SMU

School of
Computing and
Information Systems

Course Code:	**CS443**
Course Name:	**Software and Systems Security**
When was the course design document last verified by the Course Manager:	**May 2023**

NOTE: The information given in this document is for reference only; the updates given during the class sessions and/or eLearn will supersede the information given in this document.

IMPORTANT NOTICE

1. Synopsis

Software and systems security aims in equipping students with the fundamental concepts in software and systems security, as well as basic hands-on skills in understanding, analyzing, and protecting a software program and a computer system. Each lesson spends roughly 50% of the time on fundamental concepts (lecturing) and 50% of the time on hands-on exercises/assessments. Assessments focus on hands-on projects.

Previous course code & title: IS437 Software and Systems Security

2. Prerequisites/Co-requisites

Prerequisite(s): IS200 IS Software Foundations or IS111 Introduction to Programming or SMT111 Programming for Smart City Solutions or CS101 Programming Fundamentals I
(Please check Course Catalogue in BOSS for updated information!)

3. Course Areas

Advanced Business Technology Major
Technology & Entrepreneurship
Business Options
Econ Major Rel/Econ Options
Social Sciences/PLE Major-rel
IS Depth Electives
Advanced Business Technology Major: Information Security & Assurance Track
IS: Cybersecurity Track
IS: Software Development Track
CS: Cybersecurity Track
(Please check Course Catalogue in BOSS for updated information!)

4. Course Objectives

Upon completion of the course, students will be able to:

- Understand the most common vulnerabilities in software programs.
- Understand and implement various ways of exploiting software programs and computer systems.
- Understand basic security mechanisms to defend against software exploits.

5. Competencies

1. Understand what buffer overflow is and how it is introduced in C programming
2. Create exploits to buffer overflow vulnerabilities to modify critical data
3. Create exploits to buffer overflow vulnerabilities to inject and execute shellcode
4. Understand simple ways of defending against buffer overflow exploits
5. Understand what format string vulnerabilities are and how they are introduced in C programming
6. Create exploits to format string vulnerabilities to read any arbitrary memory location
7. Create exploits to format string vulnerabilities to write to any arbitrary memory location
8. Create return-to-libc exploits to execute a libc library function call

9. Create return-to-libc exploits to chain multiple libc library function calls

10. Demonstrate how vulnerabilities are introduced in real-world programs, how the corresponding exploits work, and how common defense mechanism works

6. Teaching Staff

Faculty: GAO Debin

7. Course Assessments

Assessment Categories	Weightage (%)
Attendance and class participation	10
In-class quizzes	70
Group project	20
Total	**100**

8. Course Assessment Details

In-class quizzes:

- There will be six in-class quizzes throughout the semester.
- Each quiz lasts for 20 to 30 minutes conducted at the beginning of a lesson
- Quizzes are open-book, individual assessments
- Six quizzes will be counted towards the 70% overall grade

Group project:

- Each group shall pick an open-source real-world program with vulnerabilities.
- Each group could focus on what the vulnerability is, and/or how the corresponding exploit works, and/or how it can be fixed.
- Each group will give a 20-minute presentation. No report is due.

9. Lesson Plan

Week	Topic	Remarks
1	Introduction and programming languages	
2	Debugging	
3	Function call	Quiz 1
4	Buffer overflow (1)	Quiz 2
5	Buffer overflow (2)	Quiz 3
6	In-class project	
7	Format string (1)	Quiz 4
8 (Recess Week)	Recess	
9	Format string (2)	
10	Return to libc (1)	Quiz 5
11	Return to libc (2)	
12	Group project presentation (1)	Quiz 6
13	Group project presentation (2)	

14 (Study Week)		
15 (Exam Week)		

10. Resources

Main Reading:

- No textbook
- Students are encouraged to research related topics online

Tools:

- Putty, VcXsrv, ssh

11. University Policies

Academic Integrity

All acts of academic dishonesty (including, but not limited to, plagiarism, cheating, fabrication, facilitation of acts of academic dishonesty by others, unauthorized possession of exam questions, or tampering with the academic work of other students) are serious offences.

All work (whether oral or written) submitted for purposes of assessment must be the student's own work. Penalties for violation of the policy range from zero marks for the component assessment to expulsion, depending on the nature of the offense.

When in doubt, students should consult the instructors of the course. Details on the SMU Code of Academic Integrity may be accessed at https://smu.sharepoint.com/sites/oasis/SitePages/DOS-WKLSWC/UCSC.aspx.

Copyright Notice

Please note that all course materials are meant for personal use only, namely, for the purposes of teaching, studying and research. You are strictly not permitted to make copies of or print additional copies or distribute such copies of the course materials or any parts thereof, for commercial gain or exchange.

For the full copyright notice, please visit: https://smu.sg/Copyright-notice or *OASIS -> CAMPUS LIFE & EXCHANGE -> CONDUCT & DISCIPLINE -> UNIVERSITY COUNCIL OF STUDENT DISCIPLINE*

Accessibility

SMU strives to make learning experiences accessible for all. If you anticipate or experience physical or academic barriers due to disability, please let me know immediately. You are also welcome to contact the university's student accessibility support team if you have questions or concerns about academic provisions: accessibility@smu.edu.sg. Please be aware that the accessible tables in our seminar room should remain available for students who require them.

Digital Readiness for Teaching and Learning (DRTL)

As part of emergency preparedness, instructors may conduct lessons online via the Zoom platform during the term, to prepare students for online learning. During an actual emergency, students will be notified to access the Zoom platform for their online lessons. The class schedule will mirror the current face-to-face class timetable unless otherwise stated.