《多媒体数据安全》课程报告

2023-推荐参考文献清单

注意：本清单文献**仅供大家参考**。文献是近 3 年内在信息隐藏、多媒体与人工智能安全、身份认证、新兴综合领域中的一些比较权威的新的工作，旨在扩展大家的认知范围。课程报告以大家对问题的分析和探索，以及解决问题的整个过程作为评价，目标是让大家提升考虑实际问题的能力，培养较好的科研思维。

信息隐藏

[1]. Dai D, An Z, Yang L. Inducing wireless chargers to voice out for inaudible command attacks[C]//2023 IEEE Symposium on Security and Privacy (SP). IEEE Computer Society, 2023: 503-520.

[2]. Li X, Ji X. Learning Normality is Enough: A Software-based Mitigation against Inaudible Voice Attacks[C]//2023 USENIX Security Symposium (USENIX Security), 2023

[3]. Ruochen Zhou, Xiaoyu Ji*, Chen Yan, Yi-Chao Chen, Chaohao Li, Wenyuan Xu, "DeHiREC: Detecting Hidden Voice Recorders via ADC Electromagnetic Radiation", accepted by IEEE Security & Privacy (Oakland), 2023

[4]. Lv P, Li P, Zhang S, et al. A Robustness-Assured White-Box Watermark in Neural Networks[J]. IEEE Transactions on Dependable and Secure Computing, 2023.

[5]. Li F Q, Wang S L, Liew A W C. Linear Functionality Equivalence Attack against Deep Neural Network Watermarks and a Defense Method by Neuron Mapping[J]. IEEE Transactions on Information Forensics and Security, 2023.

[6]. Lv P, Li P, Zhang S, et al. A Robustness-Assured White-Box Watermark in Neural Networks[J]. IEEE Transactions on Dependable and Secure Computing, 2023.

[7]. Wang R, Li H, Mu L, et al. Rethinking the Vulnerability of DNN Watermarking: Are Watermarks Robust against Naturalness-aware Perturbations?[C]//Proceedings of the 30th ACM International Conference on Multimedia. 2022: 1808-1818.

[8]. Ma R, Guo M, Hou Y, et al. Towards Blind Watermarking: Combining Invertible and Non-invertible Mechanisms[C]//Proceedings of the 30th ACM International Conference on Multimedia. 2022: 1532-1542.

[9]. Fang H, Jia Z, Ma Z, et al. PIMoG: An Effective Screen-shooting Noise-Layer Simulation for Deep-Learning-Based Watermarking Network[C]//Proceedings of the 30th ACM International Conference on Multimedia. 2022: 2267-2275.

[10]. Chang Q, Huang L, Liu S, et al. Blind Robust Video Watermarking Based on Adaptive Region Selection and Channel Reference[C]//Proceedings of the 30th ACM International Conference on Multimedia. 2022: 2344-2350.

[11]. Wei P, Li S, Zhang X, et al. Generative Steganography Network[C]//Proceedings of the 30th ACM International Conference on Multimedia. 2022: 1621-1629.

[12]. Jia Z, Fang H, Zhang W. Mbrs: Enhancing robustness of dnn-based watermarking by mini-batch of real and simulated jpeg compression[C]//Proceedings of the 29th ACM international conference on multimedia. 2021: 41-49.

[13]. Szyller S, Atli B G, Marchal S, et al. Dawn: Dynamic adversarial watermarking of neural networks[C]//Proceedings of the 29th ACM International Conference on Multimedia. 2021: 4417-4425.

[14]. Yoo I, Chang H, Luo X, et al. Deep 3d-to-2d watermarking: embedding messages in 3d meshes and extracting them from 2d renderings[C]//Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2022: 10031-10040.

[15]. Liu X, Ma Z, Ma J, et al. Image disentanglement autoencoder for steganography without embedding[C]//Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2022: 2303-2312.

[16]. Wang R, Li H, Mu L, et al. Rethinking the Vulnerability of DNN Watermarking: Are

[17]. Lukas N, Jiang E, Li X, et al. Sok: How robust is image classification deep neural network watermarking? [C]//2022 IEEE Symposium on Security and Privacy (SP). IEEE, 2022: 787-804.

[18]. Bansal A, Chiang P, Curry M J, et al. Certified Neural Network Watermarks with Randomized Smoothing[C]//International Conference on Machine Learning. PMLR, 2022: 1450-1465.

[19]. Cong T, He X, Zhang Y. SSLGuard: A Watermarking Scheme for Self-supervised Learning Pre-trained Encoders[C]//Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security. 2022: 579-593.

[20]. Gong J, Zhang X, Ren J, et al. The Invisible Shadow: How Security Cameras Leak Private Activities[C]//Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security. 2021: 2780-2793.

[21]. Ji X, Zhang J, Jiang S, et al. CapSpeaker: Injecting Voices to Microphones via Capacitors[C]//Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security. 2021: 1915-1929.

[22]. Iravantchi Y, Ahuja K, Goel M, et al. Privacymic: Utilizing inaudible frequencies for privacy preserving daily activity recognition[C]//Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems. 2021: 1-13.

[23]. Sayles A, Hooda A, Gupta M, et al. Invisible perturbations: Physical adversarial examples exploiting the rolling shutter effect[C]//Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2021: 14666-14675.

[24]. Zhang C, Karjauv A, Benz P, et al. Towards robust deep hiding under non-differentiable distortions for practical blind watermarking[C]//Proceedings of the 29th ACM international conference on multimedia. 2021: 5158-5166.

[25]. Qian K, Lu Y, Yang Z, et al. {AIRCODE}: Hidden {Screen-Camera} Communication on an Invisible and Inaudible Dual Channel[C]//18th USENIX Symposium on Networked Systems Design and Implementation (NSDI'21). 2021: 457-470.

[26]. Chen Y, Gao M, Li Y, et al. Big Brother is Listening: An Evaluation Framework on Ultrasonic Microphone Jammers[C]//IEEE INFOCOM 2022-IEEE Conference on Computer Communications. IEEE, 2022: 1119-1128.

[27]. Xue G, Li Y, Pan H, et al. ScreenID: Enhancing QRCode Security by Utilizing Screen Dimming Feature[J]. IEEE/ACM Transactions on Networking, 2022.

[28]. Jia H, Choquette-Choo C A, Chandrasekaran V, et al. Entangled Watermarks as a Defense against Model Extraction[C]//USENIX Security Symposium. 2021: 1937-1954.

[29]. Abdelnabi S, Fritz M. Adversarial watermarking transformer: Towards tracing text provenance with data hiding[C]//2021 IEEE Symposium on Security and Privacy (SP). IEEE, 2021: 121-140.

[30]. Guo J, Wen C K, Jin S. Eliminating CSI Feedback Overhead via Deep Learning-Based Data Hiding[J]. IEEE Journal on Selected Areas in Communications, 2022, 40(8): 2267-2281.

[31]. Tancik M, Mildenhall B, Ng R. Stegastamp: Invisible hyperlinks in physical photographs[C]//Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2020: 2117-2126.

[32]. Yang P, Lao Y, Li P. Robust watermarking for deep neural networks via bi-level optimization[C]//Proceedings of the IEEE/CVF International Conference on Computer Vision. 2021: 14841-14850.

[33]. Guan X, Feng H, Zhang W, et al. Reversible Watermarking in Deep Convolutional Neural Networks for Integrity Authentication[C]//Proceedings of the 28th ACM International Conference on Multimedia. 2020: 2273-2280.

[34]. Guan X, Feng H, Zhang W, et al. Reversible Watermarking in Deep Convolutional Neural Networks for Integrity Authentication[C]//Proceedings of the 28th ACM International Conference on Multimedia. 2020: 2273-2280.

[35]. Luo X, Zhan R, Chang H, et al. Distortion Agnostic Deep Watermarking[C]// Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2020: 13548-13557.

[36]. Wengrowski E, Dana K. Light field messaging with deep photographic steganography[C]//Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. 2019: 1515-1524.

多媒体与人工智能安全

[1]. Yang L, Chen X, Jian X, et al. Remote Attacks on Speech Recognition Systems Using Sound from Power Supply[C]//32st USENIX Security Symposium (USENIX Security 23). 2023.

[2]. Zhu W, Ji X, Cheng Y, et al. TPatch: A Triggered Physical Adversarial Patch[C]// 32st USENIX Security Symposium (USENIX Security 23). 2023.

[3]. Zizhi Jin, Xiaoyu Ji, Yushi Cheng, Bo Yang, Chen Yan, Wenyuan Xu, "PLA-LiDAR: Physical Laser Attacks against LiDAR-based 3D Object Detection in Autonomous Vehicle", accepted by IEEE Security & Privacy (Oakland), 2023.

[4]. Weber M, Xu X, Karlaš B, et al. Rab: Provable robustness against backdoor attacks, accepted by IEEE Security & Privacy (Oakland), 2023.

[5]. Li Z, Yu N, Salem A, et al. UnGANable: Defending Against GAN-based Face Manipulation//32st USENIX Security Symposium (USENIX Security 23). 2023.

[6]. Cao Y, Bhupathiraju S H, Naghavi P, et al. You can't see me: physical removal attacks on LiDAR-based autonomous vehicles driving frameworks[C]//32st USENIX Security Symposium (USENIX Security 23). 2023.

[7]. Yu Z, Chang Y, Zhang N, et al. SMACK: Semantically Meaningful Adversarial Audio Attack[C]//32st USENIX Security Symposium (USENIX Security 23). 2023.

[8]. Chang J W, Javaheripi M, Hidano S, et al. RoVISQ: Reduction of Video Service Quality via Adversarial Attacks on Deep Learning-based Video Compression[C]//Network and Distributed System Security (NDSS) Symposium 2023.

[9]. Jia W, Lu Z, Zhang H, et al. Fooling the Eyes of Autonomous Vehicles: Robust Physical Adversarial Examples Against Traffic Sign Recognition Systems[C]//Network and Distributed System Security (NDSS) Symposium 2022.

[10]. Li H, Shan S, Wenger E, et al. Blacklight: Scalable Defense for Neural Networks against {Query-Based}{Black-Box} Attacks[C]//31st USENIX Security Symposium (USENIX Security 22). 2022: 2117-2134.

[11]. Zhong Y, Liu X, Zhai D, et al. Shadows can be dangerous: Stealthy and effective physical-world adversarial attack by natural phenomenon[C]//Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2022: 15345-15354.

[12]. Yan C, Xu Z, Yin Z, et al. Rolling colors: Adversarial laser exploits against traffic light recognition[C]//31st USENIX Security Symposium (USENIX Security 22). 2022: 1957-1974..

[13]. Shan S, Ding W, Wenger E, et al. Post-breach recovery: Protection against white-box adversarial examples for leaked DNN models[C]//Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security. 2022: 2611-2625.

[14]. Hallyburton R S, Liu Y, Cao Y, et al. Security Analysis of {Camera-LiDAR} Fusion Against {Black-Box} Attacks on Autonomous Vehicles[C]//31st USENIX Security Symposium (USENIX Security 22). 2022: 1903-1920.

[15]. Ahmed S, Shumailov I, Papernot N, et al. Towards more robust keyword spotting for voice assistants[C]//31st USENIX Security Symposium (USENIX Security 22). 2022: 2655-2672.

[16]. Quiring E, Pendlebury F, Warnecke A, et al. Dos and don'ts of machine learning in computer security[C]//31st USENIX Security Symposium (USENIX Security 22), USENIX Association, Boston, MA. 2022.

[17]. Zhou C, Yan Q, Shi Y, et al. {DoubleStar}:{Long-Range} Attack Towards Depth Estimation based Obstacle Avoidance in Autonomous Systems[C]//31st USENIX Security Symposium (USENIX Security 22). 2022: 1885-1902.

[18]. Xie S, Wang H, Kong Y, et al. Universal 3-dimensional perturbations for black-box attacks on video recognition systems[C]//2022 IEEE Symposium on Security and Privacy (SP). IEEE, 2022: 1390-1407.

[19]. Zhang R, Liu J, Ding Y, et al. "Adversarial Examples" for Proof-of-Learning[C]//2022 IEEE Symposium on Security and Privacy (SP). IEEE, 2022: 1408-1422.

[20]. Liu H, Yu Z, Zha M, et al. When Evil Calls: Targeted Adversarial Voice over IP Network[C]//Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security. 2022: 2009-2023.

[21]. Liu J, Kang Y, Tang D, et al. Order-Disorder: Imitation Adversarial Attacks for Black-box Neural Ranking Models[C]//Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security. 2022: 2025-2039.

[22]. Duan R, Qu Z, Zhao S, et al. Perception-Aware Attack: Creating Adversarial Music via Reverse-Engineering Human Perception[C]//Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security. 2022: 905-919.

[23]. Lovisotto G, Turner H, Sluganovic I, et al. Slap: Improving physical adversarial examples with short-lived adversarial perturbations[C]. USENIX, 2021.

[24]. He Y, Meng G, Chen K, et al. DRMI: A Dataset Reduction Technology based on Mutual Information for Black-box Attacks[C]//USENIX Security Symposium. 2021: 1901-1918.

[25]. Xiang C, Bhagoji A N, Sehwag V, et al. PatchGuard: A Provably Robust Defense against Adversarial Patches via Small Receptive Fields and Masking[C]//USENIX Security Symposium. 2021: 2237-2254.

[26]. Hussain S, Neekhara P, Dubnov S, et al. WaveGuard: Understanding and mitigating audio adversarial examples[C]//USENIX Security Symposium. 2021.

[27]. Eisenhofer T, Schönherr L, Frank J, et al. Dompteur: Taming audio adversarial examples[C]//USENIX Security Symposium. 2021.

[28]. Sato T, Shen J, Wang N, et al. Dirty road can attack: Security of deep learning based automated lane centering under physical-world attack[C]//Proceedings of the 30th USENIX Security Symposium (USENIX Security 21). 2021.

[29]. Zhang Q, Hu S, Sun J, et al. On adversarial robustness of trajectory prediction for autonomous vehicles[C]//Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2022: 15159-15168.

[30]. Sato T, Chen Q A. Towards driving-oriented metric for lane detection models[C]//Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2022: 17153-17162.

[31]. Bahari M, Saadatnejad S, Rahimi A, et al. Vehicle trajectory prediction works, but not everywhere[C]//Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2022: 17123-17133.

[32]. Han X, Xu G, Zhou Y, et al. Physical Backdoor Attacks to Lane Detection Systems in Autonomous Driving[C]//Proceedings of the 30th ACM International Conference on Multimedia. 2022: 2957-2968.

[33]. Cao Y, Wang N, Xiao C, et al. Invisible for both camera and lidar: Security of multi-sensor fusion based perception in autonomous driving under physical-world attacks[C]//2021 IEEE Symposium on Security and Privacy (SP). IEEE, 2021: 176-194.

[34]. Zhu Y, Miao C, Zheng T, et al. Can we use arbitrary objects to attack lidar perception in autonomous driving?[C]//Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security. 2021: 1945-1960.

[35]. Lehner A, Gasperini S, Marcos-Ramiro A, et al. 3D-VField: Adversarial Augmentation of Point Clouds for Domain Generalization in 3D Object Detection[C]//Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2022: 17295-17304.

[36]. Cheng Z, Liang J, Choi H, et al. Physical attack on monocular depth estimation with optimal adversarial patches[C]//Computer Vision–ECCV 2022: 17th European Conference, Tel Aviv, Israel, October 23–27, 2022: 514-532.

[37]. Zhu Y, Miao C, Hajiaghajani F, et al. Adversarial attacks against lidar semantic segmentation in autonomous driving[C]//Proceedings of the 19th ACM Conference on Embedded Networked Sensor Systems. 2021: 329-342.

[38]. Chen G, Chenb S, Fan L, et al. Who is real bob? adversarial attacks on speaker recognition systems[C]//2021 IEEE Symposium on Security and Privacy (SP). IEEE, 2021: 694-711.

[39]. Abdullah H, Rahman M S, Garcia W, et al. Hear" no evil", see" kenansville": Efficient and transferable black-box attacks on speech recognition and voice identification systems[C]//2021 IEEE Symposium on Security and Privacy (SP). IEEE, 2021: 712-729.

[40]. Zheng B, Jiang P, Wang Q, et al. Black-box adversarial attacks on commercial speech platforms with minimal information[C]//Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security. 2021: 86-107.

[41]. Bahramali A, Nasr M, Houmansadr A, et al. Robust adversarial attacks against DNN-based wireless communication systems[C]//Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security. 2021: 126-140.

身份认证

[1]. Gavazzi A, Williams R, Kirda E, et al. A Study of Multi-Factor and Risk-Based Authentication Availability[C]//32st USENIX Security Symposium (USENIX Security 23). 2023.

[2]. Ren Y, Wang Y, Tan S, et al. Person Re-identification in 3D Space: A WiFi Vision-based Approach[C]//32st USENIX Security Symposium (USENIX Security 23). 2023.

[3]. Li A, Li J, Han D, et al. PhyAuth: Physical-Layer Message Authentication for ZigBee Networks[C]//32st USENIX Security Symposium (USENIX Security 23). 2023.

[4]. Rosenberg H, Tang B, Fawaz K, et al. Fairness properties of face recognition and obfuscation systems[C]//32st USENIX Security Symposium (USENIX Security 23). 2023.

[5]. Basin D, Schaller P, Toro-Pozo J. Inducing Authentication Failures to Bypass Credit Card PINs[C]//32st USENIX Security Symposium (USENIX Security 23). 2023.

[6]. Wenger E, Shan S, Zheng H, et al. SoK: Anti-Facial Recognition Technology, accepted by IEEE Security & Privacy (Oakland), 2023.

[7]. Cronin P, Gao X, Wang H, et al. Time-print: Authenticating USB flash drives with novel timing fingerprints[C]//2022 IEEE Symposium on Security and Privacy (SP). IEEE, 2022: 1002-1017.

[8]. Monaco J V. Device Fingerprinting with Peripheral Timestamps[C]//2022 IEEE Symposium on Security and Privacy (SP). IEEE, 2022: 1018-1033.

[9]. Huang L, Wang C. PCR-Auth: Solving Authentication Puzzle Challenge with Encoded Palm Contact Response[C]//2022 IEEE Symposium on Security and Privacy (SP). IEEE, 2022: 1034-1048.

[10]. Meng Y, Li J, Pillari M, et al. Your microphone array retains your identity: A robust voice liveness detection system for smart speakers[C]//31st USENIX Security Symposium (USENIX Security 22). 2022: 1077-1094.

[11]. Han F, Yang P, Du H, et al. Accuth: Anti-Spoofing Voice Authentication via Accelerometer[C]//Proceedings of the 20th ACM Conference on Embedded Networked Sensor Systems. 2022: 637-650.

[12]. Cardaioli M, Cecconello S, Conti M, et al. Hand Me Your {PIN}! Inferring {ATM}{PINs} of Users Typing with a Covered Hand[C]//31st USENIX Security Symposium (USENIX Security 22). 2022: 1687-1704.

[13]. Li C, Wang L, Ji S, et al. Seeing is living? rethinking the security of facial liveness verification in the deepfake era[C]//31st USENIX Security Symposium (USENIX Security 22). 2022: 2673-2690.

[14]. Blue L, Warren K, Abdullah H, et al. Who Are You (I Really Wanna Know)? Detecting Audio {DeepFakes} Through Vocal Tract Reconstruction[C]//31st USENIX Security Symposium (USENIX Security 22). 2022: 2691-2708.

[15]. Han F, Yang P, Du H, et al. Accuth: Anti-Spoofing Voice Authentication via Accelerometer[C]//Proceedings of the 20th ACM Conference on Embedded Networked Sensor Systems. 2022: 637-650.

[16]. Wu C, Chen J, He K, et al. EchoHand: High Accuracy and Presentation Attack Resistant Hand Authentication on Commodity Mobile Devices[C]//Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security. 2022: 2931-2945.

[17]. Fereidooni H, König J, Rieger P, et al. AuthentiSense: A Scalable Behavioral Biometrics Authentication Scheme using Few-Shot Learning for Mobile Platforms[C]//Network and Distributed System Security (NDSS) Symposium 2023.

[18]. Abdullah H, Karlekar A, Prasad S, et al. Attacks as Defenses: Designing Robust Audio CAPTCHAs Using Attacks on Automatic Speech Recognition Systems[C]//Network and Distributed System Security (NDSS) Symposium 2023.

[19]. Zhu H, Xiao M, et al. SoundLock: A Novel User Authentication Scheme for VR Devices Using Auditory-Pupillary Response[C]//Network and Distributed System Security (NDSS) Symposium 2023.

[20]. Ghorbani Lyastani S, Bugiel S, Backes M. A Systematic Study of the Consistency of Two-Factor Authentication User Journeys on Top-Ranked Websites[C]//Network and Distributed System Security (NDSS) Symposium 2023. 2023.

[21]. Conners J, Derbidge S, Devenport C, et al. Let's Authenticate: Automated Certificates for User Authentication[C]//Network and Distributed Systems Security (NDSS) Symposium. 2022.

[22]. Arias-Cabarcos P, Habrich T, Becker K, et al. Inexpensive brainwave authentication: new techniques and insights on user acceptance[C]//Proceedings of the 30th {USENIX} Security Symposium ({USENIX} Security 21). 2021: 55-72.

[23]. Guo C, Campbell B, Kapadia A, et al. Effect of Mood, Location, Trust, and Presence of Others on Video-Based Social Authentication[C]//USENIX Security Symposium. 2021: 1-18.

[24]. Lassak L, Hildebrandt A, Golla M, et al. " It's Stored, Hopefully, on an Encrypted Server": Mitigating Users' Misconceptions About FIDO2 Biometric WebAuthn[C]//USENIX Security Symposium. 2021: 91-108.

[25]. Golla M, Ho G, Lohmus M, et al. Driving 2FA adoption at scale: Optimizing two-factor authentication notification design patterns[C]//30th USENIX Security Symposium. USENIX, 2021: 109-126.

[26]. Cronin P, Gao X, Yang C, et al. Charger-Surfing: Exploiting a Power Line Side-Channel for Smartphone Information Leakage[C]//USENIX Security Symposium. 2021: 681-698.

[27]. Farkhani R M, Ahmadi M, Lu L. PTAuth: Temporal Memory Safety via Robust Points-to Authentication[C]//USENIX Security Symposium. 2021: 1037-1054.

[28]. Heinrich A, Hollick M, Schneider T, et al. PrivateDrop: Practical Privacy-Preserving Authentication for Apple AirDrop[C]//USENIX Security Symposium. 2021: 3577-3594.

[29]. Lee S, Choi W, Lee D H. Usable user authentication on a smartwatch using vibration[C]//Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security. 2021: 304-319.

[30]. La Cour A S, Afridi K K, Suh G E. Wireless charging power side-channel attacks[C]//Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security. 2021: 651-665.

[31]. Xu W, Song W, Liu J, et al. Mask does not matter: Anti-spoofing face authentication using mmWave without on-site registration[C]//Proceedings of the 28th Annual International Conference on Mobile Computing and Networking. 2022: 310-323.

[32]. Sharp J, Wu C, Zeng Q. Authentication for drone delivery through a novel way of using face biometrics[C]//Proceedings of the 28th Annual International Conference on Mobile Computing and Networking. 2022: 609-622.

[33]. Shi C, Xu X, Zhang T, et al. Face-Mic: inferring live speech and speaker identity via subtle facial dynamics captured by AR/VR motion sensors[C]//Proceedings of the 27th Annual International Conference on Mobile Computing and Networking. 2021: 478-490.

[34]. Ferlini A, Ma D, Harle R, et al. EarGate: gait-based user identification with in-ear microphones[C]//Proceedings of the 27th Annual International Conference on Mobile Computing and Networking. 2021: 337-349.

新兴综合

[1]. Qinhong Jiang, Xiaoyu Ji, Chen Yan, Zhixin Xie, Haina Lou, Wenyuan X. GlitchHiker: Uncovering Vulnerabilities of Image Signal Transmission with IEMI[C]//USENIX Security Symposium (USENIX Security), 2023.

[2]. Huang K, Zhou Y T, Zhang K, et al. HOMESPY: The Invisible Sniffer of Infrared Remote Control of Smart TVs[C]//USENIX Security Symposium (USENIX Security), 2023.

[3]. Ni T, Zhang X, Zuo C, et al. Uncovering User Interactions on Smartphones via Contactless Wireless Charging Side Channels[C]//2023 IEEE Symposium on Security and Privacy (SP). IEEE Computer Society, 2023: 1828-1844.

[4]. Hu P, Li W, Spolaor R, et al. mmEcho: A mmWave-based Acoustic Eavesdropping Method[C]//2023 IEEE Symposium on Security and Privacy (SP). IEEE Computer Society, 2023: 836-852.

[5]. Long Y, Yan C, Prasad S, et al. Private Eye: On the Limits of Textual Screen Peeking via Eyeglass Reflections in Video Conferencing. accepted by IEEE Security & Privacy (Oakland), 2023.

[6]. Huang P, Wei Yao, et al. InfoMasker: Preventing Eavesdropping Using Phoneme-Based Noise[C]//Network and Distributed System Security (NDSS) Symposium 2023.

[7]. Jang J, Cho M, Kim J, et al. Paralyzing Drones via EMI Signal Injection on Sensory Communication Channels[C]//Network and Distributed System Security (NDSS) Symposium 2023.

[8]. Wang Z, Yan Y, Yan Y, et al. {CamShield}: Securing Smart Cameras through Physical Replication and Isolation[C]//31st USENIX Security Symposium (USENIX Security 22). 2022: 3467-3484.

[9]. Sharma R A, Soltanaghaei E, Rowe A, et al. Lumos: Identifying and Localizing Diverse Hidden {IoT} Devices in an Unfamiliar Environment[C]//31st USENIX Security Symposium (USENIX Security 22). 2022: 1095-1112.

[10]. Sathaye H, Strohmeier M, Lenders V, et al. An Experimental Study of {GPS} Spoofing and Takeover Attacks on {UAVs}[C]//31st USENIX Security Symposium (USENIX Security 22). 2022: 3503-3520.

[11]. Maia H T, Xiao C, Li D, et al. Can one hear the shape of a neural network?: Snooping the GPU via Magnetic Side Channel[C]//31st USENIX Security Symposium (USENIX Security 22). 2022.

[12]. Nassi B, Pirutin Y, Swisa R, et al. Lamphone: Passive sound recovery from a desk lamp's light bulb vibrations[C]//31st USENIX Security Symposium (USENIX Security 22). 2022: 4401-4417.

[13]. Basak S, Gowda M. mmspy: Spying phone calls using mmwave radars[C]//2022 IEEE Symposium on Security and Privacy (SP). IEEE, 2022: 1211-1228.

[14]. Shan H, Zhang B, Zhan Z, et al. Invisible Finger: Practical Electromagnetic Interference Attack on Touchscreen-based Electronic Devices[C]//2022 IEEE Symposium on Security and Privacy (SP). IEEE, 2022: 1246-1262.

[15]. Wang C, Lin F, Liu T, et al. mmEve: eavesdropping on smartphone's earpiece via COTS mmWave device[C]//Proceedings of the 28th Annual International Conference on Mobile Computing And Networking. 2022: 338-351.

[16]. Staat P, Mulzer S, Roth S, et al. IRShield: A countermeasure against adversarial physical-layer wireless sensing[C]//2022 IEEE Symposium on Security and Privacy (SP). IEEE, 2022: 1705-1721.

[17]. Hu P, Zhuang H, Santhalingam P S, et al. Accear: Accelerometer acoustic eavesdropping with unconstrained vocabulary[C]//2022 IEEE Symposium on Security and Privacy (SP). IEEE, 2022: 1757-1773.

[18]. Ramesh S, Hadi G S, Yang S, et al. TickTock: Detecting Microphone Status in Laptops Leveraging Electromagnetic Leakage of Clock Signals[C]//Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security. 2022.

[19]. Jeong J, Kim D, Jang J, et al. Un-Rocking Drones: Foundations of Acoustic Injection

Attacks and Recovery Thereof[C]//Network and Distributed System Security (NDSS) Symposium 2023.

[20]. Chen X, Li Z, Chen B, et al. MetaWave: Attacking mmWave Sensing with Meta-material-enhanced Tags[C]//The 30th Network and Distributed System Security (NDSS) Symposium 2023.

[21]. Jang J, Cho M, Kim J, et al. Paralyzing Drones via EMI Signal Injection on Sensory Communication Channels[C]//The 30th Network and Distributed System Security (NDSS) Symposium 2023.

[22]. Zhang G, Ji X, Li X, et al. EarArray: Defending against DolphinAttack via Acoustic Attenuation[C]//NDSS. 2021.

[23]. Ning J, Xie L, Li Y, et al. MoiréPose: ultra high precision camera-to-screen pose estimation based on Moiré pattern[C]//Proceedings of the 28th Annual International Conference on Mobile Computing And Networking. 2022: 106-119.

[24]. Cheng Y, Ji X, Wang L, et al. mID: Tracing Screen Photos via Moiré Patterns[C]//USENIX Security Symposium. 2021: 2969-2986.

[25]. Wu Y, Kakaraparthi V, Li Z, et al. BioFace-3D: Continuous 3D facial reconstruction through lightweight single-ear biosensors[C]//Proceedings of the 27th Annual International Conference on Mobile Computing and Networking. 2021: 350-363.

[26]. Zhao J, Gong W, Liu J. Microphone array backscatter: an application-driven design for lightweight spatial sound recording over the air[C]//Proceedings of the 27th Annual International Conference on Mobile Computing and Networking. 2021: 710-722.

[27]. An Z, Lin Q, Zhao X, et al. One tag, two codes: identifying optical barcodes with NFC[C]//Proceedings of the 27th Annual International Conference on Mobile Computing and Networking. 2021: 108-120.

[28]. Liao Z, Luo Z, Huang Q, et al. SMART: screen-based gesture recognition on commodity mobile devices[C]//Proceedings of the 27th Annual International Conference on Mobile Computing and Networking. 2021: 283-295.