INFORMATION SECURITY - 5 - SECURE SYSTEMS ENGINEERING

PROF. CHESTER REBEIRO
Department of Computer Science and Engineering
IIT Madras

PRE-REQUISITES : C programming must be strong. Minimum understanding of digital logic/ operating systems/computer organization

INTENDED AUDIENCE : BTech/BE/ME/MTech/MS/MCA/BCA students in computer science/information technology/electrical engineering / electronics engineering /instrumentation engineering

INDUSTRIES APPLICABLE TO : All companies developing embedded products /IoT etc.

COURSE OUTLINE :
With the increase in the threat of cyber-security attacks, it is important to develop computer systems that are not only efficient but also secure. This course will discuss various vulnerabilities in systems and mechanisms by which these vulnerabilities can be mitigated. The first part of the course will discuss various security vulnerabilities in software code that, if left unfixed, can potentially lead to major cyber-attacks. We will see how these vulnerabilities can arise from simple programming flaws like a buffer that overflows, to complex application runtime characteristics that get manifested through side-channels such as the execution time and power consumption of the device. We will look at some recent cyber-attacks such as Meltdown and Spectre, Heartbleed, and Stagefright. The pre-requisites are a good understanding of C and a basic understanding of computer organization and operating systems.

ABOUT INSTRUCTOR :
Prof. Chester Rebeiro is an Assistant Professor at IIT Madras. He completed his PhD from IIT Kharagpur and a post-doc from Columbia University. His research interests are in cryptography, system security, especially hardware and operating system security. (webpage : http://www.cse.iitm.ac.in/~chester/)

COURSE PLAN :

Week 1**:** Introduction / gdb / buffer overflow

Week 2**:** Preventing buffer overflow based malware

Week 3**:** Integer overflow and buffer overread and heap overflow

Week 4**:** More on heap overflow; Access Control

Week 5**:** Confinement

Week 6**:** SGX and Trustzone

Week 7**:** Micro-architectural Attacks

Week 8**:** Hardware Security.