

CNT 6519, Wireless Security and Forensics

S. Lang, Fall 2022

Course Syllabus

August 22, 2022

Course Description (per UCF's Course Catalog):

This course provides an advanced study for those students with an interest in subjects such as wireless network security, security management, cryptography, wireless forensics and related topics.

Prerequisites:

Digital Forensics MS major (CGS 5131) or CDA 5106 or COT 5405, or consent of the instructor. More generally, knowledge and skills expected of an Information Technology (IT) undergraduate degree (such as that offered at UCF), including but not limited to, Linux systems, virtualization (VirtualBox or VMWare), college algebra and trigonometry, basic probability theory and statistics, physics (including electricity and magnetism), data communications, computer networking, and computer security, are expected as prerequisites.

Equipment (for conducting penetration testing of a wifi network running in WPA2 (or WPA3)-PSK security mode, and for Bluetooth attack on a smartphone):

Students need to have administrative rights to

- (1) a Windows PC/laptop with built-in wireless and Bluetooth hardware (the target machine);
- (2) a PC/laptop running Kali Linux with built-in wireless and Bluetooth hardware (the penetration tester's machine), see Notes on Kali Linux below;
- (3) a Wifi router (access point) running the WPA2/WPA3-PSK security protocol; and
- (4) a smart cell phone with built-in wireless and Bluetooth hardware (for Bluetooth attack on a smartphone).

Notes on Kali Linux: One method to set up a Kali Linux machine is to use a Windows PC/laptop and boot it into Kali Linux (through a bootable USB or CD) or run Kali Linux as a virtual machine on the Windows host. Note that when running Kali Linux in a virtual machine (on a desktop or laptop PC) you will need to use/purchase an external USB wifi adapter and an external USB Bluetooth adapter compatible to Kali Linux since the virtual machine does not have access to the host's wireless and Bluetooth hardware.

Instructor:

Dr. Sheau-Dong Lang
Adjunct Instructor (retired Associate Professor)
Department of Computer Science
University of Central Florida
E-mail: slang@ucf.edu

Note: The preferred method for contacting the instructor regarding course-related matters is to use WebCourses' e-mail.

Primary References (not required textbooks):

- Jim Doherty, “Wireless and Mobile Device Security”, 2nd edition, Jones & Bartlett Learning, 2021, ISBN: 128421172X
- Jon Edney and William A. Arbaugh, “Real 802.11 Security: Wi-Fi Protected Access and 802.11i,” Addison-Wesley, 2004, ISBN: 0321136209
- William Stallings, “Cryptography and Network Security”, 6th Edition (or newer), Prentice Hall, 2014
- Joshua Wright and Johnny Cache, "Hacking Exposed Wireless, Third Edition: Wireless Security Secrets & Solutions," McGraw-Hill, 2015, ISBN: 0071827633.

Additional References:

- Cory Beard and William Stallings, “Wireless Communication Networks and Systems,” Pearson Higher Education, 2016, ISBN: 0-13-359417-3
- Neil Bergman, et al., “Hacking Exposed Mobile: Security Secrets & Solutions,” McGraw-Hill, 2013, ISBN: 0071817018
- Praphul Chandra, et al., “Wireless Security: Know It All,” Newnes, 2008, ISBN: 1856175294
- Hakima Chaouchi and Maryline Laurent-Maknavicius (Editors), "Wireless and Mobile Networks Security: Security Basics, Security in On-the-shelf and Emerging Technologies," John Wiley, 2009
- Mark Ciampa "Wireless Security," Thomson Course Technology, 2006, ISBN: 1418836370
- Sherri Davidoff and Jonathan Ham, “Network Forensics”, Prentice Hall, 2012, ISBN 0-13-256471-8
- Gregory Kipper, “Wireless Crime and Forensic Investigation,” Auerbach Publications, 2007, ISBN 08493-9251-9
- Madhusanka Liyanage, et al., “A Comprehensive Guide to 5G Security,” Wiley, 2018, ISBN: 978-1119-29304-0
- William Stallings, "Wireless Communications & Networks," 2nd Edition, Pearson/Prentice Hall, 2005, ISBN: 0-13-191835-4
- Other selected papers from journals, conferences, and online resources.

Student Learning Outcomes (and Course Objectives):

The students will be able to

- Understand the current wireless technologies (including encryption algorithms AES and RSA, digital certificates), threats, vulnerabilities, and other security related issues
- Practice wireless network penetration testing using tools available in Kali Linux
- Apply digital forensic principles and tools in wireless incidents investigations
- Conduct research on existing literature, prepare report and presentation, and participate in a group project

Selected Course Topics:

- Data Transmission Fundamentals
- Wireless Technologies
- Wireless LAN (IEEE 802.11) Security
- Cryptography and Network Security (Modular Arithmetic, Advanced Encryption Standard, RSA)
- Public Key Infrastructures, Digital Certificates
- Digital Forensics Principles and Investigations

- Wireless Intrusion and Attacks, Legal Matters
- Bluetooth Security
- Cellular Network Security
- Emerging Wireless Technologies (such as 5G cellular network, IoT, satellite communication, etc.)

Grading Policy:

- (1) Homework Assignments (5 to 8): 40%
- (2) Take-home Midterm Exam: 15% (to be given around week 8/9 of the semester)
- (3) Final Exam: 20% (available online for taking but time-constrained during UCF's Final Exam Period: Monday, 12/5 – Sunday, 12/11).
- (4) One group project (2 to 4 persons per group; report and presentation): 20%
Project report (written) and presentation (slides, including audio recording), are due in week 14 of the semester; more details about the topics, formats, other requirements, grading rubrics, will be posted later
- (5) Class participation: 5%
Several discussion topics will be available on WebCourses' course page for all students to contribute (participate), see detailed requirements described in each discussion assignment.

Note: No late assigned work (homework, discussions, exams, group project) will be acceptable unless arrangements and approval by the instructor have been made prior to the due date.

The final course grades are based on the straight-percentage scale, i.e., A (90% or up), B (80 – 89.99%), C (70 – 79.99%), D (60 – 69.99%), and F (below 60%); plus/minus grades will be used sparsely (if at all).

Course Website: available on UCF WebCourses (always under construction)

Important Dates:

Deadlines (and any changes) for all assigned work (including assignments, discussions, the group project, the midterm exam, and the final exam) will be posted at the course's homepage on UCF WebCourses. Additionally, refer to UCF's fall 2022 calendar (<https://calendar.ucf.edu/2022/fall>) for university-wide important dates such as holidays or closures, drop/withdrawal deadlines, final exam, etc.

Academic Activity Requirements:

Per UCF's rule all UCF classes are required to document students' academic activity at the beginning of the semester. In order to document that you are enrolled in this class please complete the following two (2) academic activity assignments by August 26. Failure to do so may result in a delay in the disbursement of your financial aid or cause other issues.

- Logon to the course website on UCF's WebCourses and submit the "Course Prerequisites Questionnaire" online via WebCourses by 9 pm (UTC – 4), August 26, 2022

- Post a brief personal introduction on WebCourses by 9 pm (UTC – 4), August 26, 2022; the introduction must include: your name, education background, related work experience, and your expectation of this class.

Academic Honesty:

Plagiarism and Cheating of any kind on an examination, or assignment will result at least in an "F" for that assignment (and may, depending on the severity of the case, lead to an "F" for the entire course) and may be subject to appropriate referral to the Office of Student Conduct for further action. See the [UCF Golden Rule](#) for further information. I will assume for this course that you will adhere to the academic creed of this University and will maintain the highest standards of academic integrity. In other words, do not cheat by giving answers to others or taking them from anyone else. I will also adhere to the highest standards of academic integrity, so please do not ask me to change (or expect me to change) your grade illegitimately or to bend or break rules for one person that will not apply to everyone in the class.

Student Accessibility Services

The University of Central Florida is committed to providing reasonable accommodations for all persons with disabilities. This syllabus is available in alternate formats upon request. Students with disabilities who need accommodations in this course must contact the instructor at the beginning of the semester to discuss needed accommodations. No accommodations will be provided until the student has discussed with the instructor to request accommodations. Students who need accommodations must be registered with [Student Accessibility Services](#), Ferrell Commons 7F Room 185, phone (407) 823-2371, before requesting accommodations from the instructor.