

WNSP Scoring Sheet for Paper Presentation — Day 1

Rater: Date: 2025-10-29

Scoring Category and Criteria:
Organization (Org.): Relevance, clarity, integrity, and originality
Key Message Delivery (KMD.): Accuracy, stress, and clarity
Presentation Skill (PS.): Fluent expression, appropriate speed, dynamic, expressiveness, manners, gestures
Slide Design (SD.): Visual clarity, aesthetics, and relevance
Time Management (TM.): Observation of 12 mins presentation and 3 mins Q&A
Q&A Part (Q&A): Accuracy and clarity of answers
Total Score (Total): The sum of the six categories above.

Session	Time	Speaker	Paper Title	Score (1 to 5)						Total
1. Side Channel	13:30-13:45	屈子轩	I Know What You Said: Unveiling Hardware Cache Side-Channels in Local Large Language Model Inference (USENIX 2025)	Org.:	KMD.:	PS.:	SD.:	TM.:	Q&A:	
	13:45-14:00	张天译	HubBub: Contention-Based Side-Channel Attacks on USB Hubs (USENIX 2025)	Org.:	KMD.:	PS.:	SD.:	TM.:	Q&A:	
2. AI Security	14:00-14:15	Omar	JailbreakEval: An Integrated Toolkit for Evaluating Jailbreak Attempts Against Large Language Models (NDSS 2025, Best Technical Poster Award)	Org.:	KMD.:	PS.:	SD.:	TM.:	Q&A:	
	14:15-14:30	陈孟	DataSentinel: A Game-Theoretic Detection of Prompt Injection Attacks (S&P 2025, distinguished paper)	Org.:	KMD.:	PS.:	SD.:	TM.:	Q&A:	
	14:30-14:45	钟焕龙	PropertyGPT: LLM-driven Formal Verification of Smart Contracts through Retrieval-Augmented Property Generation (NDSS 2025, distinguished paper)	Org.:	KMD.:	PS.:	SD.:	TM.:	Q&A:	
	14:45-15:00	陈馨怡	SHAFT: Secure, Handy, Accurate and Fast Transformer Inference (NDSS 2025, Artifact Evaluation Award)	Org.:	KMD.:	PS.:	SD.:	TM.:	Q&A:	
	15:00-15:15	郝思诺	EmbedX: Embedding-Based Cross-Trigger Backdoor Attack Against Large Language Models (USENIX 2025)	Org.:	KMD.:	PS.:	SD.:	TM.:	Q&A:	
	15:15-15:30	王潇锐	Don't Listen To Me: Understanding and Exploring Jailbreak Prompts of Large Language Models (USENIX 2024, Best Paper Award)	Org.:	KMD.:	PS.:	SD.:	TM.:	Q&A:	
	15:30-15:45	宋颖	RAG-WM: An Efficient Black-Box Watermarking Approach for Retrieval-Augmented Generation of Large Language Models (CCS 2025)	Org.:	KMD.:	PS.:	SD.:	TM.:	Q&A:	
	15:45-16:00	陈昕磊	Prompt Inference Attack on Distributed Large Language Model Inference Frameworks (CCS 2025)	Org.:	KMD.:	PS.:	SD.:	TM.:	Q&A:	
	16:00-16:15	何益馨	SafeGuider: Robust and Practical Content Safety Control for Text-to-Image Models (CCS 2025)	Org.:	KMD.:	PS.:	SD.:	TM.:	Q&A:	
	16:15-16:30	沈子扬	Fuzz-Testing Meets LLM-Based Agents: An Automated and Efficient Framework for Jailbreaking Text-To-Image Generation Models (S&P 2025)	Org.:	KMD.:	PS.:	SD.:	TM.:	Q&A:	

WNSP Scoring Sheet for Paper Presentation — Day 2

Rater: Date: 2025-11-05

Scoring Category and Criteria:
Organization (Org.): Relevance, clarity, integrity, and originality
Key Message Delivery (KMD.): Accuracy, stress, and clarity
Presentation Skill (PS.): Fluent expression, appropriate speed, dynamic, expressiveness, manners, gestures
Slide Design (SD.): Visual clarity, aesthetics, and relevance
Time Management (TM.): Observation of 12 mins presentation and 3 mins Q&A
Q&A Part (Q&A): Accuracy and clarity of answers
Total Score (Total): The sum of the six categories above.

Session	Time	Speaker	Paper Title	Score (1 to 5)						Total
2. AI Security (Cont.)	13:30-13:45	徐卓	Neuromorphic overparameterisation and few-shot learning in multilayer physical neural networks (nature communications)	Org.:	KMD.:	PS.:	SD.:	TM.:	Q&A:	
3. Cyber Security	13:45-14:00	祝怡婷	My Model is Malware to You: Transforming AI Models into Malware by Abusing TensorFlow APIs (S&P 2025)	Org.:	KMD.:	PS.:	SD.:	TM.:	Q&A:	
	14:00-14:15	汪浩宇	ReDAN: An Empirical Study on Remote DoS Attacks against NAT Networks (NDSS 2025, distinguished paper)	Org.:	KMD.:	PS.:	SD.:	TM.:	Q&A:	
4. Sensor Security	14:15-14:30	李炫睿	ReThink: Reveal the Threat of Electromagnetic Interference on Power Inverters (NDSS 2025, distinguished paper)	Org.:	KMD.:	PS.:	SD.:	TM.:	Q&A:	
	14:30-14:45	王培旺	PowerRadio: Manipulate Sensor Measurement via Power GND Radiation (NDSS 2025)	Org.:	KMD.:	PS.:	SD.:	TM.:	Q&A:	
	14:45-15:00	吕明远	GhostShot: Manipulating the Image of CCD Cameras with Electromagnetic Interference (NDSS 2025)	Org.:	KMD.:	PS.:	SD.:	TM.:	Q&A:	
	15:00-15:15	杜衡	UnMarker: A Universal Attack on Defensive Image Watermarking (S&P 2025)	Org.:	KMD.:	PS.:	SD.:	TM.:	Q&A:	
	15:15-15:30	郑玮凡	Investigating Physical Latency Attacks against Camera-based Perception (S&P 2025)	Org.:	KMD.:	PS.:	SD.:	TM.:	Q&A:	
	15:30-15:45	席长	CamLoPA: A Hidden Wireless Camera Localization Framework via Signal Propagation Path Analysis (S&P 2025)	Org.:	KMD.:	PS.:	SD.:	TM.:	Q&A:	
	15:45-16:00	吕启飞	DiffLoc: WiFi Hidden Camera Localization Based on Electromagnetic Diffraction (USENIX 2025)	Org.:	KMD.:	PS.:	SD.:	TM.:	Q&A:	
	16:00-16:15	安腾	Neuromorphic overparameterisation and few-shot learning in multilayer physical neural networks (nature electronics)	Org.:	KMD.:	PS.:	SD.:	TM.:	Q&A:	