CS4191: MOBILE AND IOT SECURITY

Effective Term
Semester A 2025/26

Part I Course Overview

Course Title
Mobile and IoT Security

Subject Code
CS - Computer Science
Course Number
4191

Academic Unit
Computer Science (CS)

College/School
College of Computing (CC)

Course Duration
One Semester

Credit Units
3

Level
B1, B2, B3, B4 - Bachelor's Degree

Medium of Instruction
English

Medium of Assessment
English

Prerequisites
(CS2310 Computer Programming or equivalent)
AND (CS3103 Operating Systems or equivalent)
AND (CS3201 Computer Networks or equivalent)

Precursors
Nil

Equivalent Courses
Nil

Exclusive Courses
Nil

Additional Information
Nil

Part II Course Details

Abstract

This course is aimed at developing students with a solid understanding of a range of topics in the area of mobile and IoT security. Students will acquire an adequate understanding of the threats to mobile systems and applications as well as IoT firmware and protocols, acquire the skill to identify such threats, such as principled program analysis, and then specify and evaluate appropriate security measures for them, and get familiar with the emerging development paradigms in the mobile and IoT platform, such as on-device AI-assisted app deployment and mobile confidential computing.

Course Intended Learning Outcomes (CILOs)

	CILOs	Weighting (if app.)	DEC-A1	DEC-A2	DEC-A3
1	Understanding and mastering skills to identify and analyze common threats and vulnerabilities of mobile OS and applications.	35	x	x	
2	Understanding and mastering skills to classify and analyze common threats and vulnerabilities of IoT firmware and communication protocols.	25	x	x	
3	Suggest and evaluate countermeasures to vulnerabilities in the mobile and IoT platforms.	25		x	
4	Describe and analyse emerging development paradigms in mobile and IoT platforms, such as on-device AI-assisted app deployment and mobile confidential computing.	15	x	x	

A1: Attitude
Develop an attitude of discovery/innovation/creativity, as demonstrated by students possessing a strong sense of curiosity, asking questions actively, challenging assumptions or engaging in inquiry together with teachers.

A2: Ability
Develop the ability/skill needed to discover/innovate/create, as demonstrated by students possessing critical thinking skills to assess ideas, acquiring research skills, synthesizing knowledge across disciplines or applying academic knowledge to real-life problems.

A3: Accomplishments
Demonstrate accomplishment of discovery/innovation/creativity through producing /constructing creative works/new artefacts, effective solutions to real-life problems or new processes.

Learning and Teaching Activities (LTAs)

	LTAs	Brief Description	CILO No.	Hours/week (if applicable)
1	Lectures	The different types of attacks to mobile systems and applications and IoT firmware and applications will be introduced. Principles, techniques and technologies used for identifying and defending against these attacks will be discussed. Selected topics of emerging development paradigms in mobile and IoT platform and the associated threats and mitigations will also be introduced, including on-device AI deployment and on-device confidential computation.	1, 2, 3, 4	3 hours / week
2	Tutorials	Tutorials will be conducted in laboratory in the forms of discussion, demonstration, and hands-on sessions. Students will work with selected security and attacking tools. This provides students with hands-on experience in using, configuring the tools and analysing how the vulnerability was identified via principled approaches. With these exercises, student will know how the malicious behaviours are hidden and triggered in the mobile and IoT platforms, and how to secure sensitive information with the help of mobile confidential computing units. This helps support Course ILO #1, #2, #3 and #4.	1, 2, 3, 4	8 hours / semester

3	Case studies	Students will be provided with different attack scenarios and are required to identify the security threats, evaluate and critically analyse the security systems. This activity helps support Course ILO #1, #2, #3 and #4.	1, 2, 3, 4	After class

Assessment Tasks / Activities (ATs)

	ATs	CILO No.	Weighting (%)	Remarks ("-" for nil entry)	Allow Use of GenAI?
1	Individual assignment 1	1, 3	20	-	Yes
2	Individual assignment 2	2, 3	10	-	Yes
3	Individual assignment 3	3, 4	10	-	Yes

Continuous Assessment (%)

40

Examination (%)

60

Examination Duration (Hours)

2

Minimum Examination Passing Requirement (%)

30

Additional Information for ATs

For a student to pass the course, at least 30% of the maximum marks of the examination must be obtained

Assessment Rubrics (AR)

Assessment Task

Assignment 1

Criterion

Ability to apply principled approaches to identify threats and vulnerabilities in mobile systems and applications and understand the corresponding countermeasures.

Excellent (A+, A, A-)

High

Good (B+, B, B-)

Significant

Fair (C+, C, C-)

Moderate

Marginal (D)

Basic

Failure (F)
Below marginal level

Assessment Task
Assignment 2

Criterion
Ability to apply principled approaches to identify threats and vulnerabilities in IoT firmware and communication protocols and understand the corresponding countermeasures.

Excellent (A+, A, A-)
High

Good (B+, B, B-)
Significant

Fair (C+, C, C-)
Moderate

Marginal (D)
Basic

Failure (F)
Below marginal level

Assessment Task
Assignment 3

Criterion
Ability to explain emerging development paradigms in mobile and IoT platforms, and understand the corresponding countermeasures.

Excellent (A+, A, A-)
High

Good (B+, B, B-)
Significant

Fair (C+, C, C-)
Moderate

Marginal (D)
Basic

Failure (F)
Below marginal level

Assessment Task

Examination

Criterion

The exam will include questions to assess the student’ s ability to explain how various attacks work, the understanding of the principles, techniques and technologies used for identifying and defending against various attacks, and the ability to describe and analyse emerging development paradigms in mobile and IoT platform.

Excellent (A+, A, A-)

High

Good (B+, B, B-)

Significant

Fair (C+, C, C-)

Moderate

Marginal (D)

Basic

Failure (F)

Below marginal level

Part III Other Information

Keyword Syllabus

The syllabus will evolve over time as current topics change. The following are example keyword syllabus: Mobile Security; OS security, access control; Memory safety, program control hijacking and defence, malicious codes, backdoors; IoT security; Protocol Security; Static analysis tools; Dynamic analysis tools; Evaluating system security; Secure computing techniques.

Syllabus

1. Selected topics in mobile and IoT security
   - Mobile and IoT ecosystem and security
   - Reverse engineering and principled program analysis.
2. Mobile security
   - Smartphone architecture, OS, and application development
   - Vulnerability analysis, discovery, and exploitation
   - Mobile vulnerability prevention and countermeasures
3. IoT security
   - IoT architecture, firmware, and application security and countermeasures
   - Communication protocol security and countermeasures
4. Other emerging development paradigms in mobile and IoT platforms
   - On-device AI deployment
   - Mobile confidential computing
   - Bluetooth proximity tracking

Reading List

Compulsory Readings

	Title
1	Nil

Additional Readings

	Title
1	Himanshu Dwivedi (2010). Mobile Application Security, McGraw-Hill Education.
2	Jim Doherty (2014), Wireless and Mobile Device Security, Jones & Bartlett Learning
3	Nikolay Elenkov (2014), Android Security Internals: An In-Depth Guide to Android’ s Security Architecture, No Starch Press