NEHWS Day 2025
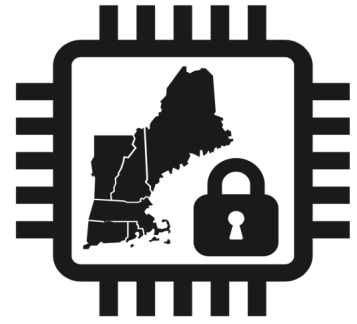
April 18th, 2025
Massachusetts Institute of Technology
Samberg Conference Center, Chang Building

Time				
9:00 - 9:15	Welcome Remarks			Session chair: Mengjia Yan
9:15 - 9:30	Opening remarks by Dean of the MIT Schwarzman College of Computing, Daniel Huttenlocher			Session chair: Mengjia Yan
	News from the NEHWS Community			
9:30 - 10:30	Invited Keynote by Todd Austin (University of Michigan)			
10:30 - 10:45	Break			
10:45 - 12:00	Submitted Talks-- Session I			Session chair: Xiaolin Xu
	Long Talk	FaultDetective: Explainable to a Fault, from the Design Layout to the Software Zhenyuan Liu, Dillibabu Shanmugam and Patrick Schaumont		
	Short Talk	BackMon: IC Backside Tamper Detection using On-Chip Impedance Monitoring Tahoura Mosavirik and Shahin Tajik		
	Long Talk	Who's in Control? Security Risks in Commercial ADAS Yingjie Cao, George Crane, Haoqi Shan and Dean Sullivan		
	Short Talk	Energy-Accuracy-Security Trade-offs in Resistive In-Memory Computing Architectures Saion Roy and Naresh Shanbhag		
	Long Talk	VGF: :Value-Guided Fuzzing -- Fuzzing Hardware as Hardware -- Ruochen Dai, Michael Lee, Patrick Hoey, Weimin Fu, Yier Jin, Xiaolong Guo, Shuo Wang, Dean Sullivan, Tuba Yavuz and Orlando Arias		
	Short Talk	USBSnoop - Revealing Device Activities via USB Congestions Davis Ranney, Yufei Wang, A. Adam Ding and Yunsi Fei		
12:00 - 1:30	Lunch and Poster Session			
1:30 - 2:30	Panel "Secure-by-Construction for Hardware Design: Mission Impossible or Walk in the Park?" - Shivam Basin (Nanyang Technical University) - Srini Devadas (Massachusetts Institute of Technology) - Sharad Malik (Princeton University) - Christof Paar (Max Planck Institute) - Dominic Rizzo (zeroRISC)			Session chair: Daniel Holcomb
2:30 - 3:30	Invited Keynote by Edward Suh (Nvidia)			Session chair: Dean Sullivan
3:30 - 3:40	Break			
3:40 - 4:45	Submitted Talks-- Session II			Session chair: Dean Sullivan
	Long Talk	Exploiting Exclusive System-Level Cache in Apple M-Series SoCs for Enhanced Cache Occupancy Attacks Tianhong Xu, Aidong Ding and Yunsi Fei		
	Short Talk	Uncertainty Estimation in Neural Network-enabled Side-channel Analysis and Links to Interpretability Seyedmohammad Nouraniboosjin and Fatemeh Ganji		
	Long Talk	Oreo: Protecting ASLR Against Microarchitectural Attacks Shixin Song, Joseph Zhang and Mengjia Yan		
	Short Talk	Cross-Layer EM Fault Injection Assessment Framework Hanqiu Wang, Ruochen Dai, Tuba Yavuz, Xiaolong Guo, Orlando Arias, Dean Sullivan, Siqi Dai, Honggang Yu, Michael Lee, Domenic Forte and Shuo Wang		
	Long Talk	IvLeague: Side Channel-resistant Secure Architectures Using Isolated Domains of Dynamic Integrity Trees Md Hafizul Islam Chowdhuryy and Fan Yao		
4:45 - 5:45	Invited Keynote by Makoto Nagata (Kobe University)			Session chair: Patrick Schaumont
5:45 - 6:00	Best Poster Award and Closing Remarks			Session chairs: Yingjie Lao
6:00 - 7:00	Networking reception			