CS 462/562, Cybersecurity Fundamentals, Fall 2015

Course Delivery

This is an asynchronous, online course, meaning that there are no regularly scheduled physical meeting times. I will hold weekly office hours on campus and be available online at regular times during the week. The course will be delivered using a pilot version of Canvas (a course management system similar to Blackboard) and the PLE.

Course Links:
- CS 462/562 Canvas
- CS 462/562 PLE

Is an online course for you? Take this short quiz to determine how suited you are for an online course.

CRNs

Since this is an online course, there are separate CRNs based on where you are:
- On-campus or in Hampton Roads: CS 462 (CRN 19883), CS 562 (CRN 19886)
- Outside of Hampton Roads, but in Virginia: CS 462 (CRN 19884), CS 562 (CRN 21329)
- Outside of Virginia: CS 462 (CRN 19885), CS 562 (CRN 21330)

Catalog Course Description

Introduction to networking and the Internet protocol stack; Vulnerable protocols such as HTTP, DNS, and BGP; Overview of wireless communications, vulnerabilities, and security protocols; Introduction to cryptography; Discussion of cyber threats and defenses; Firewalls and IDS/IPS; Kerberos; Transport Layer Security, including certificates; Network Layer Security.

Requirements

Prerequisites: The main prerequisite for this course is CS 270 – Computer Architecture.

Required Textbook:
  The book is available at the ODU bookstore or at the usual places.

Recommended (Optional) Textbooks:
  This is the same textbook used for CS 564
  available free via ODU Library
- Introduction to Computer Networks and Cybersecurity, by Wu and Irwin, 2013
  last year's textbook
  available free via ODU Library

Computer/Internet: As this is an online-only course, you must have access to a computer with high-speed Internet. If you are an on-campus student, you may use the university computer labs. Otherwise, you must provide your own computer and Internet access.

Course Objectives
After completing this course, students should have a strong foundation in the principles of the Internet architecture, an awareness of vulnerabilities in the Internet protocol stack, and an introduction to issues in cybersecurity. They should be prepared to take follow-on courses in the CS graduate online CyberSecurity certificate. After completing the entire certificate program (4 courses), students should be able to pass the CompTIA Security+ Certification Exam.

This course has the following objectives:

- Explain the general architecture of the Internet, including the role of end systems, routers, and the Internet protocol stack
- Identify security vulnerabilities in DNS and outline their potential defenses
- Identify security vulnerabilities in databases and outline their potential defenses
- Identify security vulnerabilities in the BGP Internet routing protocol and outline their potential defenses
- Identify security vulnerabilities in web applications and outline their potential defenses
- Analyze and differentiate among types of malware and attacks
- Describe various techniques used to protect networked systems from attack

**Course Responsibilities**

As with online courses, you are responsible for keeping up with required activities and readings. Each week, you will have reading assignments, a homework assignment, and discussion questions that allow you to interact with your classmates. *There will be no programming assignments.*

Your time commitment should be the same as for a regular on-campus course. Plan for 1 hour of study for every 3 hours of credit, so roughly 10 hours/week for this course.

**Course Outline**

The course will be divided into two main sections, with the first half covering networking background and the second half covering cybersecurity basics.

**Module 1 - Orientation**

- Module 2 - A Whirlwind Introduction to the Internet
- Module 3 - Cybersecurity Overview
- Module 4 - Application Layer and HTTP
- Module 5 - DNS
- Module 6 - Transport Layer and Network Layer
- Module 7 - Routing
- Module 8 - Link Layer and Wireless

**Module 9 - MID-TERM EXAM**

- Module 10 - Cryptography
- Module 11 - General Attacks
- Module 12 - Application Attacks
- Module 13 - Firewalls and IDS/IPS
- Module 14 - Network Access Control
- Module 15 - Transport Layer Security and Network Layer Security

**Module 16 - FINAL EXAM - covering all material**