CS6501, Defense Against the Dark Arts, Spring 2018
General Information

Instructors:	Jack Davidson (jwd@virginia.edu) Michele Co (mcz2k@virginia.edu) Abbas Naderi Afoosheth (abiusx@virginia.edu)
Office:	Jack Davidson: Rice Hall, Room 426 Michele Co: Rice Hall, Room 409 Abbas Naderi Afoosheth, Rice Hall, Room 440
Online Materials:	Class Collab Site
Phone:	Jack Davidson: 982-2209 Michele Co: 982 -2203
Office Hours:	Jack Davidson: Tuesdays: 1:30 pm - 2:30 pm and by appointment. Michele Co: Mondays: 2:30 pm - 3:30 pm and by appointment. Abbas Naderi Afoosheth: Mondays and Wednesdays, 12:15 pm - 1:15 pm For e-mail contact, always include "CS 6501" in the subject line.
Prerequisites:	You should be able to write C/C++ code and read x86 assembly language.
Texts:	None. We will be reading various papers throughout the semester. There are a variety of online resources that you can use to come up to speed on computer security. An example is Virus Bulletin, at the URL: http://www.virusbtn.com/. Other great resources are the Black Hat conferences (http://www.blackhat.com). You can view the talks by going to their archives.
Grading:	There will be three exams (15% each and the low exam score is dropped), a semester project (30%), and continuous programming assignments (40% total). Some of the programming projects will be group projects. The above percentages may be adjusted depending on the number of assignments and the complexity of the project. Keep all graded material to provide evidence of grades in case there is an error in transcription. Attendance in class is noted and counted towards class participation. Excessive unexcused absences from class is grounds for receiving a failing grade.

Course Rules:	1. You are fully responsible for all material presented in class. 2. There may be an occasional unannounced quiz. Exams and due dates are scheduled in advance. 3. A grade of zero will be recorded for missed exams and late assignments unless prior arrangements are made. 4. Assignments turned in after the due date, but before the next scheduled class are penalized 10%. 5. Assignments that are more than one class period late will not be accepted. 6. You are free to develop assignments on any platform/OS you wish. However, you are responsible for porting your code to the platform the class is using and ensuring that it runs correctly. Our reference system will be 32-bit Ubuntu 16.04.3 LTS.
Cheating:	Students are encouraged to discuss programs in general and to help one another find bugs in existing programs, but using another's code or writing code for someone else is cheating and a violation of the Universitys Honor System. This includes consulting solutions to assignments from previous years or tests from previous years. Keep listings to provide evidence of creative development.
Projects:	There will be programming assignments as well as some pencil and paper assignments.

Course Objectives and Syllabus

Course Objectives

1. Understand the nature and types of malware (e.g., viruses, worms, spyware, botnets, ransomware, trojans, etc.) and how they are threats to computer systems.
2. Learn the techniques used to prevent, detect, repair, and defend against malware.
3. Learn to use program binary examination tools to detect malicious code.
4. Understand the ethical issues surrounding computer security violations.
5. Understand the nature of software vulnerabilities, how a malicious adversary exploits them, and how to defend against them.

Syllabus

The following syllabus gives you a rough idea of the time spent on each topic. The syllabus may change depending how quickly or slowly we move. Regardless, the tests and exams will be on the dates shown. Make any travel plans accordingly.

Week 1:	01/17	Course introduction, ethics guidelines, and pledge x86 architecture
Week 2:	01/22	x86 architecture and calling convention
Week 3:	01/29	Terminology Virus arms race: Oligomorphic, polymorphic, and metamorphic viruses
Week 4:	02/05	Virus detection Web vulnerabilities, exploits, defenses
Week 5:	02/12	Web vulnerabilities, exploits, defenses Exam 1 (02/14)
Week 6:	02/19	Exploits and defensive techniques: stack smashing, buffer overflow, arc injection
Week 7:	02/26	Exploits and defensive techniques: format string, integer overflow, ROP, blind ROP
Week 8:	03/05	Spring Break
Week 9:	03/12	TBD Exam 2 (03/14)
Week 10:	03/19	TBD
Week 11:	03/26	TBD
Week 12:	04/02	TBD
Week 13:	04/09	Exam 3 (04/11)
Week 14:	04/16	Project presentations.
Week 15:	04/23	Project presentations.
Week 16:	04/30	Last day of class (04/30). Final exam (05/05/2018): 09:0012:00, Rice Hall 032