		A	B	C
Monday 25	**1**	1A - Network Protocols	1B - Smartphones	1C - Cyber-crime and Forensics
	2	2A - IoT and Networks	2B - Fuzzing	2C - ML and AI 1
Tuesday 26	**3**	3A - Web Security	3B - Run-time Defenses	3C - Cyber-physical Systems
	4	4A - Wireless	4B - Secure Computing	4C - ML and AI 2
	5	5A - Special Problems and Use Cases	5B - Cloud and Edge Computing	5C - Attacks on ML/AI
Wednesday 27	**6**	6A - Privacy and Anonymity	6B - Kernel Security	6C - Keys and Authentication
	7	7A - Blockchains	7B - Software Components and Interactions	7C - Human Factors

	ID	Title
▼ **1A - Network Protocols**		
	#f214	ROV-MI: Large-Scale, Accurate and Efficient Measurement of ROV Deployment
	#f234	HeadStart: Efficiently Verifiable and Low-Latency Participatory Randomness Generation at Scale
	#f381	PMTUD is not Panacea: Revisiting IP Fragmentation Attacks against TCP
	#s037	Subverting Stateful Firewalls with Protocol States
▼ **1B - Smartphones**		
	#f097	PHYjacking: Physical Input Hijacking for Zero-Permission Authorization Attacks on Android
	#f254	GhostTalk: Interactive Attack on Smartphone Voice System Through Power Line
	#s056	The Droid is in the Details: Environment-aware Evasion of Android Sandboxes
	#s166	Uncovering Cross-Context Inconsistent Access Control Enforcement in Android
▼ **1C - Cyber-crime and Forensics**		
	#f043	Evaluating Susceptibility of VPN Implementations to DoS Attacks Using Adversarial Testing
	#f133	The Truth Shall Set Thee Free: Enabling Practical Forensic Capabilities in Smart Environments
	#f324	LogicMEM: Automatic Profile Generation for Binary-Only Memory Forensics via Logic Inference
	#s057	Forensic Analysis of Configuration-based Attacks
▼ **2A - IoT and Networks**		
	#f056	ditto: WAN Traffic Obfuscation at Line Rate
	#f208	A Lightweight IoT Cryptojacking Detection Mechanism in Heterogeneous Smart Home Networks
	#f349	FANDEMIC: Firmware Attack Construction and Deployment on Power Management Integrated Circuit and Impacts on IoT Applications
	#s154	EqualNet: A Secure and Practical Defense for Long-term Network Topology Obfuscation
▼ **2B - Fuzzing**		
	#f296	Context-Sensitive and Directional Concurrency Fuzzing for Data-Race Detection
	#f314	MobFuzz: Adaptive Multi-objective Optimization in Gray-box Fuzzing
	#s136	FirmWire: Transparent Dynamic Analysis for Cellular Baseband Firmware
	#s162	EMS: History-Driven Mutation for Coverage-based Fuzzing
▼ **2C - ML and AI 1**		
	#f058	Tetrad: Actively Secure 4PC for Secure Training and Inference
	#f335	MIRROR: Model Inversion for Deep LearningNetwork with High Fidelity
	#s054	Local and Central Differential Privacy for Robustness and Privacy in Federated Learning
	#s156	DeepSight: Mitigating Backdoor Attacks in Federated Learning Through Deep Model Inspection
▼ **3A - Web Security**		
	#f150	Testability Tarpits: the Impact of Code Patterns on the Security Testing of Web Applications
	#f308	Probe the Proto: Measuring Client-Side Prototype Pollution Vulnerabilities of One Million Real-world Websites
	#f382	ScriptChecker: To Tame Third-party Script Execution With Task Capabilities
	#s062	HARPO: Learning to Subvert Online Behavioral Advertising
▼ **3B - Run-time Defenses**		
	#f015	Chosen-Instruction Attack Against Commercial Code Virtualization Obfuscators
	#f031	Building Embedded Systems Like It's 1996
	#s060	The Taming of the Stack: Isolating Stack Data from Memory Errors
	#s165	CFInsight: A Comprehensive Metric for CFI Policies
▼ **3C - Cyber-physical Systems**		
	#f177	Too Afraid to Drive: Systematic Discovery of Semantic DoS Vulnerability in Autonomous Driving Planning under Physical-World Attacks
	#f244	RVPLAYER: Robotic Vehicle Forensics by Replay with What-if Reasoning
	#f298	Hiding My Real Self! Protecting Intellectual Property in Additive Manufacturing Systems Against Optical Side-Channel Attacks
	#s077	PoF: Proof-of-Following for Vehicle Platoons
▼ **4A - Wireless**		
	#f210	Packet-Level Open-World App Fingerprinting on Wireless Traffic
	#s023	SpiralSpy: Exploring a Stealthy and Practical Covert Channel to Attack Air-gapped Computing Devices via mmWave Sensing
	#s071	SemperFi: Anti-spoofing GPS Receiver for UAVs
	#s151	V-Range: Enabling Secure Ranging in 5G Wireless Networks
▼ **4B - Secure Computing**		
	#f173	Hybrid Trust Multi-party Computation with Trusted Execution Environment
	#f215	SynthCT: Towards Portable Constant-Time Code
	#s106	Binary Search in Secure Computation
	#s110	Chunked-Cache: On-Demand and Scalable Cache Isolation for Security Architectures
▼ **4C - ML and AI 2**		
	#f001	What You See is Not What the Network Infers: Detecting Adversarial Examples Based on Semantic Contradiction
	#f107	Euler: Detecting Network Lateral Movement via Scalable Temporal Graph Link Prediction
	#f130	Fooling the Eyes of Autonomous Vehicles: Robust Physical Adversarial Examples Against Traffic Sign Recognition Systems
	#s153	FedCRI: Federated Mobile Cyber-Risk Intelligence
▼ **5A - Special Problems and Use Cases**		
	#f082	FakeGuard: Exploring Haptic Response to Mitigate the Vulnerability in Commercial Fingerprint Anti-Spoofing
	#f092	On Utility and Privacy in Synthetic Genomic Data
	#s103	ProvTalk: Towards Interpretable Multi-level Provenance Analysis in Networking Functions Virtualization (NFV)
	#s127	Privacy in Urban Sensing with Instrumented Fleets, Using Air Pollution Monitoring As A Usecase
▼ **5B - Cloud and Edge Computing**		
	#f161	Titanium: A Metadata-Hiding File-Sharing System with Malicious Security
	#s081	Remote Memory-Deduplication Attacks
	#s102	Interpretable Federated Transformer Log Learning for Cloud Threat Forensics
	#s149	Repttack: Exploiting Cloud Schedulers to Guide Co-Location Attacks
▼ **5C - Attacks on ML/AI**		
	#f012	ATTEQ-NN: Attention-based QoE-aware Evasive Backdoor Attacks
	#f200	RamBoAttack: A Robust and Query Efficient Deep Neural Network Decision Exploit
	#s019	Property Inference Attacks Against GANs
	#s064	Get a Model! Model Hijacking Attack Against Machine Learning Models
▼ **6A - Privacy and Anonymity**		
	#f093	DRAWN APART : A Device Identification Technique based on Remote GPU Fingerprinting
	#f141	Clarion: Anonymous Communication from Multiparty Shuffling Protocols
	#f285	VPNalyzer: Systematic Investigation of the VPN Ecosystem
	#s120	hbACSS: How to Robustly Share Many Secrets
▼ **6B - Kernel Security**		
	#f159	An In-depth Analysis of Duplicated Linux Kernel Bug Reports
	#f221	Kasper: Scanning for Generalized Transient Execution Gadgets in the Linux Kernel
	#f345	Semantic-Informed Driver Fuzzing Without Both the Hardware Devices and the Emulators
	#f380	Progressive Scrutiny: Incremental Detection of UBI bugs in the Linux Kernel
▼ **6C - Keys and Authentication**		
	#f241	F-PKI: Enabling Innovation and Trust Flexibility in the HTTPS Public-Key Infrastructure
	#f272	Let's Authenticate: Automated Certificates for User Authentication
	#s143	Transparency Dictionaries with Succinct Proofs of Correct Operation
▼ **7A - Blockchains**		
	#f158	Multi-Certificate Attacks against Proof-of-Elapsed-Time and Their Countermeasures
	#f203	Shaduf: Non-Cycle Payment Channel Rebalancing
	#f370	NC-Max: Breaking the Security-Performance Tradeoff in Nakamoto Consensus
	#f385	Speeding Dumbo: Pushing Asynchronous BFT Closer to Practice
▼ **7B - Software Components and Interactions**		
	#f026	Preventing Kernel Hacks with HAKCs
	#f053	D-Box: DMA-enabled compartmentalization for embedded applications
	#f078	Cross-Language Attacks
	#f353	COOPER: Testing the Binding Code of Scripting Languages with Cooperative Mutation
▼ **7C - Human Factors**		
	#f284	Demystifying Local Business Search Poisoning for Illicit Drug Promotion
	#f387	Hazard Integrated: Understanding Security Risks in App Extensions to Team Chat Systems
	#s107	Above and Beyond: Organizational Efforts to Complement U.S. Digital Security Compliance Mandates
	#s109	Fighting Fake News in Encrypted Messaging with the Fuzzy Anonymous Complaint Tally System (FACTS)