IEEE Conference on Communications and Network Security (IEEE CNS)

October 2 – 5, 2023

Orlando, Florida, USA

CONFERENCE PROGRAM

(as of September 26, 2023)

Program at a Glance

TIME (all in EDT)	Monday October 2	Tuesday October 3	Wednesday October 4	Thursday October 5
8:00 AM – 9:00 AM	**Breakfast** **Opening Session** (8:40 AM – 9:00 AM)	**Breakfast**	**Breakfast**	**Breakfast**
9:00 AM – 10:00 AM	**Keynote 1:** **Wenjing Lou**	**Keynote 2:** **Patrick McDaniel**	**Keynote 2:** **Ninghui Li**	**WORKSHOP DAY:** - Cyber Resilience Workshop - Cyber-Physical Systems Security (CPS-Sec 2023)
10:00 AM – 10:30 AM	**Break**	**Break**	**Break**	
10:30 AM – 12:00 PM	**SESSION 1:** **MACHINE LEARNING 1**	**SESSION 3: MOBILE & WIRELESS SECURITY**	**SESSION 6:** **NETWORK SECURITY**	
12:00 PM – 1:30 PM	**Lunch**	**Lunch**	**Lunch**	
1:30 PM – 3:00 PM	**PANEL:** **AI for xG Security**	**SESSION 4:** **MACHINE LEARNING 2**	**SESSION 7:** **CRYPTOGRAPHY**	
3:00 PM – 3:30 PM	**Break**	**Break**	**Break**	
3:30 PM – 5:00 PM	**SESSION 2: PRIVACY**	**SESSION 5: CYBER-PHYSICAL SYSTEMS** (3:30 PM – 5:25PM)	**SESSION 8:** **SOFTWARE SECURITY** (3:30 PM – 4:40 PM)	
		Break	**Closing** (4:40 – 4:45 PM)	
6:00 PM – 8:00 PM	**Conference banquet**	**Poster Session and Reception** (5:45 PM – 7:30PM)		

Program Details

Monday, October 2

TIME	SESSION	ROOM
8:00 AM – 6:00 PM	**Registration**	Majestic Foyer
8:00 AM – 8:40 AM	**Breakfast**	Majestic Ballroom
8:40 AM – 9:00 AM	**Opening Session**	Grand Ballroom I
9:00 AM – 10:00 AM	**Keynote 1: Wenjing Lou, Virginia Tech** *Strengthening Machine Learning-based Intrusion Detection Systems in Adversarial Environments*	Grand Ballroom I
10:00 AM – 10:30 AM	**Break**	Majestic Foyer
10:30 AM – 12:00 PM	**SESSION 1: MACHINE LEARNING 1** **Session Chair: Wenhai Sun (Purdue University)** *SecureImgStego: A Keyed Shuffling-based Deep Learning Model for Secure Image Steganography* Trishna Chakraborty (University of California, Irvine, USA), Imranur Rahman (North Carolina State University, USA), Hasan Murad (Chittagong University of Engineering and Technology, Bangladesh), Md Shohrab Hossain (Bangladesh University of Engineering and Technology, Bangladesh), Shagufta Mehnaz (The Pennsylvania State University, USA) *Machine Learning-Based Intrusion Detection for Swarm of Unmanned Aerial Vehicles* Umair Ahmad Mughal (Tennessee Tech University, USA), Samuel Hassler (Tennessee Tech University, USA), Muhammad Ismail (Tennessee Tech University, USA) *Byzantine-Robust Federated Learning with Variance Reduction and Differential Privacy* Zikai Zhang (University of Nevada, Reno, USA), Rui Hu (University of Nevada Reno, USA)	Grand Ballroom I

	Backdoor Attacks in Peer-to-Peer Federated Learning Gokberk Yar (Northeastern University, USA), Simona Boboila (Northeastern University, USA), Cristina Nita-Rotaru (Northeastern University, USA), Alina Oprea (Northeastern University, USA)	
12:00 PM – 1:30 PM	**Lunch**	Majestic Ballroom
1:30 PM – 3:00 PM	**PANEL: AI for xG Security** **Moderator: Chunyi Peng (Purdue University)** **Panelists:** • **Ehab Al-Shaer (Carnegie Mellon University)** • **Shagufta Mehnaz (Pennsylvania State University)** • **Guan-Hua Tu (Michigan State University)** • **Kai Zeng (George Mason University)**	Grand Ballroom I
3:00 PM – 3:30 PM	**Break**	Majestic Foyer
3:30 PM – 5:00 PM	**SESSION 2: PRIVACY** **Session Chair: Danda B. Rawat (Howard University)** *When Good Turns Evil: Encrypted 5G/4G Voice Calls Can Leak Your Identities* Jingwen Shi (Michigan State University, USA), Tian Xie (Utah State University, USA), Guan-Hua Tu (Michigan State University, USA) Chunyi Peng (Purdue University, USA), Chi-Yu Li (National Yang Ming Chiao Tung University, Taiwan), Andrew Hou (Michigan State University, USA), Sihan Wang (Michigan State University, USA), Yiwen Hu (Michigan State University, USA), Xinyu Lei (Michigan Technological University, USA), Min-Yue Chen (Michigan State University, USA), Li Xiao (Michigan State University, USA), Xiaoming Liu (Michigan State University, USA) *Speaker Anonymity and Voice Conversion Vulnerability: A Speaker Recognition Analysis* Shalini Saini (Texas A&M University, USA), Nitesh Saxena (Texas A&M University, USA) *P3LI5: Practical and Confidential Lawful Interception on the 5G Core* Francesco Intoci (EPFL & Armasuisse, Switzerland), Apostolos Pyrgelis (EPFL, Switzerland), Julian Sturm (ZITiS, Germany), Daniel Fraunholz (ZITiS, Germany), Colin Barschel (Armasuisse, Switzerland)	Grand Ballroom I

	Enhancing Security in NOMA-Based Networks: An Effective Deceptive Approach to Thwart Multiple Eavesdroppers Neji Mensi (Howard University, USA), Danda B. Rawat (Howard University, USA)	
6:00 PM – 8:00 PM	**Conference banquet**	Majestic Ballroom

Tuesday, October 3

TIME	SESSION	ROOM
8:00 AM – 6:00 PM	**Registration**	Majestic Foyer
8:00 AM – 9:00 AM	**Breakfast**	Majestic Ballroom
9:00 AM – 10:00 AM	**Keynote 2: Patrick McDaniel, University of Wisconsin, Madison** *The Evolving Landscape of the Security of Machine Learning: A Systems Perspective*	Grand Ballroom I
10:00 AM – 10:30 AM	**Break**	Majestic Foyer
10:30 AM – 12:00 PM	**SESSION 3: MOBILE AND WIRELESS SECURITY** **Session Chair: Tao Wang (University of North Carolina at Charlotte)** *Using Phone Sensors to Augment Vehicle Reliability* Noah T. Curran (University of Michigan, USA), Arun Ganesan (University of Michigan, USA), Mert D Pese (Clemson University, USA), Kang Shin (University of Michigan, USA) *RMDM: Using Random Meta-Atoms to Send Directional Misinformation to Eavesdroppers* Fahid Hassan (Rice University, USA), Zhambyl Shaikhanov (Rice University, USA), Hichem Guerboukha (Brown University, USA), Daniel Mittleman (Brown University, USA), Kaushik Sengupta (Princeton University, USA), Edward W. Knightly (Rice University, USA) *On the Domain Generalizability of RF Fingerprints Through Multifractal Dimension Representation*	Grand Ballroom I

	Benjamin Johnson (Oregon State University, USA), Bechir Hamdaoui (Oregon State University, USA) *Inter-Temporal Reward Decisions with Strategic Ethical Hackers* Jing Hou (California State University San Marcos, USA), Xuyu Wang (Florida International University, USA), Amy Z. Zeng (Suffolk University, USA)	
12:00 PM – 1:30 PM	**Lunch**	Majestic Ballroom
1:30 PM – 3:00 PM	**SESSION 4: MACHINE LEARNING 2** **Session Chair: Neji Mensi (Florida Institute of Technology)** *Are Existing Out-Of-Distribution Techniques Suitable for Network Intrusion Detection?* Andrea Corsini (University of Modena and Reggio Emilia, Italy), Shanchieh Jay Yang (Rochester Institute of Technology, USA) *A Stealthy Inference Attack on Split Learning with a Split-Fuse Defensive Measure* Sean Dougherty (Microsoft, USA), Abhinav Kumar (Saint Louis University, USA), Jie Hou (Saint Louis University, USA), Reza Tourani (Saint Louis University, USA), Atena Mtabakhi (Washington University in St. Louis, USA) *A Needle in a Haystack: Distinguishable Deep Neural Network Features for Domain-Agnostic Device Fingerprinting* Abdurrahman Elmaghbub (Oregon State University, USA), Bechir Hamdaoui (Oregon State University, USA) *VeriActor: Dynamic Generation of Challenge-Response Questions for Enhanced Email Sender Verification* Basel Abdeen (University of Texas at Dallas, USA), Ehab Al-Shaer (Carnegie Mellon University, USA), Waseem Shadid (UNC Charlotte, USA)	Grand Ballroom I
3:00 PM – 3:30 PM	**Break**	Majestic Foyer

3:30 PM – 5:25 PM	**SESSION 5: CYBER-PHYSICAL SYSTEMS** **Session Chair: Xuyu Wang (Florida International University)** *VetIoT: On Vetting IoT Defenses Enforcing Policies at Runtime* Akib Jawad Nafis (Syracuse University, USA), Omar Chowdhury (Stony Brook University, USA), Endadul Hoque (Syracuse University, USA) *Stealthy False Data Injection Attack on Unmanned Aerial Vehicles with Partial Knowledge* Umair Ahmad Mughal (Tennessee Tech University, USA), Muhammad Ismail (Tennessee Tech University, USA), Syed Ali Asad Rizvi (Tennessee Tech University, USA) *SmartLens: Robust Detection of Rogue Device via Frequency Domain Features in LoRa-Enabled IIoT* Subir Halder (University of Limerick, Ireland), Amrita Ghosal (University of Limerick, Ireland), Thomas Newe (University of Limerick, Ireland), Sajal K. Das (Missouri University of Science and Technology, USA) *Protecting Control Commands Using Low-Cost EM Sensors in the Smart Grid* Kylie L McClanahan (University of Arkansas, USA), Jingyao Fan (Pennsylvania State University, USA), Qinghua Li (University of Arkansas, USA), Guohong Cao (The Pennsylvania State University, USA) *Characterizing Cyber Attacks against Space Systems with Missing Data: Framework and Case Study* Ekzhin Ear (University of Colorado, Colorado Springs, USA), Jose L. C. Remy (University of Colorado, Colorado Springs, USA), Antonia Feffer (University of Colorado, Colorado Springs, USA), Shouhuai Xu (University of Colorado Colorado Springs, USA)	Grand Ballroom I
5:45 PM – 7:30 PM	**Poster Session and Reception**	Grand Ballroom II/III, and Terrace

Wednesday, October 4

TIME	SESSION	ROOM
8:00 AM – 6:00 PM	**Registration**	Majestic Foyer
8:00 AM – 9:00 AM	**Breakfast**	Majestic Ballroom
9:00 AM – 10:00 AM	**Keynote 3: Ninghui Li, Purdue University** *Membership Inference Attacks against Classifiers*	Grand Ballroom I
10:00 AM – 10:30 AM	**Break**	Majestic Foyer
10:30 AM – 12:00 PM	**SESSION 6: NETWORK SECURITY** **Session Chair: Mohammad Ashiqur Rahman (Florida International University)** *Toward Adaptive DDoS-Filtering Rule Generation* Jun Li (University of Oregon, USA), Devkishen Sisodia (University of Oregon, USA), Yebo Feng (University of Oregon, USA), Lumin Shi (University of Oregon, USA), Mingwei Zhang (University of Oregon, USA), Chris Early (University of Oregon, USA), Peter Reiher (UCLA, USA) *Autonomous Cyber Defense Against Dynamic Multi-strategy Infrastructural DDoS Attacks* Ashutosh Dutta (UNC Charlotte, USA), Ehab Al-Shaer (Carnegie Mellon University, USA), Samrat Chatterjee (Pacific Northwest National Laboratory, USA), Qi Duan (CyberDNA Security, USA) *Application-layer Characterization and Traffic Analysis for Encrypted QUIC Transport Protocol* Qianqian Zhang (Hughes Network Systems, USA & Virginia Tech, USA), Chi-Jiun Su (Hughes Network Systems, USA) *Authenticating Outsourced Location-Based Skyline Queries under Shortest Path Distance* Yidan Hu (Rochester Institute of Technology, USA), Yukun Dong (University of Delaware, USA), Wenxin Chen (University of Hawaii, USA), Yingfei Dong (University of Hawaii, USA), Rui Zhang (University of Delaware, USA)	Grand Ballroom I

12:00 PM – 1:30 PM	**Lunch**	Majestic Ballroom
1:30 PM – 3:00 PM	**SESSION 7: CRYPTOGRAPHY** **Session Chair: David Mohaisen (University of Central Florida)** *FAKey: Fake Hashed Key Attack on Payment Channel Networks* Alvi Ataur Khalil (Florida International University, USA), Mohammad Ashiqur Rahman (Florida International University, USA), Hisham A. Kholidy (State University of New York (SUNY) Polytechnic Institute, USA) *High-speed OFDM Physical-Layer Key Exchange* Radi Abubaker (University of Waterloo, Canada), Guang Gong (University of Waterloo, Canada) *BeamSec: A Practical mmWave Physical Layer Security Scheme Against Strong Adversaries* Afifa Ishtiaq (Technical University of Darmstadt, Germany), Arash Asadi (TU Darmstadt, Germany), Ladan Khaloopour (Technical University of Darmstadt, Germany), Waqar Ahmed (TU Darmstadt, Germany), Vahid Jamali (Technical University of Darmstadt, Germany), Matthias Hollick (Technische Universität Darmstadt & Secure Mobile Networking Lab, Germany) *Homomorphic Comparison Method Based on Dynamically Polynomial Composite Approximating Sign Function* Xiameng Feng (Xidian University, China), Xiaodong Li (Beijing Electronic Science and Technology Institute, China), Suya Zhou (Beijing Electronic Science and Technology Institute, China), Xin Jin (Beijing Electronic Science and Technology Institute, China)	Grand Ballroom I
3:00 PM – 3:30 PM	**Break**	Majestic Foyer
3:30 PM – 4:40 PM	**SESSION 8: SOFTWARE SECURITY** **Session Chair: Murat Kantarcioglu (University of Texas at Dallas)** *SecDINT: Preventing Data-oriented Attacks via Intel SGX Escorted Data Integrity*	Grand Ballroom I

	Dakun Shen (Zhejiang Lab, China), Tao Hou (Texas State University, USA), Zhuo Lu (University of South Florida, USA), Yao Liu (University of South Florida, USA), Tao Wang (New Mexico State University, USA) *MMIO Access-Based Coverage for Firmware Analysis* Ken (Yihang) Bai (University of Florida, USA), Tuba Yavuz (University of Florida, USA) *Empirical Analysis of Software Vulnerabilities Causing Timing Side Channels* M. Mehdi Kholoosi (The University of Adelaide, Australia), M. Ali Babar (The University of Adelaide, Australia), Cemal Yilmaz (Sabanci University, Turkey)	
4:40PM – 4:45 PM	**Closing**	Grand Ballroom I

Thursday, October 5

TIME	SESSION	ROOM
8:00 AM – 4:00 PM	Registration	Majestic Foyer
8:00 AM – 9:00 AM	Breakfast	Majestic Ballroom
9:00 AM – 5:00 PM	Cyber Resilience Workshop	Grand Ballroom II
9:00 AM – 5:00 PM	Cyber-Physical Systems Security (CPS-Sec 2023)	Grand Ballroom III