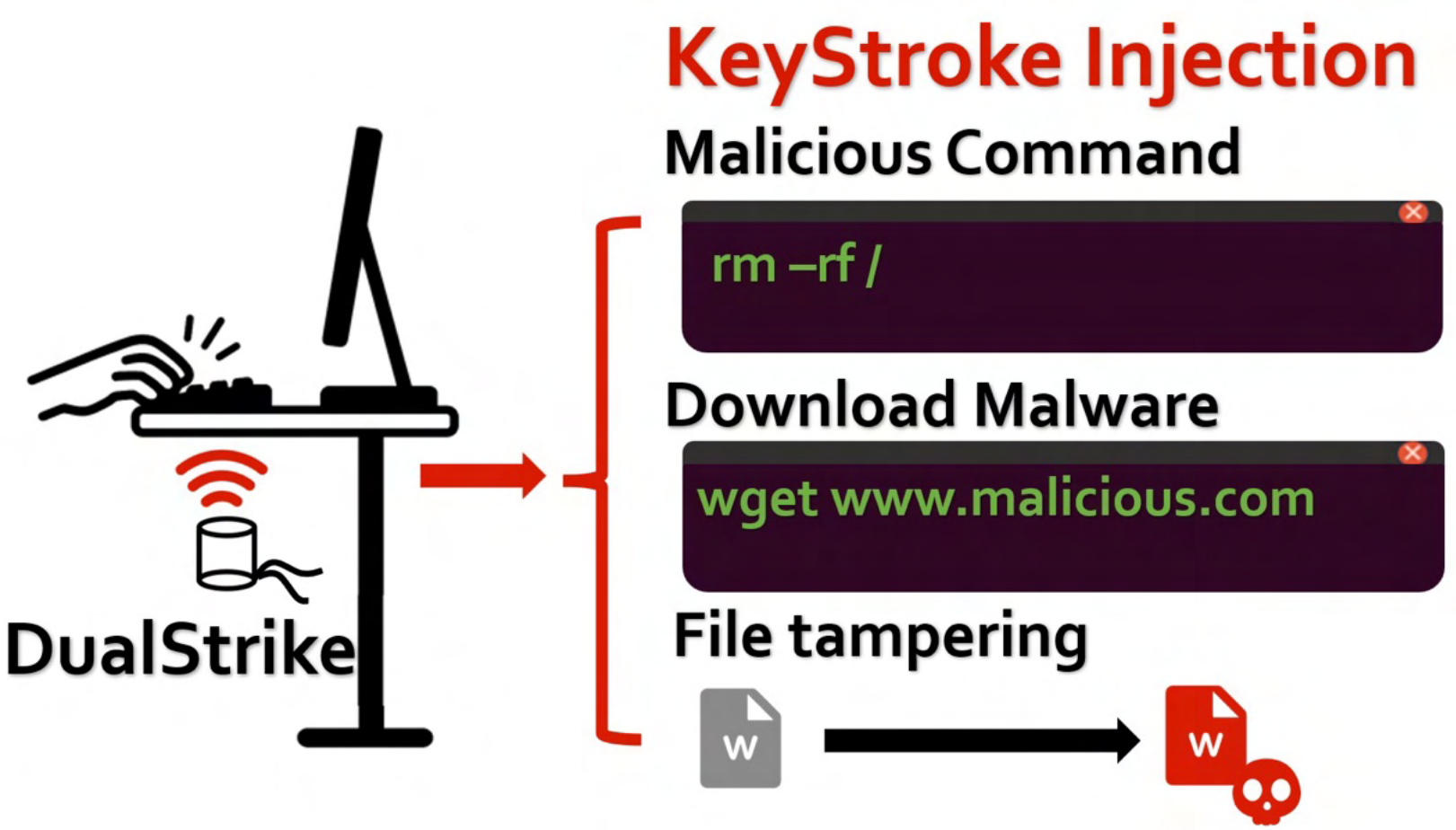
DualStrike: Enabling Practical Keyboard Attacks

Attack scenario



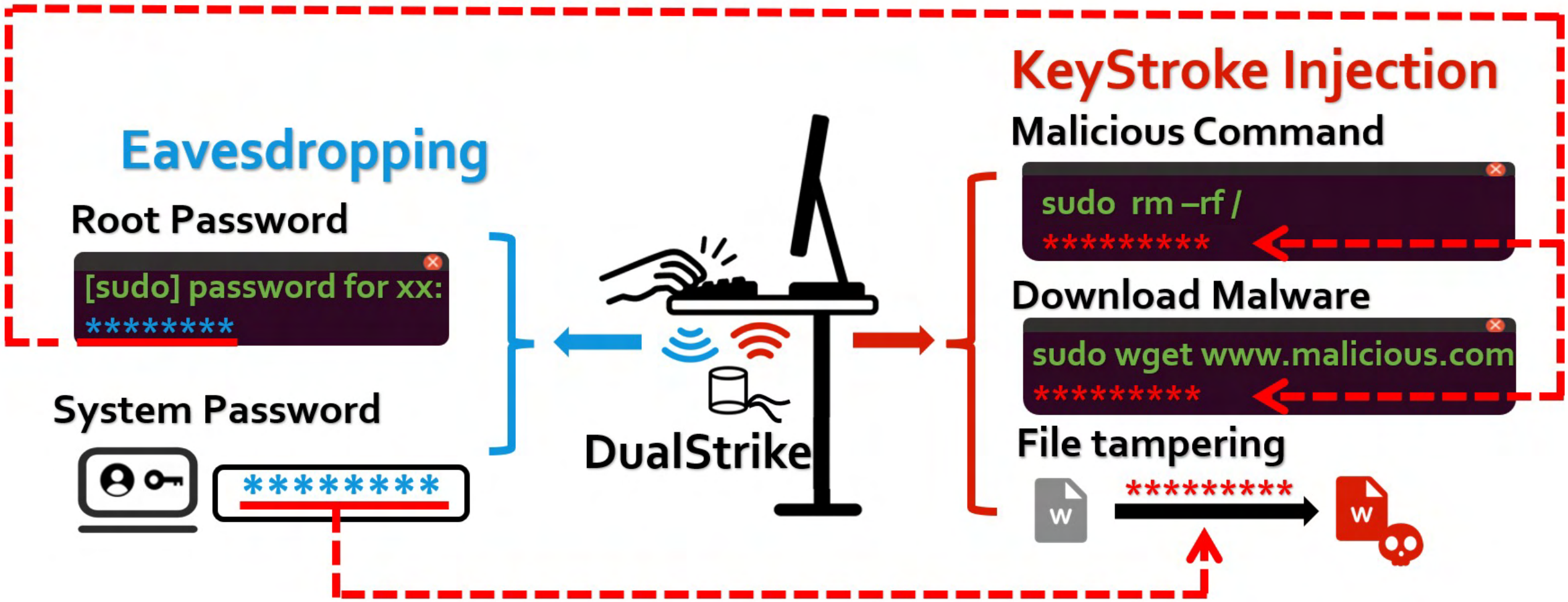
DualStrike: Enabling Practical Keyboard Attacks

Attack scenario



DualStrike: Enabling Practical Keyboard Attacks

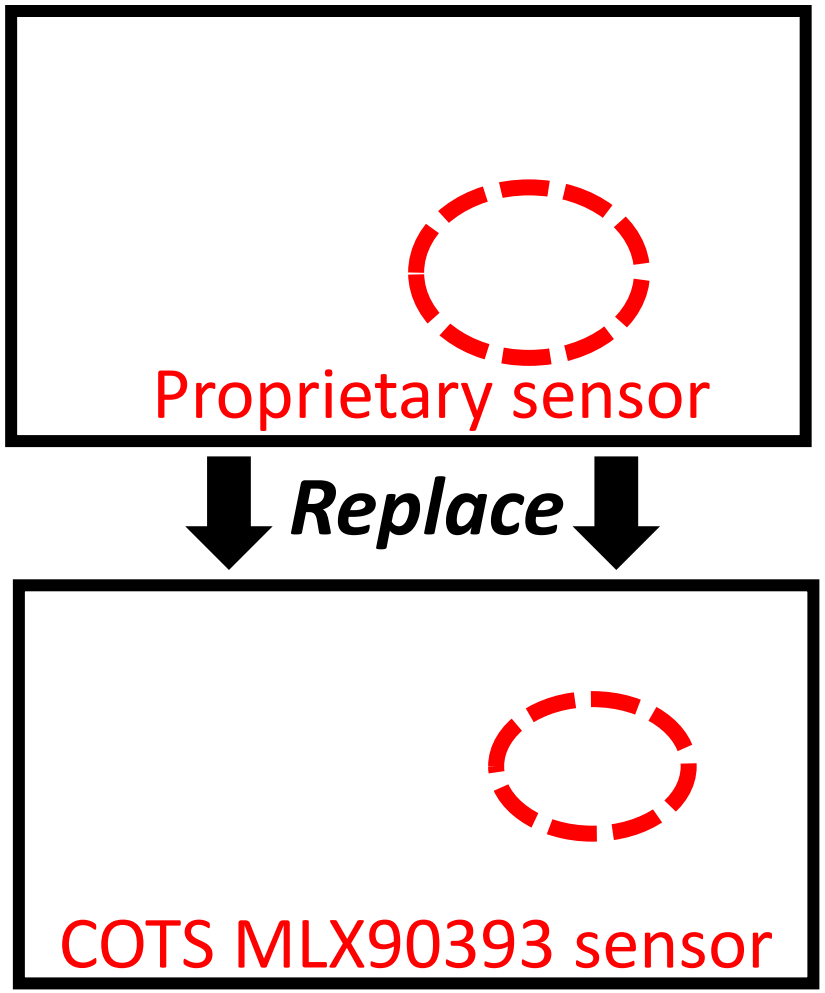
Attack scenario



Characterizing Hall-effect Keyboards

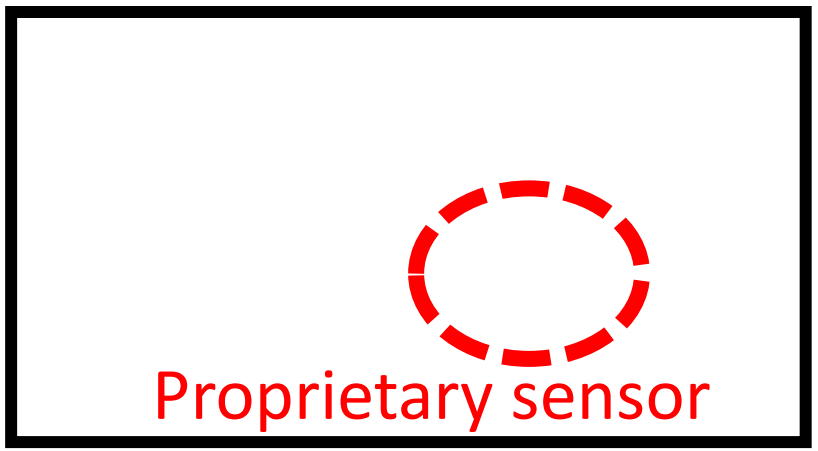
Characterizing Hall-effect Switches

- Characterizing via Reverse Engineering (Wooting 60 HE keyboard):



Characterizing Hall-effect Switches

- Characterizing via Reverse Engineering (Wooting 60 HE keyboard):

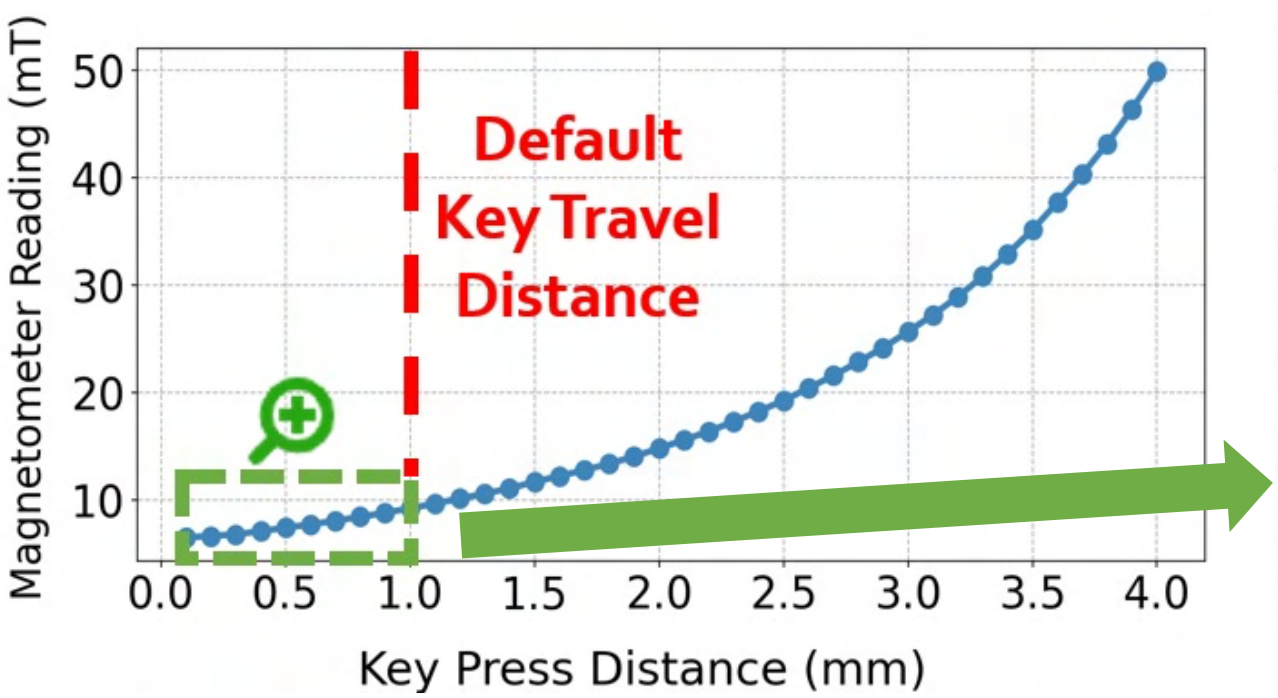


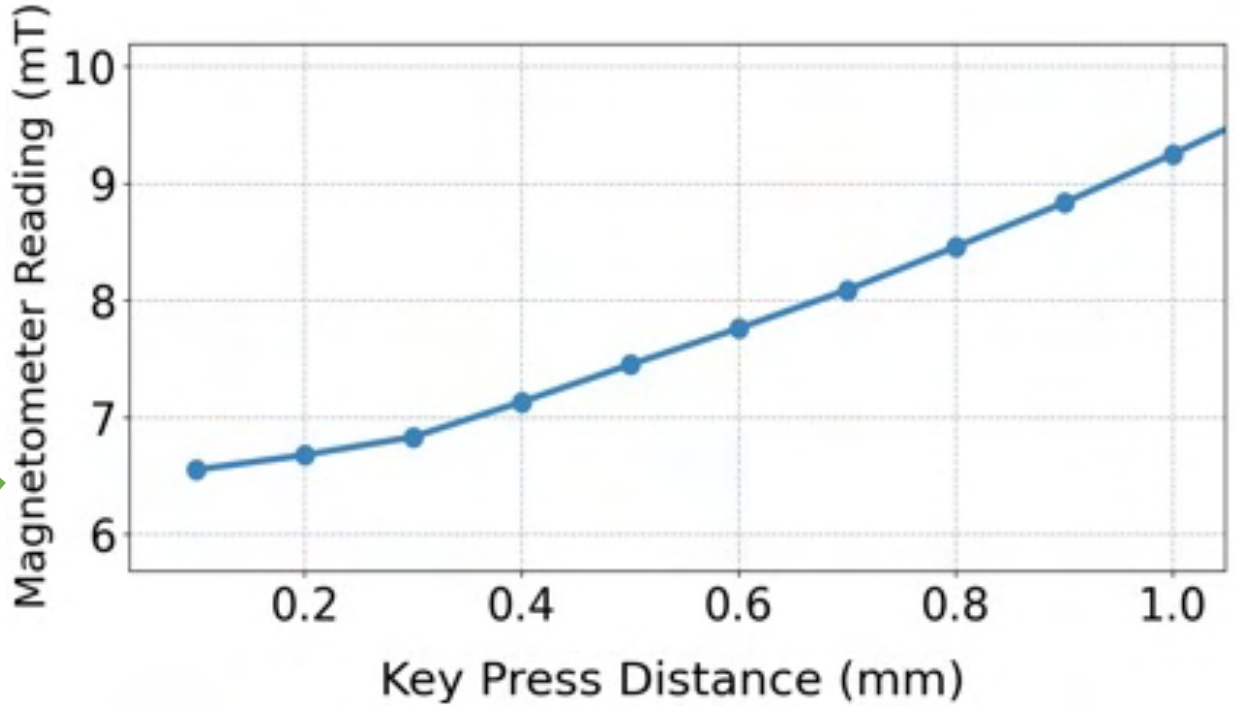
Replace

Vernier caliper

Characterizing Hall-effect Switches

- Characterizing via Reverse Engineering (Wooting 60 HE keyboard):





1. **Commodity magnetometers** can capture the variance of the magnetic field

2. Below the default travel distance, only **9 mT** is needed to trigger a keystroke

Characterizing Scanning Circuit

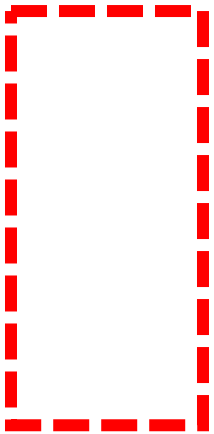
- We use an oscilloscope for reverse engineering.

Setup

Matrix circuit

Multiplexer-integrated circuit

Result of 6 keyboards



Shorter than traditional keyboards (2.4–8.2 ms)

Can enable faster keystroke injection!

Design of DualStrike

Attack Design

Keystroke Eavesdropping Module

- How to accurately catch each tap and tapped key in real-time?

Keystroke Injection Module

- How to achieve non-invasive, per-key injection?

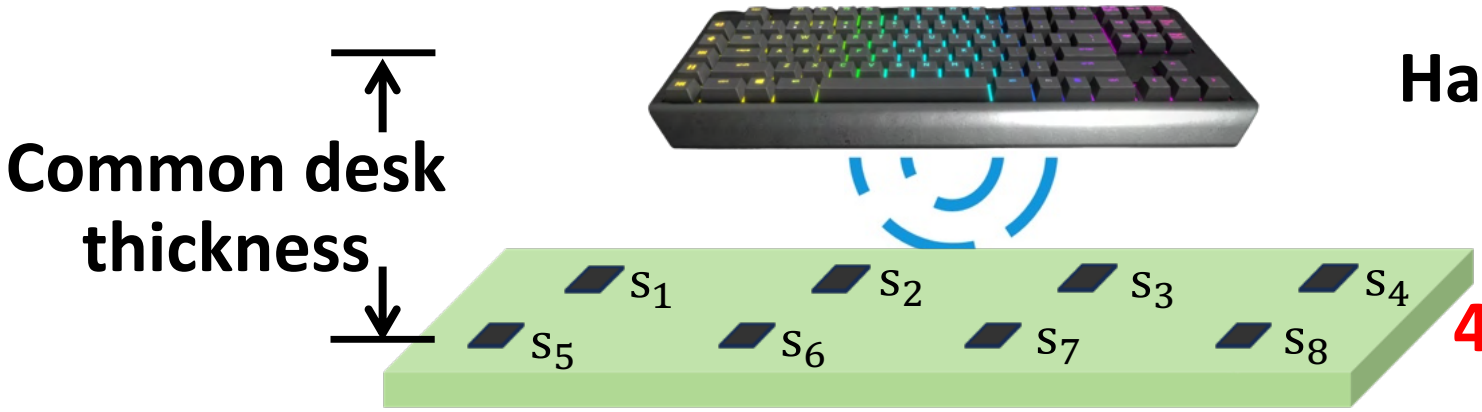
Attack Device Design

- How to integrate two modules into a complete attack device?

Misalignment Calibration

- How to calibrate real-world disturbances, e.g. displacement?

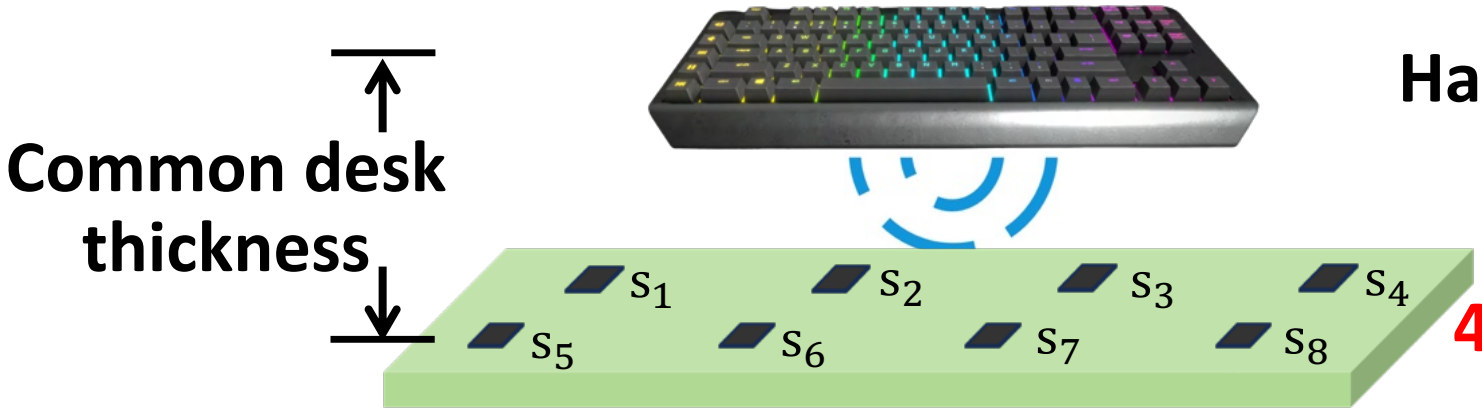
Attack Design - Keystroke Eavesdropping Module



Hall-effect keyboard

4*2 mlx90393 magnetometer array

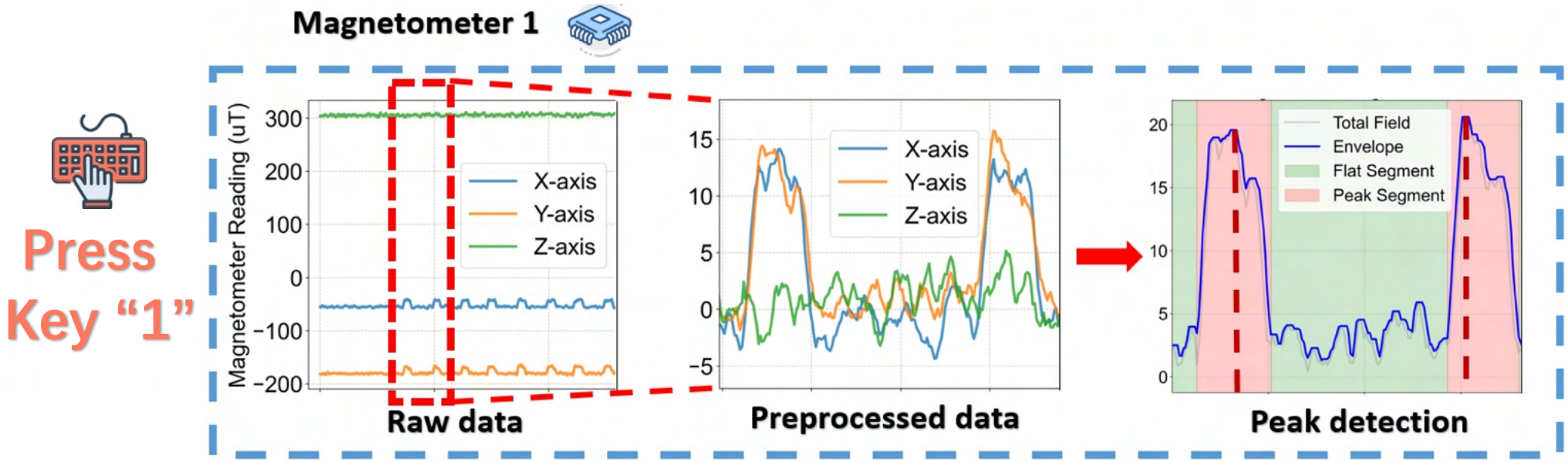
Attack Design - Keystroke Eavesdropping Module



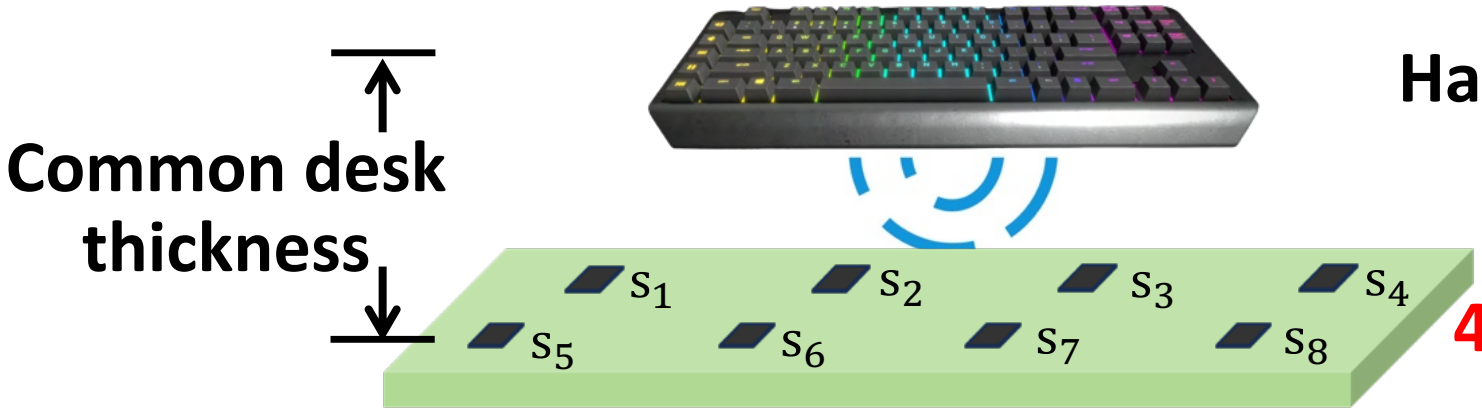
Hall-effect keyboard

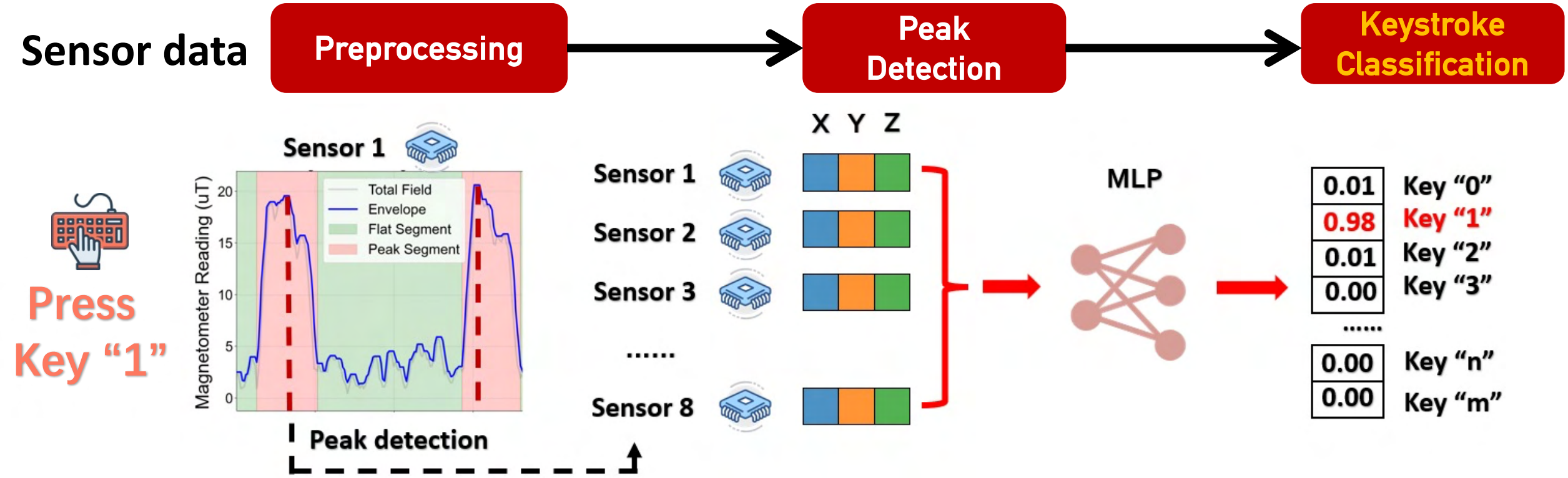
4*2 mlx90393 magnetometer array

Sensor data → Preprocessing → Peak Detection → Keystroke Classification



Attack Design - Keystroke Eavesdropping Module





Attack Design

Keystroke Eavesdropping Module

- How to accurately catch each tap and tapped key in real-time?

Keystroke Injection Module

- How to achieve non-invasive, per-key injection?

Attack Device Design

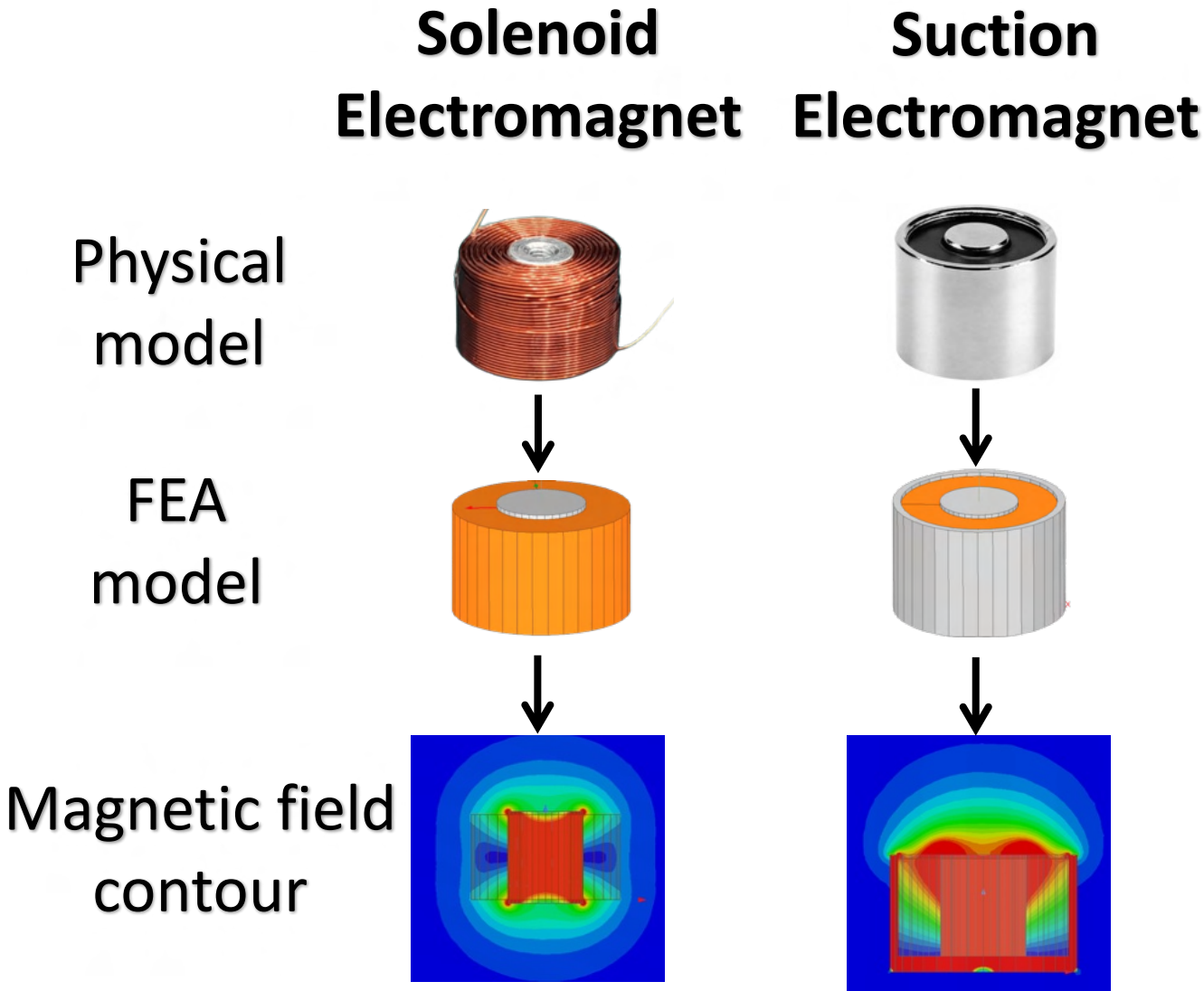
- How to integrate two modules into a complete attack device?

Misalignment Calibration

- How to calibrate real-world disturbances, e.g. displacement?

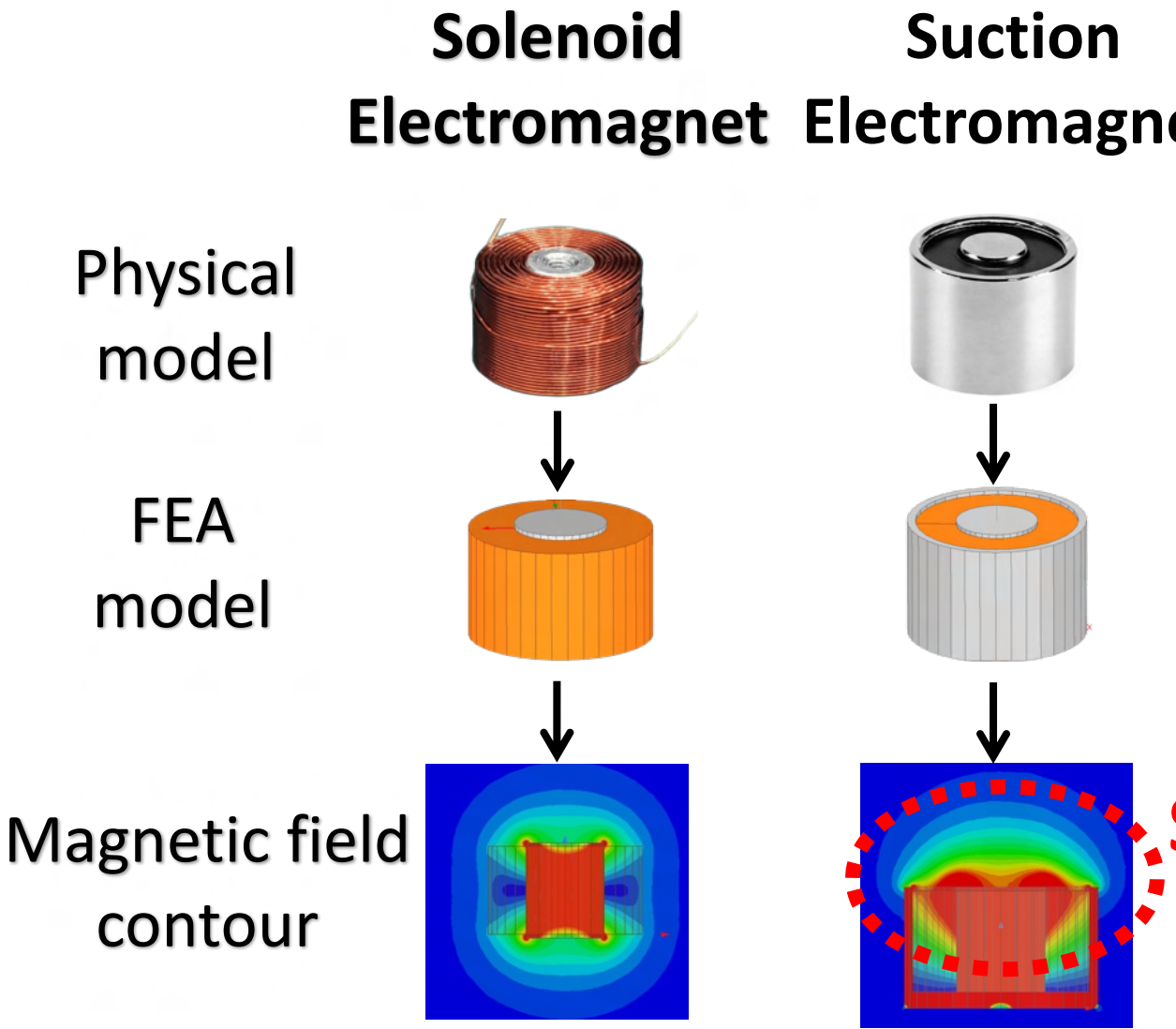
Attack Design - Keystroke Injection Module

- The suction electromagnet is selected as the attack unit.



Attack Design - Keystroke Injection Module

- The suction electromagnet is selected as the attack unit.

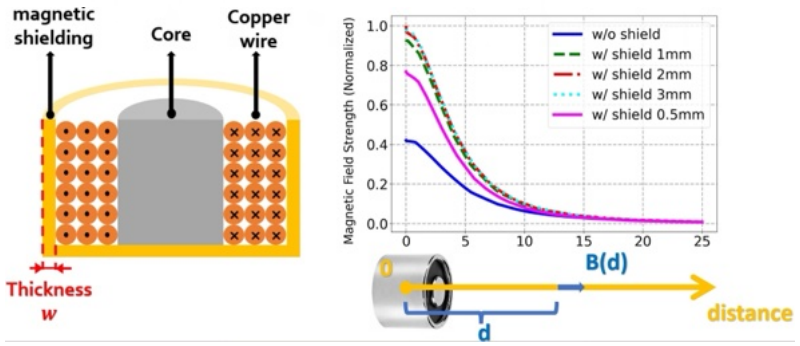


Suction exhibits stronger magnetic field strength on one side

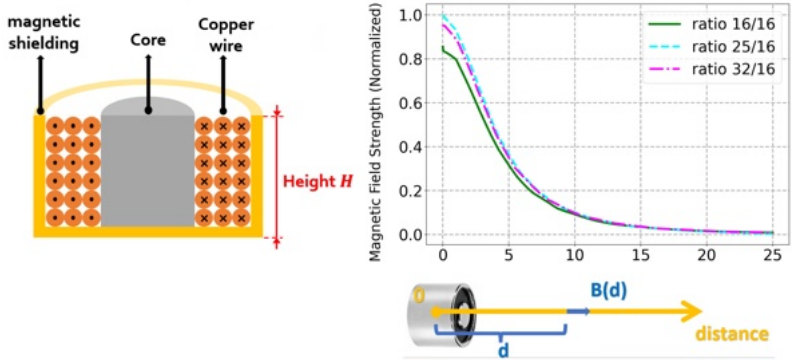
Attack Design - Keystroke Injection Module

- Through FEA simulation, we determine the optimal size that produces the strongest magnetic field.

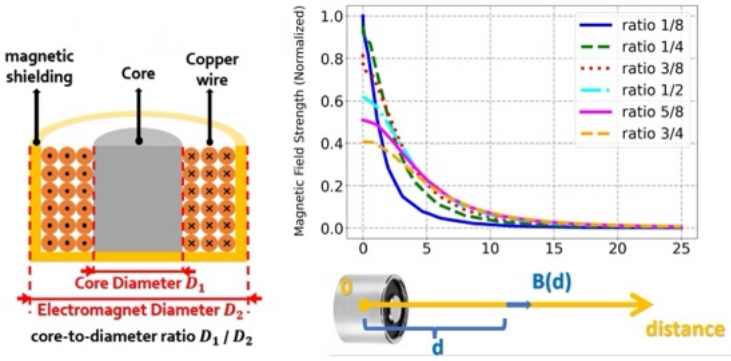
Thickness simulation



Height simulation



Core-to-diameter simulation

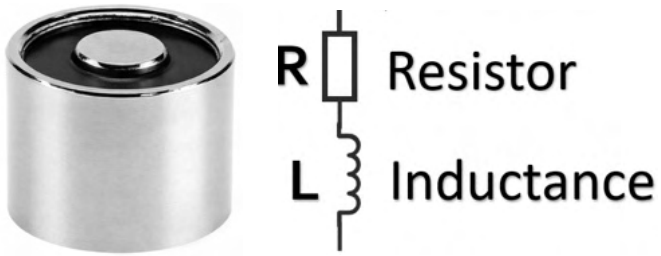


Shell thickness: 1mm
Height: 25mm
core diameter: 8mm
overall diameter: 16mm

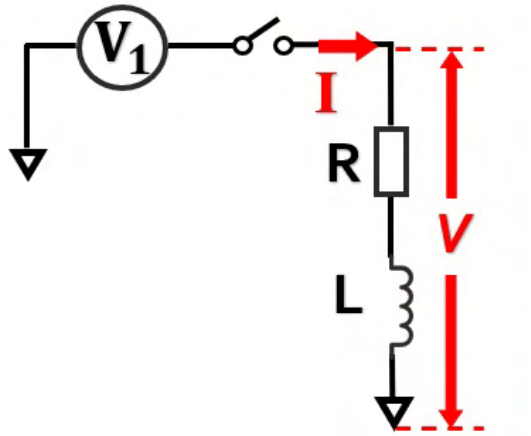
Attack Design - Keystroke Injection Module

- High-frequency magnetic spoofing circuit design.

RL model



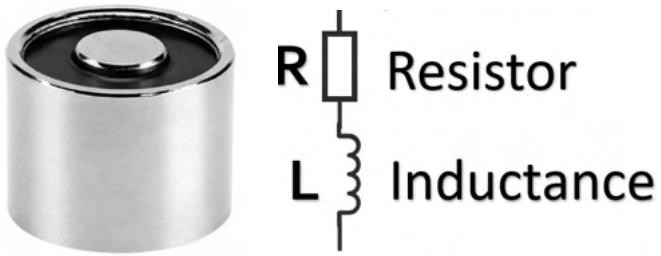
Equivalent Circuit



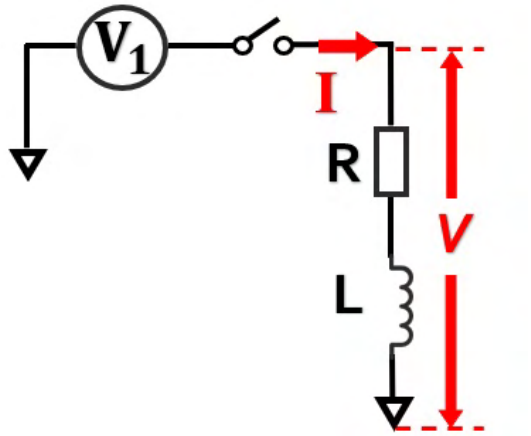
Attack Design - Keystroke Injection Module

- High-frequency magnetic spoofing circuit design.

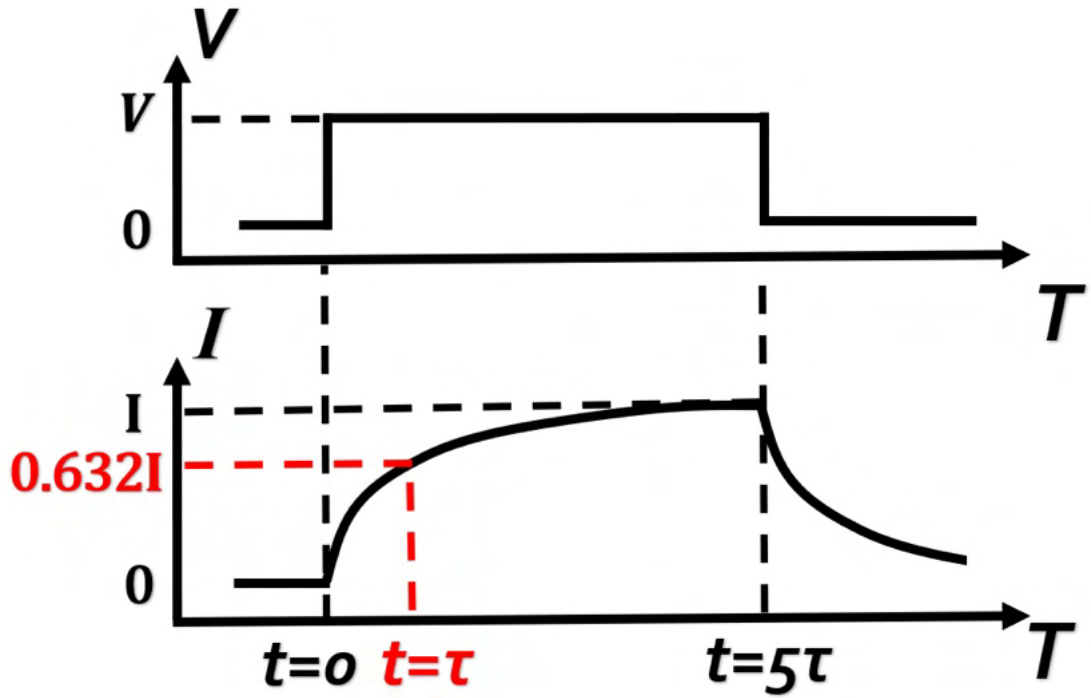
RL model



Equivalent Circuit



V/I – T



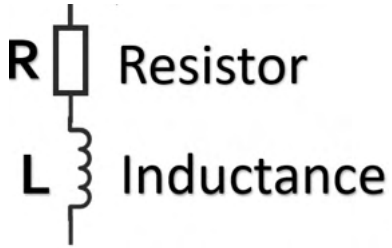
$$I = \frac{v}{R}\left(1 - e^{-t/\tau}\right)$$

Current rise is too slow!

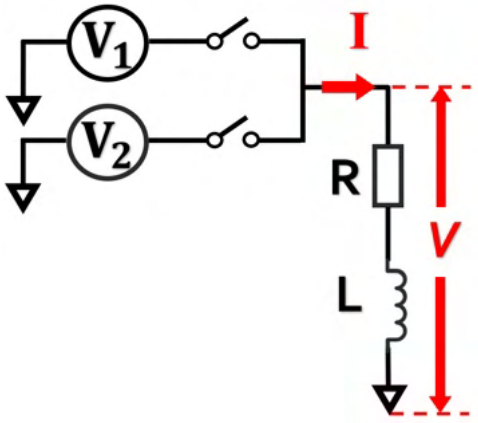
Attack Design - Keystroke Injection Module

- High-frequency magnetic spoofing circuit design.

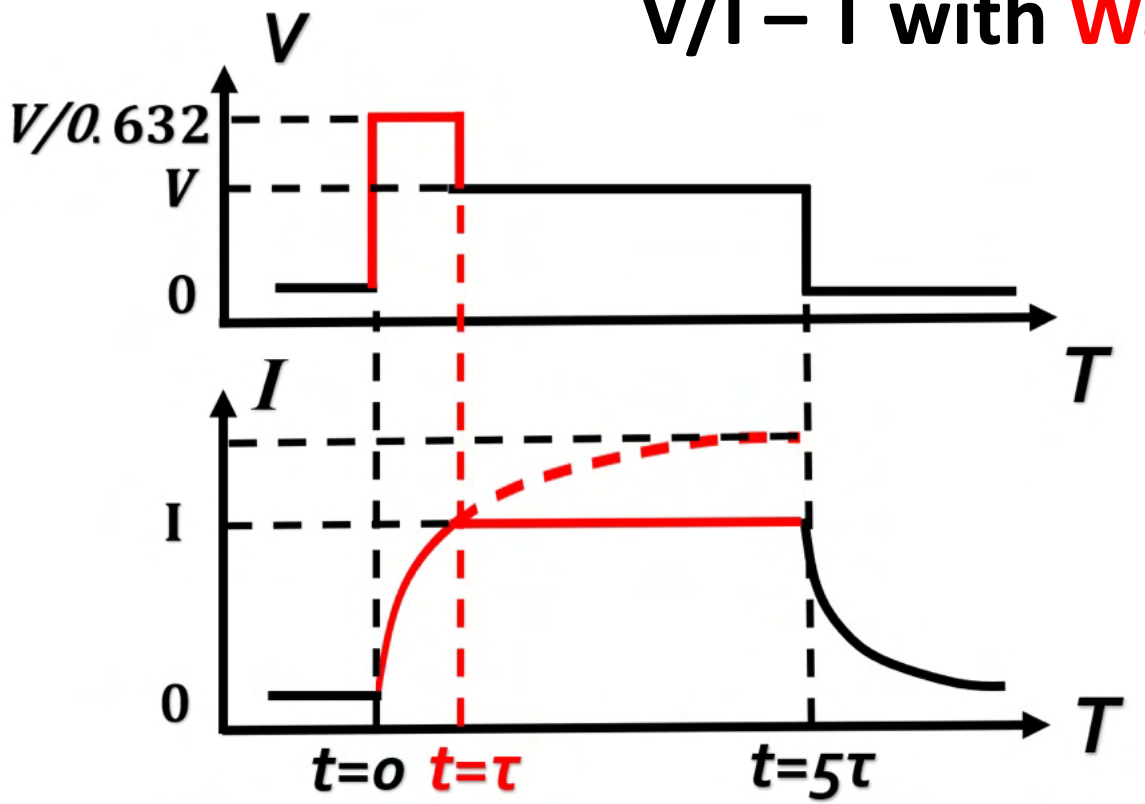
RL model



Circuit with Warm-up



V/I – T with Warm up



rise time from 5τ → τ

enabling a 5× switching frequency

Attack Design

Keystroke Eavesdropping Module

- How to accurately catch each tap and tapped key in real-time?

Keystroke Injection Module

- How to achieve non-invasive, per-key injection?

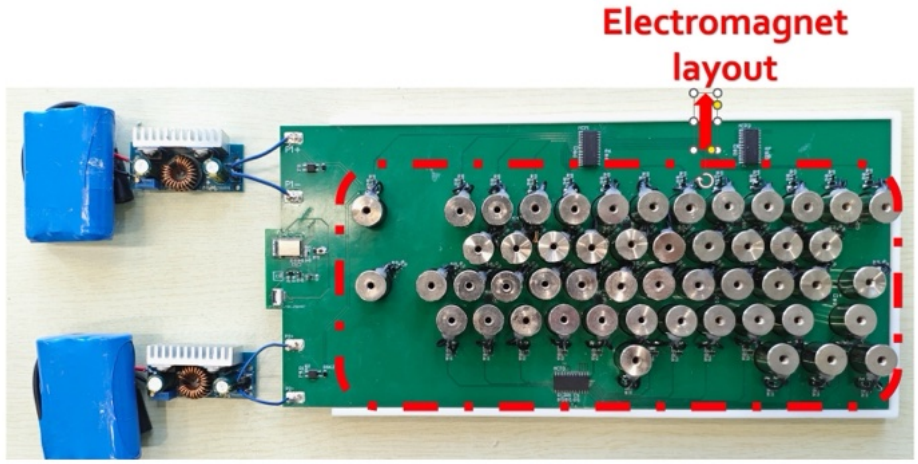
Attack Device Design

- How to integrate two modules into a complete attack device?

Misalignment Calibration

- How to calibrate real-world disturbances, etc. displacement?

Attack Design - Attack Device Design



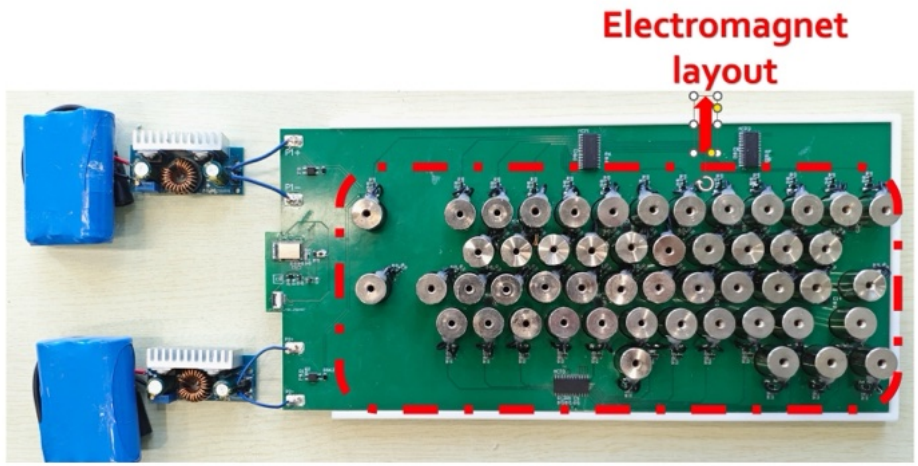
Electromagnet Layout

- Layout aligned with the main keyboard area

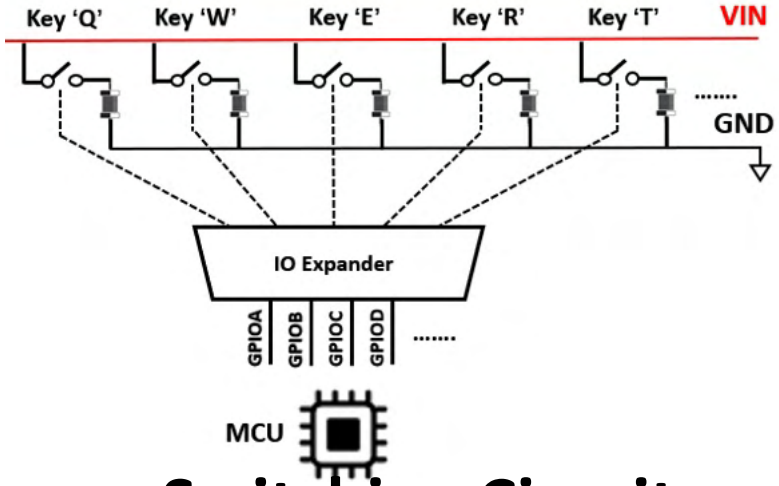
Type	Details
Letters	abcdefghijklmnopqrstuvwxyz
Symbol Keys	,./;’-
Control Keys	Shift,Ctrl,alt,OS,Esc,Backspace,Enter,CapsLk
Numeric Keys	1234567890
Whitespace	’ ’

- Target **51** keys.

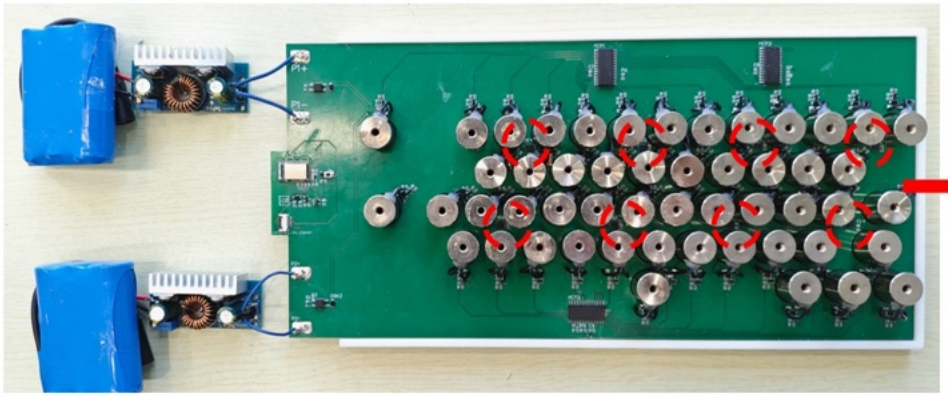
Attack Design - Attack Device Design

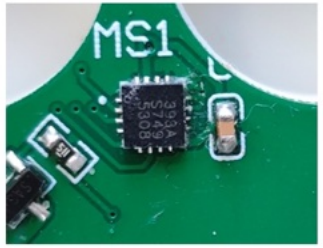


Electromagnet Layout



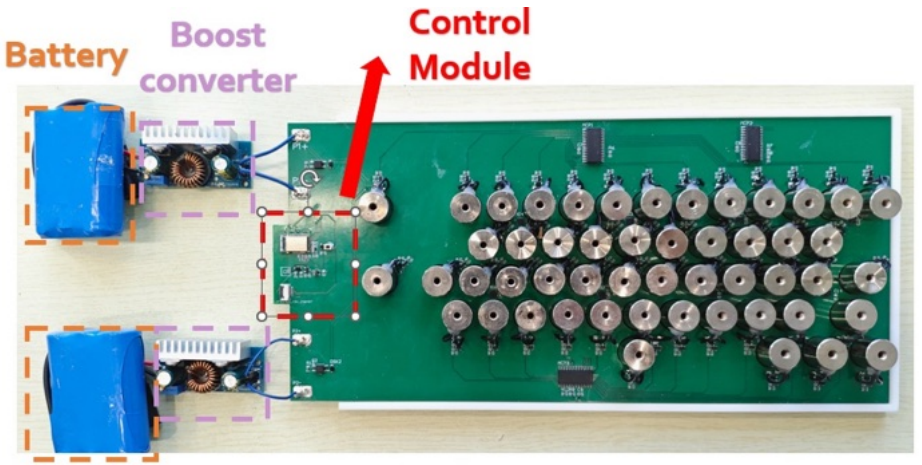
Switching Circuit





4*2 magnetometer array

Magnetometer Array



Control Module & Power Supply

Attack Design

- **Keystroke Eavesdropping Module**
  - How to accurately catch each tap and tapped key in real-time?
- **Keystroke Injection Module**
  - How to achieve non-invasive, per-key injection?
- **Attack Device Design**
  - How to integrate two modules into a complete attack device?
- **Misalignment Calibration**
  - How to calibrate real-world disturbances, e.g. displacement?

Attack Design - Misalignment Calibration

- Now we can accurately listen and inject when aligned

→what if displaced during usage?

Attack Design - Misalignment Calibration

- Now we can accurately listen and inject when aligned

→what if displaced during usage?

dx = 6cm
dy = 2cm

Attack Design - Misalignment Calibration

Step1: Attacker can prompt victim to input specific pre-determined keys

E.g. predetermined Wi-Fi password in library/coffee shop

Attack Design - Misalignment Calibration

Step1: Attacker can prompt victim to input specific pre-determined keys

Step2: Estimate displacement (dx, dy, θ)

$(\text{key}_{\text{true}}, \text{key}_{\text{predicted}}, p)$

(2,T,0.98)

(6,O,0.97)

(B,S,0.99)

(.,H,0.99)

dx = 6.50cm
dy = 2.00cm
theta = 0.0rad

$$\min_{\mathrm{dx},\mathrm{dy},\theta} \sum_{i=1}^{n} \|\mathbf{pos}_{\text{predicted},i} - (\mathbf{R}(\theta) \cdot \mathbf{pos}_{\text{true},i} + [\mathrm{dx}, \mathrm{dy}]^{\top})\|^2 \cdot \mathrm{p}_i$$

➡ **(dx, dy, θ)**

Attack Design - Misalignment Calibration

- Step1: Attacker can prompt victim to input specific pre-determined keys
- Step2: Estimate displacement (dx, dy, θ)
- **Step3: Calibrate eavesdropping results / injection targets**

Eavesdropping:

$$\mathbf{pos}^{cali}_{\text{eavesdrop}} = \mathbf{R}^{-1}(\theta) \cdot (\mathbf{pos}_{\text{eavesdrop}} - [\text{dx}, \text{dy}]^\top)$$

key nearest to $pos^{cali}_{eavesdrop}$ is the actual key pressed

Injection:

$$\mathbf{pos}^{cali}_{\text{inject}} = \mathbf{R}(\theta) \cdot \mathbf{pos}_{\text{inject}} + [dx, dy]^\top$$

key nearest to pos^{cali}_{inject} is the actual key injected

Evaluation

Evaluation

- We evaluated 6 latest Hall-effect keyboards

- Environmental setup

Can be replaced with different thickness and material

Evaluation

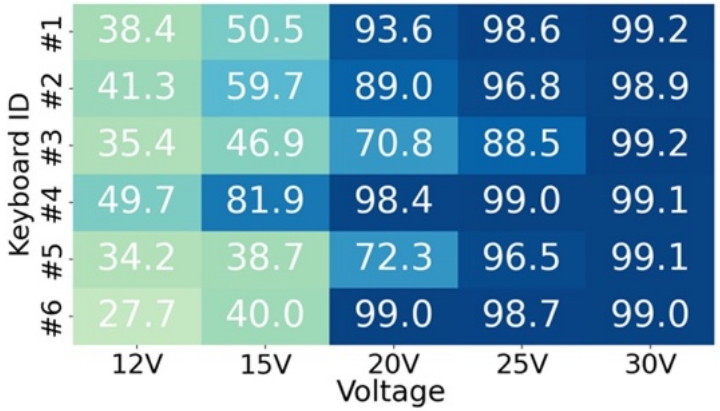
1. **Eavesdropping Module**

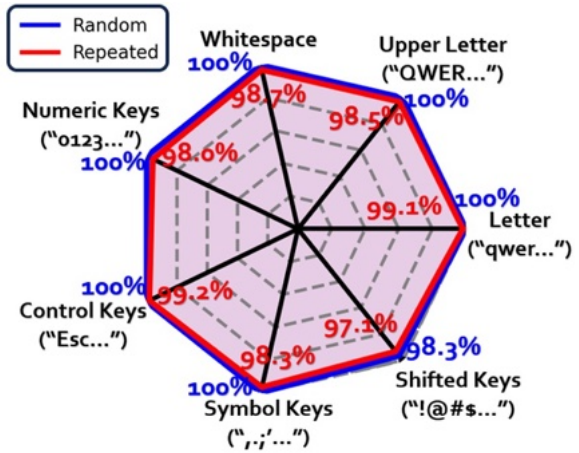
- MLP trained on 51 keys × 30 presses (7:3 split)
- Achieving 99.41% and 99.54% accuracy on keyboards #1 and #6

Evaluation

2. Keystroke Injection Module

Accuracy

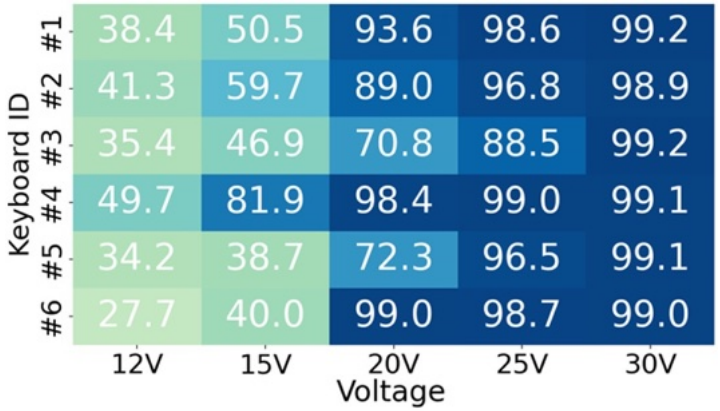


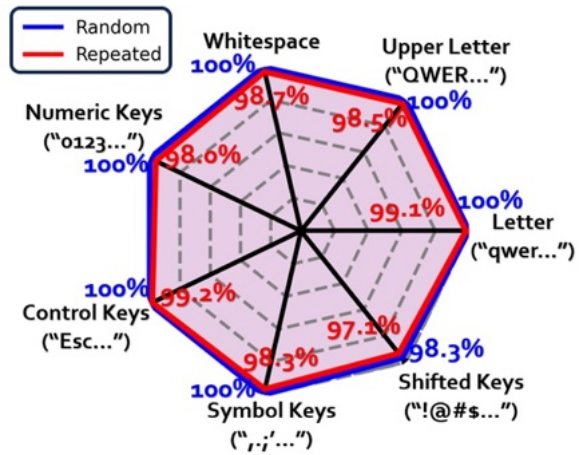


when $V_{attack} \geqslant V_{required}$, ~100% accuracy over all keys

Evaluation

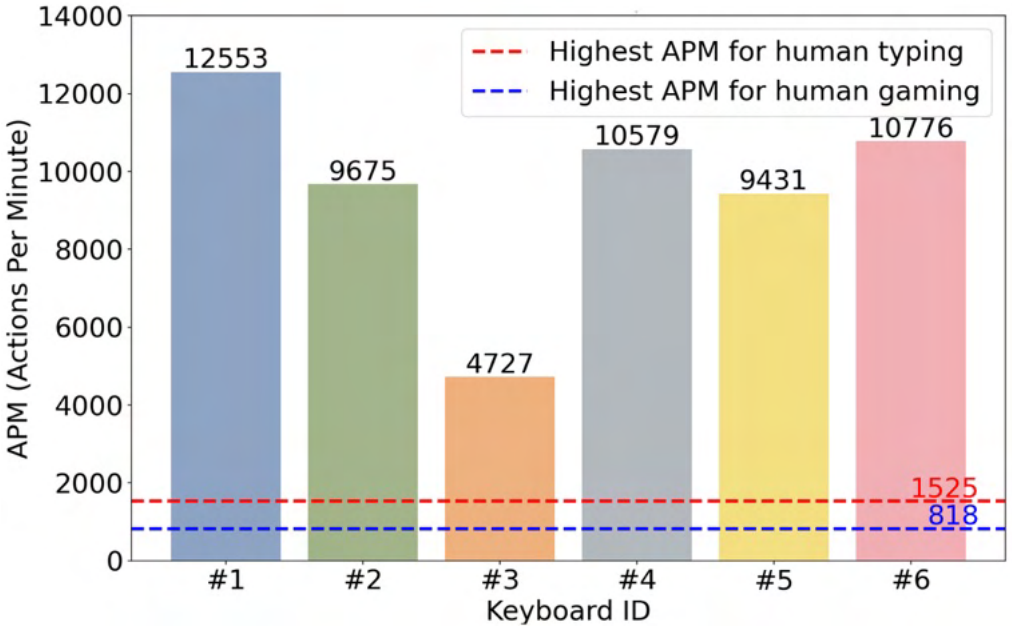
2. Keystroke Injection Module Accuracy





when $V_{attack} \geqslant V_{required}$, ~100% accuracy

Injection Speed

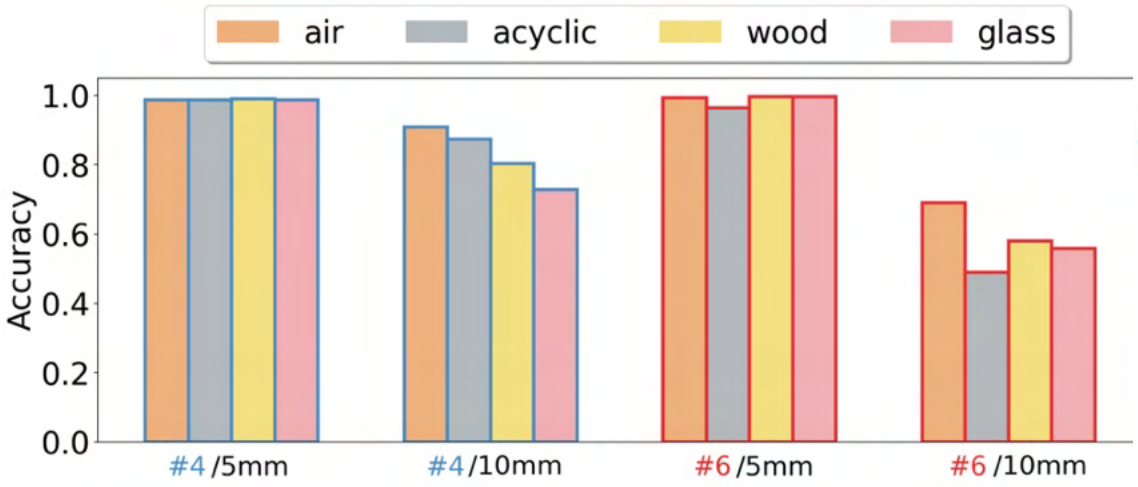


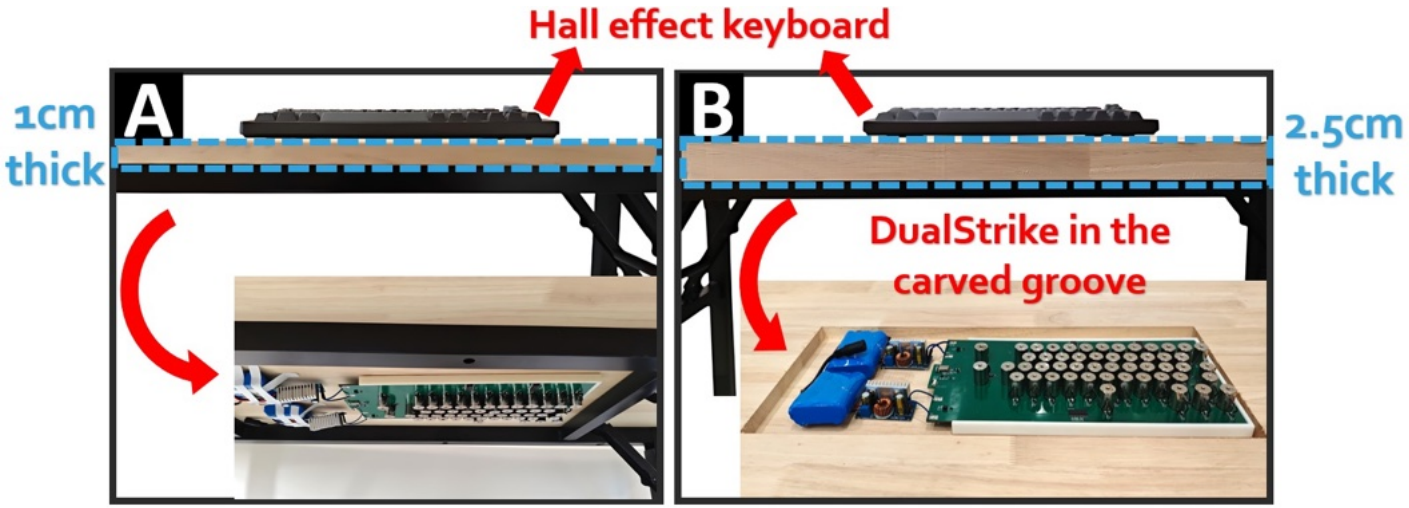
Up to 12,553 actions per minute(APM)

e.g. inject 40 characters within 200 ms

Evaluation

3. Environmental Factors of Injection

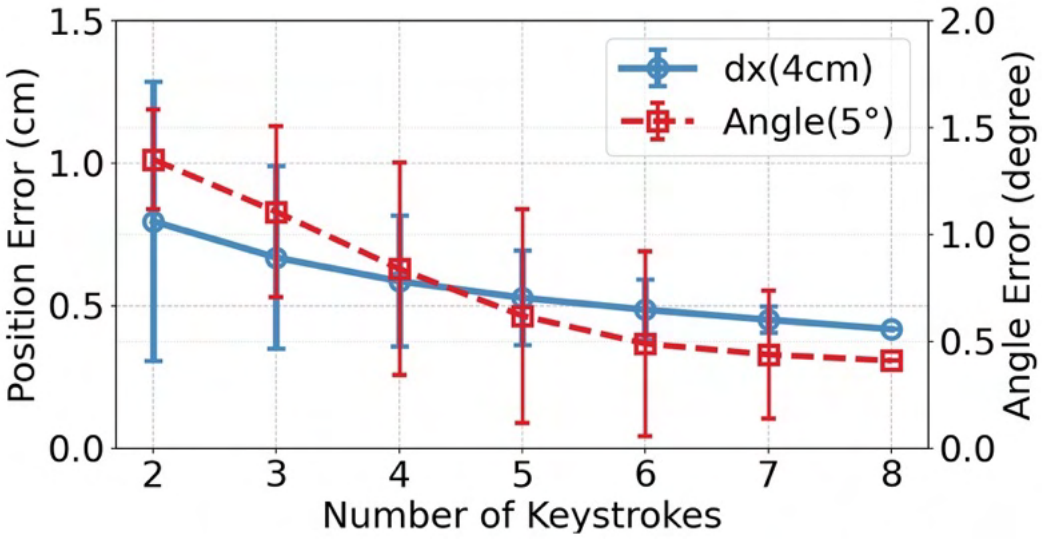




DualStrike can be concealed under a desk or embedded in a carved groove beneath it

Evaluation

4. Performance of Misalignment Calibration



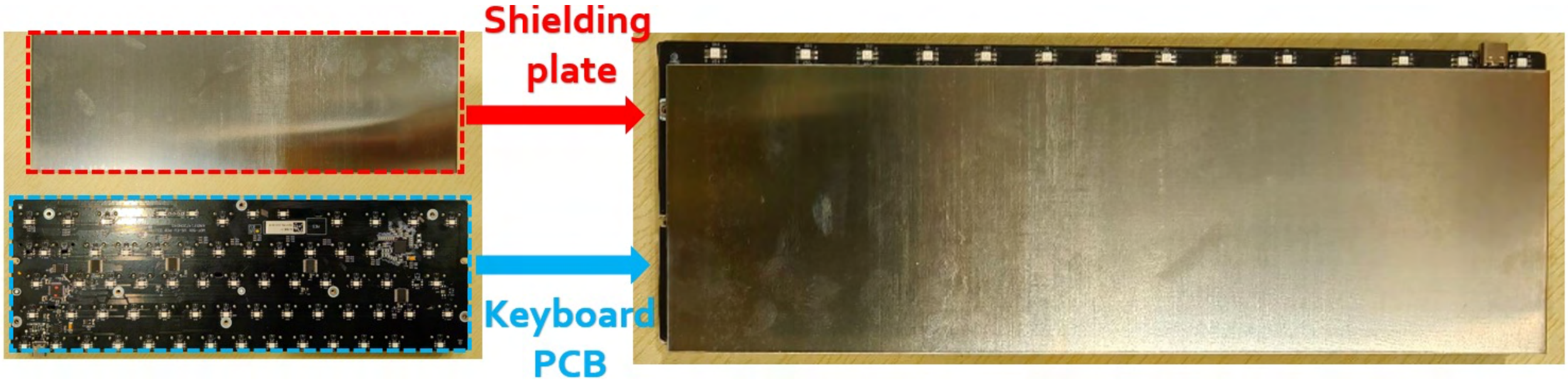
Scenarios	Keyboard	Displacement			Rotation
		→2cm	→4cm	↗(3,2)	5°
Error	#1 keyboard	0.40 cm	0.41 cm	0.44cm	0.61°
	#6 keyboard	0.41 cm	0.47 cm	0.38cm	0.43°
Accuracy	#1 keyboard	98.7%	98.5%	99.0%	98.1%
	#6 keyboard	98.2%	98.4%	98.8%	98.8%

With a 6-key calibration sequence, e.g. ‘qruzvm’,
DualStrike maintains 98.5% injection accuracy even with offsets up to 4 cm.

Countermeasures

Defenses against DualStrike

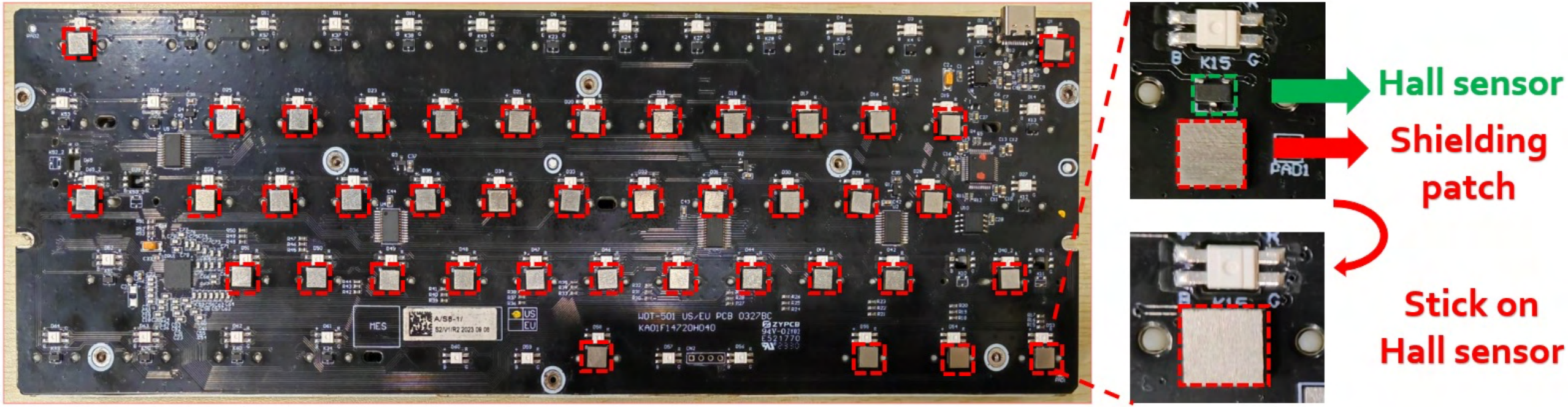
- **Existing magnetic shielding requires a full keyboard-sized shielding plate.**



Defenses against DualStrike

❑ **We propose a per-sensor shielding approach:**

attaching small shielding patches directly to each Hall-effect sensor.



Defenses against DualStrike

- **We propose a per-sensor shielding approach:**

  attaching small shielding patches directly to each Hall-effect sensor.

Material	Thickness	Keyboard #4			Keyboard #6		
		30V	35V	40V	30V	35V	40V
Steel	0.2mm	99.0%	98.8%	99.1%	98.9%	98.7%	98.7%
	0.5mm	99.2%	99.0%	99.0%	98.6%	99.2%	99.0%
Mu metal	0.2mm	93.4%	99.1%	99.0%	73.1%	86.2%	98.7%
	0.5mm	7.8%	16.2%	41.0%	0%	0%	11.2%
Per-sensor shielding		**0%**	**0%**	**0%**	**0%**	**0%**	**0%**

10% material → injection accuracy: 0%

Conclusion

- **We proposed DualStrike, a new attack on Hall-effect keyboards that can:**
  (i) Perform keyboard listening and
  (ii) Perform non-invasive, per-key keystroke injection
  (iii) Incorporating a calibration mechanism to mitigate real world disruptions such as keyboard displacement.

- **We performed the first reverse-engineering effort to help design practical attacks on Hall-effect keyboards**

Demo site:
https://sites.google.com/view/magkey-anonymous

DualStrike is open-sourced:

https://github.com/blankchenxm/DualStrike

Thanks!
Q&A


NDSS
SYMPOSIUM/2026


SHANGHAI JIAO TONG UNIVERSITY
1896


THE UNIVERSITY OF CALIFORNIA
IRVINE
LET THERE BE LIGHT