|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Date | Session | Paper ID | Paper | Presenter | |
| 10.11 | Adversarial AI/ML | 9 | When Does Machine Learning FAIL? Generalized Transferability for Evasion and Poisoning Attacks | 胡怡霜  罗敏 | |
| 10 | With Great Training Comes Great Vulnerability: Practical Attacks against Transfer Learning | 何国立  钱佳莹  李露 | |
| 13 | Model-Reuse Attacks on Deep Learning Systems | 李泽宇  丁一凡  孙铭徽 | |
| 16 | Machine Learning with Membership Privacy using Adversarial Regularization | 汪汉宁  丁俐夫 | |
| 21 | A Machine Learning Approach to Prevent Malicious Calls Over Telephony Networks | 何诗鸣  王少帅 | |
| 4 | CommanderSong: A Systematic Approach for Practical Adversarial Voice Recognition | 李彦君  江铁 |
| 10.18 | Mobile Sensing Security | 7 | All Your GPS Are Belong To Us: Towards Stealthy Manipulation of Road Navigation Systems | 应樱  何挺 |
| 8 | Injected and Delivered: Fabricating Implicit Control over Actuation Systems by Spoofing Inertial Sensors | 卢开诚  赵家悦 |
| 14 | Deep Fingerprinting: Undermining Website Fingerprinting Defenses with Deep Learning | 谢之皓  赵恒飞 |
| 20 | Crowd-GPS-Sec: Leveraging Crowdsourcing to Detect and Localize GPS Spoofing Attacks | 韩波  虞舾 | |
| 22 | K-means++ vs. Behavioral Biometrics: One Loop to Rule Them All | 陈仲锴  黎经元 | |
| 1 | Fear the Reaper: Characterization and Fast Detection of Card Skimmers | 王之昀 | |
| 10.25 | Hardware/Device Security | 12 | No Training Hurdles: Fast Training-Agnostic Attacks to Infer Your Typing | 蔡婉琪  李丹一 | |
| 15 | Screaming Channels: When Electromagnetic Side Channels Meet Radio Transceivers | 方晓伦  叶杨莉 | |
| 23 | Exploiting a Thermal Side Channel for Power Attacks in Multi-Tenant Data Centers | 卢倚平  熊奎翔 | |
| 24 | On the Power of Optical Contactless Probing: Attacking Bitstream Encryption of FPGAs | 劳凯垚  杜舟野 | |
| 3 | Skill Squatting Attacks on Amazon Alexa | 李星辉  徐胜蓝 | |
| 5 | Polisis: Automated Analysis and Presentation of Privacy Policies Using Deep Learning | 穆亚楠  楼冠廷 | |
| 11.1 | Network Security/Privacy | 6 | AttriGuard: A Practical Defense Against Attribute Inference Attacks via Adversarial Machine Learning | 张佳欣  梁斯铭  齐风扬 | |
| 18 | Speechless: Analyzing the Threat to Speech Privacy from Smartphone Motion Sensors | 赵涛 | |
| 17 | Securify: Practical Security Analysis of Smart Contracts | 沈莹  田一玮 | |
| 19 | Sonar: Detecting SS7 Redirection Attacks With Audio-Based Distance Bounding | 莫建烨  吴子晔 | |
| 2 | BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid | 卫璇  周璐  姚子睿 | |
| 11.8 | Others | 11 | PrinTracker: Fingerprinting 3D Printers using Commodity Scanners | 傅雨荷  胡丹尔 | |
| 25 | Understanding and Mitigating the Security Risks of Voice-Controlled Third-Party Skills on Amazon Alexa and Google Home | 孙婧卓  俞烨隆  李永浩 | |
| 26 | Blue Note: How Intentional Acoustic Interference Damages Availability and Integrity in Hard Disk Drives and Operating Systems | 程雨诗  李超豪 | |
|  |  |  | |
|  |  |  | |