CSEC 467: Mobile Device Security and Forensics
Section 01
Fall 2021

Instructor	Prof. Robert Olson
Office Location	**Main CSEC Office Suite**
Phone	585-475-4601 (My office) 585-475-5433 (CSEC Main Office)* * - Preferred
E-mail	rob.olson@rit.edu
Office Hours	(Tentatively, via Zoom) T / TH 9:30 am – 11am
Course Time	MWF 12:20-1:10
Course Place	SLA-2150

1. Catalog description: This course will be an in-depth study of security, incident response, and forensics as applied to the hardening and protection of mobile devices. Students will learn issues specific to the security of and vulnerabilities of mobile devices as well as forensics tools and incident response techniques used to reveal activities and information related to mobile devices.

2. Prerequisite(s):

(CSEC 101 OR CSEC 140) AND
(CSEC/SWEN 124 OR GCIS 124 OR CSCI 142) [Java programming]

3. Course Textbook: None

4. Course Learning Outcomes:
After completing this course, the student will be able to:

1. Describe the major mobile operating systems, mobile hardware, and mobile security threat models
2. Describe strategies used in mobile application sandboxing and their importance to mobile security
3. Describe the cryptographic mechanisms used by mobile devices to improve mobile operating system security and approaches to using cryptographic primitives available to mobile applications for data security.
4. Describe mobile application security vulnerabilities and recommend controls for mitigation
5. Exploit security vulnerabilities in mobile applications
6. Reverse engineer mobile applications to identify security vulnerabilities and mobile malware to identify indicators of compromise.

5. Program Learning Outcomes:
After completing this course, the student will be able to:

- Apply the theory and principles of computing security
- Demonstrate fluency in creating programs to solve security problems
- Demonstrate understanding of adversarial thinking, vulnerabilities, and developing defensive strategies
- Demonstrate advanced knowledge of a selected area within the computing security discipline
- Assess the ethical considerations that arise in the computing security field

7. Course Structure:

This course will, primarily, be a lecture-driven course and will focus on Android mobile devices over iOS mobile devices. The reason for this focus is because of readily available cross-platform tools and because of the relative ease of access operating system components in Android. Performing similar activities requires Apple hardware/software and often requires that mobile devices be jailbroken, voiding warrantees.

Many of the lectures will be focused on practical demonstrations rather than traditional PowerPoint slide decks and lectures will be reinforced by lab activities. These will be given, approximately, at a rate of one-lab per week. Most labs will require developing small proof-of-concept Android apps in Java or analyzing Android app source code. **You should expect to be constantly programming in this course**. Along with Java programming skills, a base-level understanding and familiarity of the Linux operating system is expected/needed.

This course will also have a significant project/paper component. The goal of this will be for the student to produce a research work of sufficient quality that it could be presented in a '101' track of a security industry conference. More information about this will be given out during the second week of the semester. A list of topics will be provided, although students may come up with their own topics with approval from the instructor.

8. Tentative Course Outline:

Week 1:	M1: Mobile Architecture & Ecosystems	Lab 1: Write/deploy/extract app	8/23
1A:	Course Overview, Mobile Architecture, Business Analysis		
1B:	Mobile App Development Basic		
1C:	Android Emulators		
Week 2:	M2: Basic Android App Reversing	Lab 2: Analysis of APKs	8/30
2A:	App Compilation & Installation		
2B:	Manual De-compilation & Extraction		
2C:	Tools for Analyzing APKs		
Week 3:	M3: Android Users and Permissions	Lab 3: App Permissions	9/6
3A:	NO CLASS		
3B:	Android User Accounts, Android Permissions, & Group Membership		
3C:	Developing Apps using Permissions		
Week 4:	M4: Android Code Signing/Package Mgmt	Lab 4: App File Sharing	9/13
4A:	Android Application Sandboxing		
4B:	Android Application Code Signing & Updates		
4C:	Working with Shared App IDs		

Week 5-7:	M5: Android Crypto & Device Encryption	Lab 5: Credential Storage	9/20
5A:	Mobile Device Threat Modeling & Cryptography-related Controversies		
5B-C:	Android Credential Manager		
5D:	Review of Crypto & PKI	Lab 6: File Encryption	9/27
5E-F:	Android Encryption & Key Management		
5G:	File Integrity	Lab 7: Data Integrity	10/4
5H:	Android Full Disk Encryption		
5I:	iOS Full Disk Encryption		
Week 8:	M6: Current Topics (No Quiz)		10/11
6A:	NO CLASS		
6B:	Signal Protocol		
8C:	Mobile Tech in the Time of COVID		
Week 9-10:	M7: Android Application Security	Lab 8: App Security Analysis	10/18
7A:	Mobile App Architectures		
7B:	Mobile OWASP Top 10 & Security Controls (including certificate pinning)		
7C:	Vulnerability Scoring		
7D:	Automated Application Security Tools		10/25
7E:	API Analysis and Testing		
7F:	Case Studies (See: https://samsclass.info/128/lec/WorstMobileApps_DEFCON.pptx)		
Week 11/12:	M8: Mobile Networking Protocols & 2FA	Lab 9: Mobile Networking	11/1
8A:	(2-3-4-5)G Technologies		
8B:	SS7, RRC signaling		
8C:	SMS		
Week 12/13:	M9: Android Malware	Lab 10: Mobile Malware Reversing	
9A:	Mobile Malware Categories & Mechanisms of Infection		11/10
9B:	Mobile Malware Reversing		11/12
9C:	Case Studies. See… - https://github.com/ashishb/android-malware - https://github.com/ytisf/theZoo/tree/master/malware/Binaries		11/15
9D/E:	Developing Android Malware	Lab 11: Making Mobile Malware (Optional)	
9F:	Mobile Malware & Current Events		

Weeks 13.5 / 14 / 15: Student Presentations (11/22, 11/29, 12/1, 12/3, 12/6)

10. Grading:

The relative weight of each component of your grade is shown on the table below.

Component	**Percentage**
Labs/Assignments	40% (~10 labs)
Semester Project	30%
Exams	30% (15% x 2)

The table below lists student's grade for a given percentage achieved.

94%-100%	90%-93%	88%-89%	82%-87%	80%-81%	78%-79%	72%-77%	70%-71%	60-69	0%-59%
A	A-	B+	B	B-	C+	C	C-	D	Fail

9. Exams, Projects, and Labs/Assignments:

All exams must be taken on the day(s) specified. All projects and lab assignments are due on the date listed in the hand-out provided by the instructor. Exceptions will be made at the sole discretion of the instructor. Some valid reasons may include:

1. Illness of the student or serious illness of a member of the student's immediate family.
2. A death in the student's immediate family
3. Trips sponsored by official RIT student groups, academic units, or athletic teams.
4. Major religious holidays

A student requiring special considerations for reasons 3 or 4 should talk to the instructor at least a week in advance, whenever possible.

11. Class Attendance

All students are expected to participate in this course for the entire duration of the semester. "Attending class" is recommended, although it may take different forms because of the COVID-19 pandemic. It is my intention to stream all lecture content via Zoom for this course, allowing students to participate even if they cannot attend in-person.

At the time of writing this syllabus, it is unclear if I'll be able to record these streamed lectures and distribute them via MyCourses.

You should not physically attend class if you are feeling sick and you do not need to ask my permission to attend via Zoom instead of in person. There are a host of valid reasons, ranging from transportation challenges to mental health, why a student may choose not to attend CSEC 467 in person. This course will move at a rapid pace, however, and it is your responsibility to ensure that you are continuing to actively participate.

12. Academic Honesty

The following statement is the Policy on Academic Dishonesty for the Computing Security Department.

The Computing Security Department (CSEC) does not condone any form of academic dishonesty. Any act of improperly representing another person's work as one's own (or allowing someone else to represent your work as their own) is construed as an act of academic dishonesty. These acts include, but are not limited to, plagiarism in any form or use of information and materials not authorized by the instructor during an examination or for any assignment.

If a faculty member judges a student to be guilty of any form of academic dishonesty, the student will receive a failing grade for the course. Academic dishonesty involving the abuse of RIT computing facilities may result in the pursuit of more severe action.

If the student believes the action by the instructor to be incorrect or the penalty too severe, the faculty member will arrange to meet jointly with the student and with the faculty member's immediate supervisor. If the matter cannot be resolved at this level, an appeal may be made to the Academic Conduct Committee of the college in which the course is offered.

If the faculty member or the faculty member's immediate supervisor feels that the alleged misconduct warrants more severe action than failure in the course, the case may be referred to the Academic Conduct Committee. The Academic Conduct Committee can recommend further action to the dean of the college including academic suspension or dismissal from the Institute.

The following definitions will be used to clarify and explain unacceptable conduct.
This is not intended to be an exhaustive list of specific actions but a reasonable description to guide one's actions.

CHEATING includes knowingly using, buying, stealing, transporting or soliciting in whole or part the contents of an administered/un-administered test, test key, homework solution, paper, project, software project or computer program, or any other assignment.
It also includes using, accessing, altering, or gaining entry to information held in a computer account or disk owned by another.

COLLUSION means the unauthorized collaboration with another person in preparing written work or computer work (including electronic media) offered for credit. Final work submitted by a student must be substantially the work of that student. Collaboration on an assignment is expressly forbidden unless it is explicitly designated as a group project. When there is any doubt, a student should consult the instructor (NOT ANOTHER STUDENT) as to whether some action Is considered collusion.

Whenever there is any question as to whether a particular action is considered academic dishonesty, the instructor should be consulted PRIOR to commencing that action.

13. Responsible Disclosure

During the course of the semester, students in CSEC 467 may uncover previously unknown security vulnerabilities in mobile applications or mobile devices. In the event that this happens, students will be expected to practice responsible disclosure practices, in consultation with the instructor. This includes, but may not be limited to, submitting the vulnerability to a bug bounty program or notifying the company of the vulnerability far enough in advance of releasing details to give the company sufficient time to respond. The instructor reserves the right to penalize a students' grade if the student fails to practice responsible disclosure and to recommend the student for further academic discipline if needed.

14. Course Success

Success in this course depends heavily on your personal health and wellbeing. Recognize that stress is an expected part of the college experience, and it often can be compounded by unexpected setbacks or life changes outside the classroom. Moreover, those with marginalized identities may be faced with additional social stressors. Your other instructors and I strongly encourage you to reframe challenges as an unavoidable pathway to success. Reflect on your role in taking care of yourself throughout the term, before the demands of exams and projects reach their peak. Please feel free to reach out to me about any difficulty you may be having that may impact your performance in this course as soon as it occurs and before it becomes unmanageable. In addition to your academic advisor, I strongly encourage you to contact the many other support services on campus that stand ready to assist you.