Non-intrusive and Unconstrained Keystroke Inference in VR Platforms via Infrared Side Channel

Tao Ni, Yuefeng Du, Qingchuan Zhao, Cong Wang

Department of Computer Science, City University of Hong Kong

NDSS'25 - Session Side Channel 1
February 26, 2025

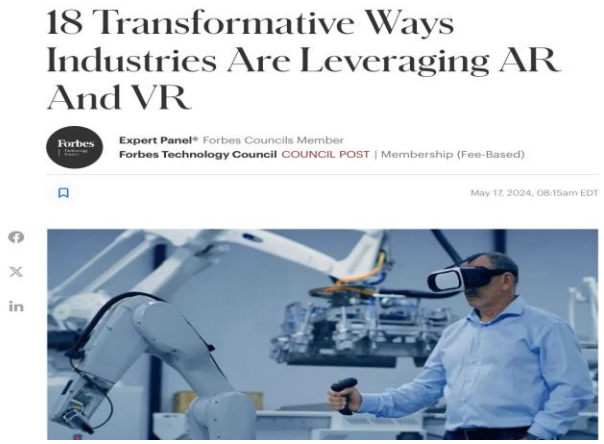
Virtual Reality (VR) Applications

Immersive Gaming

Healthcare Digitalization

Online Meeting

Virtual Tourism



Industrial Prototype Design

Real Estate Visualization

Why Should We Care About VR Security?

Why Should We Care About VR Security?


Technology

AI can steal passwords in virtual reality from avatar hand motions

Artificial intelligence can work out what someone is privately typing in VR meetings in Meta Horizon Workrooms by looking at the way their avatar's hands move

By Jeremy Hsu

14 November 2023

USENIX Security'24


Virtual reality headsets are vulnerable to hackers

UCR computer scientists to present findings at international cyber security conference

DAVID DANELSKI

August 8, 2023

While Augmented Reality (AR) and Virtual Reality (VR) are envisioned as the next iteration of the internet immersing us in new digital worlds, the associated headset hardware and virtual keyboard interfaces create new opportunities for hackers.

Such are the findings of computer scientists at the University of California, Riverside, which are detailed in two papers to be presented this week at the annual Usenix Security Symposium in Anaheim, a leading international conference on cyber security.

The emerging metaverse technology, now under intensive development by Facebook's Mark Zuckerberg and other tech titans,

USENIX Security'23


How hackers are using Apple Vision Pro's eye-tracking technology to steal passwords

TOI Tech Desk / TIMESOFINDIA.COM / Sep 15, 2024, 20:11 IST

SHARE AA FOLLOW US

Researchers have identified a vulnerability called GAZEploit in Apple Vision Pro's eye-tracking technology, allowing hackers to predict user keystrokes by analysing eye movements. This flaw poses a risk during virtual meetings and calls.

Do you know?

You can access your daily TOI newspaper anytime, anywhere with TOI+ membership.

READ MORE

CCS'24

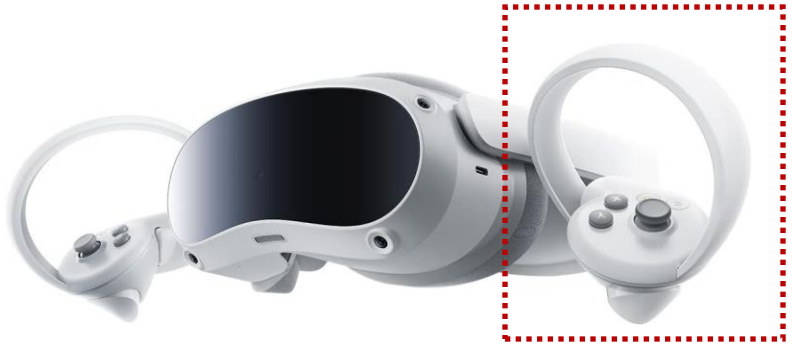

Rutgers Researchers Discover Security Vulnerabilities in Virtual Reality Headsets

MobiCom'21

An Interesting Design in VR Controllers

An Interesting Design in VR Controllers

An Interesting Design in VR Controllers



Why is there a ring arc on the VR controller?

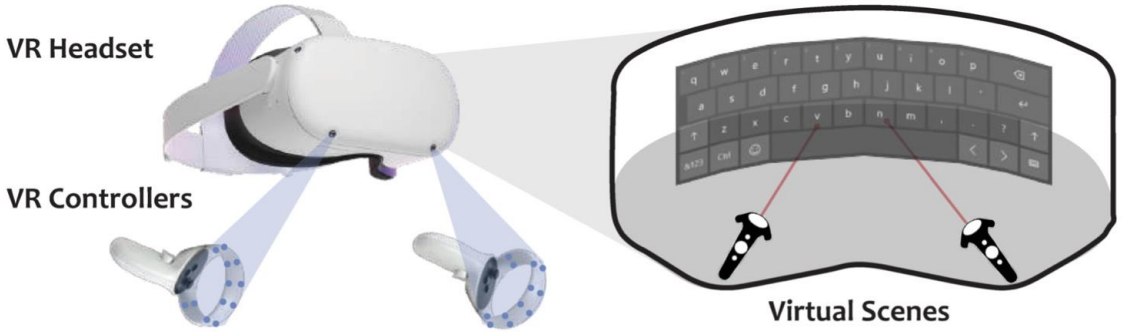
Constellation Tracking Systems

Constellation Tracking Systems

- Multiple infrared LED lights embedded in the ring arcs COTS VR controllers

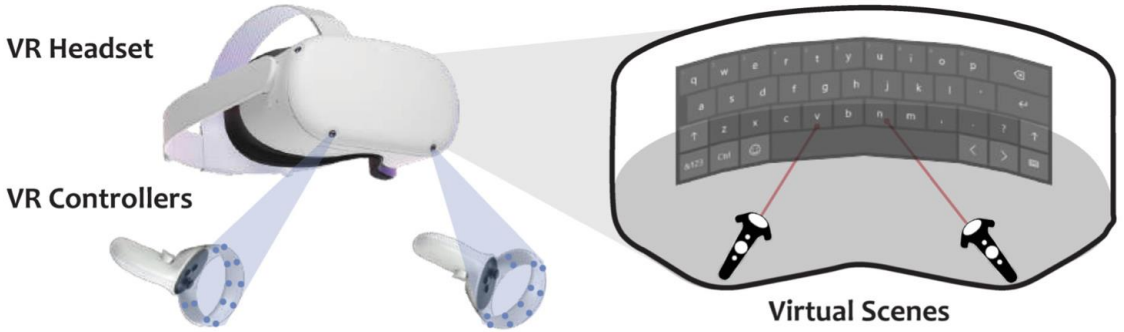
Constellation Tracking Systems

- Multiple infrared LED lights embedded in the ring arcs COTS VR controllers
- Continuous communications between VR headsets and two hand-held controllers



Constellation Tracking Systems

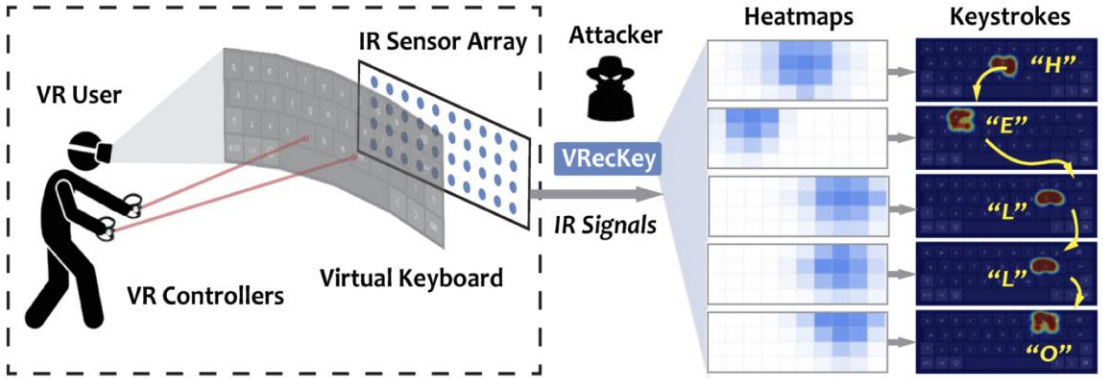
- Multiple infrared LED lights embedded in the ring arcs COTS VR controllers
- Continuous communications between VR headsets and two hand-held controllers
- Body movement and hand gesture tracking with cameras and embedded LED lights to achieve user-VR interactions



With Greater Interactions Comes...

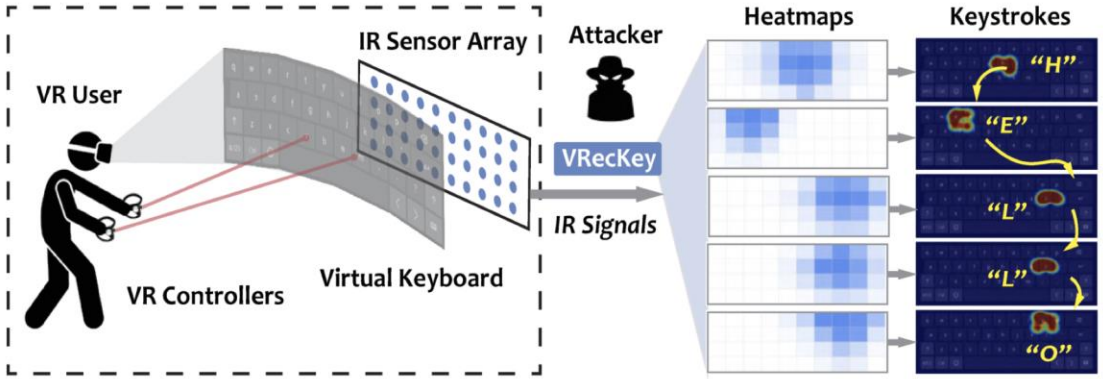
With Greater Interactions Comes...

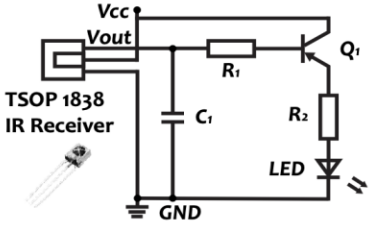
- Infrared (IR) sensors emit IR signals for tracking and communication, leading to potential keystroke inference side-channel attacks

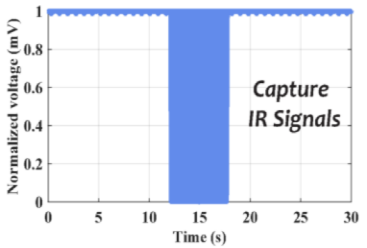


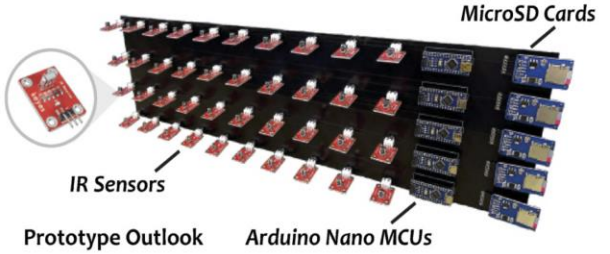
With Greater Interactions Comes...

- Infrared (IR) sensors emit IR signals for tracking and communication, leading to potential keystroke inference side-channel attacks
- Attackers can place a small IR sensor array near the target victim to capture IR leakages emitted from VR interactions (e.g., typing virtual keys)





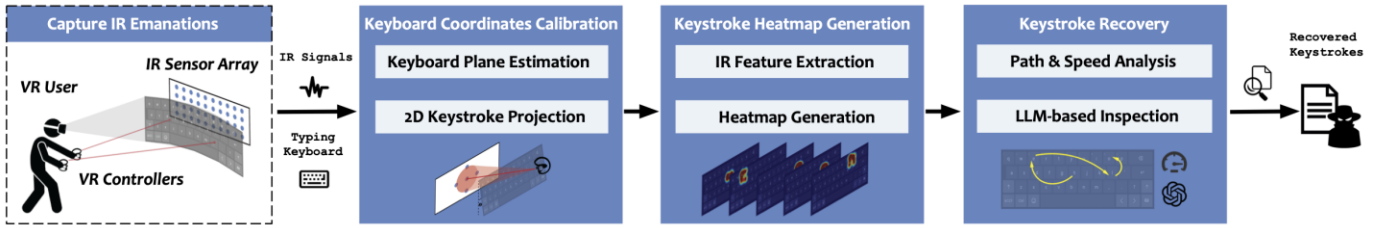




Threat Model - VRecKey

Threat Model - VRecKey

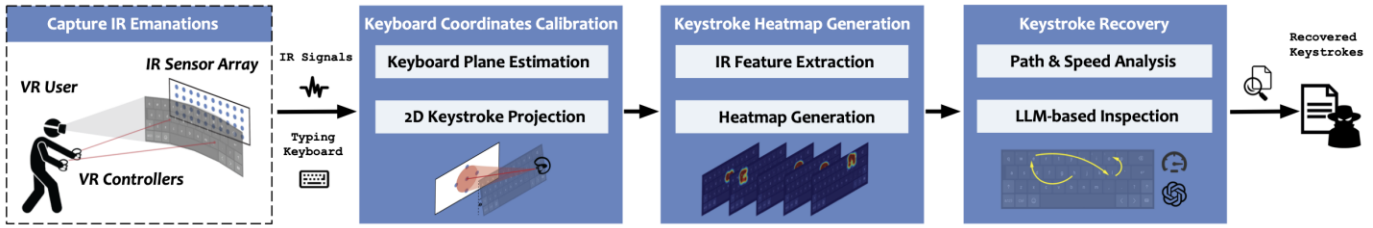
- An end-to-end framework to **non-intrusively** reconstruct **unconstrained** virtual keystrokes via leakages from infrared side channel



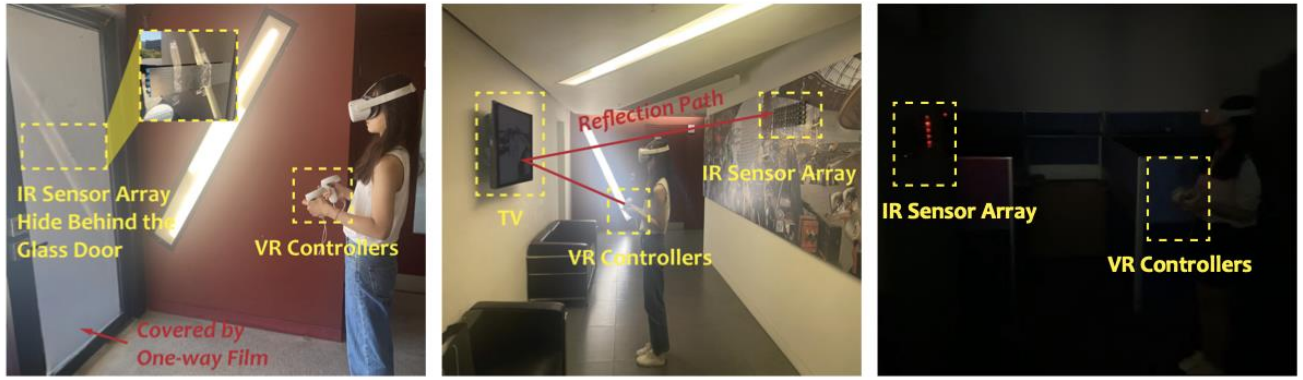
VRecKey Overview

Threat Model - VRecKey

- An end-to-end framework to **non-intrusively** reconstruct **unconstrained** virtual keystrokes via leakages from infrared side channel
- High effectiveness in different real-world scenarios: (1) Concealed Attack, (2) Reflection-based Attack, and (3) Low-visibility Attack.



VRecKey Overview

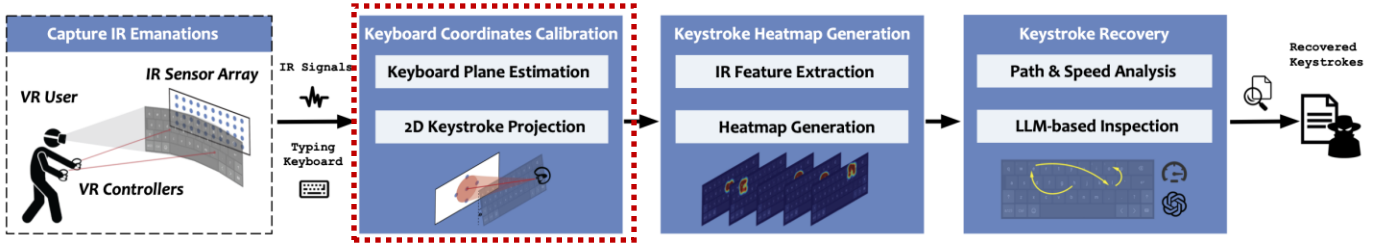


Three Real-world Attack Scenarios

Keyboard Coordinates Calibration

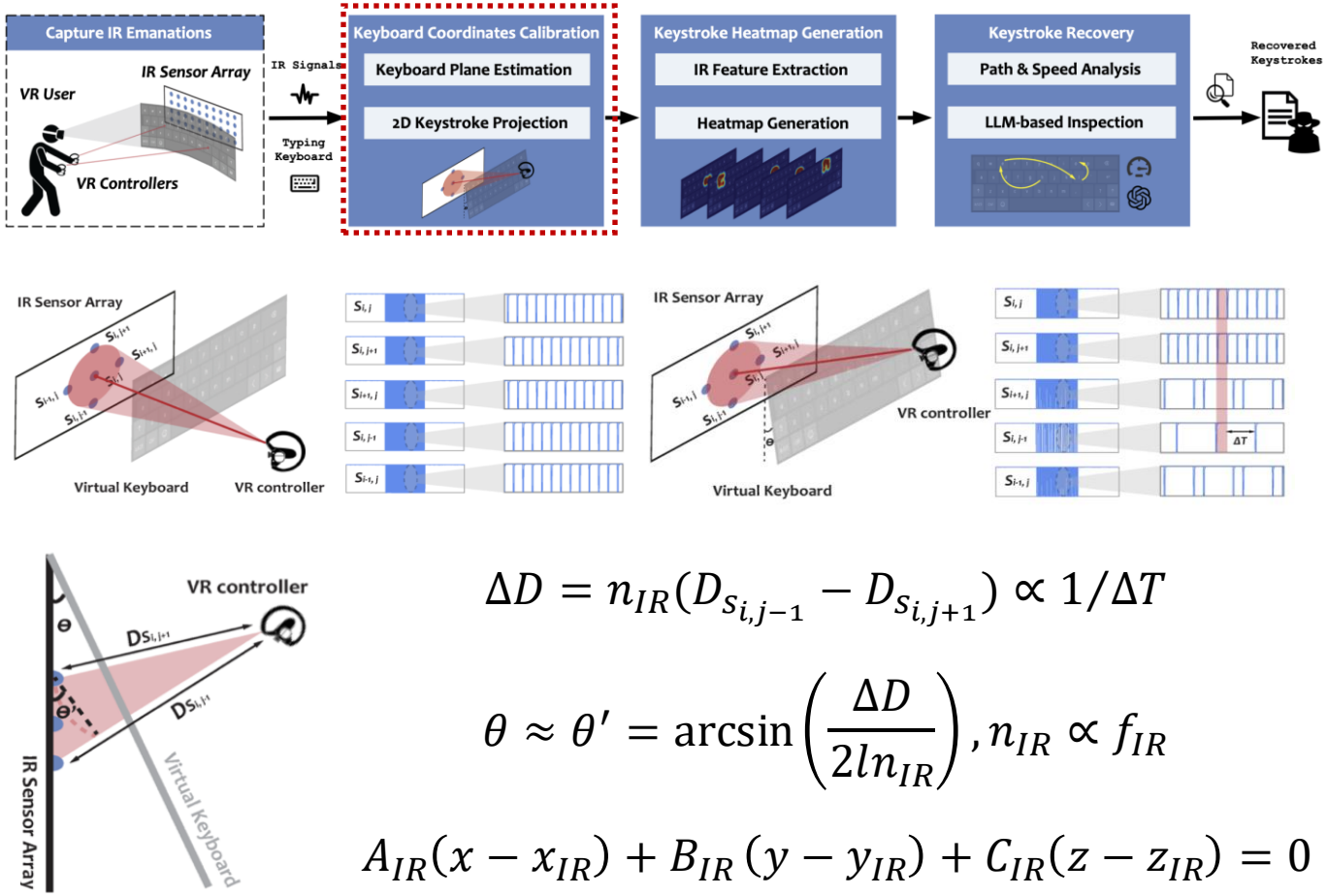
Keyboard Coordinates Calibration

- **Keyboard Plane Estimation:** Use variations in response times of IR signals captured by multiple IR sensors to obtain the orientation angle θ



Keyboard Coordinates Calibration

- **Keyboard Plane Estimation:** Use variations in response times of IR signals captured by multiple IR sensors to obtain the orientation angle θ
- **2D Keystroke Projection:** Project typed keystrokes from the IR sensor array plane to the virtual keyboard plane for coordinate calibration.



$$\Delta D = n_{IR}(D_{S_{i,j-1}} - D_{S_{i,j+1}}) \propto 1/\Delta T$$

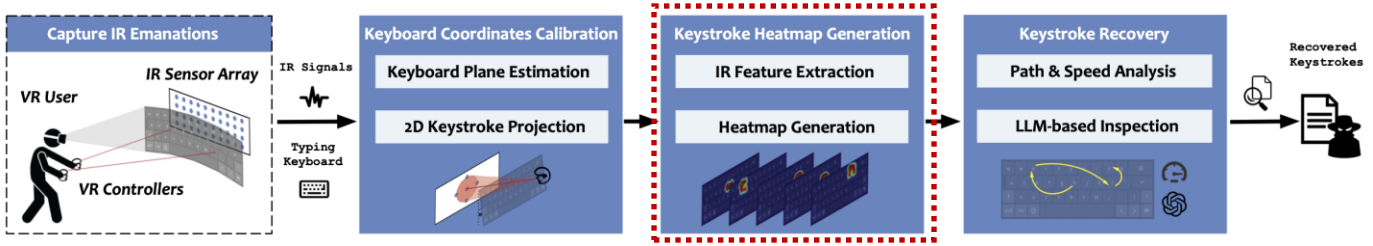
$$\theta \approx \theta' = \arcsin\left(\frac{\Delta D}{2ln_{IR}}\right), n_{IR} \propto f_{IR}$$

$$A_{IR}(x - x_{IR}) + B_{IR}(y - y_{IR}) + C_{IR}(z - z_{IR}) = 0$$

Keystroke Heatmap Generation

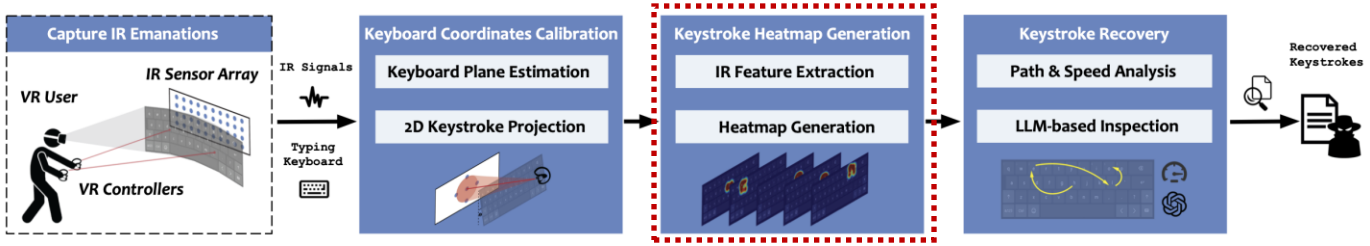
Keystroke Heatmap Generation

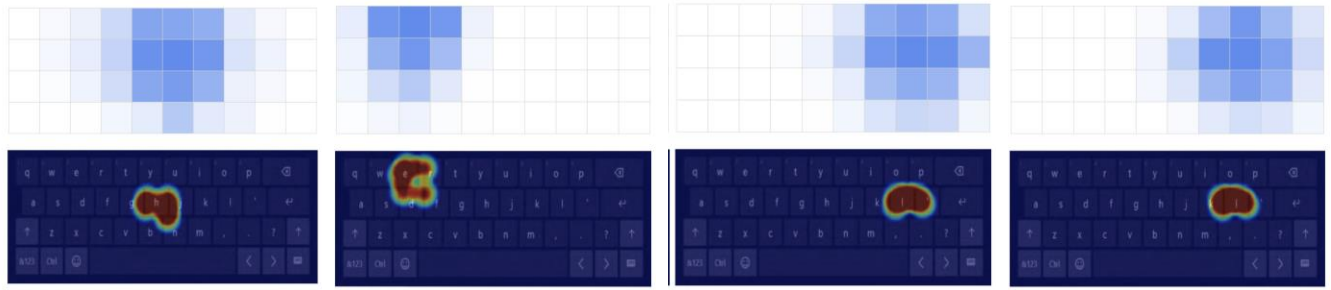
- **IR Feature Extraction:** Time-domain and Frequency-domain features to describe the typing points and durations



Keystroke Heatmap Generation

- **IR Feature Extraction:** Time-domain and Frequency-domain features to describe the typing points and durations
- **Heatmap Generation:** Generate weight-based confusion matrices and overlay heatmaps to determine the typed virtual keystrokes with data visualization algorithms (e.g., OpenCV).

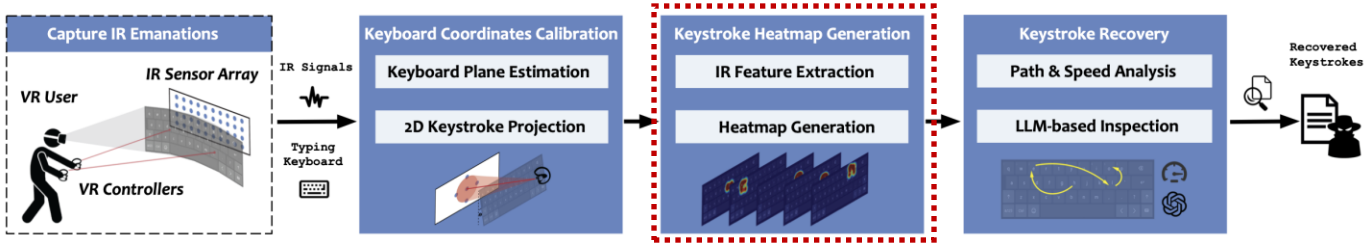


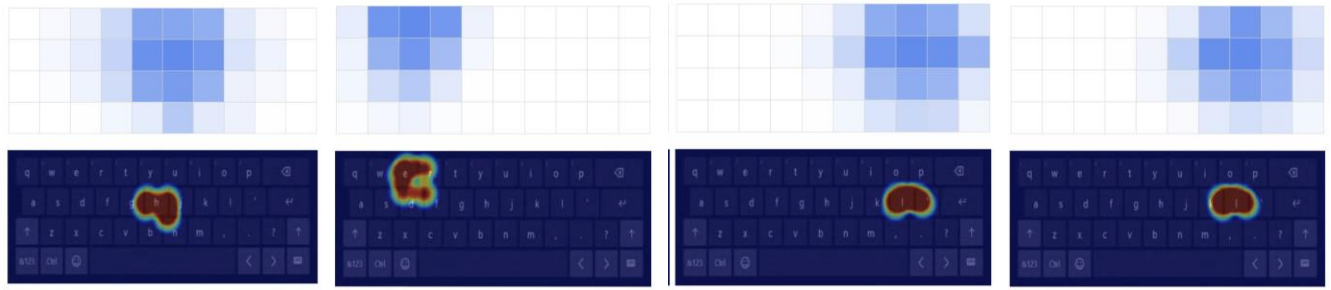


Mapping function: $(x_i, y_i) = \mathcal{M}(\Sigma\alpha_i f_{t_i} + \Sigma\beta_j f_{f_j})$

Keystroke Heatmap Generation

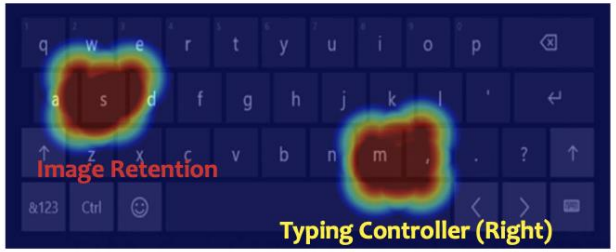
- **IR Feature Extraction:** Time-domain and Frequency-domain features to describe the typing points and durations
- **Heatmap Generation:** Generate weight-based confusion matrices and overlay heatmaps to determine the typed virtual keystrokes with data visualization algorithms (e.g., OpenCV).





Mapping function: $(x_i, y_i) = \mathcal{M}(\Sigma\alpha_i f_{t_i} + \Sigma\beta_j f_{f_j})$

Time t

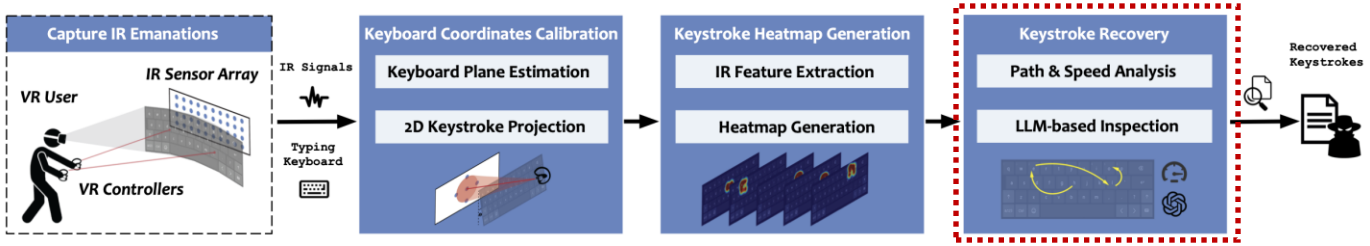


Time $t + \Delta t$

Keystroke Recovery

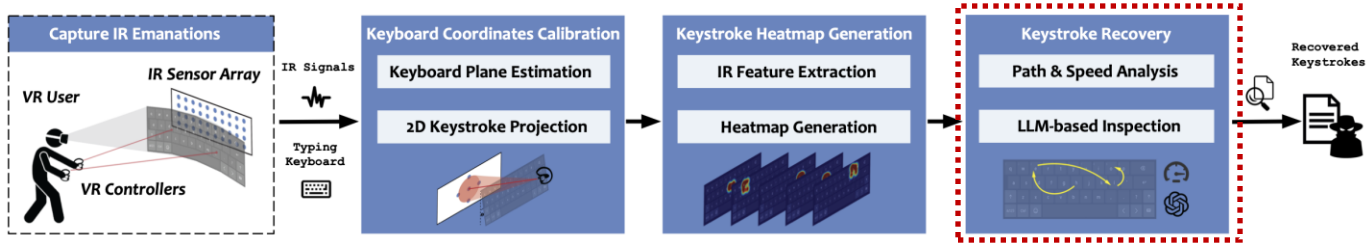
Keystroke Recovery

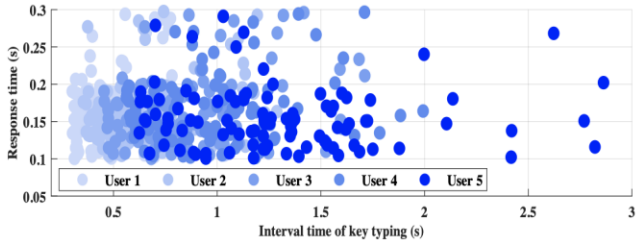
- **Typing Path & Speed Analysis:** Analyze the typing speed and reconstruct the typing path for unconstrained keystroke recovery



Keystroke Recovery

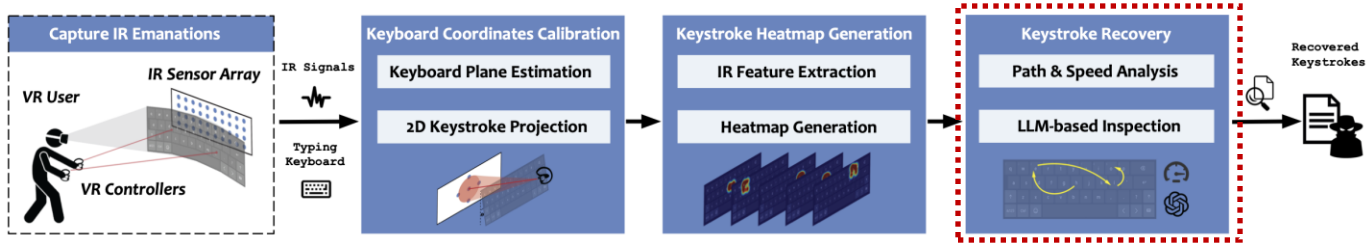
- **Typing Path & Speed Analysis:** Analyze the typing speed and reconstruct the typing path for unconstrained keystroke recovery

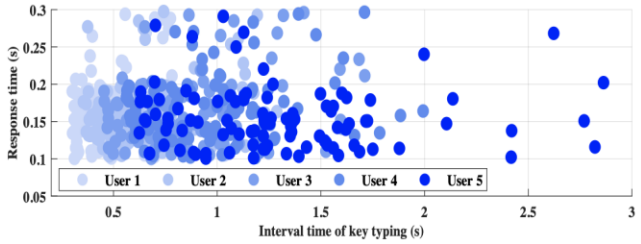


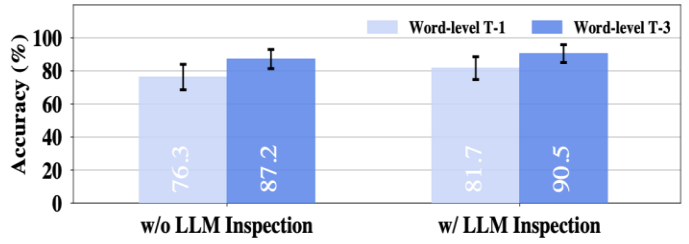


Keystroke Recovery

- **Typing Path & Speed Analysis:** Analyze the typing speed and reconstruct the typing path for unconstrained keystroke recovery
- **LLM-based Inspections:** Leverage a zero-shot prompt in LLMs to inspect the semantics and grammar of the reconstructed keystrokes



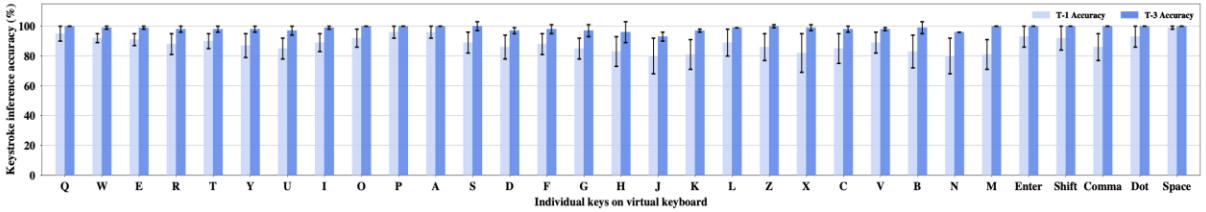


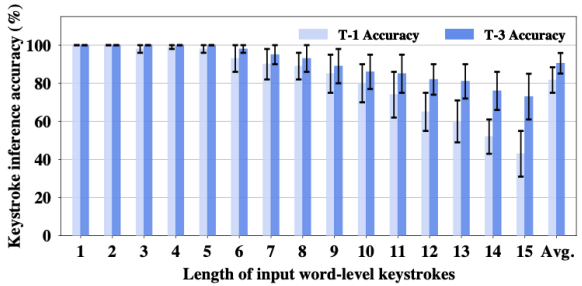


Effectiveness Evaluation

Effectiveness Evaluation

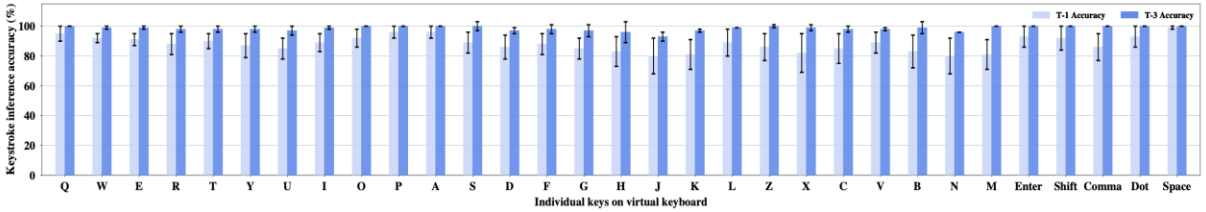
- Character-level and word-level virtual keystroke inference

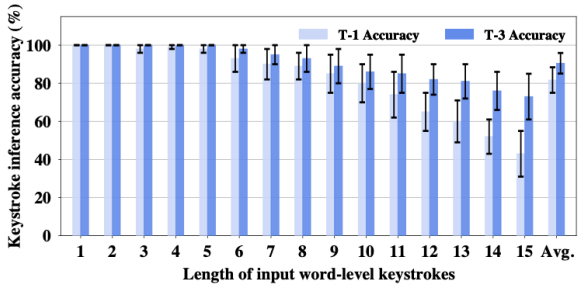


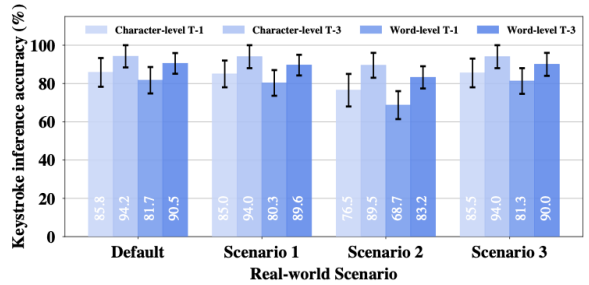


Effectiveness Evaluation

- Character-level and word-level virtual keystroke inference
- Effectiveness in three real-world attack scenarios

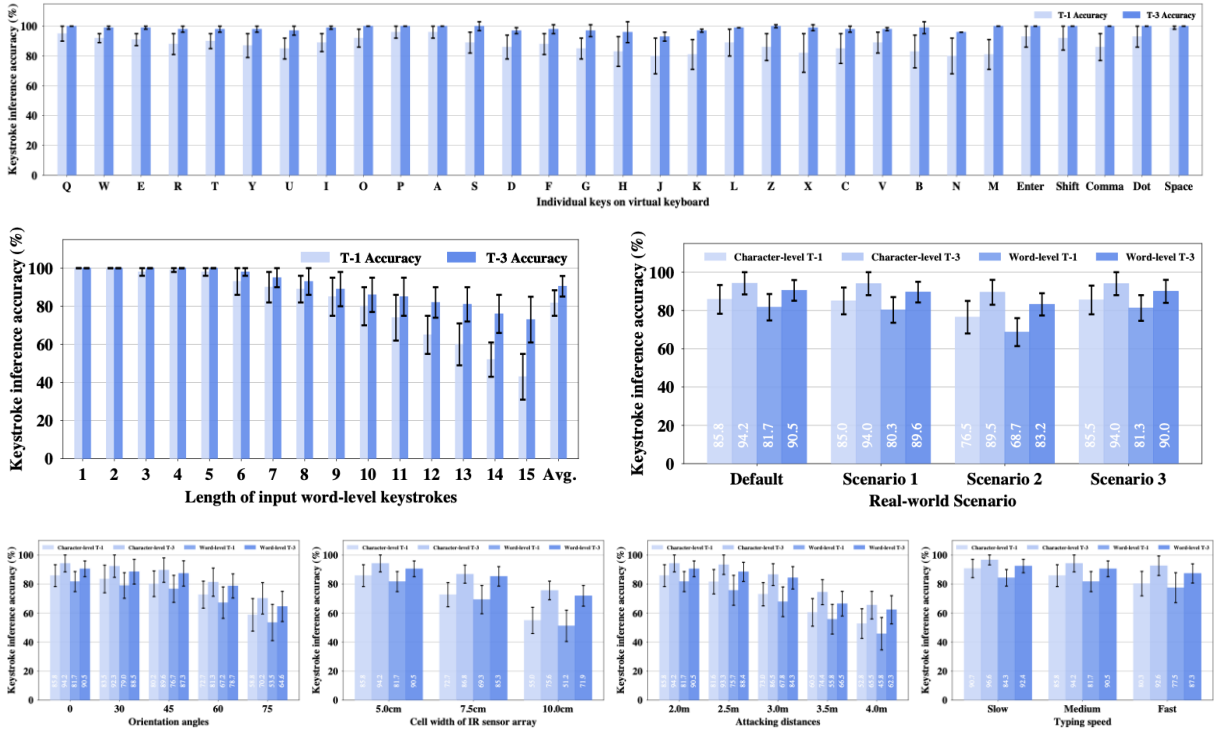






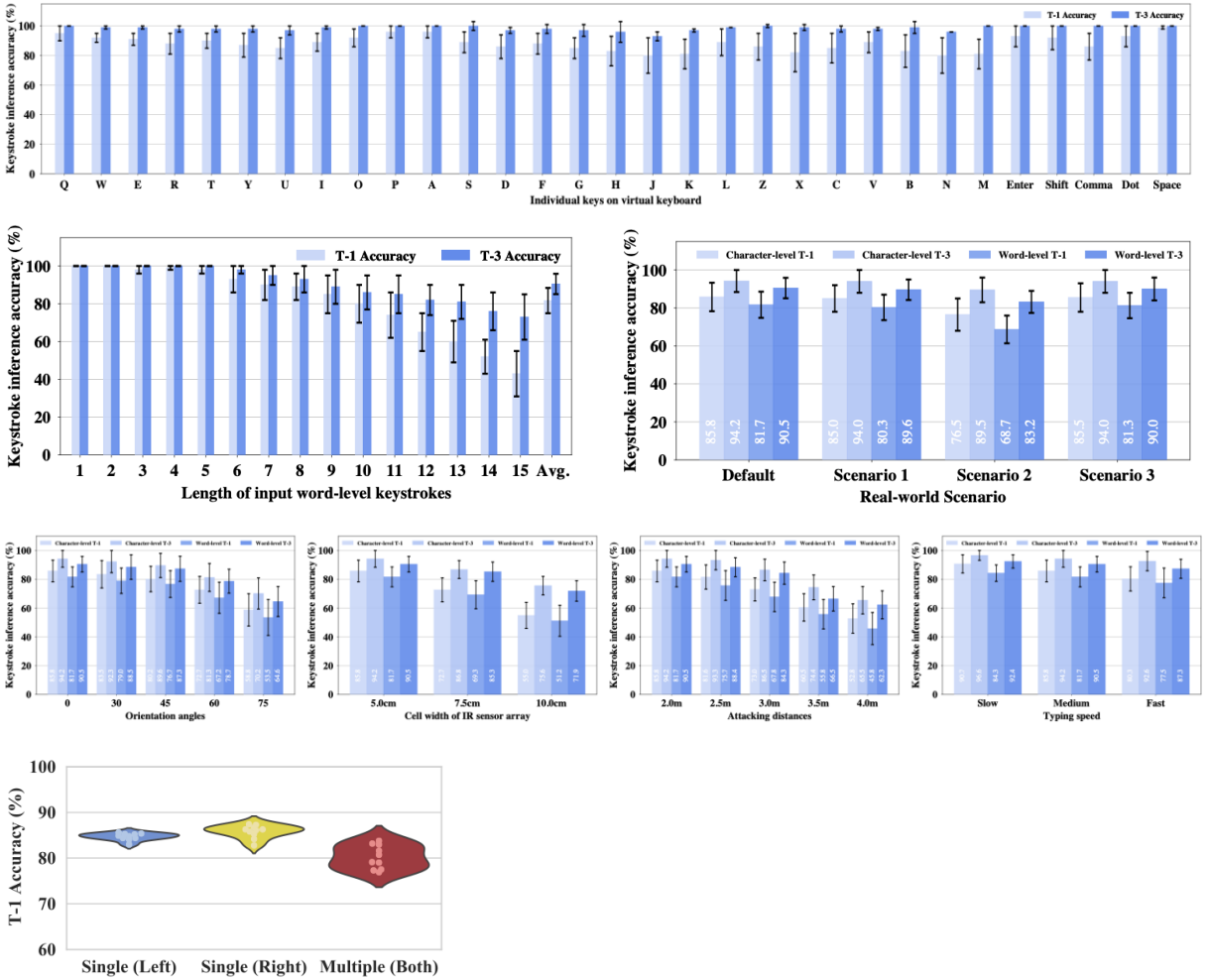
Effectiveness Evaluation

- Character-level and word-level virtual keystroke inference
- Effectiveness in three real-world attack scenarios
- Robustness to the impact of different external conditions



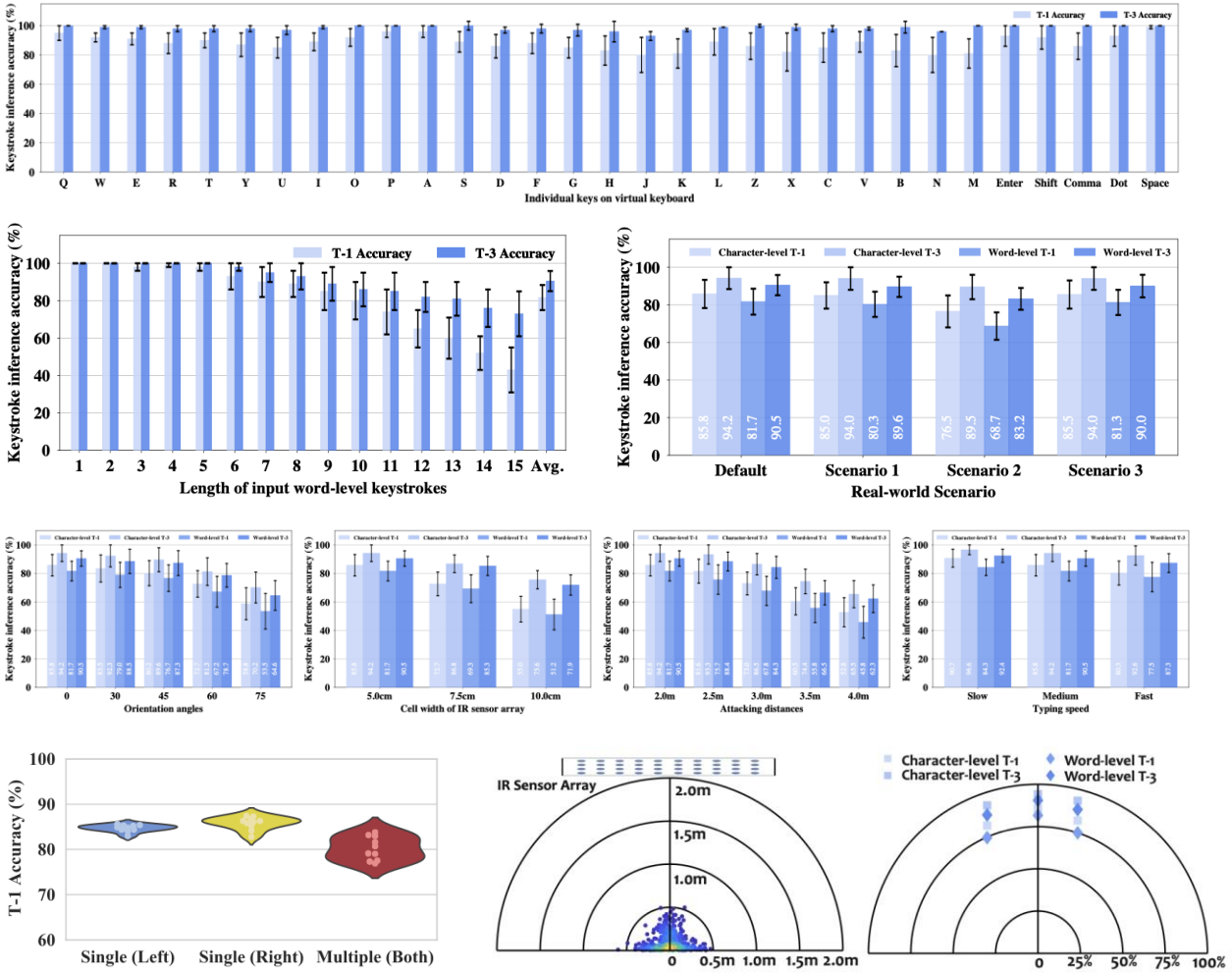
Effectiveness Evaluation

- Character-level and word-level virtual keystroke inference
- Effectiveness in three real-world attack scenarios
- Robustness to the impact of different external conditions
- Single- and multi-source keystroke inference



Effectiveness Evaluation

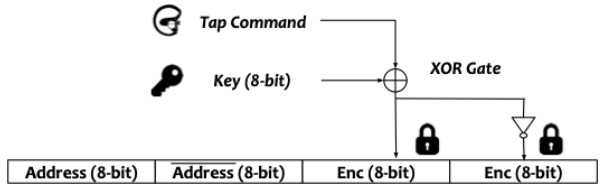
- Character-level and word-level virtual keystroke inference
- Effectiveness in three real-world attack scenarios
- Robustness to the impact of different external conditions
- Single- and multi-source keystroke inference
- User movements evaluations

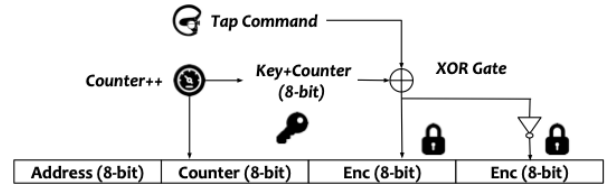


Countermeasures

Countermeasures

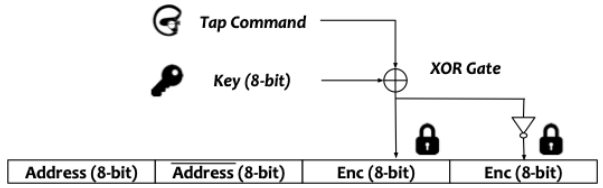
- **IR Encryption:** Redesign the IR communication protocol to incorporate encryption and modify IR patterns

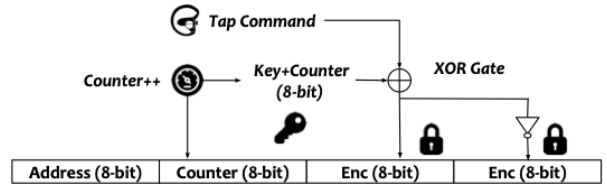


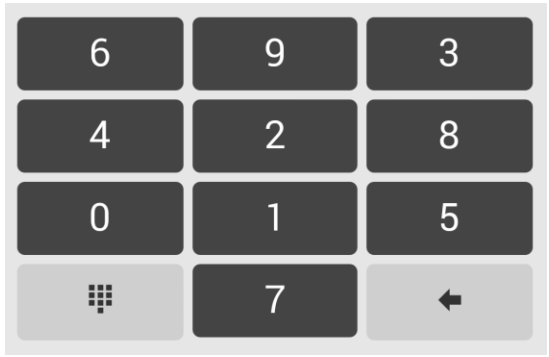


Countermeasures

- **IR Encryption:** Redesign the IR communication protocol to incorporate encryption and modify IR patterns
- **Shuffling Keyboards:** Signal masking by changing the layout of virtual keyboards in specific interfaces (e.g., bank accounts and passwords)







Conclusion

Conclusion

- An orthogonal, non-intrusive, unconstrained, and model-free side-channel attack to infer virtual keystrokes at character- and word-level

Related VR Attacks	Attack Surface	Side Channel	NI	NPC	WMI	UKI	Distance	Character Level	Word Level
TyPose [1]	Motion sensors in VR headset	Malware	○	◐	○	○	–	○	◐ (82.0% T-5)
Zhang *et al.* [2]	Motion sensors in VR headset	Malware	○	◐	○	○	–	◐ (93.8% T-1)	○
Wu *et al.* [3]	Motion sensors in VR headset	Malware	○	◐	○	○	–	● (89.7% T-1)	● (84.9% T-3)
HoloLogger [4]	Motion sensors in VR headset	Malware	○	◐	●	●	–	● (73.0% T-1)	● (89.0% T-3)
VR-Spy [5]	Wi-Fi channel state data	Wi-Fi CSI data	●	○	○	○	1.3m	● (69.8% T-1)	○
Meteriz-Yıldıran *et al.* [6]	Users' hand gestures	Hand tracker/Camera	●	◐	○	○	0.6–0.8m	● (99.0% T-1)	● (87.0% T-5)
Su *et al.* [7]	Unencrypted Photon protocol	Network traffic	◐	●	○	●	–	● (97.6% T-1)	● (98.1% T-3)
GAZEploit [8]	Video of users' virtual avatars	Gaze information	◐	●	○	●	–	● (38.7% T-1)	● (85.9% T-5)
Gopal *et al.* [9]	Video of VR users' gestures	Camera	●	◐	●	○	3.0–6.0m	● (82.3% T-1)	● (57.0% T-3)
Heimdall [10]	Sound from VR controllers	Acoustic signal	●	◐	○	○	1.0–2.2m	● (96.5% T-1)	● (91.2% T-5)
VRecKey	IR signals from VR controllers	IR signal	●	◐	●	●	2.0–4.0m	● (85.8% T-1)	● (90.5% T-3)

Conclusion

- An orthogonal, non-intrusive, unconstrained, and model-free side-channel attack to infer virtual keystrokes at character- and word-level
- Effective in most VR devices that support constellation tracking systems, except Apple Vision Pro which adopts 100% hand-tracking

VR Devices	Hand Controllers?	Constellation?	Hand-tracking?
Meta Oculus Quest 2	●	●	●
PICO 4 All-in-One	●	●	●
HTC Vive Pro 2	●	●	●
Sony PlayStation VR 2	●	○	○
Meta Oculus Quest Pro	●	●	●
Meta Oculus Quest 3	●	●	●
Valve Index	●	●	○
HP WMR Headset	●	●	○
Dell Visor	●	○	○
Apple Vision Pro	○	○	●

Related VR Attacks	Attack Surface	Side Channel	NI	NPC	WMI	UKI	Distance	Character Level	Word Level
TyPose [1]	Motion sensors in VR headset	Malware	○	◐	○	○	–	○	◐ (82.0% T-5)
Zhang *et al.* [2]	Motion sensors in VR headset	Malware	○	◐	○	○	–	◐ (93.8% T-1)	○
Wu *et al.* [3]	Motion sensors in VR headset	Malware	○	◐	○	○	–	● (89.7% T-1)	● (84.9% T-3)
HoloLogger [4]	Motion sensors in VR headset	Malware	○	◐	●	●	–	● (73.0% T-1)	● (89.0% T-3)
VR-Spy [5]	Wi-Fi channel state data	Wi-Fi CSI data	●	○	○	○	1.3m	● (69.8% T-1)	○
Meteriz-Yıldıran *et al.* [6]	Users' hand gestures	Hand tracker/Camera	●	◐	○	○	0.6–0.8m	● (99.0% T-1)	● (87.0% T-5)
Su *et al.* [7]	Unencrypted Photon protocol	Network traffic	◐	●	○	●	–	● (97.6% T-1)	● (98.1% T-3)
GAZEploit [8]	Video of users' virtual avatars	Gaze information	◐	●	○	●	–	● (38.7% T-1)	● (85.9% T-5)
Gopal *et al.* [9]	Video of VR users' gestures	Camera	●	◐	●	○	3.0–6.0m	● (82.3% T-1)	● (57.0% T-3)
Heimdall [10]	Sound from VR controllers	Acoustic signal	●	◐	○	○	1.0–2.2m	● (96.5% T-1)	● (91.2% T-5)
VRecKey	IR signals from VR controllers	IR signal	●	◐	●	●	2.0–4.0m	● (85.8% T-1)	● (90.5% T-3)

Non-intrusive and Unconstrained Keystroke Inference in VR Platforms via Infrared Side Channel

Thank you for Listening!

Q&A

Tao Ni, Yuefeng Du, Qingchuan Zhao, Cong Wang

Department of Computer Science, City University of Hong Kong

Non-intrusive and Unconstrained Keystroke Inference in VR Platforms via Infrared Side Channel

Thank you for Listening!

Q&A

I'm on the job market now.
Feel free to reach out.

Tao Ni, Yuefeng Du, Qingchuan Zhao, Cong Wang

Department of Computer Science, City University of Hong Kong