IEEE Conference on Communications and Network Security (IEEE CNS)

October 3 – 5, 2022

Austin, Texas, USA

CONFERENCE PROGRAM

(as of September 19)

Program At-a-Glance

IEEE CNS 2022 (Hybrid), Austin, Texas, USA, October 3 -5, 2022																									
PROGRAM SPACE ALLOCATION																									
SUNDAY, OCTOBER 2																									
ROOM NAME	**7:00**	**7:30**	**8:00**	**8:45**	**9:00**	**9:30**	**10:00**	**10:30**	**11:00**	**11:30**	**12:00**	**12:30**	**1:00**	**1:30**	**2:00**	**2:30**	**3:15**	**3:45**	**4:00**	**4:30**	**5:00**	**5:30**	**6:00**	**6:30**	**7:00**	**7:30**
Foyer																								Opening Reception		
MONDAY, OCTOBER 3																									
ROOM NAME	**7:00**	**7:30**	**8:00**	**8:45**	**9:00**	**9:30**	**10:00**	**10:30**	**11:00**	**11:30**	**12:00**	**12:30**	**1:00**	**1:30**	**2:00**	**2:30**	**3:15**	**3:45**	**4:00**	**4:30**	**5:00**	**5:30**	**6:00**	**6:30**	**7:00**	**7:30**
Room 400 and 402				Opening Session	Keynote: Guevara Noubir						Conf Lunch							Panel 1								
Room 417 AB								Session 1A						Session 2A												
Room 416 AB								Session 1B						Session 2B												
Foyer							Break										Break				Poster session					
Room 406																								Conference banquet		
TUESDAY, OCTOBER 4																									
ROOM NAME	**7:00**	**7:30**	**8:00**	**8:30**	**9:00**	**9:30**	**10:00**	**10:30**	**11:00**	**11:30**	**12:00**	**12:30**	**1:00**	**1:30**	**2:00**	**2:30**	**3:15**	**3:45**	**4:00**	**4:30**	**5:00**	**5:30**	**6:00**	**6:30**	**7:00**	**7:30**
Room 400 and 402					Keynote 2: Kevin Fu						Conf Lunch															
Room 417 AB								Session 3A						Session 4A				Session 5A (remote)								
Room 416 AB								Session 3B						Session 4B				Session 5B (remote)								
Room 406							Break										Break									
WEDNESDAY, OCTOBER 5																									
ROOM NAME	**7:00**	**7:30**	**8:00**	**8:30**	**9:00**	**9:30**	**10:00**	**10:30**	**11:00**	**11:30**	**12:00**	**12:30**	**1:00**	**1:30**	**2:00**	**2:30**	**3:00**	**3:30**	**4:00**	**4:30**	**5:00**	**5:30**	**6:00**	**6:30**	**7:00**	**7:30**
Room 400 and 402																										
Room 417 AB					CRW Workshop																					
Room 416 AB					CPS-SEC 2022 Workshop																					

Program Details

Sunday, October 2

TIME	SESSION	ROOM
4:00 PM – 7:00 PM	Registration	Foyer
6:30 PM – 8:30 PM	Welcome reception	Foyer

Monday, October 3

TIME	SESSION	ROOM
8:00 AM – 6:00 PM	**Registration**	Foyer
8:45 AM – 9:00 AM	**Opening Session**	400/402
9:00 AM – 10:00 AM	**Keynote 1: Guevara Noubir, Northeaster University**	400/402
10:00 AM – 10:30 AM	**Break**	Foyer
10:30 AM – 12:00 PM	**Session 1A: Adversarial ML** *ACADIA: Efficient and Robust Adversarial Attacks Against Deep Reinforcement Learning* Haider Ali and Mohannad Al Ameedi (Virginia Tech, USA); Ananthram Swami (Army Research Lab., USA); Rui Ning (Old Dominion University, USA); Jiang Li (Old Dominion University & Electrical and Computer Engineering, USA); Hongyi Wu (The University of Arizona, USA); Jin-Hee Cho (Virginia Tech, USA) *MultiEvasion: Evasion Attacks Against Multiple Malware Detectors*	417AB

	Hao Liu (University of Cincinnati, USA); Wenhai Sun (Purdue University, USA); Nan Niu and Boyang Wang (University of Cincinnati, USA) *Network-Level Adversaries in Federated Learning* Giorgio Severi (Northeastern University, USA); Matthew Jagielski (Google Research, USA); Gokberk Yar (Northeastern University, USA); Yuxuan Wang (LinkedIn Corporation, USA); Alina Oprea and Cristina Nita-Rotaru (Northeastern University, USA) *Transferability of Adversarial Examples in Machine Learning-based Malware Detection* Yang Hu (Virgina Tech, USA); Ning Wang (Virginia Tech, USA); Yimin Chen (University of Massachusetts Lowell, USA); Wenjing Lou and Thomas Hou (Virginia Tech, USA)	
10:30 AM – 12:00 PM	**Session 1B: Wireless Security** *5G Messaging: System Insecurity and Defenses* Jinghao Zhao (University of California, Los Angeles, USA); Qianru Li, Zengwen Yuan and Zhehui Zhang (UCLA, USA); Songwu Lu (University of California at Los Angeles, USA) *Absolute Security in High-Frequency Wireless Links* Alejandro Cohen (Technion, Israel); Rafael D'Oliveira (Clemson University, USA); Chia-Yi Yeh (MIT & Brown University, USA); Hichem Guerboukha, Rabi Shrestha and Zhaoji Fang (Brown University, USA); Edward W. Knightly (Rice University, USA); Muriel Médard (MIT, USA); Daniel Mittleman (Brown University, USA) *Learning-Based Radio Fingerprinting for RFID Secure Authentication Scheme* Jiaqi Xu (the Ohio State University, USA); Xingya Zhao, Arjun Bakshi and Kannan Srinivasan (The Ohio State University, USA) *Systematically Analyzing Vulnerabilities in Connection Establishment Phase of Wi-Fi Systems* Naureen Hoque, Hanif Rahbari and Cullen Rezendes (Rochester Institute of Technology, USA)	416AB
12:00 PM – 1:30 PM	**Lunch**	400/402

1:30 PM – 3:15 PM	**Session 2A: IoT & Authentication** *DASK: Driving-Assisted Secret Key Establishment* Edwin Yang and Song Fang (University of Oklahoma, USA); Dakun Shen (Central Michigan University, USA) *HoneyCam: Scalable High-Interaction Honeypot for IoT Cameras Based on 360-Degree Video* Chongqi Guan (Penn State University, USA); Xianda Chen, Guohong Cao, Sencun Zhu and Thomas La Porta (The Pennsylvania State University, USA) *A User-Friendly Two-Factor Authentication Method against Real-Time Phishing Attacks* Yuanyi Sun (Pennsylvania State University, USA); Sencun Zhu (The Pennsylvania State University, USA); Yao Zhao and Pengfei Sun (Shape Security, USA) *Eolo: IoT Proximity-based Authentication via Pressure Correlated Variations* Omar Ibrahim and Gabriele Oligeri (HBKU - CSE - ICT Division, Qatar); Roberto Di Pietro (Hamad Bin Khalifa University, Qatar) *GateKeeper: Operator-centric Trusted App Management Framework on ARM TrustZone* Balachandar Gowrisankar (National University of Singapore, Singapore); Daisuke Mashima (Advanced Digital Sciences Center & National University of Singapore, Singapore); Wen Shei Ong (Illinois at Singapore Pte Ltd, Singapore); Quanqi Ye and Ertem Esiner (Advanced Digital Sciences Center, Singapore); Binbin Chen (Singapore University of Technology and Design, Singapore); Zbigniew Kalbarczyk (University of Illinois at Urbana Champaign, USA)	417AB
1:30 PM – 3:15 PM	**Session 2B: Privacy** *Multi-Protocol IoT Network Reconnaissance* Stefan Gvozdenovic, Johannes K Becker, John Mikulskis and David Starobinski (Boston University, USA) *Agent-Level Differentially Private Federated Learning via Compressed Model Perturbation*	416AB

	Yuanxiong Guo (University of Texas at San Antonio, USA); Rui Hu (University of Nevada Reno, USA); Yanmin Gong (University of Texas at San Antonio, USA) *PRM - Private Interference Discovery for IEEE 802.15.4 Networks* Dominik Roy George (Eindhoven University of Technology, The Netherlands); Savio Sciancalepore (Eindhoven University of Technology (TU/e), The Netherlands) *TrafficSpy: Disaggregating VPN-encrypted IoT Network Traffic for User Privacy Inference* Qi Li, Keyang Yu and Dong Chen (Colorado School of Mines, USA); Mo Sha (Florida International University, USA); Long Cheng (Clemson University, USA)	
3:15 PM – 3:45 PM	**Break**	Foyer
3:45 PM – 5:00 PM	**Panel**	417AB
5:00 PM – 6:30 PM	**Poster session**	Foyer
6:30 PM – 8:30 PM	**Conference banquet**	406

Tuesday, October 4

TIME	SESSION	ROOM
8:00 AM – 6:00 PM	**Registration**	Foyer
9:00 AM – 10:00 AM	**Keynote 2: Kevin Fu, the University of Michigan** Title: *Wicked bizarre physics of analog sensor security*	400/402
10:00 AM – 10:30 AM	**Break**	Foyer
10:30 AM – 12:00 PM	**Session 3A: ML for Security** *An Active Learning Approach to Dynamic Alert Prioritization for Real-time Situational Awareness* Yeongwoo Kim and György Dán (KTH Royal Institute of Technology, Sweden) *AutoDefense: Reinforcement Learning Based Autoreactive Defense Against Network Attacks* Yu Mi (Case Western Reserve University, USA); David Mohaisen (University of Central Florida, USA); An Wang (Case Western Reserve University, USA) *Returning to Port: Efficient Detection of Home Router Devices* Thomas Papastergiou (Georgia Institute of Technology, USA); Roberto Perdisci (University of Georgia, USA); Manos Antonakakis (Georgia Tech, USA) *Supporting Law-Enforcement to Cope with Blacklisted Websites: Framework and Case Study* Mir Mehedi Ahsan Pritom (University of Texas at San Antonio, USA); Shouhuai Xu (University of Colorado Colorado Springs, USA)	417AB
10:30 AM – 12:00 PM	**Session 3B: PHY-Layer Security** *RadioNet: Robust Deep-Learning Based Radio Fingerprinting*	416AB

	Haipeng Li (University of Cincinnati, USA); Kaustubh Gupta (University of Nebraska - Lincoln, USA); Chenggang Wang (University of Cincinnati, USA); Nirnimesh Ghose (University of Nebraska - Lincoln, USA); Boyang Wang (University of Cincinnati, USA) *Securing Wireless Channels: Reliable Shared Secret Extraction through OTFS* Usama Saeed and Lingjia Liu (Virginia Tech, USA); Kai Zeng (George Mason University, USA); Robert Calderbank (Duke University, USA) *SIGTAM: A Tampering Attack on Wi-Fi Preamble Signaling and Countermeasures* Zhengguang Zhang and Marwan Krunz (University of Arizona, USA) *Stealthy Off-Target Coupled-Control-Plane Jamming* Shreya Gupta (Rice University, USA); Chia-Yi Yeh (MIT & Brown University, USA); Edward W. Knightly (Rice University, USA)	
12:00 PM – 1:30 PM	**Lunch**	400/402
1:30 PM – 3:15 PM	**Session 4A: Smartphone and System Security** *NL2GDPR: Automatically Develop GDPR Compliant Android Application Features from Natural Language* Faysal Hossain Shezan (University of Virginia, USA); Yingjie Lao (Clemson University, USA); Minlong Peng (Baidu Research, USA); Xin Wang (Baidu Research, China); Mingming Sun and Ping Li (Baidu Research, USA) *A Study on the Testing of Android Security Patches* Christopher D Brant and Tuba Yavuz (University of Florida, USA) *Performant Binary Fuzzing without Source Code using Static Instrumentation* Eric Pauley (University of Wisconsin-Madison); Gang Tan (Penn State University, USA); Danfeng Zhang and Patrick McDaniel (Pennsylvania State University, USA)	417AB

	SysCap: Profiling and Crosschecking Syscall and Capability Configurations for Docker Images Yunlong Xing (George Mason University, USA); Jiahao Cao (Tsinghua University, China); Xinda Wang, Sadegh Torabi and Kun Sun (George Mason University, USA); Fei Yan (Wuhan University, China); Qi Li (Tsinghua University, China) *HallMonitor: A Framework for Identifying Network Policy Violations in Software* Daniel Olszewski, Patrick Traynor, Kevin Butler, Weidong Zhu and Sandeep Sathyanarayana (University of Florida, USA)	
1:30 PM – 3:15 PM	**Session 4B: IDS and Network Security** *Error Prevalence in NIDS datasets: A Case Study on CIC-IDS-2017 and CSE-CIC-IDS-2018* Lisa Liu (University of New South Wales, Australia); Gints Engelen (imec-DistriNet, KU Leuven, Belgium); Timothy Lynar (University of New South Wales at the Australian Defence Force Academy, Australia); Daryl Essam (University of New South Wales at the Australian Defence Force Academy UNSW@ADFA, Australia); Wouter I Joosen (University of Leuven, Belgium) *Enhancing Load Balancing by Intrusion Detection System Chain on SDN Data Plane* Nadia Niknami and Jie Wu (Temple University, USA) *Detecting DNS hijacking by using NetFlow data* Martin Fejrskov (Aalborg University & Telenor Denmark, Denmark); Emmanouil Vasilomanolakis (Technical University of Denmark, Denmark); Jens M. Pedersen (Aalborg University, Denmark) *Refining Network Message Segmentation with Principal Component Analysis* Stephan Kleber (Ulm University & Mercedes-Benz Tech Innovation, Germany); Frank Kargl (Ulm University, Germany) *When Third-Party JavaScript Meets Cache: Explosively Amplifying Security Risks on the Internet* Tao Hou (Texas State University, USA); Shengping Bi (New Mexico State University, USA); Mingkui Wei (George Mason University, USA); Tao Wang (New Mexico State University, USA); Zhuo Lu and Yao Liu (University of South Florida, USA)	416AB

3:15 PM – 3:45 PM	**Break**	Foyer
3:45 PM – 5:00 PM	**Session 5A (remote presentations): ML/Blockchain** *Membership Inference Attack in Face of Data Transformations* Jiyu Chen (University of California, Davis, USA); Yiwen Guo (USA); Hao Chen (UC Davis, USA); Neil Gong (Duke University, USA) *Efficient Public Verification of Confidential Supply-Chain Transactions* Kilian Becher and Mirko Schaefer (Technische Universität Dresden & SAP SE, Germany); Axel Schroepfer (SAP AG, Germany); Thorsten Strufe (Karlsruhe Institute of Technology & Centre for Tactile Internet (CeTI)/TU Dresden, Germany) *On Security of Proof-of-Policy (PoP) in the Execute-Order-Validate Blockchain Paradigm* Shan Wang and Ming Yang (Southeast University, China); Bryan Pearson (University of Central Florida, USA); Tingjian Ge (University of Massachusetts, Lowell, USA); Xinwen Fu (University of Massachusetts Lowell, USA); Wei Zhao (Shenzhen Institute of Advanced Technology, China) *Ransomware Detection in Databases through Dynamic Analysis of Query Sequences* Christoph Sendner, Lukas Iffländer, Sebastian Schindler, Michael Jobst and Alexandra Dmitrienko (University of Würzburg, Germany); Samuel Kounev (University of Wuerzburg, Germany)	417AB
3:45 PM – 5:00 PM	**Session 5B (remote presentations): IoT/Wireless** *Alexa Skills: Security Vulnerabilities and Countermeasures* Dan Su (Beijing Jiaotong University, China); Jiqiang Liu (Beijing Jiao Tong University, China); Sencun Zhu (The Pennsylvania State University, USA); Wei Wang and Xiaoyang Wang (Beijing Jiaotong University, China) *Securing Communication Against Leaky Switches* Leila Rashidi, Sogand Sadrhaghighi and Majid Ghaderi (University of Calgary, Canada); Cristina Nita-Rotaru (Northeastern University, USA); Reihaneh Safavi-Naini (University of Calgary, Canada)	416AB

	Security Analysis of Mixed RF-FSO Blockage Attack Over Generalized RF Fading and Atmospheric Turbulence Neji Mensi, Danda B. Rawat and Chunmei Liu (Howard University, USA) *Tweak: Towards Portable Deep Learning Models for Domain-Agnostic LoRa Device Authentication* Jared Gaskin, Bechir Hamdaoui and Weng-Keen Wong (Oregon State University, USA)	

Wednesday, October 5

TIME	SESSION	ROOM
8:00 AM – 10:00 AM	Registration	Foyer
9:00 AM – 12:00 PM	CRW Workshop	417AB
9:00 AM – 12:00 PM	CPS-SEC 2022 Workshop	416AB