Course Syllabus

Course Information

Course Prefix, Number, Section: cs6332.001
Course Title: System Security and Malicious Program Analysis
Term: Fall 2023
Meetings: Traditional (In-person)

Professor Contact Information

Instructor: Kangkook Jee
Office Phone: 972-883-3853
Office Location: ECSS 3.226
Email Address: <firstname>‘dot’<lastname> ‘at’ utdallas ‘dot’ edu
Office Hours:TBD
Course Website: https://cs6332.syssec.org

Course Modality and Expectations

Instructional Mode	Traditional / Flexible
Course Platform	The course will be taught face-to-face. Instructor and students meet according to the schedule. Limited availability due to classroom spacing.
Expectations	After completing the course, students will enhance their understanding and knowledge on (1) Design considerations for secure bootstrapping procedures of traditional computer systems, (2) Analysis of program written in ARM and x86 architectures, (3) Primary attack vectors and their defenses for standalone programs and network services, and (5) Dynamic and static program analysis techniques to analyze and harden the software programs.
Asynchronous Learning Guidelines	By default, students are mandated to attend class synchronously. Students *should* consult to the instruction *in advance* and get excuses, in case they cannot attend the class on time for any reasons.

Course Pre-requisites, Co-requisites, and/or Other Restrictions

Students are required to satisfy the following prerequisites:

- Operating System Concepts (cs4348)
- Computer Architecture (cs2340)
- Cyber Attack and Defense Lab (cs4301)

The following courses are not required but recommended:

- Compiler Design (cs4386)
- Advanced Operating Systems (cs6378)
- Language Based Security (cs6301)

Optionally, the course assignment would require students with the following programming skills:

- Fluency in C/C++
- Intermediate understanding on how program runs at low-level machine instructions-level (e.g., IA32, ARM assemblies)

Course Description

The course aims to deliver the fundamental / overarching principles of the latest system security research for the layered components of software execution stack, reviewing different system architectures for desktop and server computers, and embedded IoT devices.

Throughout the course, students will learn the following topics:

1. Computer system fundamentals for desktop and server computers, and embedded devices.
2. Primary *attack techniques* against the standalone programs and remote services written in x86 and ARM architecture.
3. Different *defense mechanisms* to counter the cyber-attack and protect software systems.
4. *Static analysis* techniques leveraging static program code analysis and transformation techniques.
5. *Dynamic analysis* techniques leveraging static program code analysis and transformation techniques.

Student Learning Objectives/Outcomes

After completing the course, students are expected to gain experiences and expand their knowledge on following topics:

- Software bootstrapping process and its runtime operation
- Machine code representations for ARM and Intel architectures
- Principles on software system attack and their countermeasure defenses
- Static and dynamic anlysis techinques to monitor and protect software process

Required Textbooks and Materials

The course does not require mandatory textbooks. However, the followings are resources that would cover large portion of the course topics.

- (Optional) Computer Systems: A Programmer's Perspective by Randal Bryant, David O'Hallaron
- (Optional) Practical Binary Analysis: Build Your Own Linux Tools for Binary Instrumentation, Analysis, and Disassembly by Dennis Andriesse

Suggested Course Materials

Instructor will post suggested resources / materials on the course website.

Assignments & Academic Calendar

Weeks	Date	Topic (Tentative)	Assignments
1	8/27/23	System Security Intro / computer architecture intro	
2	9/3/23	x86 assembly	
3	9/10/23	ARM assembly	
4	9/17/23	ELF format and program loading	Assignment 1 due
5	9/24/23	Control Hijacking Attacks and Defenses 1	
6	10/1/23	Control Hijacking Attacks and Defenses 2	
7	10/8/23	Binary disassmebly principles	Assignment 2 due
8	10/15/23	Mid-term week (No class)	
9	10/22/23	ARM architecture disassembly	
10	10/29/23	Intel architecture disassembly	Assignment 3 due
11	11/5/23	Static code analysis	
12	11/12/23	Binary code re-writing	
13	11/19/23	Virtualization and code instrumentation	Assignment 4 due
14	11/26/23	Thanks Giving break (No class)	
15	12/3/23	Class overview and closing	

Grading Policy

(including percentages for assignments, grade scale, etc.)

Evaluation		
Assignment 1	Control hijacking attacks defenses for x86 architecture	15%
Assignment 2	Control hijacking attacks defenses for x86 architecture	15%
Assignment 3	Implementing binary defense with PINTOOL	20%
Assignment 4	Dynamic code instrumentation ARM and x86	30%
Assignment 5	NSA Codebreaker challenge (Optional)	(20%)
	Class participations and quizes	20%

Grading Scale: Based on 4 assignments anc extra scores

Scaled Score (%)	Letter Equivalent
97.1-100	A+
93.1-97	A+
90.1-93	A-
87.1-90	B+
83.1-87	B
80.1-83	B-
77.1-80	C+
73.1-77	C
70.1-73	C-
60.1-70	D
Less than 60	F

COVID-19 Guidelines and Resources

The information contained in the following link lists the University's COVID-19 resources for students and instructors of record.

Please see http://go.utdallas.edu/syllabus-policies.

Class Attendance

The University's attendance policy requirement is that individual faculty set their course attendance requirements. Regular and punctual class attendance is expected regardless of modality. Students who fail to attend class regularly are inviting scholastic difficulty. In some courses, instructors may have special attendance requirements; these should be made known to students during the first week of classes. These attendance requirements will not be used as part of grading (see Class Participation below for grading information).

In-person participation records may be used to assist the University or local public health authorities in performing COVID-19 occurrence monitoring. Please note – in-person attendance requires consistently adhering to University requirements, including wearing a face covering and other public safety requirements related to COVID-19, as presented in this syllabus. Failure to comply with these University requirements is a violation of the Student Code of Conduct.

Class Participation

Regular class participation is expected regardless of course modality. Students who fail to participate in class regularly are inviting scholastic difficulty. A portion of the grade for this course is directly tied to your participation in this class. It also includes engaging in group or other activities during class that solicit your feedback on homework assignments, readings, or materials covered in the lectures (and/or labs). Class participation is documented by faculty. Successful participation is defined as consistently adhering to University requirements, as presented in this syllabus. Failure to comply with these University requirements is a violation of the Student Code of Conduct.

Class Recordings

The instructor may record meetings of this course. Any recordings will be available to all students registered for this class as they are intended to supplement the classroom experience.

Students are expected to follow appropriate University policies and maintain the security of passwords used to access recorded lectures. Unless the Office of

Student Access Ability has approved the student to record the instruction, students are expressly prohibited from recording any part of this course. Recordings may not be published, reproduced, or shared with those not in the class, or uploaded to other online environments except to implement an approved Office of Student Access Ability accommodation. If the instructor or a UTD school/department/office plans any other uses for the recordings, consent of the students identifiable in the recordings is required prior to such use unless an exception is allowed by law. Failure to comply with these University requirements is a violation of the Student Code of Conduct.

Class Materials

The instructor may provide class materials that will be made available to all students registered for this class as they are intended to supplement the classroom experience. These materials may be downloaded during the course; however, these materials are for registered students' use only. Classroom materials may not be reproduced or shared with those not in class or uploaded to other online environments except to implement an approved Office of Student Access Ability accommodation. Failure to comply with these University requirements is a violation of the Student Code of Conduct.

Off-campus Instruction and Course Activities
(Below is a description of any travel and/or risk-related activity associated with this course.)

Comet Creed
This creed was voted on by the UT Dallas student body in 2014. It is a standard that Comets choose to live by and encourage others to do the same:

“As a Comet, I pledge honesty, integrity, and service in all that I do.”

Academic Support Resources

The information contained in the following link lists the University’s academic support resources for all students.

Please see http://go.utdallas.edu/academic-support-resources.

UT Dallas Syllabus Policies and Procedures

The information contained in the following link constitutes the University's policies and procedures segment of the course syllabus.

Please go to http://go.utdallas.edu/syllabus-policies for these policies.

The descriptions and timelines contained in this syllabus are subject to change at the discretion of the Professor.