CCS2021	
Web Security 1: Cybercrime	Chunk-Level Password Guessing: Towards Modeling Refined Password Composition Representations
	Out of Sight, Out of Mind: Detecting Orphaned Web Pages at Internet-Scale
	Catching Transparent Phish: Analyzing and Detecting MITM Phishing Toolkits
	Reverse Attack: Black-box Attacks on Collaborative Recommendation
	It's Not What It Looks Like: Manipulating Perceptual Hashing based Applications
Machine Learning and Security 1: Attacks on Robustness	Black-box Adversarial Attacks on Commercial Speech Platforms with Minimal Information
	A Hard Label Black-box Adversarial Attack Against Graph Neural Networks
	Robust Adversarial Attacks Against DNN-Based Wireless Communication Systems
	AI-Lancet: Locating Error-inducing Neurons to Optimize Neural Networks
Applied Crypto 1: Zero Knowledge I	Doubly Efficient Interactive Proofs for General Arithmetic Circuits with Linear Prover Time
	Constant-Overhead Zero-Knowledge for RAM Programs
	Appenzeller to Brie: Efficient Zero-Knowledge Proofs for Mixed-Mode Arithmetic and Z2*k*
	Shorter and Faster Post-Quantum Designated-Verifier zkSNARKs from Lattices
Usability and Measurement 1: Authentication and Click Fraud	"Hello, It's Me": Deep Learning-based Speech Synthesis Attacks in the Real World
	Don't Forget the Stuffing! Revisiting the Security Impact of Typo-Tolerant Password Authentication
	Dissecting Click Fraud Autonomy in the Wild
	Understanding and Detecting Mobile Ad Fraud Through the Lens of Invalid Traffic
	Usable User Authentication on a Smartwatch using Vibration

CCS2021	
Software Security 1: Fuzzing and Bug Finding	Automated Bug Hunting With Data-Driven Symbolic Root Cause Analysis
	SNIPUZZ: Black-box Fuzzing of IoT Firmware via Message Snippet Inference
	Same Coverage, Less Bloat: Accelerating Binary-only Fuzzing with Coverage-preserving Coverage-guided Tracing
	HyperFuzzer: An Efficient Hybrid Fuzzer for Virtual CPUs
	HardsHeap: A Universal and Extensible Framework for Evaluating Secure Allocators
Formal Methods and PL 1: Formal Analysis and Verification	DPGen: Automated Program Synthesis for Differential Privacy
	A Formally Verified Configuration for Hardware Security Modules in the Cloud
	Solver-Aided Constant-Time Hardware Verification
	Exorcising Spectres with Secure Compilers
	Structured Leakage and Applications to Cryptographic Constant-Time and Cost
Machine Learning and Security 2: Defenses for ML Robustness	Learning Security Classifiers with Verified Global Robustness Properties
	On the Robustness of Domain Constraints
	Cert-RNN: Towards Certifying the Robustness of Recurrent Neural Networks
	TSS: Transformation-Specific Smoothing for Robustness Certification
Applied Crypto 2: Secure Multiparty Computation	Efficient Online-friendly Two-Party ECDSA Signature
	One Hot Garbling
	The Return of Eratosthenes: Secure Generation of RSA Moduli using Distributed Sieving
	Secure Graph Analysis at Scale
	Oblivious Linear Group Actions and Applications
Hardware, Side Channels, and CPS 1: Side Channel	Wireless Charging Power Side-Channel Attacks

CCS2021	
	Indistinguishability Prevents Scheduler Side Channels in Real-Time Systems
	Rosita++: Automatic Higher-Order Leakage Elimination from Cryptographic Code
	Periscope: A Keystroke Inference Attack Using Human Coupled Electromagnetic Emanations
	Constantine: Automatic Side-Channel Resistance Using Efficient Control and Data Flow Linearization
Software Security 2: Operating Systems	ECMO: Peripheral Transplantation to Rehost Embedded Linux Kernels
	SyzGen: Automated Generation of Syscall Specification of Closed-Source macOS Drivers
	Demons in the Shared Kernel: Abstract Resource Attacks Against OS-level Virtualization
	SmashEx: Smashing SGX Enclaves Using Exceptions
	CPscan: Detecting Bugs Caused by Code Pruning in IoT Kernels
	Statically Discovering High-Order Taint Style Vulnerabilities in OS Kernels
Privacy and Anonymity 1: Inference Attacks	Honest-but-Curious Nets: Sensitive Attributes of Private Inputs Can Be Secretly Coded into the Classifiers' Outputs
	Quantifying and Mitigating Privacy Risks of Contrastive Learning
	Membership Inference Attacks Against Recommender Systems
	Membership Leakage in Label-Only Exposures
	When Machine Unlearning Jeopardizes Privacy
Network Security 1: DoS	Deterrence of Intelligent DDoS via Multi-Hop Traffic Divergence
	Scan, Test, Execute: Adversarial Tactics in Amplification DDoS Attacks
	Warmonger: Inflicting Denial-of-Service via Serverless Functions in the Cloud
	United We Stand: Collaborative Detection and Mitigation of Amplification DDoS Attacks at Scale

CCS2021	
Blockchain and Distributed Systems 1: Modeling Blockchains and Distributed Ledgers	Revisiting Nakamoto Consensus in Asynchronous Networks: A Comprehensive Analysis of Bitcoin Safety and Chain Quality
	How Does Blockchain Security Dictate Blockchain Implementation?
	The Exact Security of BIP32 Wallets
	A Security Framework for Distributed Ledgers
Network Security 2: Wireless, Mobile, and IoT	This Sneaky Piggy Went to the Android Ad Market: Misusing Mobile Sensors for Stealthy Data Exfiltration
	Noncompliance as Deviant Behavior: An Automated Black-box Noncompliance Checker for 4G LTE Cellular Devices
	All your Credentials are Belong to Us: On Insecure WPA2-Enterprise Configurations
	On-device IoT Certificate Revocation Checking with Small Memory and Low Latency
Applied Crypto 3: Private Set Intersection	Labeled PSI from Homomorphic Encryption with Reduced Computation and Communication
	Simple, Fast Malicious Multiparty Private Set Intersection
	Compact and Malicious Private Set Intersection for Small Sets
	Efficient Linear Multiparty PSI and Extensions to Circuit/Quorum PSI
Privacy and Anonymity 2: Differential Privacy	Differential Privacy for Directional Data
	Differentially Private Sparse Vectors with Low Error, Optimal Space, and Fast Access
	Continuous Release of Data Streams under both Centralized and Local Differential Privacy
	Side-Channel Attacks on Query-Based Data Anonymization
	AHEAD: Adaptive Hierarchical Decomposition for Range Query under Local Differential Privacy
Hardware, Side Channels, and CPS 2: Control System Security	Who's In Control? On Security Risks of Disjointed IoT Device Management Channels

CCS2021	
	DroneKey: A Drone-Aided Group-Key Generation Scheme for Large-Scale IoT Networks
	You Make Me Tremble: A First Look at Attacks Against Structural Control Systems
	MaMIoT: Manipulation of Energy Market Leveraging High Wattage IoT Botnets
	Aion: Enabling Open Systems through Strong Availability Guarantees for Enclaves
Network Security 3: PKI and Access Control	Rusted Anchors: A National Client-Side View of Hidden Root CAs in the Web PKI Ecosystem
	On Re-engineering the X.509 PKI with Executable Specification for Better Implementation Guarantees
	APECS: A Distributed Access Control Framework for Pervasive Edge Computing Services
	Let's Downgrade Let's Encrypt
Applied Crypto 4: Messaging and Privacy	A Concrete Treatment of Efficient Continuous Group Key Agreement via Multi-Recipient PKEs
	Modular Design of Secure Group Messaging Protocols and the Security of MLS
	Secure Complaint-Enabled Source-Tracking for Encrypted Messaging
	Fuzzy Message Detection
	Meteor: Cryptographically Secure Steganography for Realistic Distributions
	Hiding the Lengths of Encrypted Messages via Gaussian Padding
Software Security 3: Misc: Android and Vulnerabilities	Android on PC: On the Security of End-user Android Emulators
	Ghost in the Binder: Binder Transaction Redirection Attacks in Android System Services
	Dissecting Residual APIs in Custom Android ROMs
	VIP: Safeguard Value Invariant Property for Thwarting Critical Memory Corruption Attacks
	Detecting Missed Security Operations Through Differential Checking of Object-based Similar Paths
Blockchain and Distributed Systems 2: Consensus and Attacks	DETER: Denial of Ethereum Txpool sERvices

CCS2021	
	SyncAttack: Double-spending in Bitcoin Without Mining Power
	Multi-Threshold Byzantine Fault Tolerance
	Securing Parallel-chain Protocols under Variable Mining Power