《多媒体数据安全》课程报告

2024-推荐参考文献清单

注意：本清单文献仅供大家参考。文献是近年在信息隐藏、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]. Liu C, Zhang J, Zhang T, et al. Detecting Voice Cloning Attacks via Timbre Watermarking[C]//Network and Distributed System Security (NDSS) Symposium 2024.

[2]. Lv P, Li P, Zhu S, et al. Ssl-wm: A black-box watermarking approach for encoders pre-trained by self-supervised learning[C]//Network and Distributed System Security (NDSS) Symposium 2024.

[3]. Yang B, Li W, Xiang L, et al. SrcMarker: Dual-Channel Source Code Watermarking via Scalable Code Transformations[C]//2024 IEEE Symposium on Security and Privacy (SP). IEEE Computer Society, 2024: 97-97.

[4]. Lv P, Ma H, Chen K, et al. MEA-Defender: A Robust Watermark against Model Extraction Attack[C]//2024 IEEE Symposium on Security and Privacy (SP), 2024.

[5]. Jiang Z, Zhang J, Gong N Z. Evading watermark based detection of AI-generated content[C]//Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security. 2023: 1168-1181.

[6]. 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.

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

[8]. 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

[9]. 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.

[10]. 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.

[11]. 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.

[12]. 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.

[13]. 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.

[14]. 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.

[15]. 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.

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

[17]. 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.

[18]. 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.

[19]. 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.

[20]. 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.

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

[22]. 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.

[23]. 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.

[24]. 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.

[25]. 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.

[26]. 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.

[27]. 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.

[28]. 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.

[29]. 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.

[30]. 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.

[31]. 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.

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

[33]. 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.

[34]. 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.

[35]. 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.

[36]. 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.

[37]. 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.

[38]. 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.

[39]. 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.

[40]. 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.

多媒体与人工智能安全

[1]. Wang S, Sun K, Li Q. Compensating Removed Frequency Components: Thwarting Voice

Spectrum Reduction Attacks[C]//Network and Distributed System Security (NDSS) Symposium 2024.

[2]. Li X, Yan C, Lu X, et al. Inaudible adversarial perturbation: Manipulating the recognition of user speech in real time[C]//Network and Distributed System Security (NDSS) Symposium 2024.

[3]. Sato T, Bhupathiraju S H V, Clifford M, et al. Invisible Reflections: Leveraging Infrared Laser Reflections to Target Traffic Sign Perception[C]//Network and Distributed System Security (NDSS) Symposium 2024.

[4]. Duan R, Qu Z, Ding L, et al. Parrot-Trained Adversarial Examples: Pushing the Practicality of Black-Box Audio Attacks against Speaker Recognition Models[C]//Network and Distributed System Security (NDSS) Symposium 2024.

[5]. He C, Ma X, Zhu B B, et al. DorPatch: Distributed and Occlusion-Robust Adversarial Patch to Evade Certifiable Defenses[C]//Network and Distributed System Security (NDSS) Symposium 2024.

[6]. Hunt D, Angell K, Qi Z, et al. MadRadar: A Black-Box Physical Layer Attack Framework on mmWave Automotive FMCW Radars[C]//Network and Distributed System Security (NDSS) Symposium 2024.

[7]. Sato T, Hayakawa Y, Suzuki R, et al. LiDAR Spoofing Meets the New-Gen: Capability Improvements, Broken Assumptions, and New Attack Strategies[C]//ISOC Network and Distributed System Security Symposium (NDSS). ISOC, 2024.

[8]. Chen M, Xu X, Lu L, et al. Devil in the Room: Triggering Audio Backdoors in the Physical World[C]//33st USENIX Security Symposium (USENIX Security 24). 2024.

[9]. Wang K, Xu X, Lu L, et al. FraudWhistler: A Resilient, Robust and Plug-and-play Adversarial Example Detection Method for Speaker Recognition[C]//33st USENIX Security Symposium (USENIX Security 24). 2024.

[10]. Cheng P, Wang Y, Huang P, et al. ALIF: Low-Cost Adversarial Audio Attacks on Black-Box Speech Platforms using Linguistic Features[C]//2024 IEEE Symposium on Security and Privacy (SP). IEEE Computer Society, 2024: 56-56.

[11]. Meng X, Wang L, Guo S, et al. AVA: Inconspicuous Attribute Variation-based Adversarial Attack bypassing DeepFake Detection[C]//2024 IEEE Symposium on Security and Privacy (SP). IEEE Computer Society, 2024.

[12]. He R, Cheng Y, Ze J, et al. Understanding and Benchmarking the Commonality of Adversarial Examples[C]//2024 IEEE Symposium on Security and Privacy (SP). IEEE Computer Society, 2024: 111-111.

[13]. Ye H, Lan G, Jia J, et al. Screen Perturbation: Adversarial Attack and Defense on Under-Screen Camera[C]//Proceedings of the 29th Annual International Conference on Mobile Computing and Networking. 2023: 1-16.

[14]. Yu Z, Zhai S, Zhang N. Antifake: Using adversarial audio to prevent unauthorized speech synthesis[C]//Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security. 2023: 460-474.

[15]. Zhu Y, Miao C, Xue H, et al. TileMask: A Passive-Reflection-based Attack against mmWave Radar Object Detection in Autonomous Driving[C]//Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security. 2023: 1317-1331.

[16]. 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.

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

[18]. 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.

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

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

[21]. 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.

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

[23]. 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.

[24]. 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.

[25]. 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.

[26]. 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.

[27]. 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..

[28]. 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.

[29]. 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.

[30]. 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.

[31]. 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.

[32]. 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.

[33]. 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.

[34]. 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.

[35]. 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.

[36]. 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.

[37]. 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.

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

[39]. 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.

[40]. 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.

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

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

[43]. 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.

[44]. 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.

[45]. 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.

[46]. 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.

[47]. 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.

[48]. 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.

[49]. 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.

[50]. 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.

[51]. 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.

[52]. 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.

[53]. 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.

[54]. 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.

[55]. 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.

[56]. 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]. Wu Z, Cheng Y, Zhang S, et al. UniID: Spoofing Face Authentication System by Universal Identity[C]//Network and Distributed System Security Symposium (NDSS). 2024.

[2]. Lassak L, Pan E, Ur B, et al. Why Aren’t We Using Passkeys? Obstacles Companies Face Deploying FIDO2 Passwordless Authentication[C]//33st USENIX Security Symposium (USENIX Security 24). 2024.

[3]. Yu H, Du C, Xiao Y, et al. AAKA: An Anti-Tracking Cellular Authentication Scheme Leveraging Anonymous Credentials[C]//Network and Distributed System Security Symposium (NDSS). 2024.

[4]. Zhu W, Sun Y, Liu J, et al. CamPro: Camera-based Anti-Facial Recognition[C]//Network and Distributed System Security Symposium (NDSS). 2024.

[5]. He F, Jia Y, Zhao J, et al. Maginot Line: Assessing a New Cross-app Threat to PII-as-Factor Authentication in Chinese Mobile Apps[C]//Network and Distributed System Security Symposium (NDSS). 2024.

[6]. Zhou M, Su S, Wang Q, et al. PrintListener: Uncovering the Vulnerability of Fingerprint Authentication via the Finger Friction Sound[C]//Network and Distributed System Security Symposium (NDSS). 2024.

[7]. Kuchhal D, Saad M, Oest A, et al. Evaluating the Security Posture of Real-World FIDO2 Deployments[C]//Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security. 2023: 2381-2395.

[8]. Liu L, Fu X, Chen X, et al. Fits: Matching camera fingerprints subject to software noise pollution[C]//Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security. 2023: 1660-1674.

[9]. Marchiori F, Conti M. Your battery is a blast! safeguarding against counterfeit batteries with authentication[C]//Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security. 2023: 105-119.

[10]. Guo H, Chen X, Guo J, et al. Masterkey: Practical backdoor attack against speaker verification systems[C]//Proceedings of the 29th Annual International Conference on Mobile Computing and Networking. 2023: 1-15.

[11]. Mahdad A T, Jubur M, Saxena N. Breaking Mobile Notification-based Authentication with Concurrent Attacks Outside of Mobile Devices[C]//Proceedings of the 29th Annual International Conference on Mobile Computing and Networking. 2023: 1-15.

[12]. Kim S, Tan Y K, Jeong B, et al. Scores Tell Everything about Bob: Non-adaptive Face Reconstruction on Face Recognition Systems[C]//2024 IEEE Symposium on Security and Privacy (SP). IEEE Computer Society, 2024: 161-161.

[13]. 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.

[14]. 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.

[15]. 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.

[16]. 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.

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

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

[19]. 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.

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

[21]. 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.

[22]. 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.

[23]. 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.

[24]. 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.

[25]. 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.

[26]. 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.

[27]. 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.

[28]. 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.

[29]. 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.

[30]. 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.

[31]. 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.

[32]. 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.

[33]. 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.

[34]. 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.

[35]. 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.

[36]. 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.

[37]. 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.

[38]. 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.

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

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

[41]. 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.

[42]. 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.

[43]. 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.

[44]. 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.

[45]. 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.

[46]. 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]. Long Y, Jiang Q, Yan C, et al. EM Eye: Characterizing Electromagnetic Side-channel Eavesdropping on Embedded Cameras[C]//Network and Distributed System Security (NDSS) Symposium 2024.

[2]. Hunt D, Angell K, Qi Z, et al. MadRadar: A Black-Box Physical Layer Attack Framework on mmWave Automotive FMCW Radars[C]//Network and Distributed System Security (NDSS) Symposium 2024.

[3]. Luo J, Cao H, Jiang H, et al. MIMOCrypt: Multi-User Privacy-Preserving Wi-Fi Sensing via MIMO Encryption[C]//2024 IEEE Symposium on Security and Privacy (SP). IEEE Computer Society, 2024.

[4]. Xiao S, Ji X, Yan C, et al. MicPro: Microphone-based Voice Privacy Protection[C]//Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security. 2023: 1302-1316.

[5]. Ni T, Zhang X, Zhao Q. Recovering Fingerprints from In-Display Fingerprint Sensors via Electromagnetic Side Channel[C]//Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security. 2023: 253-267.

[6]. Ni T, Li J, Zhang X, et al. Exploiting Contactless Side Channels in Wireless Charging Power Banks for User Privacy Inference via Few-shot Learning[C]//Proceedings of the 29th Annual International Conference on Mobile Computing and Networking. 2023: 1-15.

[7]. Ni T, Chen Y, Xu W, et al. XPorter: A Study of the Multi-Port Charger Security on Privacy Leakage and Voice Injection[C]//Proceedings of the 29th Annual International Conference on Mobile Computing and Networking. 2023: 1-15.

[8]. Wang W, He Y, Jin M, et al. Meta-Speaker: Acoustic Source Projection by Exploiting Air Nonlinearity[C]//Proceedings of the 29th Annual International Conference on Mobile Computing and Networking. 2023: 1-15.

[9]. Fan T, Wu H, Jin M, et al. Towards Spatial Selection Transmission for Low-end IoT devices with SpotSound[C]//Proceedings of the 29th Annual International Conference on Mobile Computing and Networking. 2023: 1-14.

[10]. Fan X, Pearl D, Howard R, et al. APG: Audioplethysmography for Cardiac Monitoring in Hearables[C]//Proceedings of the 29th Annual International Conference on Mobile Computing and Networking. 2023: 1-15.

[11]. Iizuka T, Sasatani T, Nakamura T, et al. MilliSign: mmWave-Based Passive Signs for Guiding UAVs in Poor Visibility Conditions[C]//Proceedings of the 29th Annual International Conference on Mobile Computing and Networking. 2023: 1-15.

[12]. Yu T H, Tsai H M. ReMark: Privacy-preserving Fiducial Marker System via Single-pixel Imaging[C]//Proceedings of the 29th Annual International Conference on Mobile Computing and Networking. 2023: 1-15.

[13]. Cao S, Li D, Lee S I, et al. PowerPhone: Unleashing the Acoustic Sensing Capability of Smartphones[C]//Proceedings of the 29th Annual International Conference on Mobile Computing and Networking. 2023: 1-16.

[14]. Dai D, An Z, Pan Q, et al. Magcode: Nfc-enabled barcodes for nfc-disabled smartphones[C]//Proceedings of the 29th Annual International Conference on Mobile Computing and Networking. 2023: 1-14.

[15]. 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.

[16]. 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.

[17]. 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.

[18]. 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.

[19]. 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.

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

[22]. Shahid I, Roy N. " Is this my president speaking?" Tamper-proofing Speech in Live Recordings[C]//Proceedings of the 21st Annual International Conference on Mobile Systems, Applications and Services. 2023: 219-232.

[23]. 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.

[24]. 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.

[25]. 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.

[26]. 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.

[27]. 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.

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

[29]. 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.

[30]. 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.

[31]. 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.

[32]. 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.

[33]. 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.

[34]. 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.

[35]. 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.

[36]. 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.

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

[38]. 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.

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

[40]. 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.

[41]. 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.

[42]. 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.

[43]. 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.