Secure Systems Engineering (cs6570)

Aug - Nov 2018

Chester Rebeiro, IIT Madras

Schedule

Quiz and End Sem Schedule **Mid Semester :** 28/8/2018 **EndSem :** 9/11/2018	**Grading Policy** MidSemester Exam: 25% Endsem Exam / Project: 25% Assignments : 50%
Attendance requirements as per Institute norms	

Google Group (https://groups.google.com/forum/#!forum/sse_iitm_2018)

Class	Coverage
[1] 31/7/2018 (Tu)	Introduction
[2] 1/8/2018 (W)	Security Engineering
[3] 2/8/2018 (Th)	**Binary Exploitation:** Buffer Overflow Attacks
[4] 3/7/2018 (Fr)	GDB tutorial; Threat assumptions, security goals and security policy
[5] 7/8/2018 (Tu)	Buffer overflow attacks (payloads), Canaries
[6] 9/8/2018 (W)	W^X, return-to-libc
[7] 10/8/2018 (F)	Tutorial 1 (Buffer overflows; stack format)
[8] 13/8/2018 (M)	ROP Attacks

[9] 14/8/2018 (W)	ROP Attacks; Creating Gadgets
[10] 16/8/2018 (Th)	ELF, ASLR
[11] 17/8/2018 (F)	Tutorial 1b (Buffer overflow Attack; writing a payload)
[12] 21/8/2018 (Tu)	PLT, GOT Tables, etc.
[13] 23/8/2018 (Th)	PLT
[14] 24/8/2018 (F)	Tutorial 2 (PLT, Reloc, GOT)
[15] 28/8/2018 (Tu)	Binary Exploits 2: Buffer Overreads
[16] 29/8/2018 (W)	Format String Vulnerabilities; Integer Overflow Vulnerability
[17] 30/8/2018 (Th)	Integer Overflow Vulnerability and Heap Exploits
[18] 31/8/2018 (Fr)	Tutorial 2b (PLT, Reloc, GOT executing a payload)
[19] 4/9/2018 (Tu)	Heap Exploits / course project description
[20] 5/9/2018 (W)	Heap Exploits
[21] 6/9/2018 (Th)	**Access Control Policies** DAC
[22] 7/9/2018 (Fr)	Processor Enhancements for Memory Security (Gnanambikai Krishnakumar)
[23] 11/9/2018 (Tu)	Unix Security Mechanisms
[24] 12/9/2018 (W)	MAC: Bell LaPadula
[25] 14/9/2018 (F)	Tutorial 3: Heap Tracer
[26] 17/9/2018 (M)	Tutorial 3b: Heap Exploit
[27] 18/9/2018 (Tu)	Covert Channel
[28] 19/9/2018 (W)	Biba Model **Confinement** OKWS : Process based confinement
[29] 20/9/2018 (Th)	OKWS, Software Fault Isolation
[31] 25/9/2018 (Tu)	Software Fault Isolation (SFI)
[32] 27/9/2018 (Th)	SFI: Software Fault Isolation

[33] 28/9/2018 (F)	Mid Semester Quiz
[34] 3/10/2018 (W)	**Trusted Execution Environments** ARM Trustzone
[35] 4/10/2018 (Th)	ARM Trustzone
[36] 5/10/2018 (Fr)	ARM Trustzone; Secure Boot
[37] 6/10/2018 (Sat)	Tutorial 4: Ethical Hacking Workshop
[38] 9/10/2018 (Tu)	Intel SGX
[39] 10/10/2018 (W)	Intel SGX; PoET
[40] 11/10/2018 (Th)	**Hardware Security** Physically Unclonable Functions
[41] 12/10/2018 (Fr)	Tutorial 5: Covert channels tutorial
[42] 16/10/2018 (Tu)	Physically Unclonable Functions
[43] 17/10/2018 (W)	Hardware Trojans
[44] 18/10/2018 (Th)	Hardware Trojans
[45] 23/10/2018 (Tu)	**Micro-architectural Attacks** Cache Timing Attacks (flush+reload, prime+probe, evict+time (external collisions), time-driven (internal collisions))
[46] 24/10/2018 (W)	Cache Timing Attacks : Beyond Cryptography (cloud computing, keyboard sniffing, machine learning, breaking ASLR)
[47] 25/10/2018 (Th)	Time-driven attacks
[48] 26/10/2018 (Fr)	Tutorial 6: Meltdown / Spectre Tutorial
[49] 30/10/2018 (Tu)	Spectre, Meltdown / Spectre Countermeasures
[50] 31/10/2018 (W)	**Hardware Security (continued)** Power Analysis Attacks
[51] 1/11/2018 (Th)	Power Attacks and Countermeasures
[52] 7/11/2018 (W)	Q and A sessions (clearing doubts etc.) by Nikhilesh Singh
[53] 8/11/2018 (Th)	Q and A sessions (clearing doubts etc.)

[54] 9/11/2018 (F)	End Semester Examination
16/11/2018	Deadline for project submissions