

Secure Systems Engineering (cs6570)

Feb-May 2021

Chester Rebeiro, IIT Madras

Schedule

Google Meet Link: <https://meet.google.com/fhk-hznx-rkc>

Day	Topics Covered	Video
1) 1/2/2021 (M)	Introduction to the Course	link
2) 2/2/2021 (Tu)	Binary Exploitation 1 Buffer Overflows in the Stack	link
3) 3/2/2021 (W)	First exploit!	link
4) 4/2/2021 (Th)	Demonstration of a buffer overflow in the stack	link
5) 8/2/2021 (M)	layers of Defense	link
6) 9/2/2021 (Tu)	W^X and canaries	link
7) 10/2/2021 (W)	Return to lib C attacks	link
8) 11/2/2021 (Th)	Tutorial 1 & Assignment 1 Buffer Overflows on the Stack	link
9) 15/2/2021 (M)	ROP attacks (1)	link
10) 16/2/2021 (Tu)	ROP attacks (2)	link
11) 17/2/2021 (W)	ROP attacks (3)	link
12) 18/2/2021 (Th)	Tutorial 2 & Assignment 2 Buffer Overflows on the Stack.	link
13) 22/2/2021 (M)	ASLR: Load time relocation	link
14) 23/2/2021 (Tu)	ASLR: Position Independent Code	link

15) 24/2/2021 (W)	ASLR: lazy binding for function calls	link
16) 25/2/2021 (Th)	Assignment 2 continued	link
17) 1/3/2021 (M)	Binary Exploitation 2 Heart Bleed Attack	link
18) 2/3/2021 (Tu)	Format string vulnerabilities	link
19) 3/3/2021 (W)	format string and integer vulnerabilities	link
20) 4/3/2021 (Th)	Tutorial 3 & Assignment 3 ROP attacks	link
21) 8//3/2021 (M)	format string and heap exploits	link
22) 9/3/2021 (Tu)	Heap internals	link
23) 10/3/2021 (W)	Heap Internals	link
24) 11/3/2021 (Th)	Tutorial 4 & Assignment 4 Format String Vulnerabilities	link
25) 15/3/2021 (M)	Heap internals	link
26) 16/3/2021 (Tu)	Heap internals and vulnerability	link
27) 17/3/2021 (W)	Access Control Policies	link
28) 22/3/2021 (M)	Access Control Policies and Unix Access Control policies	link
29) 23/3/2021 (Tu)	Mid-semester exam *syllabus till and including heaps*	
30) 24/3/2021 (W)	Unix Access Control Policies	link
31) 25/3/2021 (Th)	Tutorial 5 Heap exploit	link
32) 5/4/2021 (M)	Information flow policies	link
33) 7/4/2021 (W)	Confinement	link
34) 8/4/2021 (Th)	discussions on tutorial 5	link
35) 12/4/2021 (M)	Design of a webserver with least privileges (OKSW)	link
36) 15/4/2021 (Th)	OKWS	link
37) 17/4/2021 (Sat)	CTF	link

38) 19//4/2021 (M)	OKWS and web-browser security	link
39) 20/4/2021 (Tu)	Web-browser security	link
40) 21/4/2021 (W)	Web-browser Security	link
41) 22/4/2021 (Th)	Trusted Execution Environments ARM Trustzone	link
42) 26/4/2021 (M)	ARM Trustzone	link
43) 27/4/2021 (Tu)	Secure boot	link
44) 28/4/2021 (W)	Intel SGX	link
45) 29/4/2021 (Th)	Intel SGX	link
46) 3/5/2021 (M)	Micro-architectural Attacks flush+reload	link
47) 4/5/2021 (Tu)	prime+probe	link
48) 5/5/2021 (W)	Meltdown	link
49) 6/5/2021 (Th)	Spectre	link