Table 1: An overview of XR Attack Methods

Approach	Layer	Technique	Dimension		Complexity		Impact
			Attack Vector	Component	Requisite	Expertise	
Keystroke Inference Attacks [62]	Device	Keystroke Inference	Side-Channel	Hand Motion Telemetry	①	◓	
FaceReader [64]	Device	Eavesdropping	AR/VR headset IMU	Unrestricted Motion Sensors	②	◓	
TyPose[47]	Device	Keystroke Inference	IMU/head tracking	On-device motion sensors	③	●	
User Identification [21, 31, 33, 39]	Device	Inference from motion	IMU/VR motion telemetry	Motion sensors	②	◓	
LensHack[18]	Device	Keystroke Inference	Video side-channel	External camera	②	●	
HoloLogger[24]	Device	Monitoring head motion	Malicious MR App	HMD	②	◓	
User Profiling[34, 35, 38, 51]	Device	Inference from motion	Head motion	HMD	①	◓	
Chaperone[56]	Device	VR boundaries	Spatial boundary APIs	HMD	②	◓	
Human Joystick[5]	Device	Redirecting user paths	Motion guidance	Spatial rendering	②	◓	
Snooping[58, 61]	Device	Keystroke Inference	Side- Channel	Sensors	②	◓	
Shared State AR[48]	Device	Behavioral inference	Implicit Sensor Access	HMD & controller	②	◓	
Concurrent-App Fingerprinting[65]	Device	Launch-induced patterns	Side-Channel	Unreal Engine RHI	②	●	
Bystander Ranging[9, 65]	Device	Update spatial meshes	Side-Channel	Spatial-mapping	③	●	
Biosensor[14]	Device	EEG-based Identification	Raw EEG data	HMD	②	◓	
Mobile AR[19]	Device	Stealthy Frame-Capture	High-level AR library	ARCore rendering	①	◓	
INTRUDE[36]	Device	Deep-learning	Visual side-channel	External camera	②	●	
Implicit Identification[22, 30]	Device	Gaze–Head–Based	VR sensor APIs	IMU pipeline	①	◓	
VR-Gear[23]	Device	Computer Vision based	Video side-channel	HMD touchpad	②	◓	
Face-Mic[44]	Device	Eavesdropping	Sensor data API	Motion sensors	①	●	
Keylogging[28]	Device	Key-tap inference	Hand-tracking data	Air-tap keyboard	①	◓	
Hand gesture [13]	User	Exploit typing gesture	Side-Channel	Video segment	③	●	
AvatarHunter[27]	User	Exploit avatar motion	Side-Channel	VR Avatars	①	◓	
Password theft[45]	User	Exploit hand gesture	Video side-channel	Touch-keyboard UI	②	●	
GAZEploit [57]	User	Remote Keystroke Inference	Gaze typing	Video segment	③	◓	
Shoulder Surfing [1, 2]	User	Visual surveillance	Physical or screen-based	User interface	①	◓	
EyeTell[6, 7]	User	Video-assisted gaze	video side-channel	Eye-tracking system	①	◓	
VR-Spy [3, 11]	Network	Wireless Sniffing	Virtual Keystrokes	CSI data	③	●	
Denial of Service[46, 55]	Network	Overload of requests	Network session	Local app	①	◓	
Hijacking[52, 63]	Network	Token theft	Session token	Session backend	②	●	
Jamming[40]	Network	Radio signal interference	Wireless spectrum	Network interface	②	●	
ARSpy[43]	Network	Triangulation	Proximity updates	Network protocol	②	◓	
Run malicious code [53]	Cloud	Remote code execution	Software	Cloud storage	③	●	
Unauthorized access[15]	Cloud	Spoofed identity	Social engineering	User account	③	●	

Table 2: An overview of XR Defense Approaches

Approach	Group	Mitigation	Defense Vector	Deployability		Robustness	
				Trade-off	Maintenance	Efficacy	Stage
Keystroke inference [62]	Data Obfuscation	Limit access to telemetry	Hand tracking API	○	①		P
Rate-limiting [47]	Data Obfuscation	Reduced IMU sampling to 5Hz	Motion signals	◐	①		P
Noise Addition [62]	Data Obfuscation	Adding zero-mean Gaussian noise	3D hand-tracking data	○	①		P
Randomized Keyboard[57]	Data Obfuscation	Randomization of virtual keyboard	Feedback of keystrokes	◐	②		P
Avatars[27]	Data Obfuscation	Adding noise to gait data	Motion data	○	①		P
Privacy in motion[50]	Data Obfuscation	Adding Laplace noise	Motion data stream	◐	②		P
Eye Tracking[49]	Data Obfuscation	Using controlled noise	Sensor O/P layer	◐	②		P
Location Privacy[37, 43]	Data Obfuscation	Reduce location precision	Network layer	●	②		P
Biometric Auth.[12, 59]	Authentication	Head-neck movement modeling	IMU telemetry	○	②		P
Biometric anonymization[29, 32]	Authentication	Feature Suppression	Application Layer	●	②		P
Eye Tracking[4, 8]	Authentication	Gatekeeper API	Gaze data API	◐	②		P
Shoulder Surfing[10]	Authentication	Graphical Password	Application layer	◐	②		P
EyeVEIL[17]	Authentication	Gaussian blur	Eye-camera O/P	◐	②		P
Video Encryption[16]	Authentication	ROI video encryption	Video encoder	◐	②		P
ShareAR[41]	Access Control	Physical-world integration controls	App-level APIs	○	②		P
Privacy-Manager[20]	Access Control	Context-aware policy	OS middleware	◐	③		P
Privacy Leakage[26, 61]	Access Control	Precision Reduction	Sensor API middleware	○	②		P
PrivXR[60]	Access Control	Privacy panel	XR feature APIs	◐	②		P
Collaborative AR[54]	Access Control	Salted-hash passwords	Application layer	◐	②		P
Cloth try-on[42]	Access Control	secure computation	Client-server data	●	②		P
Knowledge[25]	Access Control	PIN entry+biometric	Hand movement	◐	②		P

1 Evaluation

Adversary Prerequisites. The *Requiste* column is represented by ① as low-level, ② as mid-level and ③ as high-level prerequisites to conduct an attack.

Attacker's Expertise. Based on the prerequisites and skills such as multithreaded synthetic input injection, proficiency in signal preprocessing, signal reconstruction, coordinate-system alignment, saliency detection, and side-channel trace analysis that an attacker must muster to launch an attack successfully, the *Expertise* is mapped as (◯) for low-level, (◓) for mid-level and (●) for high-level.

Attack Impact. The degree to which an attack exposes sensitive patient data (e.g., head-tracking patterns as biometric identifiers, session recordings) has been included as a metric here to consider the impact which has been depicted via a progress bar.

Defense Trade-off. The defense method's overhead such as additional hardware components, new system configuration and trade-off from implementation such as lower immersion, high latency, is measured by this criterion, and it can be either zero (◯), negligible (◐) or significant (●).

Defense Maintenance. This criterion measures how much post deployment maintenance of a certain defense strategy is required. A defense strategy may need continuous maintenance (③),intermittent maintenance (②), or very negligible maintenance (①).

Defense Efficacy. The efficacy of the defense strategy indicates how effective it is and the papers themselves provide the accuracy values. If the accuracy was not reported or specified, most papers reported the percentage to which the attack success rate (ASR) decreased. Since accuracy is the most frequently mentioned metric in defense method studies, we chose it.

References

[1] Yasmeen Abdrabou, Sheikh Radiah Rivu, Tarek Ammar, Jonathan Liebers, Alia Saad, Carina Liebers, Uwe Gruenefeld, Pascal Knierim, Mohamed Khamis, Ville Makela, et al. Understanding shoulder surfer behavior and attack patterns using virtual reality. In *Proceedings of the 2022 International Conference on Advanced Visual Interfaces*, pages 1–9, 2022.

[2] Devon Adams, Alseny Bah, Catherine Barwulor, Nureli Musaby, Kadeem Pitkin, and Elissa M Redmiles. Ethics emerging: the story of privacy and security perceptions in virtual reality. In *Fourteenth symposium on usable privacy and security (SOUPS 2018)*, pages 427–442, 2018.

[3] Abdullah Al Arafat, Zhishan Guo, and Amro Awad. Vr-spy: A side-channel attack on virtual key-logging in vr headsets. In *2021 IEEE Virtual Reality and 3D User Interfaces (VR)*, pages 564–572. IEEE, 2021.

[4] Efe Bozkir, Onur Günlü, Wolfgang Fuhl, Rafael F Schaefer, and Enkelejda Kasneci. Differential privacy for eye tracking with temporal correlations. *Plos one*, 16(8):e0255979, 2021.

[5] Peter Casey, Ibrahim Baggili, and Ananya Yarramreddy. Immersive virtual reality attacks and the human joystick. *IEEE Transactions on Dependable and Secure Computing*, 18(2):550–562, 2019.

[6] Yimin Chen, Tao Li, Rui Zhang, Yanchao Zhang, and Terri Hedgpeth. Eyetell: Video-assisted touchscreen keystroke inference from eye movements. In *2018 IEEE Symposium on Security and Privacy (SP)*, pages 144–160. IEEE, 2018.

[7] Kaiming Cheng, Arkaprabha Bhattacharya, Michelle Lin, Jaewook Lee, Aroosh Kumar, Jeffery F Tian, Tadayoshi Kohno, and Franziska Roesner. When the user is inside the user interface: An empirical study of {UI} security properties in augmented reality. In *33rd USENIX Security Symposium (USENIX Security 24)*, pages 2707–2723, 2024.

[8] Brendan David-John, Diane Hosfelt, Kevin Butler, and Eakta Jain. A privacy-preserving approach to streaming eye-tracking data. *IEEE Transactions on Visualization and Computer Graphics*, 27(5):2555–2565, 2021.

[9] Jaybie A De Guzman, Kanchana Thilakarathna, and Aruna Seneviratne. Security and privacy approaches in mixed reality: A literature survey. *ACM Computing Surveys (CSUR)*, 52(6):1–37, 2019.

[10] Reyhan Düzgün, Peter Mayer, and Melanie Volkamer. Shoulder-surfing resistant authentication for augmented reality. In *Nordic Human-Computer Interaction Conference*, pages 1–13, 2022.

[11] Zhangjie Fu, Jiashuang Xu, Zhuangdi Zhu, Alex X Liu, and Xingming Sun. Writing in the air with wifi signals for virtual reality devices. *IEEE Transactions on Mobile Computing*, 18(2):473–484, 2018.

[12] Markus Funk, Karola Marky, Iori Mizutani, Mareike Kritzler, Simon Mayer, and Florian Michahelles. Lookunlock: Using spatial-targets for user-authentication on hmds. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*, pages 1–6, 2019.

[13] Sindhu Reddy Kalathur Gopal, Diksha Shukla, James David Wheelock, and Nitesh 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)*, pages 859–876, 2023.

[14] Ihsân Grichi, Mina Jaberi, and Tiago H Falk. Biosensor-instrumented xr headsets: A double-edged sword for user identity and privacy management in the metaverse. In *2024 IEEE International Symposium on Mixed and Augmented Reality Adjunct (ISMAR-Adjunct)*, pages 17–19. IEEE, 2024.

[15] Aniket Gulhane, Akhil Vyas, Reshmi Mitra, Roland Oruche, Gabriela Hoefer, Samaikya Valluripally, Prasad Calyam, and Khaza Anuarul Hoque. Security, privacy and safety risk assessment for virtual reality learning environment applications. In *2019 16th IEEE annual consumer communications & networking conference (CCNC)*, pages 1–9. IEEE, 2019.

[16] Yongquan Hu, Dongsheng Zheng, Kexin Nie, Junyan Zhang, Wen Hu, and Aaron Quigley. Exploring device-oriented video encryption for hierarchical privacy protection in ar content sharing. In *2024 IEEE International Symposium on Mixed and Augmented Reality Adjunct (ISMAR-Adjunct)*, pages 427–428. IEEE, 2024.

[17] Brendan John, Sanjeev Koppal, and Eakta Jain. Eyeveil: degrading iris authentication in eye tracking headsets. In *Proceedings of the 11th ACM Symposium on Eye Tracking Research & Applications*, pages 1–5, 2019.

[18] Hossein Khalili, Alexander Chen, Theodoros Papaiakovou, Timothy Jacques, Hao-Jen Chien, Changwei Liu, Aolin Ding, Amin Hass, Saman Zonouz, and Nader Sehatbakhsh. Virtual keymysteries unveiled: Detecting keystrokes in vr with external side-channels. In *2024 IEEE Security and Privacy Workshops (SPW)*, pages 260–266. IEEE, 2024.

[19] Sarah M Lehman, Abrar S Alrumayh, Haibin Ling, and Chiu C Tan. Stealthy privacy attacks against mobile ar apps. In *2020 IEEE Conference on Communications and Network Security (CNS)*, pages 1–5. IEEE, 2020.

[20] Sarah M Lehman and Chiu C Tan. Privacymanager: An access control framework for mobile augmented reality applications. In *2017 IEEE Conference on Communications and Network Security (CNS)*, pages 1–9. IEEE, 2017.

[21] Jonathan Liebers, Mark Abdelaziz, Lukas Mecke, Alia Saad, Jonas Auda, Uwe Gruenefeld, Florian Alt, and Stefan Schneegass. Understanding user identification in virtual reality through behavioral biometrics and the effect of body normalization. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pages 1–11, 2021.

[22] Jonathan Liebers, Patrick Horn, Christian Burschik, Uwe Gruenefeld, and Stefan Schneegass. Using gaze behavior and head orientation for implicit identification in virtual reality. In *Proceedings of the 27th ACM Symposium on Virtual Reality Software and Technology*, pages 1–9, 2021.

[23] Zhen Ling, Zupei Li, Chen Chen, Junzhou Luo, Wei Yu, and Xinwen Fu. I know what you enter on gear vr. In *2019 IEEE Conference on Communications and Network Security (CNS)*, pages 241–249. IEEE, 2019.

[24] Shiqing Luo, Xinyu Hu, and Zhisheng Yan. Hololologger: Keystroke inference on mixed reality head mounted displays. In *2022 IEEE Conference on Virtual Reality and 3D User Interfaces (VR)*, pages 445–454. IEEE, 2022.

[25] Florian Mathis, Hassan Ismail Fawaz, and Mohamed Khamis. Knowledge-driven biometric authentication in virtual reality. In *Extended abstracts of the 2020 CHI conference on human factors in computing systems*, pages 1–10, 2020.

[26] Kate McNamara, Antonio Padilha Lanari Bo, Andrea McKittrick, Giovanna Tornatore, Sue Laracy, and Mathilde Desselle. Markerless motion capture system to detect upper limb movement during rehabilitation using video games. In *2022 IEEE 10th International Conference on Serious Games and Applications for Health (SeGAH)*, pages 1–6. IEEE, 2022.

[27] Yan Meng, Yuxia Zhan, Jiachun Li, Suguo Du, Haojin Zhu, and Xuemin Shen. De-anonymizing avatars in virtual reality: Attacks and countermeasures. *IEEE Transactions on Mobile Computing*, 2024.

[28] Ülkü Meteriz-Yıldıran, Necip Fazıl Yıldıran, Amro Awad, and David Mohaisen. A keylogging inference attack on air-tapping keyboards in virtual environments. In *2022 IEEE Conference on Virtual Reality and 3D User Interfaces (VR)*, pages 765–774. IEEE, 2022.

[29] Robert Miller, Natasha Kholgade Banerjee, and Sean Banerjee. Using siamese neural networks to perform cross-system behavioral authentication in virtual reality. In *2021 IEEE Virtual Reality and 3D User Interfaces (VR)*, pages 140–149. IEEE, 2021.

[30] Robert Miller, Natasha Kholgade Banerjee, and Sean Banerjee. Combining real-world constraints on user behavior with deep neural networks for virtual reality (vr) biometrics. In *2022 IEEE conference on virtual reality and 3D user interfaces (VR)*, pages 409–418. IEEE, 2022.

[31] Alec G Moore, Ryan P McMahan, Hailiang Dong, and Nicholas Ruozzi. Personal identifiability of user tracking data during vr training. In *2021 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW)*, pages 556–557. IEEE, 2021.

[32] Tahrima Mustafa, Richard Matovu, Abdul Serwadda, and Nicholas Muirhead. Unsure how to authenticate on your vr headset? come on, use your head! In *Proceedings of the Fourth ACM International Workshop on Security and Privacy Analytics*, pages 23–30, 2018.

[33] Vivek Nair, Wenbo Guo, Justus Mattern, Rui Wang, James F O'Brien, Louis Rosenberg, and Dawn Song. Unique identification of 50,000+ virtual reality users from head & hand motion data. In *32nd USENIX Security Symposium (USENIX Security 23)*, pages 895–910, 2023.

[34] Vivek Nair, Christian Rack, Wenbo Guo, Rui Wang, Shuixian Li, Brandon Huang, Atticus Cull, James F O'Brien, Marc Latoschik, Louis Rosenberg, et al. Inferring private personal attributes of virtual reality users from head and hand motion data. *arXiv preprint arXiv:2305.19198*, 2023.

[35] Vivek Nair, Louis Rosenberg, James F O'Brien, and Dawn Song. Truth in motion: The unprecedented risks and opportunities of extended reality motion data. *IEEE Security & Privacy*, 22(1):24–32, 2023.

[36] Anh Nguyen, Xiaokuan Zhang, and Zhisheng Yan. Penetration vision through virtual reality headsets: identifying 360-degree videos from head movements. In *33rd USENIX Security Symposium (USENIX Security 24)*, pages 2779–2796, 2024.

[37] Omego Nnamonu, Mohammad Hammoudeh, and Tooska Dargahi. Metaverse cybersecurity threats and risks analysis: The case of virtual reality towards security testing and guidance framework. In *2023 IEEE International Conference on Metaverse Computing, Networking and Applications (MetaCom)*, pages 94–98. IEEE, 2023.

[38] Ilesanmi Olade, Charles Fleming, and Hai-Ning Liang. Biomove: Biometric user identification from human kinesiological movements for virtual reality systems. *Sensors*, 20(10):2944, 2020.

[39] Ken Pfeuffer, Matthias J Geiger, Sarah Prange, Lukas Mecke, Daniel Buschek, and Florian Alt. Behavioural biometrics in vr: Identifying people from body motion and relations in virtual reality. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pages 1–12, 2019.

[40] Muhammad Usman Rafique and S Cheung Sen-ching. Tracking attacks on virtual reality systems. *IEEE Consumer Electronics Magazine*, 9(2):41–46, 2020.

[41] Kimberly Ruth, Tadayoshi Kohno, and Franziska Roesner. Secure {Multi-User} content sharing for augmented reality applications. In *28th USENIX Security Symposium (USENIX Security 19)*, pages 141–158, 2019.

[42] Yoones A Sekhavat. Privacy preserving cloth try-on using mobile augmented reality. *IEEE Transactions on Multimedia*, 19(5):1041–1049, 2016.

[43] Jiacheng Shang, Si Chen, Jie Wu, and Shu Yin. Arspy: Breaking location-based multi-player augmented reality application for user location tracking. *IEEE Transactions on Mobile Computing*, 21(2):433–447, 2020.

[44] Cong Shi, Xiangyu Xu, Tianfang Zhang, Payton Walker, Yi Wu, Jian Liu, Nitesh Saxena, Yingying Chen, and Jiadi Yu. Face-mic: inferring live speech and speaker identity via subtle facial dynamics captured by ar/vr motion sensors. In *Proceedings of the 27th Annual International Conference on Mobile Computing and Networking*, pages 478–490, 2021.

[45] Diksha Shukla and Vir V Phoha. Stealing passwords by observing hands movement. *IEEE Transactions on Information Forensics and Security*, 14(12):3086–3101, 2019.

[46] Tânia Silva, Sara Paiva, Pedro Pinto, and António Pinto. A survey and risk assessment on virtual and augmented reality cyberattacks. In *2023 30th international conference on systems, signals and image processing (IWSSIP)*, pages 1–5. IEEE, 2023.

[47] Carter Slocum, Yicheng Zhang, Nael Abu-Ghazaleh, and Jiasi Chen. Going through the motions:{AR/VR} keylogging from user head motions. In *32nd USENIX Security Symposium (USENIX Security 23)*, pages 159–174, 2023.

[48] Carter Slocum, Yicheng Zhang, Erfan Shayegani, Pedram Zaree, Nael Abu-Ghazaleh, and Jiasi Chen. That doesn't go there: Attacks on shared state in {Multi-User} augmented reality applications. In *33rd USENIX Security Symposium (USENIX Security 24)*, pages 2761–2778, 2024.

[49] Julian Steil, Inken Hagestedt, Michael Xuelin Huang, and Andreas Bulling. Privacy-aware eye tracking using differential privacy. In *Proceedings of the 11th ACM Symposium on Eye Tracking Research & Applications*, pages 1–9, 2019.

[50] RUOXI SUN, HANWEN WANG, MINHUI XUE, and HSIANG-TING CHEN. Privacy in motion: Implementing differential privacy for user motion in vr.

[51] Pier Paolo Tricomi, Federica Nenna, Luca Pajola, Mauro Conti, and Luciano Gamberini. You can't hide behind your headset: User profiling in augmented and virtual reality. *IEEE Access*, 11:9859–9875, 2023.

[52] Rahmadi Trimananda, Hieu Le, Hao Cui, Janice Tran Ho, Anastasia Shuba, and Athina Markopoulou. {OVRseen}: Auditing network traffic and privacy policies in oculus {VR}. In *31st USENIX security symposium (USENIX security 22)*, pages 3789–3806, 2022.

[53] Wen-Jie Tseng, Elise Bonnail, Mark McGill, Mohamed Khamis, Eric Lecolinet, Samuel Huron, and Jan Gugenheimer. The dark side of perceptual manipulations in virtual reality. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, pages 1–15, 2022.

[54] Giacomo Vallasciani, Andrea Schinoppi, Pasquale Cascarano, Gustavo Marfia, and Lorenzo Donatiello. Handling privacy and security aspects in a collaborative ar session. In *2024 IEEE International Symposium on Mixed and Augmented Reality Adjunct (ISMAR-Adjunct)*, pages 20–22. IEEE, 2024.

[55] Samaikya Valluripally, Aniket Gulhane, Khaza Anuarul Hoque, and Prasad Calyam. Modeling and defense of social virtual reality attacks inducing cybersickness. *IEEE Transactions on Dependable and Secure Computing*, 19(6):4127–4144, 2021.

[56] Samaikya Valluripally, Aniket Gulhane, Reshmi Mitra, Khaza Anuarul Hoque, and Prasad Calyam. Attack trees for security and privacy in social virtual reality learning environments. In *2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC)*, pages 1–9. IEEE, 2020.

[57] Hanqiu Wang, Zihao Zhan, Haoqi Shan, Siqi Dai, Maximilian Panoff, and Shuo Wang. Gazeploit: Remote keystroke inference attack by gaze estimation from avatar views in vr/mr devices. In *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security*, pages 1731–1745, 2024.

[58] Junjue Wang, Brandon Amos, Anupam Das, Padmanabhan Pillai, Norman Sadeh, and Mahadev Satyanarayanan. A scalable and privacy-aware iot service for live video analytics. In *Proceedings of the 8th ACM on Multimedia Systems Conference*, pages 38–49, 2017.

[59] Xue Wang and Yang Zhang. Nod to auth: Fluent ar/vr authentication with user head-neck modeling. In *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*, pages 1–7, 2021.

[60] Chris Warin, Dominik Seeger, Shirin Shams, and Delphine Reinhardt. Privxr: A cross-platform privacy-preserving api and privacy panel for extended reality. In *2024 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops)*, pages 417–420. IEEE, 2024.

[61] Yi Wu, Cong Shi, Tianfang Zhang, Payton Walker, Jian Liu, Nitesh Saxena, and Yingying Chen. Privacy leakage via unrestricted motion-position sensors in the age of virtual reality: A study of snooping typed input on virtual keyboards. In *2023 IEEE Symposium on Security and Privacy (SP)*, pages 3382–3398. IEEE, 2023.

[62] Zhuolin Yang, Zain Sarwar, Iris Hwang, Ronik Bhaskar, Ben Y Zhao, and Haitao Zheng. Can virtual reality protect users from keystroke inference attacks? In *33rd USENIX Security Symposium (USENIX Security 24)*, pages 2725–2742, 2024.

[63] Ananya Yarramreddy, Peter Gromkowski, and Ibrahim Baggili. Forensic analysis of immersive virtual reality social applications: a primary account. In *2018 IEEE Security and Privacy Workshops (SPW)*, pages 186–196. IEEE, 2018.

[64] Tianfang Zhang, Zhengkun Ye, Ahmed Tanvir Mahdad, Md Mojibur Rahman Redoy Akanda, Cong Shi, Yan Wang, Nitesh Saxena, and Yingying Chen. Facereader: unobtrusively mining vital signs and vital sign embedded sensitive info via ar/vr motion sensors. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*, pages 446–459, 2023.

[65] Yicheng Zhang, Carter Slocum, Jiasi Chen, and Nael Abu-Ghazaleh. It's all in your head (set): Side-channel attacks on {AR/VR} systems. In *32nd USENIX Security Symposium (USENIX Security 23)*, pages 3979–3996, 2023.