33rd USENIX Security Symposium

August 14–16, 2024
Philadelphia, PA, USA

Wednesday, August 14

User Studies I: Social Media Platforms

Hardware Security I: Attacks and Defense

System Security I: OS

Network Security I: DDoS

ML I: Federated Learning

Security Analysis I: Source Code and Binary

Crypto I: Secret Key Exchange

Social Issues I: Phishing and Password

Side Channel I: Transient Execution

Mobile Security I

Web Security I

LLM for Security

Fuzzing I: Software

Differential Privacy I

Deepfake and Synthesis

Hardware Security II: Architecture and Microarchitecture

System Security II: OS Kernel

Network Security II: Attacks

ML II: Fault Injection and Robustness

Security Analysis II: Program Analysis

Zero-Knowledge Proof I

Measurement I: Fraud and Malware and Spam

Side Channel II: RowHammer

Forensics

ML for Security

LLM I: Attack and Defense

Software Vulnerability Detection

Cryptographic Protocols I: Multi-Party Computation

Thursday, August 15

User Studies II: At-Risk Users

Side Channel III

ML III: Secure ML

Measurement II: Network

ML IV: Privacy Inference I

Fuzzing II: Method

Crypto II: Searchable Encryption

Social Issues II: Surveillance and Censorship

AR and VR

User Studies III: Privacy I

ML V: Backdoor Defense

ML VI: Digital Adversarial Attacks

Security Analysis III: Protocol

Cryptographic Protocols II

User Studies IV: Policies and Best Practices I

Side Channel IV

Cloud Security

Blockchain I

ML VII: Adversarial Attack Defense

Language-Based Security

Zero-Knowledge Proof II

Measurement III: Auditing and Best Practices I

Hardware Security III: Signals

System Security III: Memory I

Web Security II: Privacy

ML VIII: Backdoors and Federated Learning

Software Security + ML 1

Crypto III: Password and Secret Key

Social Issues III: Social Media Platform

Wireless Security I: Cellular and Bluetooth

Mobile Security II

Measurement IV: Web

LLM II: Jailbreaking

Fuzzing III: Network

Differential Privacy II

Friday, August 16

User Studies V: Policies and Best Practices II

User Studies VI: Privacy II

Measurement V: App

Network Security III: Detection

ML IX: Model Extraction and Watermark

Fuzzing IV: Hardware and Firmware

Crypto IV: Position and Elections

Measurement VI: Human Behavior and Security

Hardware Security IV: Firmware

Mobile Privacy

Network Security IV: Infrastructure

LLM III: Abuse

Security Analysis IV: OS

Crypto V: Private Information Retrieval

User Studies VII: Policies and Best Practices III

Wireless Security II: Sky and Space

System Security IV: Multithreading

Blockchain II

Autonomous and Automatic Systems

Crypto VI: Security Analysis

Crypto VII: Private Set Operations

Social Issues IV

IoT and CPS

Crypto VIII: Side Channel

Web Security III: XSS and PHP

ML X: Privacy Inference II

Security Analysis V: ML

Cryptographic Protocols III

Measurement VII: Auditing and Best Practices II

Hardware Security V: Embedded

System Security V: Memory II

User Studies VIII: Cryptography

ML XI: Physical Adversarial Attacks

Software Security + ML 2

Crypto IX: Attacks