Program

Day 1 (Monday 28, October 2024)

Day 1 (Monday 28, October 2024) *Metropolitan Hotel Dubai - Room: Al Shindagah Ballroom A*	
08:00 – 16:00	Registration
Morning	
09:00 – 09:30	Opening Remarks (General Co-Chairs' Welcome Address, TPC Co-Chairs' Report)
09:30 - 10:30	Keynote Speaker I: "Safeguarding the usage of AI in the intelligent world" Speaker: Aloysius Cheang, Huawei Middle East & Central Asia, UAE Session Chair: Saed Alrabaee
10:30 - 11:00	Coffee break
11:00 – 12:20	**Session 1: Privacy** **Session Chair:**
11:00 – 11:20	*Byzantine-Robust Federated Learning for Unreliable Environments by Random-Matching Verification and Credibility Table*
11:20 – 11:40	*PPSA: Polynomial Private Stream Aggregation for Time-Series Data Analysis*
11:40 – 12:00	*SPADE: Digging into Selective and PArtial DEcryption using Functional Encryption*
12:00 – 12:20	*Stuck in the SAND: When Your Neighbor Becomes Your Enemy*
11:00 – 12:30	**Online Session 1: Deep Learning Security and Adversarial Attacks** **Session Moderator:** **Room: Zoom Meeting Room #1**
11:00 – 11:15	*Enhancing Runtime Application Self-Protection with Unsupervised Deep Learning*
11:15 – 11:30	*Optical Lens Attack on Deep Learning Based Monocular Depth Estimation*
11:30 - 11:45	*RootES: A Method for Generating Text Adversarial Examples Using Root Embedding Space*
11:45 – 12:00	*Boosting GAN Performance: Feature Transformation for Heavy-Tailed Malware Data Generation*
12:00 – 12:15	*SPC-GAN-Attack: Attacking Slide Puzzle CAPTCHAs by Human-Like Sliding Trajectories Based on Generative Adversarial Network*

12:15 – 12:30	*Improving Interpretability: Visual Analysis of Deep Learning-Based Multi-Channel Attacks*
12:30 – 14:00	**Lunch**
14:00 – 15:00	Keynote Speaker II: "Trustworthy AI: Explanation and Exploitation" Speaker: My Thai, University of Florida, USA Session Chair: Saed Alrabaee
15:00 – 16:40	**Session 2: AI & Quantum Computing in Cybersecurity** **Session Chair:**
15:00 – 15:20	*Harnessing the Power of Quantum Computing for URL Classification: A Comprehensive Study*
15:20 – 15:40	*A Comparative Study on Source Code Attribution Using AI*
15:40 – 16:00	*Comprehensive Classification and Analysis of Cyber Attack Surface on Quantum Key Distribution Networks*
16:00 – 16:20	*A Secure Blockchain Network with Quantum Key Encryption and Authentication*
16:20 – 16:40	*Deep Reinforcement Learning from Drifting Network Environments in Anomaly Detection*
15:00 – 16:30	**Online Session 2: Privacy and Cryptography** **Session Moderator:** **Room: Zoom Meeting Room #2**
15:00 – 15:15	*Optimized Privacy-Preserving Clustering with Fully Homomorphic Encryption*
15:15 – 15:30	*Noya: An Efficient, Flexible and Secure CNN Inference Model based on Homomorphic Encryption*
15:30 – 15:45	*OCE-PTree: An Online Communication Efficient Privacy–preserving Decision Tree Evaluation*
15:45 – 16:00	*An Effective Multiple Private Set Intersection*
16:00 – 16:15	*BCPIR: More Efficient Keyword PIR via Block Building Codewords*
16:15 – 16:30	*Embedding-optimized Steganography Based on Post-quantum Encryption and BPNN*
16:40 – 17:00	Coffee Break

17:00 – 18:40	**Session 3: Network Security I** **(Session Chair:)**
17:00 – 17:20	*RFI: Enhancing Network Intrusion Detection through Robust Feature Selection Techniques*
17:20 – 17:40	*HyperBC: Hypergraph-based Approach for Behavior Cluster of Suspicious APT Attacks*
17:40 – 18:00	*MEMO: Detecting Unknown Malicious Encrypted Traffic via Metric Learning and Order-aware Pre-training*
18:00 – 18:20	*Interoperable Security Information and Event Management Framework for Multi Cloud Environment*
17:00 – 18:30	**Online Session 3: Blockchain and Cryptocurrencies** **Session Moderator:** **Room: Zoom Meeting Room #3**
17:00 – 17:15	*ASOZ: Anonymous and Auditable Cryptocurrency with Enhanced Confidential Transaction*
17:15 – 17:30	*Identity Inference in Ethereum: Towards Financial Security for Blockchain Ecosystem*
17:30 – 17:45	*SMDT: A Blockchain-based Secure Multi-version Data Trading Scheme with Fair Profit Sharing*
17:45 – 18:00	*Substitution Attacks on Asymmetric (Group) Message Franking*
18:00 – 18:15	*Symerge: Replacing Calls in Under-Constrained Symbolic Execution and Find Vulnerabilities*
18:15 – 18:30	*Threshold Key Management and Signature in Dynamic Distributed System*
18:30	**Trip to Dubai Mall**
Day 2 (Tuesday 29, 2024) Metropolitan Hotel Dubai - Room: Al Shindagah Ballroom A	
09:30 – 10:30	**Keynote Speaker III**: Privacy Enhancing Technologies for IoT and Decentralized Systems: Approaches and Challenges **Speaker**: Guomin Yang, Singapore Management University, Singapore **Session Chair**: Saed Alrabaee
10:30 – 11:00	Coffee Break
11:00 – 12:40	**Session 4: Fuzzing & IoT Security** **Session Chair:**

11:00 – 11:20	*Fast Firmware Fuzz with Input/Output Reposition*
11:20 – 11:40	*ChipFuzzer: Towards Fuzzing Matter-based IoT Devices for Vulnerability Detection*
11:40 – 12:00	*Reusablity Evaluation of Reports in Security Operation Centers for IoT with Sentence ALBERT and Jaccard Similarity*
12:00 – 12:20	*Multi-Server Publicly Verifiable Computation of polynomials*
12:20 - 12:40	*Siamese Neural Network for Robust IoT Device-Type Identification: A Few-Shot Learning Approach*
11:00 – 12:30	**Online Session 4: Malware Detection and Security Assessment** **Session Moderator:** **Room: Zoom Meeting Room #4**
11:00 – 11:15	*Mal-POBM: Malware Adversarial Sample Generation Method Based on Population Optimisation and Bidirectional Mutation*
11:15 – 11:30	*Graphite: Real-Time Graph-Based Detection of Windows Fileless Malware Attacks*
11:30 – 11:45	*Robust Network Intrusion Detection via Semi-Supervised Deep Reinforcement Learning*
11:45 – 12:00	*BinSimDB: Benchmark Dataset Construction for Fine-Grained Binary Code Similarity Analysis*
12:00 – 12:15	*FISFuzzer: A Grey-Box Protocol Fuzzer Based on Field Inference and Scheduling*
12:15 – 12:30	*OnionPeeler: A Novel Input-Enriched Website Fingerprinting Attack on Tor Onion Services*
12:50 – 14:00	Lunch
	Session 5: Blockchain and Web Security **Session Chair:**
14:00 – 14:20	*Beyond the Public Mempool: Catching DeFi Attacks Before They Happen with Real-Time Smart Contract Analysis*
14:20 – 14:40	*Ensuring Integrity in Online Content Usage and Download Counting with Smart Contracts*
14:40 – 15:00	*ChatSpamDetector: Leveraging Large Language Models for Effective Phishing Email Detection*

15:00 – 15:20	*EasyCSPeasy: A Server-side and Language-agnostic XSS Mitigation by Devising and Ensuring Compliance with CSP*
13:45 – 15:15	**Online Session 5: Authentication and IoT Security** **Session Moderator:** **Room: Zoom Meeting Room #5**
13:45 – 14:00	*Pulse-to-Pair: Heartbeat-based Authentication of IoT Devices for Elderly Care*
14:00 – 14:15	*A Lightweight Group Authentication Framework for Cross-Domain Internet of Things*
14:15 – 14:30	*DPU-LARK: DPU-Leveraged Remote Attestation of Remote Kernels for Security of OT Networks*
14:30 – 14:45	*Gait4Auth: Enhancing Identification and Security in Gait-Based Authentication*
14:45 – 15:00	*A Hardware-Oriented Lightweight Block Cipher and Its Application in Surveillance Video*
15:00 – 15:15	*TGSA: Trajectory Group Semantic Anonymization*
15:20 – 15:40	Coffee break
	Session 6: Network Security II **Session Chair:**
15:40 – 16:00	*Anti-EMP: Encrypted Malware Packets Filtering Algorithm Leveraging Ciphertext Patterns under Zero Knowledge Setting*
16:00 – 16:20	*Is This the Same Code? A Comprehensive Study of Decompilation Techniques for WebAssembly Binaries*
16:20 – 16:40	*Distributed Intrusion Detection in Dynamic Networks of UAVs using Few-Shot Federated Learning*
16:40 – 17:00	*Interference Avoidance and Mitigation Technique Utilizing Cooperative Characterization of Interferers in Dense Wireless Networks*
15:40 – 17:00	**Online Session 6: AI and NLP for Cybersecurity** **Session Moderator:** **Room: Zoom Meeting Room #6**

15:40 – 15:55	*Can't say cant? Measuring and Reasoning of Dark Jargons in Large Language Models*
15:55 – 16:10	*Cybersecurity with LLMs and RAGs: Challenges and Innovations*
16:10 – 16:15	*Enhancing Pre-Trained Language Models for Vulnerability Detection via Semantic-Preserving Data Augmentation*
16:15 – 16:30	*K-BOOST: A Cyber Security NER Model with Knowledge Augmentation via BERT*
16:30 – 16:45	*FLKT: Improving the Fidelity and Robustness of Federated Learning Aggregation Rules via the Key-data and Trap-model*
16:45- 17:00	*Poisoning Attack on Federated Learning with Non-IID Data: A Historical-Global-Model-Based Approach*
19:30- 22:00	**Conference Banquet + Best Paper Awards Announcement**
Day 3 (Wednesday 30, 2024) Metropolitan Hotel Dubai - Room: Al Shindagah Ballroom A	
09:00 – 10:30	**Online Session 7: Network and Protocol Security** **Session Moderator:** **Room: Zoom Meeting Room #7**
09:00 – 09:15	*A Border Management Protocol for Multi-Identifier Network within the Network Layer and Its Attack Detection Extension*
09:15 – 09:30	*VLDoS Variable Low-rate DoS Attack Model for BBR Algorithm in TCP*
09:30 – 09:45	*FullView: Using Bidirectional Group Sequences to Achieve Accurate Encrypted Traffic Classification*
09:45 – 10:00	*TEE-Receipt: A TEE-based Non-repudiation Framework for Web Applications*
10:00 – 10:15	*An Incentive Mechanism for Enhancing Transaction Privacy Based on Reputation Perception and Double Auction*
10:15 – 10:30	*Dynamically Expanding Factor Base of Index Calculus Algorithm to Solve Massive Discrete Logarithm Problems Faster*
10:30 – 11:00	Coffee Break
	Online Session 8: Web and Application Security **Session Moderator:**

	Room: Zoom Meeting Room #8
11:00 – 11:15	*Encoder-based Multimodal Ensemble Learning for High Compatibility and Accuracy in Phishing Website Detection*
11:15 – 11:30	*Bag-of-Characters: A Multiple Instance Learning Framework for URL Embedding in Web Security*
11:30 – 11:45	*AutoS2ploit: From Automotive Safety-Critical Functionalities to Security Exploit*
11:45 – 12:00	*Pitfalls of Data Masking Techniques: Re-identification Attacks*
12:00 – 12:15	*Faster Three-Party Constant-round Comparison with Application in Neural Network Inference*
12:15 - 12:30	*WtLDP: Generating Synthetic Decentralized Weighted Graphs with Local Differential Privacy*
12:30 – 12:45	*Tarnhelm: Using Adversarial Samples to Protect User Privacy Against Traffic Identification*
12:50 – 14:00	Lunch
	Online Session 9: Security Assessment II **Session Moderator:** **Room: Zoom Meeting Room #9**
14:00 – 14:15	*A Comprehensive Evaluation of the Impact on Tor Network Anonymity Caused by ShadowBridge*
14:15 – 14:30	*ADG-Dedup: Adaptive Dynamic Grained Deduplication Scheme for IoT Data in Cloud Storage*
14:30 – 14:45	*Enhancing Reliability in Open Rating Systems: A Trust-Aware Filtering Approach*
14:45 – 15:00	*Graph Injection Attack based on Node Similarity and Non-linear Feature Injection Strategy*
15:00 – 15:15	*Assessing and Prioritizing Ransomware Risk Based on Historical Victim Data*
15:15 – 15:30	*Solving ILWE Problem More Efficiently and Application to BLISS Side-Channel Attack*
15:30 – 16:00	Coffee Break
16:00 – 16:30	Closing Remarks