32nd USENIX Security Symposium

August 9–11, 2023
Anaheim, CA, USA

Wednesday, August 9

Breaking Wireless Protocols

Interpersonal Abuse

Inferring User Details

Adversarial ML beyond ML

Private Set Operations

Logs and Auditing

Fighting the Robots

Perspectives and Incentives

Traffic Analysis

Adversarial Patches and Images

Decentralized Finance

Memory

Security in Digital Realities

Password Guessing

Privacy Policies, Labels, Etc.

ML Applications to Malware

Secure Messaging

x-Fuzz

Programs, Code, and Binaries

IoT Security Expectations and Barriers

Differential Privacy

Poisoning

Smart Contracts

x-Fuzz and Fuzz-x

Cache Attacks

Authentication

Private Data Leaks

Generative AI

Security Worker Perspectives

Deep Thoughts on Deep Learning

Thursday, August 10

Smart? Assistants

Security-Adjacent Worker Perspectives

Censorship and Internet Freedom

Machine Learning Backdoors

Integrity

Fuzzing Firmware and Drivers

Vehicles and Security

Verifying Users

DNS Security

Graphs and Security

Ethereum Security

Supply Chains and Third-Party Code

Cellular Networks

Usability and User Perspectives

Entomology

Adversarial Examples

Private Record Access

It's All Fun and Games Until...

Enclaves and Serverless Computing

Email and Phishing

OSes and Security

Intrusion Detection

Privacy Preserving Crypto Blocks

Warm and Fuzzing

Remote Attacks

Understanding Communities, Part 1

Keeping Computations Confidential

Towards Robust Learning

Network Cryptographic Protocols

Warmer and Fuzzers

Friday, August 11

Kernel Analysis

It's Academic

De-anonymization and Re-identification

Thieves in the House

Distributed Secure Computations

Mobile Security and Privacy

Web Security

Understanding Communities, Part 2

Routing and VPNs

Embedded Systems and Firmware

Attacks on Cryptography

Cloud Insecurity

More Web and Mobile Security

Networks and Security

Arming and Disarming ARM

More ML Attacks and Defenses

Cryptography for Privacy

Vulnerabilities and Threat Detection

Automated Analysis of Deployed Systems

Manipulation, Influence, and Elections

Side Channel Attacks

Transportation and Infrastructure

Language-Based Security

Browsers

Speculation Doesn't Pay

Facing the Facts

More Hardware Side Channels

Deeper Thoughts on Deep Learning

Attacks on Deployed Cryptosystems

Attacking, Defending, and Analyzing