

時間戳記	Name	Student ID	Time	Topic			
2022/5/5 上午 8:40:18	Muhammad Nasar	110064891	6/9 (Thursday) 10:10~10:	MaMloT: Manipulation of Energy Market Leveraging High Wattage IoT Botnets			
2022/5/5 下午 12:10:34	劉奎元	110064558	6/2 (Thursday) 11:35~12:	Packet scheduling with optional client privacy			
2022/5/5 下午 12:42:47	莊孝萱	106062105	5/19 (Thursday) 10:10~10:	"I need a better description": An Investigation Into User Expectations For Differential Privacy			
2022/5/5 下午 3:01:50	陳劭圻	110064533	5/16 (Monday) 9:00~9:25	DNS Cache Poisoning Attack: Resurrections with Side Channels			
2022/5/5 下午 10:26:47	李嘉淳	110064537	5/19 (Thursday) 11:10~11:	Let's Downgrade Let's Encrypt			
2022/5/6 上午 12:38:31	郭孟軒	110064532	5/19 (Thursday) 10:35~11:	COINN: Crypto/ML Codesign for Oblivious Inference via Neural Networks			
2022/5/6 上午 11:26:05	石富凱	110064515	5/23 (Monday) 9:00~9:25	Android on PC: On the Security of End-user Android Emulators			
2022/5/6 下午 2:20:19	林柔	110064851	5/23 (Monday) 9:25~9:50	Hidden Backdoors in Human-Centric Language Models			
2022/5/6 下午 10:16:45	黃毅瑄	110064559	5/16 (Monday) 9:25~9:50	Usable User Authentication on a Smartwatch using Vibration			
2022/5/7 上午 1:45:57	陳品諤	110064506	5/26 (Thursday) 10:10~10:	"Hello, It's Me": Deep Learning-based Speech Synthesis Attacks in the Real World			
2022/5/7 上午 2:17:08	蕭欣倫	110064536	5/19 (Thursday) 11:35~12:	RealSWATT: Remote Software-based Attestation for Embedded Devices under Realtime Constraints			
2022/5/7 上午 3:18:49	石哲瑋	110064552	6/6 (Monday) 9:00~9:25	Cert-RNN: Towards Certifying the Robustness of Recurrent Neural Networks			
2022/5/8 上午 3:32:44	楊舒晴	106091221	6/2 (Thursday) 10:35~11:	The Invisible Shadow: How Security Cameras Leak Private Activities			
2022/5/8 下午 4:57:05	邱琬晶	107062261	5/26 (Thursday) 10:35~11:	FakeWake: Understanding and Mitigating Fake Wake-up Words of Voice Assistants			
2022/5/8 下午 5:14:10	黃振維	107062163	5/26 (Thursday) 11:10~11:	Can We Use Arbitrary Objects to Attack LiDAR Perception in Autonomous Driving?			
2022/5/9 上午 1:17:54	藍婷瑜	110064553	6/2 (Thursday) 11:10~11:	T-Reqs: HTTP Request Smuggling with Differential Fuzzing			
2022/5/9 上午 2:26:49	Phone Myint Ko	110064893	6/2 (Thursday) 10:10~10:	I Can See the Light: Attacks on Autonomous Vehicles Using Invisible Lights			
2022/5/9 上午 11:47:54	張家修	110064503	5/30 (Monday) 9:25~9:50	Wireless Charging Power Side-Channel Attacks			
2022/5/10 下午 12:59:22	孫槐駿	110062466	5/26 (Thursday) 11:35~12:	Realtime Robust Malicious Traffic Detection via Frequency Domain Analysis			
2022/5/11 下午 5:33:52	羅詔文	107021206	6/6 (Monday) 9:25~9:50	Verifying Table-Based Elections			