

Syllabus for APC 480 Computer Security II

NOTE: This syllabus document contains the basic information of this course. The most current syllabus is available in the full course.

Course Description

This course covers topics spanning communication and network security, security assessment and testing, software development security, and asset security. Specific topics include operating system security, network security (e.g. firewalls, tunneling, intrusion detection, and wireless networking), browser security, and application security (e.g. database security, email security, payment system security, and digital-rights management).

Prerequisite(s)

- APC 360: Database Management I
- APC 400: Applied Communication Networks
- APC 420: Computer Security I
- APC 450: Operating Systems Theory and Practice

Course Outcomes

Upon completing this course, you will be able to do the following:

- Study security mechanisms for conventional operating systems, explain common vulnerabilities in computer programs and their countermeasures.
- Identify network security threats, investigate solutions to network security issues.
- Analyze internet security protocols, understand security policies, and apply firewalls and intrusion detection systems.
- Gain familiarity in recent security related developments such as the disruptive blockchain technology.

Course Requirements/Components

- Assignments

- Projects

Grading

The following grading scale will be used to evaluate all course requirements and to determine your final grade:

Grade	Percentage Range
A	90% - 100%
B	80% - 89%
C	70% - 79%
D	60% - 69%
F	0% - 59%

Evaluation Methods	Percentage of final grade
Homework Assignments	81.25%
Projects	18.75%