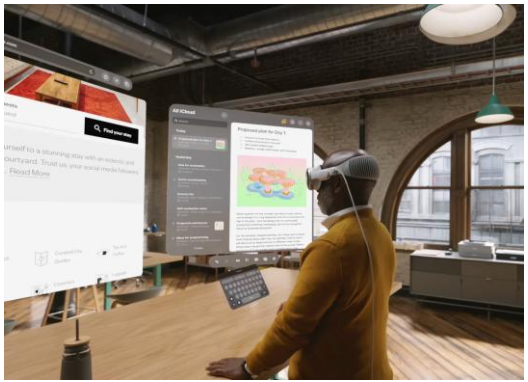
XR Devices Send WiFi Packets When They Should Not: Cross-Building Keylogging Attacks via Non-Cooperative Wireless Sensing

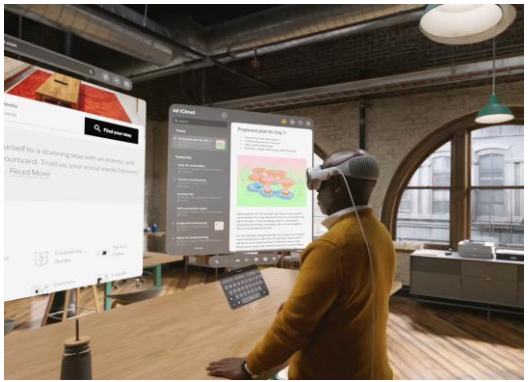
Christopher Vattheuer, **Justin Feng**, Hossein Khalili, Nader Sehatbakhsh, Omid Abari

University of California, Los Angeles

VR Headsets are Ubiquitous

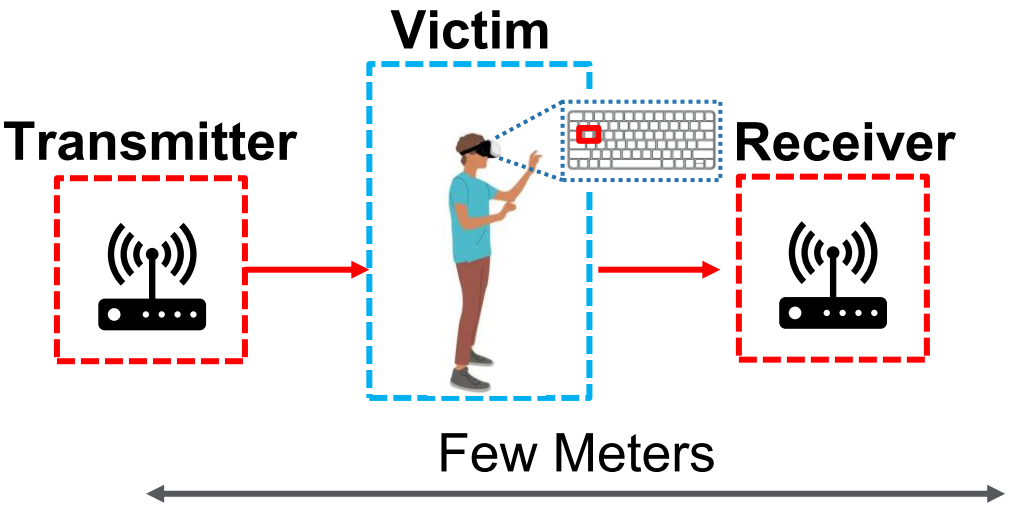


VR Headsets are Ubiquitous



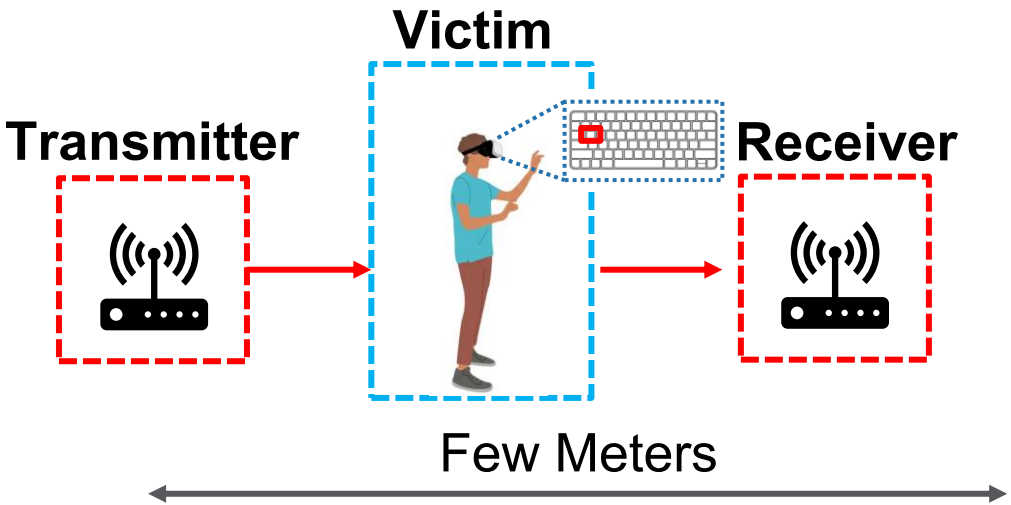
While VR is popular, they are also vulnerable to keylogging attacks.

Prior Attacks



Modality	Limitations
Malware [1]	Requires access, No NLOS, short range
Camera [2]	No NLOS, short range
RF [3]	Short range, difficulty adapting to environment

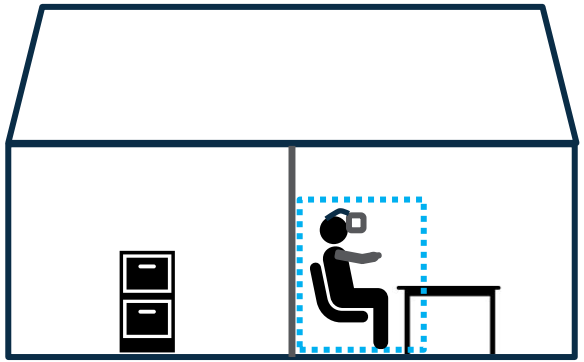
Prior Attacks

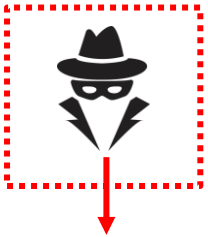


Modality	Limitations
Malware [1]	Requires access, No NLOS, short range
Camera [2]	No NLOS, short range
RF [3]	Short range, difficulty adapting to environment

Prior works have limitations that limit the practicality of the attack.

Our Work: TwiST

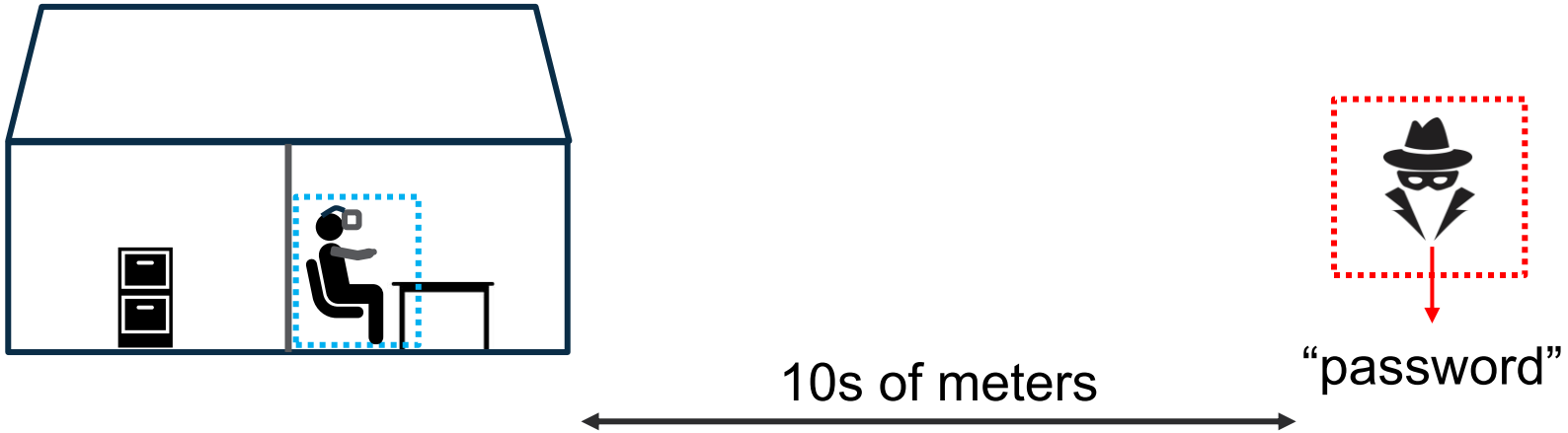




10s of meters

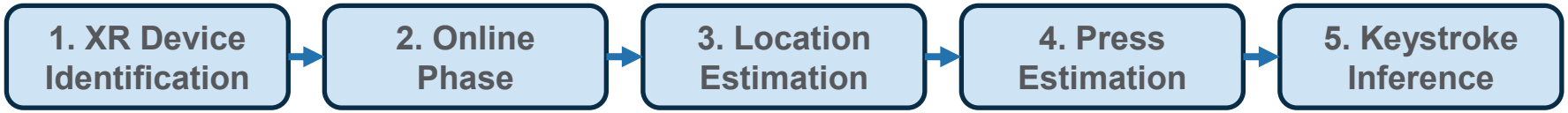
“password”

Our Work: TwiST



Our attack, “TwiST”, overcomes the limitations of prior works and enables VR keylogging at long range.

Attack Steps: TwiST



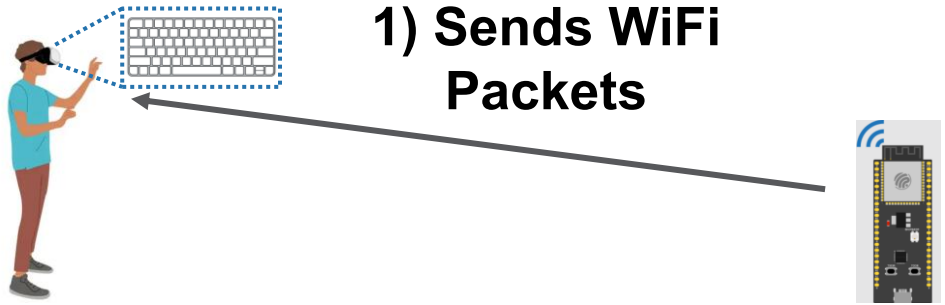
Attack Steps: TwiST

1. XR Device Identification
2. Online Phase
3. Location Estimation
4. Press Estimation
5. Keystroke Inference

1) Find MAC Address
2) Derandomize (if necessary)

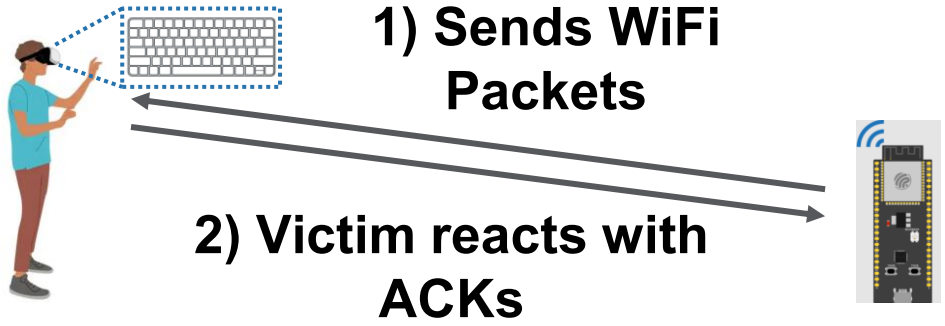
Attack Steps: TwiST

1. XR Device Identification	2. Online Phase	3. Location Estimation	4. Press Estimation	5. Keystroke Inference



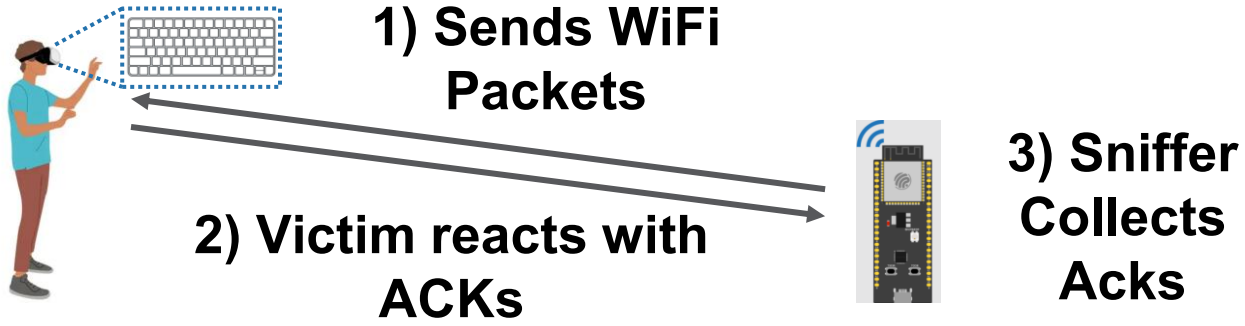
Attack Steps: TwiST

1. XR Device Identification	2. Online Phase	3. Location Estimation	4. Press Estimation	5. Keystroke Inference

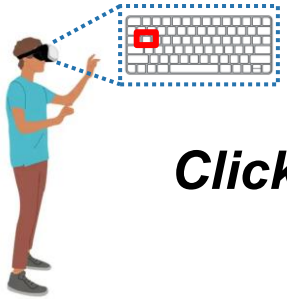


Attack Steps: TwiST

1. XR Device Identification
2. Online Phase
3. Location Estimation
4. Press Estimation
5. Keystroke Inference

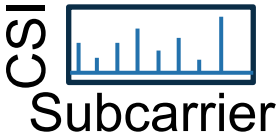


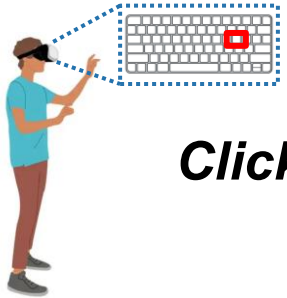
Presses Correlate to CSI Changes



Click "Q"

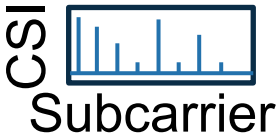
"q"



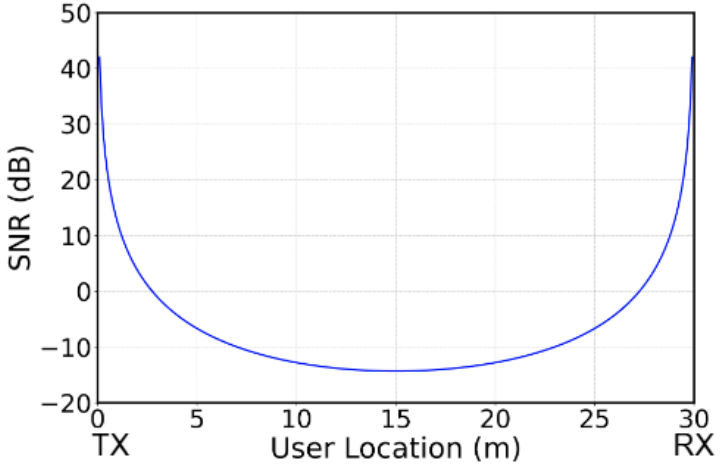


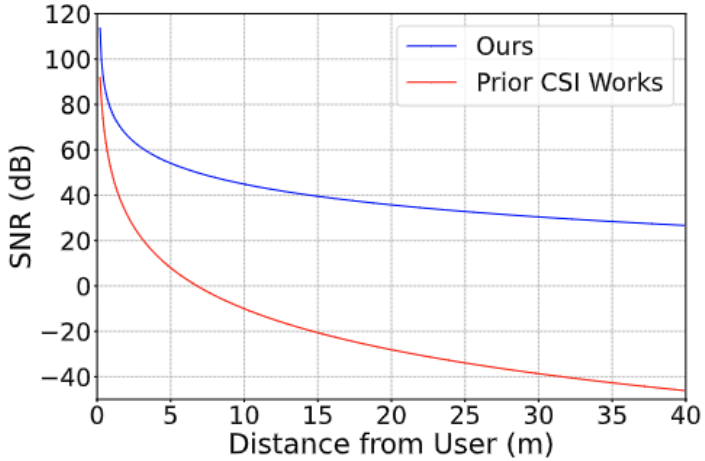
Click "P"

"p"

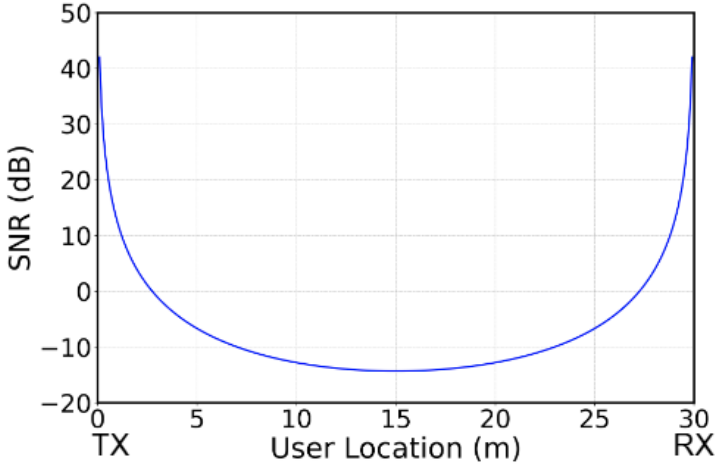


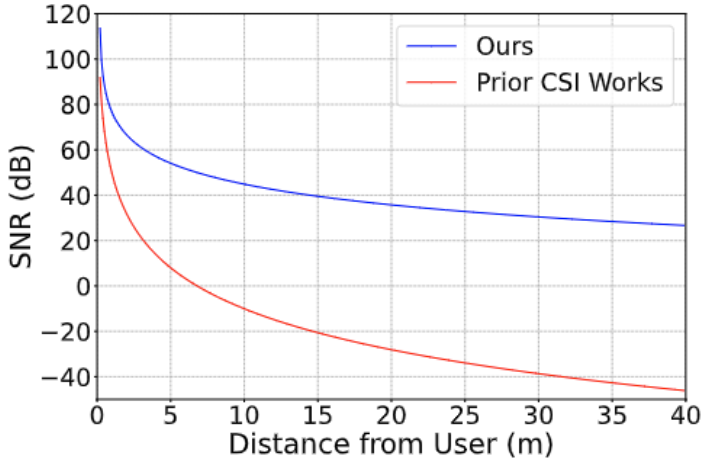
Victim Headset as Involuntary Transmitter





Victim Headset as Involuntary Transmitter





Utilizing a collocated Tx and Rx setup and turning the victim headset into an involuntary transmitter increases the SNR of the victim signal.

Attack Steps: TwiST

1. XR Device Identification
2. Online Phase
3. Location Estimation
4. Press Estimation
5. Keystroke Inference

CSI

[0.8,0.6,…]

Attack Steps: TwiST

1. XR Device Identification
2. Online Phase
3. Location Estimation
4. Press Estimation
5. Keystroke Inference

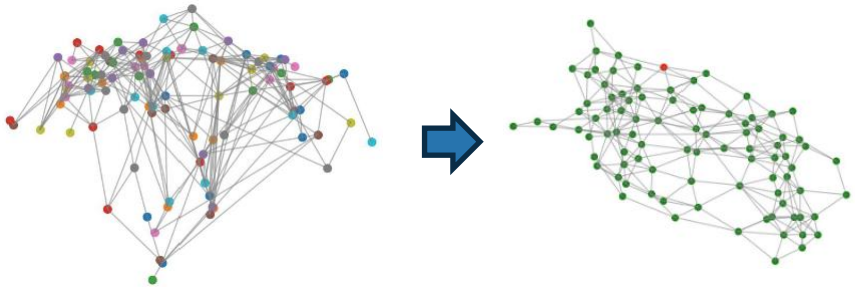
CSI **Clusters and Graph**

[0.8,0.6,…] ➡

Attack Steps: TwiST

1. XR Device Identification
2. Online Phase
3. Location Estimation
4. Press Estimation
5. Keystroke Inference

CSI **Clusters and Graph** **Projection**

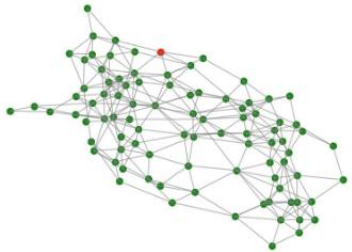
[0.8,0.6,…] 

Attack Steps: TwiST

1. XR Device Identification
2. Online Phase
3. Location Estimation
4. Press Estimation
5. Keystroke Inference

CSI → Clusters and Graph → Projection → Transformation

[0.8,0.6,…]



Attack Steps: TwiST

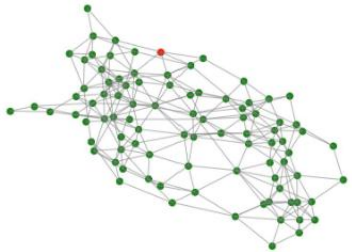
1. XR Device Identification
2. Online Phase
3. Location Estimation
4. Press Estimation
5. Keystroke Inference

CSI

[0.8,0.6,…]

Clusters and Graph

Projection

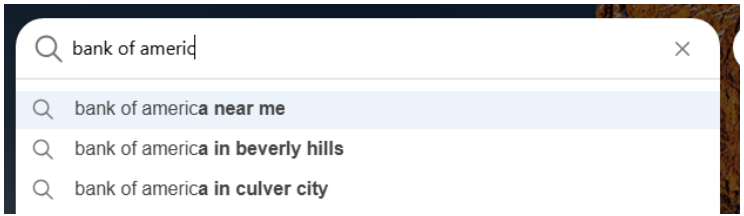


Transformation

Aggregate

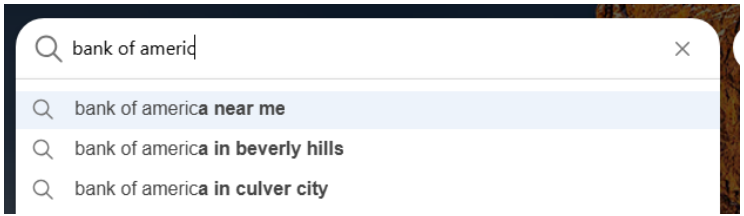
Attack Steps: TwiST

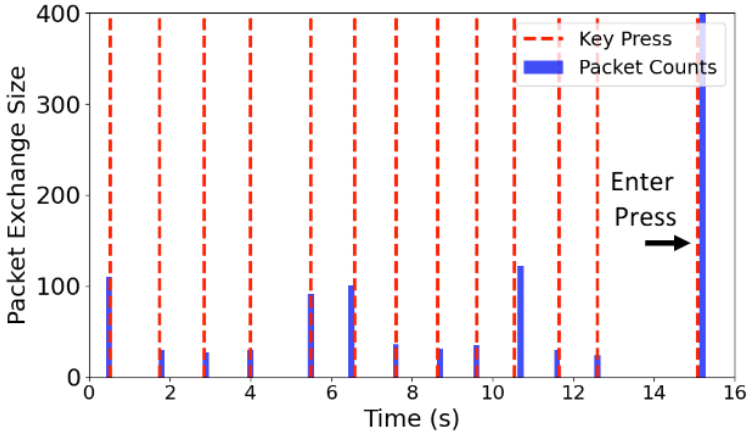
1. XR Device Identification
2. Online Phase
3. Location Estimation
4. Press Estimation
5. Keystroke Inference



Attack Steps: TwiST

1. XR Device Identification
2. Online Phase
3. Location Estimation
4. Press Estimation
5. Keystroke Inference





Attack Steps: TwiST

1. XR Device Identification
2. Online Phase
3. Location Estimation
4. Press Estimation
5. Keystroke Inference

Option 1: Uniform Key Estimation

1. H
2. G, J, Y, U, B, N

Attack Steps: TwiST

1. XR Device Identification
2. Online Phase
3. Location Estimation
4. Press Estimation
5. Keystroke Inference

Option 1: Uniform Key Estimation

1. H
2. G, J, Y, U, B, N

Option 2: Dictionary-Aided Word Ranking

Dictionary
"HI"
5.0+2.1=7.1

Setup

Setup

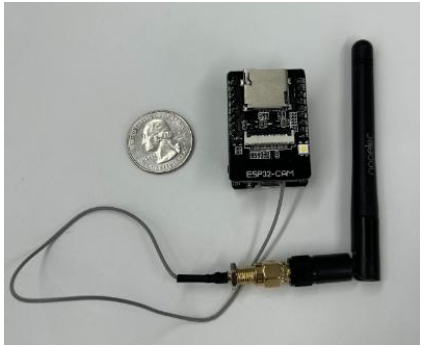


TABLE I: Conditions for each experiment type.

Experiment Type	Conditions
Baseline	1m
Distance	1m, 2m, 4m, 10m
Angle	1m: -90°, -45°, 0°, 45°, 90°
Through Wall	1m: -90°, -45°, 0°, 45°, 90°
Indoor Extreme	8m NLOS through wall
Cross Building	30m
New User and Headset	1m: LOS and NLOS

Setup

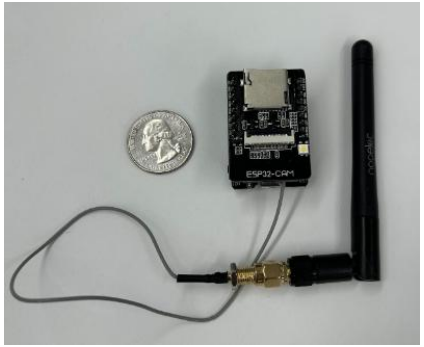
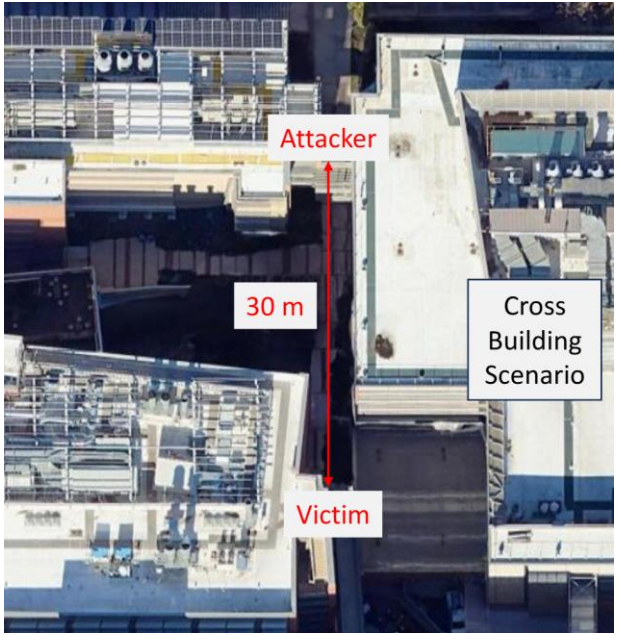
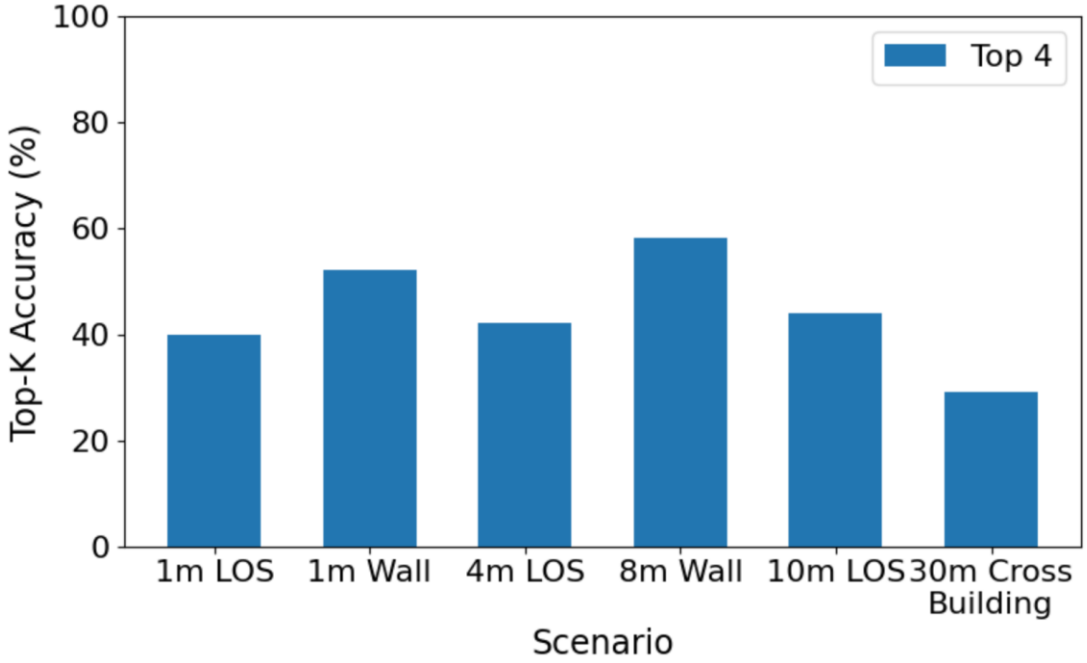


TABLE I: Conditions for each experiment type.

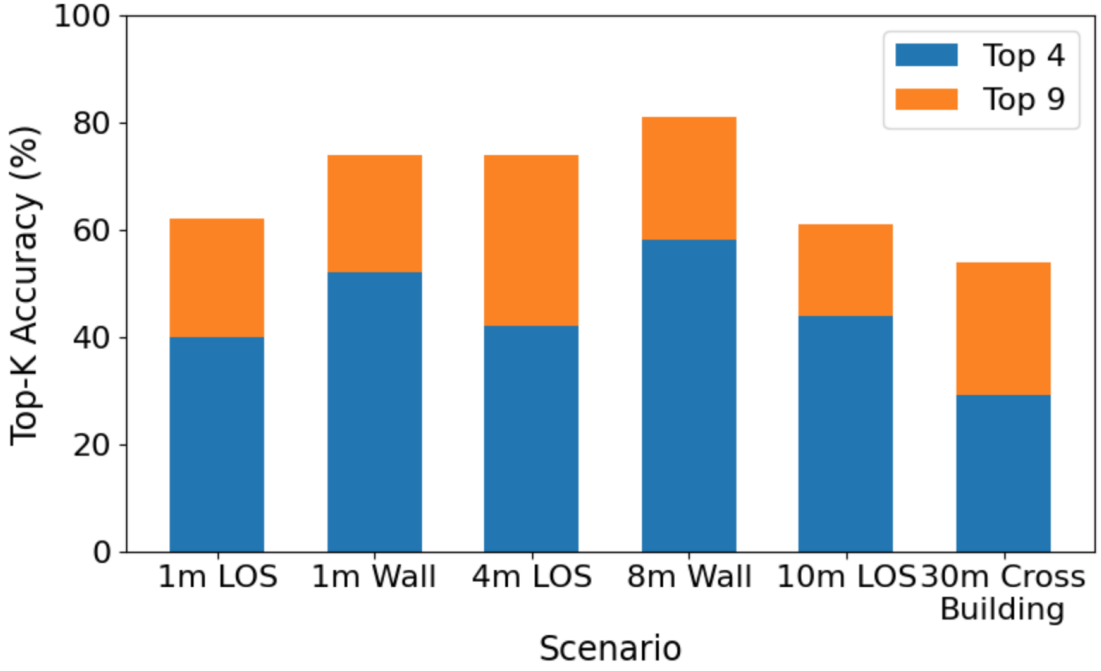
Experiment Type	Conditions
Baseline	1m
Distance	1m, 2m, 4m, 10m
Angle	1m: -90°, -45°, 0°, 45°, 90°
Through Wall	1m: -90°, -45°, 0°, 45°, 90°
Indoor Extreme	8m NLOS through wall
Cross Building	30m
New User and Headset	1m: LOS and NLOS



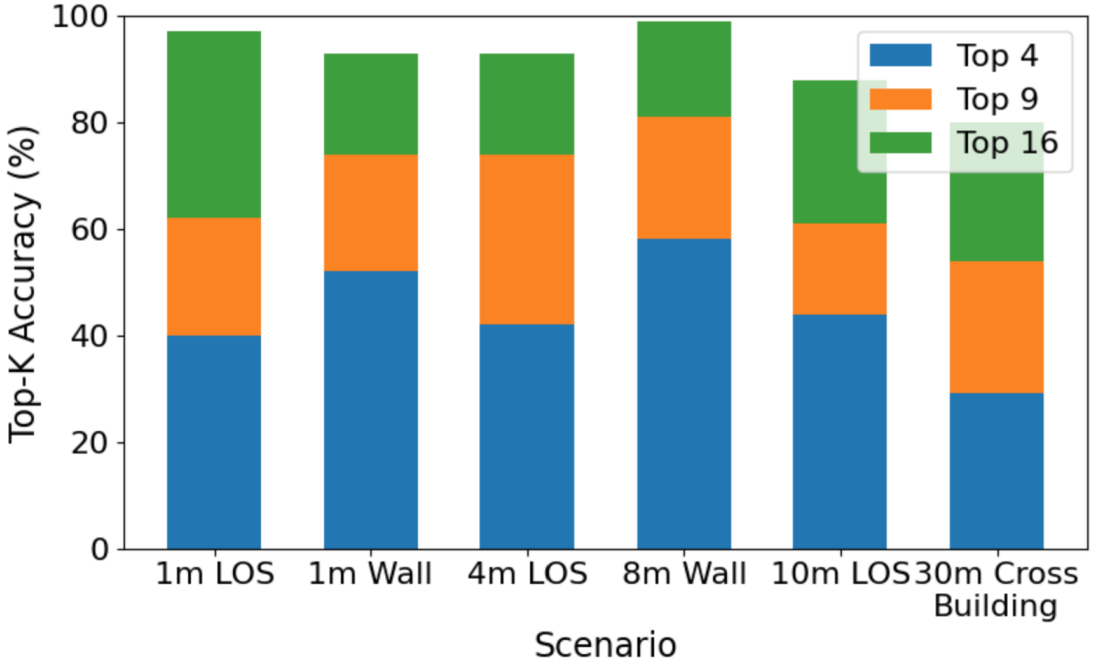
Results: Different Environment



Results: Different Environment

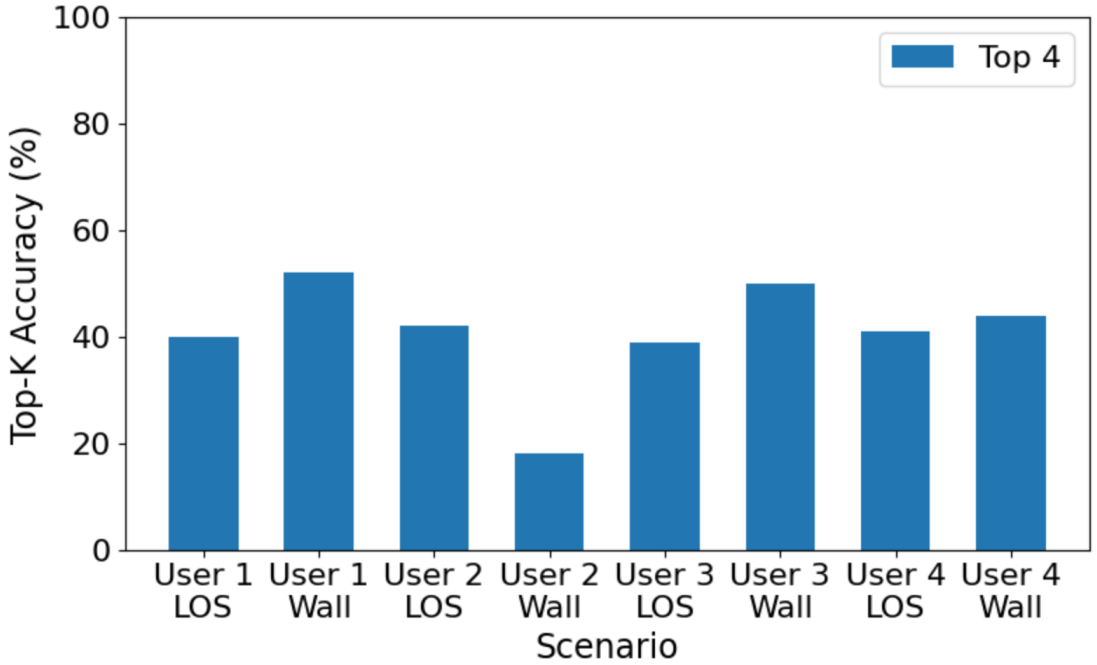


Results: Different Environment

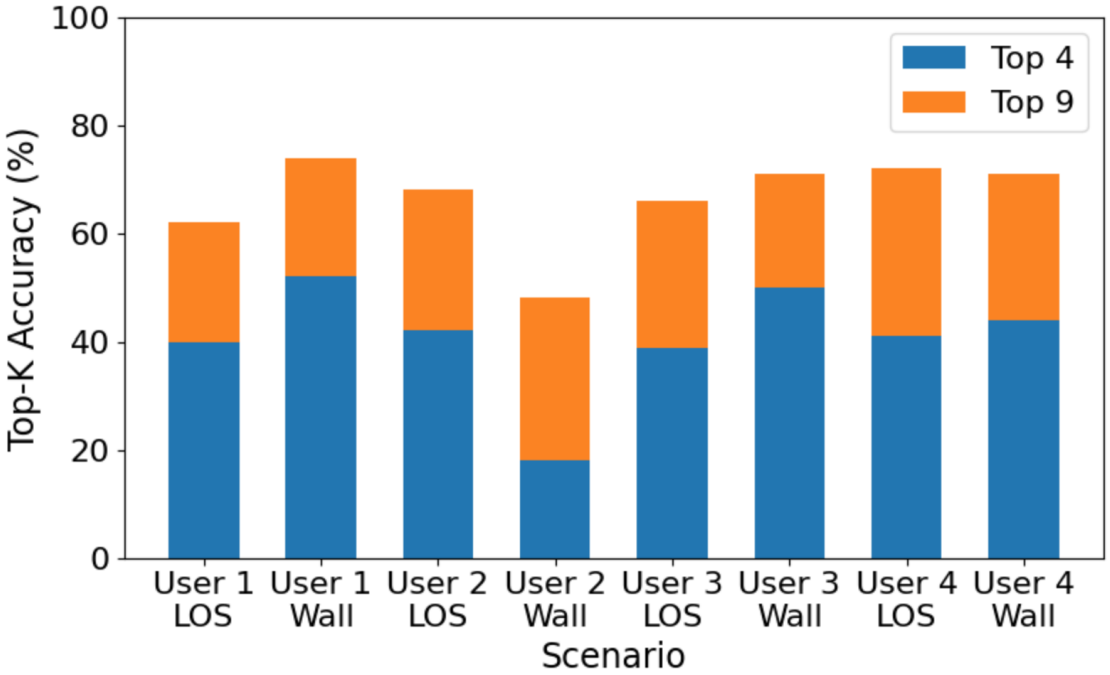


TwiST works across different environments.

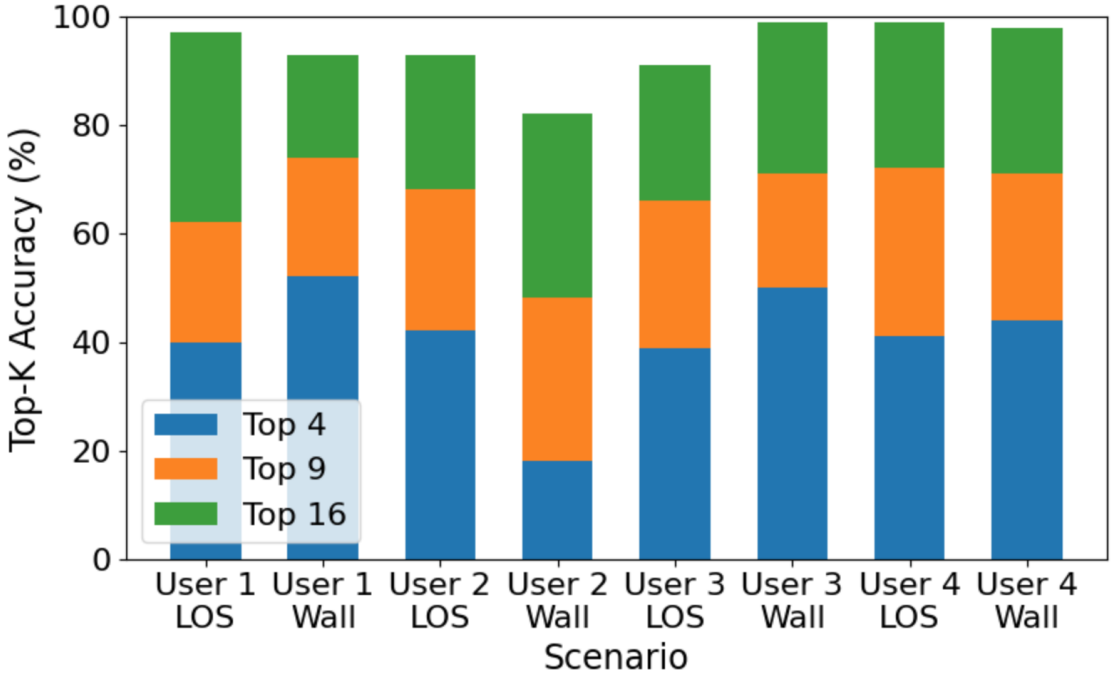
Results: Different Users



Results: Different Users

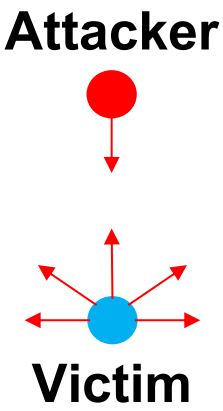


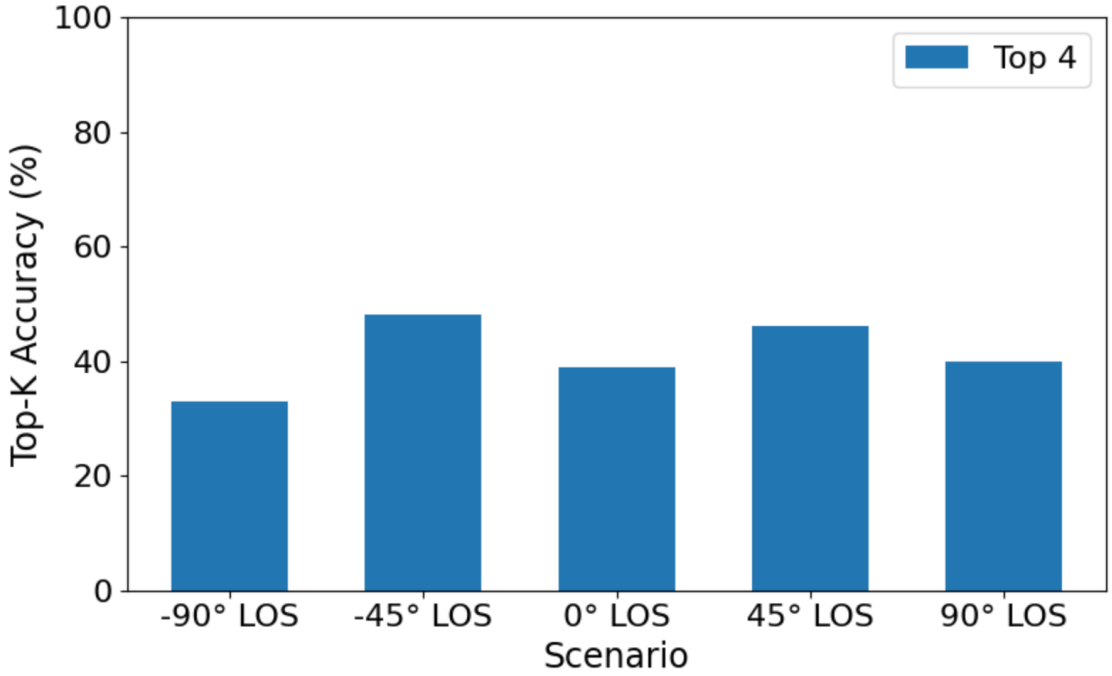
Results: Different Users



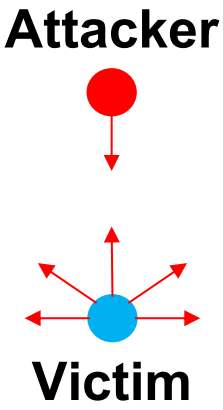
TwiST translates to different users.

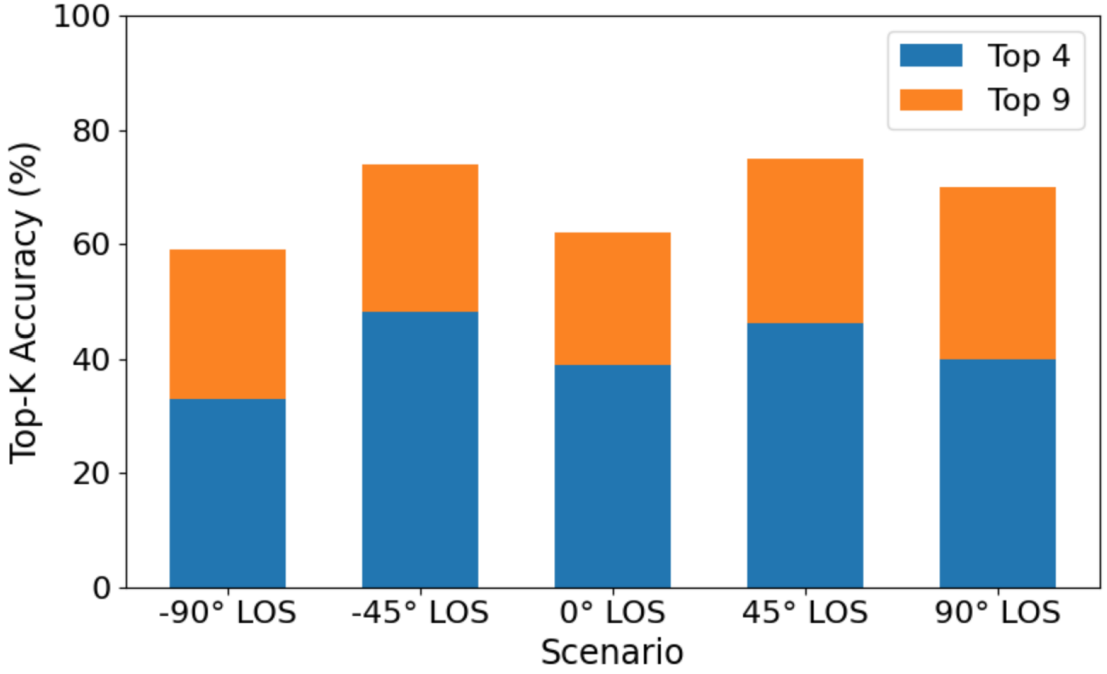
Results: Different Angles



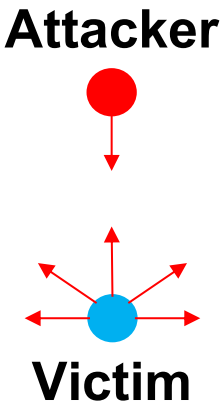


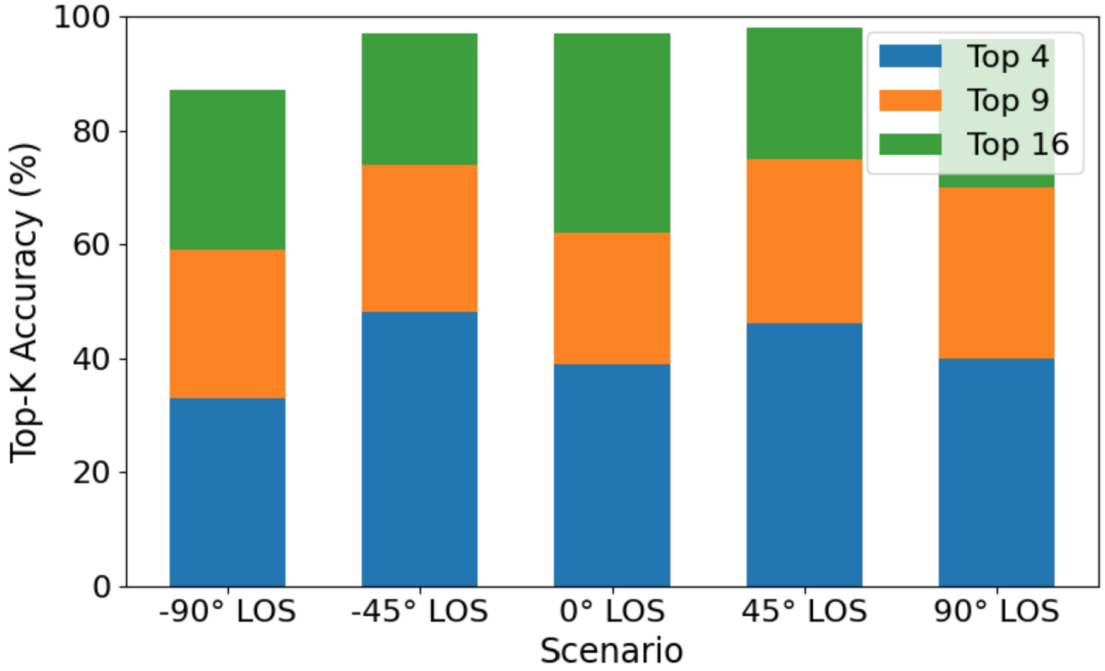
Results: Different Angles





Results: Different Angles

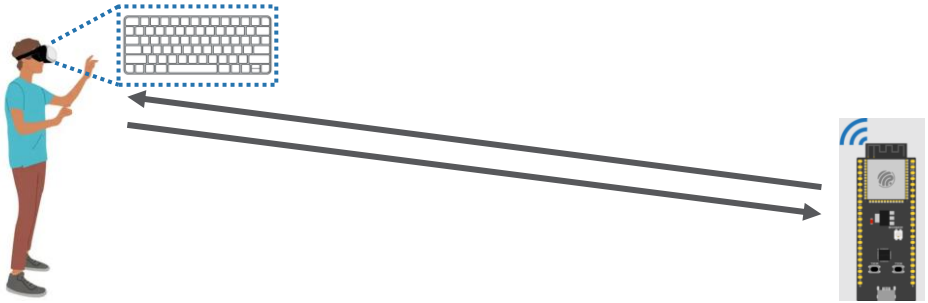




TwiST is robust to orientation.

Conclusion

XR keylogging can be done using non-cooperative WiFi sensing at long range. Works in LoS, through-wall, and 30m cross-building settings with low-cost hardware.



References

[1] C. Slocum, Y. Zhang, N. Abu-Ghazaleh, and J. Chen, “Going through the motions: {AR/VR} keylogging from user head motions,” in 32nd USENIX Security Symposium (USENIX Security 23), 2023, pp. 159–174.
[2] S. R. K. Gopal, D. Shukla, J. D. Wheelock, and N. Saxena, “Hidden reality: Caution, your hand gesture inputs in the immersive virtual world are visible to all!” in 32nd USENIX Security Symposium (USENIX Security 23), 2023, pp. 859–876.
[3] A. Al Arafat, Z. Guo, and A. Awad, “Vr-spy: A side-channel attack on virtual key-logging in vr headsets,” in 2021 IEEE Virtual Reality and 3D User Interfaces (VR). IEEE, 2021, pp. 564–572.
[4] Ali Abedi and Omid Abari. 2020. WiFi Says "Hi!" Back to Strangers! In Proceedings of the 19th ACM Workshop on Hot Topics in Networks (HotNets '20). Association for Computing Machinery, New York, NY, USA, 132–138. https://doi.org/10.1145/3422604.3425951