

CNIT 128: Hacking Mobile Devices

37712 Weds 06:10-09:00 pm SCIE 204

Spring 2017 Sam Bowne

Catalog Description

Mobile devices such as smartphones and tablets are now used for making purchases, emails, social networking, and many other risky activities. These devices run specialized operating systems have many security problems. This class will cover how mobile operating systems and apps work, how to find and exploit vulnerabilities in them, and how to defend them. Topics will include phone call, voicemail, and SMS intrusion, jailbreaking, rooting, NFC attacks, malware, browser exploitation, and application vulnerabilities. Hands-on projects will include as many of these activities as are practical and legal.

Advisory: CNIT 113 and 123, or equivalent familiarity with hacking computers and operating mobile devices.

Upon successful completion of this course, the student will be able to:

- A. Describe the risks of using mobile devices for common activities such as making phone calls, emailing, and shopping
- B. Explain cellular network functions, attacks, and countermeasures for voice calls, voicemail, and SMS
- C. Perform and analyze jailbreaks for iOS devices
- D. Analyze the Android security model and rooting
- E. Recognize types of mobile malware and anti-malware options
- F. Identify Web browser services and attacks on mobile platforms and recommend countermeasures
- G. Configure and defeat locking, remote location and wiping services
- H. Explain common mobile app risks and make intelligent decisions when installing and using them
- I. Evaluate the functions and risks of mobile payment services, such as Google Wallet

Textbook

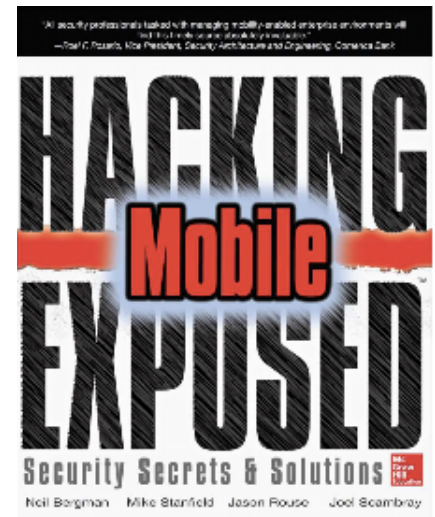
"Hacking Exposed Mobile: Security Secrets & Solutions", by Bergman, Stanfield, Rouse, Scambray, Geethakumar, Deshmukh, Matsumoto, Steven and Price, McGraw-Hill Osborne Media; 1 edition (July 9, 2013) ISBN-10: 0071817018 [Buy from Amazon](#)

Quizzes

The quizzes are multiple-choice, online, and open-book. However, you may not ask other people to help you during the quizzes. You will need to study the textbook chapter before the lecture covering it, and take the quiz before that class. Each quiz is available for one week, up till 5:30 pm Weds. Each quiz has 5 questions, you have ten minutes to take it, and you can make two attempts. If you take the quiz twice, the second score is the one that counts, not necessarily the higher score.

To take quizzes, log in to CCSF's online class site here:

<https://ccsf.instructure.com>



Schedule (may be revised)

<u>Date</u>	<u>Quiz & Proj</u>	<u>Topic</u>
Wed 1-18		Is Your Mobile App Secure?
Wed 1-25		1: The mobile risk ecosystem
Wed 2-1		2: Hacking the cellular network
<i>Fri 2-3</i>	<i>Last Day to Add Classes</i>	
Wed 2-8	Ch 1 Quiz due before class Ch 2 Quiz due before class Proj 1 due	3: iOS (Part 1)
<i>Wed 2-15</i>	<i>Class Cancelled for RSA</i>	
Wed 2-22	Ch 3 Quiz due before class Proj 2-4 due	3: iOS (Part 2)
Wed 3-1	Ch 4 (Part 1) Quiz due before class Proj 5 due	4: Android (Part 1)
Wed 3-8	Ch 4 (Part 2) Quiz due before class Proj 6 due	4: Android (Part 2)
Wed 3-15	Ch 5 Quiz due before class Proj 7 due	5: Mobile malware
Wed 3-22	Ch 6 (Part 1) Quiz due before class	6: Mobile services and mobile Web (Part 1)
<i>Wed 3-29</i>	<i>Holiday -- No Class</i>	
Wed 4-5	Ch 6 (Part 2) Quiz due before class	6: Mobile services and mobile Web (Part 2)
Wed 4-12	Ch 7 Quiz due before class Proj 8 and 9 due	7: Mobile Device Management
Wed 4-19	Ch 8 Quiz due before class Proj 8 and 9 due	8: Mobile development security
Wed 4-26	Ch 9 Quiz due before class	9: Mobile payments
Wed 5-3	No Quiz	TBA
Wed 5-10	No Quiz	TBA
Wed 5-17	Last class No Quiz All Extra Credit Projects Due	TBA
Wed 5-24		<i>Final Exam</i>