CSCE 5753 Wireless Systems Security (3 credit hours), Elective

Catalog Description: Wireless systems such as wireless local area networks, cellular and mobile networks, and sensor networks are vulnerable to attacks. The goal of the class is for students to understand how to design secure wireless systems. Security topics include confidentiality, integrity, availability, privacy, and control of fraudulent usage of networks. Issues addressed include basic wireless theory, cryptography, threat modeling, risks, and mitigation techniques.

Prerequisites: Graduate Standing or Instructor Consent

Textbook/required material: None.

Goals: The goal of the class is for students to understand how to design secure wireless systems.

Student Learning Outcomes. By the end of this course, students will be able to:

- Identify wireless access points on a network using network tools
- Use offensive cybersecurity tools to attack computer and network systems to understand how to defend against attacks
- Differentiate different security levels of typical WiFi systems
- Create a new lab that implements an attack to a wireless system
- Evaluate the threats to a computer or network system

Topics covered:

- Wireless Background: Hacking, applications, ethics, and basic wireless theory (2 weeks)
- Wireless Local Area Networks (LANs) Security: IEEE 802.11 (WiFi), reconnaissance, WEP, WPA, WPA2, WPS, threat modeling, offensive and defensive security tools (5 weeks)
- Cryptography: Symmetric key, asymmetric key, hash functions, message authentication codes, digital signatures, authentication, AES, block ciphers, modes of operation (2 weeks)
- Cellular and Mobile Network Security: Background, cloning, fraudulent usage, GSM, SIM, UMTS, and CDMA (2 weeks)
- Security Project (4 weeks)

Grading

Course grades will be determined by these weights:

Participation:	25%
Assignments:	50%
Project:	25%

The final class grade will be assigned according to the 10-point scale shown below. The grades may or may not be curved.

A	90 – 100%
B	80 – 89.9%
C	70 – 79.9%
D	60 – 69.9%
F	< 60%

Participation
Attendance will be taken and factor into the grade. Participation both in-class discussions and on the class blog will be graded. Brief in-class quizzes may be given.

Assignments
Assignments will consist of homework and labs. All assignments will be given with a strict deadline, and students are required to submit their assignments on or before the deadline. Assignments will be collected at the start of the class on the due date, and late submissions will not be accepted. In case of extenuating circumstances, students are advised to contact the professor as soon as practical.

Project
Each student will do a final project and present the project to the class, possibly as a team.

Attendance
Attendance will be taken. Attendance will be used as a deciding factor when the final average is between grades. For example, if you have an average of 89.5 and you have attended a high percentage of the classes it may be rounded up to an "A". If you have an average of 89.5 and you have attended a small percentage of the classes, it will probably still be a "B".

Academic Dishonesty Policy
As a core part of its mission, the University of Arkansas provides students with the opportunity to further their educational goals through programs of study and research in an environment that promotes freedom of inquiry and academic responsibility. Accomplishing this mission is only possible when intellectual honesty and individual integrity prevail. Each University of Arkansas student is required to be familiar with and abide by the university's 'Academic Integrity Policy' at honesty.uark.edu/policy. Students with questions about how these policies apply to a particular course or assignment should immediately contact their instructor.

Ethics and Responsibilities
In this class, we will apply both offensive and defensive security techniques to non-production hardware/software systems. Extra caution is required because it is more difficult to constrain wireless systems. Every student must act responsibly adhering to the University of Arkansas Code of Computing Practices and the Computer and Network Security Policy.

Class/laboratory schedule: Meets either 3 times a week for 50 minutes or 2 times a week for 1 hour 15 minutes for 15 weeks.

Prepared by: Dale Thompson **Date**: 10/27/18