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)	
3 & 4	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	
5	Isolation and Sandboxing	1. The confinement principle 2. Processes and system call interposition 3. Virtual machines 4. Threads and software fault isolation	

6	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. Acoustic side-channel attacks	
7	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	
8	Automotive and AI (LLM, agents)	1. Digital controls and software 2. CAN Bus and ECUs 3. Automotive connectivity a) OBD-II b) Bluetooth c) Cellular 4. Self-driving vehicles 5. AI Security vs. AI Safety 6. Adversarial machine learning 7. Poisoning, backdoors, and privacy attacks 8. LLM jailbreaks and prompt injection 9. Security of tool-using agents	

		10. AI-assisted cyber offense and defense 11. Alignment and reward hacking Safety evaluation, interpretability, and runtime control	
9	Web Security I (Model & Attacks)	1. Web security model 2. HTTP 3. Cookies and sessions 4. Cross-site request forgery (CSRF) 5. SQL injection 6. Cross site scripting (XSS)	
11	Cryptography Overview And Invited Special Speaker	1. Symmetric encryption 2. Crypto and compression 3. Public key encryption 4. TLS 5. **SPECIAL TOPIC**: How real security research in industry is	
12	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	

13	Internet Security; Privacy, Anonymity and Censorship	1. Internet Protocols a) IP b) TCP c) DNS 2. DNS cache poisoning 3. DNS spoofing 4. Kaminsky Attack 5. DNS rebinding 6. Denial of Service (DoS) Attacks 7. Amplification Attacks 8. Botnet and Mirai malware 9. Network defenses 10. Remote access 11. Privacy, cookies and tracking 12. Anonymity and Tor 13. Internet censorship 14. Email protection 15. Off the Record (OTR) chat	
10, 14-16	Course Projects	1. Course project discussion and presentation	