List of papers for in-class study

1. Understanding the Security Risks of Websites Using Cloud Storage for Direct User File Uploads
2. Physical Layer-Based Device Fingerprinting for Wireless Security: From Theory to Practice
3. WF-Transformer: Learning Temporal Features for Accurate Anonymous Traffic Identification by Using Transformer Networks
4. Jailbreak Vision Language Models via Bi-Modal Adversarial Prompt
5. Adversarial XAI Methods in Cybersecurity
6. GNSS Jammer Localization and Identification With Airborne Commercial GNSS Receivers
7. AVoiD-DF: Audio-Visual Joint Learning for Detecting Deepfake
8. LD-PA: Distilling Univariate Leakage for Deep Learning-Based Profiling Attacks
9. FakeBench: Probing Explainable Fake Image Detection via Large Multimodal Models
10. Open Set Learning for RF-Based Drone Recognition via Signal Semantics
11. AutoPT: How Far Are We From the Fully Automated Web Penetration Testing?
12. AdvNeRF: Generating 3D Adversarial Meshes With NeRF to Fool Driving Vehicles
13. A Forensic Framework With Diverse Data Generation for Generalizable Forgery Localization
14. Toward Open-World Network Intrusion Detection via Open Recognition and Inspection
15. SF2Net: Sequence Feature Fusion Network for Palmprint Verification
16. Unveiling Malware Visual Patterns: A Self-Analysis Perspective
17. Traceable Access Control Encryption With Parallel Multiple Sanitizers
18. Feature Reconstruction: Far Field EM Side-Channel Attacks in Complex Environment
19. ArcGen: Generalizing Neural Backdoor Detection Across Diverse Architectures
20. Enhancing Model Generalization for Efficient Cross-Device Side-Channel Analysis
21. Fine-Grained and Class-Incremental Malicious Account Detection in Ethereum via Dynamic Graph Learning
22. PREXP: Uncovering and Exploiting Security-Sensitive Objects in the Linux Kernel
23. Identifying Adversarial Cyber-Activity in Operational Technology Environments Using Bayesian Networks
24. LMAE4Eth: Generalizable and Robust Ethereum Fraud Detection by Exploring Transaction Semantics and Masked Graph Embedding
25. MOJO: MOtion Pattern Learning and JOint-Based Fine-Grained Mining for Person Re-Identification Based on 4D LiDAR Point Clouds
26. Hard-Label Black-Box Adversarial Attacks for Implicit Scene Interactions
27. Identifying Backdoored Graphs in Graph Neural Network Training: An Explanation-Based Approach With Novel Metrics

28. XIPHOS: Adaptive In-Vehicle Intrusion Detection via Unsupervised Graph Contrastive Learning
29. Two-Stage Jamming Detection and Channel Estimation for UAV-Based IoT Systems
30. A Security Mechanism Against Inference Attacks on Networked Systems
31. UDFed: A Universal Defense Scheme for Various Poisoning Attacks on Federated Learning
32. F2Attack: Two-Factors Scoring Method for Query-Efficient Hard-Label Black-Box Textual Adversarial Attacks
33. Flow Microelement-Driven Traffic Relationship Analysis: Robust Detection of Malicious Encrypted Traffic
34. Mixed-Bit Sampling Marking: Toward Unifying Document Authentication in Copy-Sensitive Graphical Codes
35. Detection of Unknown Attacks Through Encrypted Traffic: A Gaussian Prototype-Aided Variational Autoencoder Framework
36. Facilitating Access Control Vulnerability Detection in Modern Java Web Applications With Accurate Permission Check Identification
37. Digital Scapegoat: An Incentive Deception Model for Resisting Unknown APT Stealing Attacks on Critical Data Resource
38. An Image Robust Batch Steganography Framework With Minimum Embedding Signs
39. Channel-Robust RF Fingerprint Identification for Multi-Antenna 5G User Equipments
40. Fine-Grained Textual Guidance for Generalized Multi-Modal Face Anti-Spoofing