Week	Chapter	Teaching Contents	Presenters
1	Course Introduction	1. Cybersecurity Overview 2. The Motivation of Attacks 3. The Marketplace for Exploits 4. Trust Model	
2	Memory Safety and Control Hijacking Attacks	1. Control hijacking overview 2. Process memory layout 3. Attack Techniques: a) Buffer overflows b) Use after free c) Double free d) Format string bugs 4. Write^Exec tradeoff 5. Return-oriented programming 6. Defense Techniques: a) Architecture platform defenses b) Software executable hardening 7. Control Flow Integrity (CFI)	毛宸炀 徐启翰
3	Security Principles and OS Security	1. Threat model 2. Security principles 3. UNIX security model 4. UNIX processes 5. Windows security model 6. Chrome security architecture	杨在洲
4	Isolation and Sandboxing	1. The confinement principle	陈炫昕 林亚旋

		2. Processes and system call interposition 3. Virtual machines 4. Threads and software fault isolation	宋子宁
5	Microarchitecture security I Trusted Execution Environments (TEE) and Side Channels	1. Trusted computing base (TCB) 2. Enclaves 3. Intel SGX and TDX 4. Covert channels and side channels 5. Timing side-channel attacks	赵俊阳 卢昱州
6	Microarchitecture security II Side-channel and Transient Execution Attacks	1. Cache side-channel attacks 2. Other side-channel attacks a) Timing b) Power c) etc. 3. Speculative execution 4. Spectre Attack and its variants 5. Out-of-order execution 6. Meltdown Attack and its variants	刘培富 李浩宇 卢健均
7	Web Security I (Model & Attacks)	1. Web security model 2. HTTP 3. Cookies and sessions 4. Cross-site request forgery (CSRF) 5. SQL injection	丁翰飞 陆天成 江骏

		6. Cross site scripting (XSS)	
8	Cryptography Overview	1. Symmetric encryption 2. Crypto and compression 3. Public key encryption 4. TLS	蒋天昊 王润森 夏嘉璟 余宜芯 陈汤林
9	Web Security II (Defenses and HTTPS)	1. CSRF defenses 2. XSS defenses 3. Clickjacking 4. Sub-resource integrity 5. Secure cookies 6. Authentication and session management 7. Phishing 8. Password+ 9. TLS and certificates 10. HTTPS	
10	Internet Protocols	1. OSI 5 layer model 2. Internet Protocol (IP) 3. Transmission Control Protocol (TCP) 4. TCP connection spoofing and TCP reset attack 5. Domain Name Service (DNS) 6. Packets	
11	Internet Security; Privacy,	1. DNS cache poisoning 2. DNS spoofing 3. Kaminsky Attack	

	Anonymity and Censorship	4. DNS rebinding 5. Denial of Service (DoS) Attacks 6. Amplification Attacks 7. Botnet and Mirai malware 8. Network defenses 9. Remote access 10. Privacy, cookies and tracking 11. Anonymity and Tor 12. Internet censorship 13. Email protection 14. Off the Record (OTR) chat	
12	Automotive and Adversarial Machine Learning	1. Digital controls and software 2. CAN Bus and ECUs 3. Automotive connectivity a) Media player b) OBD-II c) Bluetooth d) Cellular 4. Self-driving car 5. Vision sensors 6. Adversarial Learning 7. GPS sensors and spoofing	杜佳颖
13-16	Course Projects	1. Course project discussion and presentation	