

Course Syllabus

[Jump to Today](#) [Edit](#)

IST 451: Network Security, Sections 002 - Spring 2017 Syllabus

Please note that the specifics of this Course Syllabus are subject to change. Instructors will notify students of any changes and students will be responsible for abiding them. Please check the online version often.

Description

IST 451 focuses on network and information security. Students will learn fundamentals of computer security, formal models of security, aspects of information systems such as access control, hacks/attacks, systems and programs security, intrusion detection, cryptography, networks and distributed systems security, worms, and viruses, and other Internet secure applications. Students will develop the skills necessary to formulate and address the security needs of enterprise and personal environments.

Prerequisites

- IST 220
- SRA 221

Objectives

By the end of the course, you will be able to:

- Develop an understanding of information systems security practiced in computer operating systems, distributed systems, networks, and representative applications.
- Gain familiarity with prevalent network and distributed system attacks, defenses against them, and forensics to investigate the aftermath.
- Develop a basic understanding of cryptography, how it has evolved, and some key encryption techniques used today.
- Develop an understanding of security policies (such as authentication, integrity, and confidentiality) as well as protocols to implement such policies in the form of message exchanges.

Instructor

Please use email for all course communication. Every attempt will be made for the instructor (or a substitute) to respond to email questions within 24 hours. Your instructor and learning assistant for this section is:

- Section 002: Dr. Michael Hills, mkh179@psu.edu (instructor) and Yu Fu, Yu (yuf123@psu.edu) (teaching assistant)

For additional information, visit the instructor profile under the People link.

Office Hours

Dr. Hills and Yu Fu will be holding office hours by appointment. If you would like to meet with us about an assignment or project, please email both of us. In this message please suggest a couple days and times that you are available and we will set up an appointment with one or the other of us based on schedule. If you need to meet with one of us specifically, be sure to mention it in your email.

1. Yu Fu: yuf123@psu.edu
2. Dr. Hills: mkh179@ist.psu.edu

Materials

- Stallings, W., & Brown, L. (2012). *Computer security: Principles and practice*(3rd ed.). Boston: Pearson. ISBN 978-013377392-7
- Additional selected readings may also be made available

Assignments & Grading

- The course will be graded in accordance with the following assignments and rubric.
- You can earn extra points by doing additional assignments which will be announced in class when available.

Course Grading Breakdown

Assignments	# of Course Assignments	Individual or Team	Points for Each Assignment	% of Total Grade	Total Points
Labs	4	Team	50 each	20%	200
Homework Assignments	5	Individual	50 each	25%	250
Term Paper	3 Milestones	Team	50 each (milestones 1 and 2) 100 (milestone 3)	20%	200
Term Paper Presentation	1	Team	100 (milestone 4)	10%	100

Course Grading Breakdown

Assignments	# of Course Assignments	Individual or Team	Points for Each Assignment	% of Total Grade	Total Points
Exams	2	Individual	100 each	20%	200
Class Discussion Participation	10	Individual	5 each	5%	50
TOTAL				100%	1000

Attendance

Attendance for class is taken every day in-class. Mark your initials on the attendance name card and return it to the teacher/LA at the end of each class. If you cannot make a class due to an illness, out of town interview, or school-sponsored activity, email the "Teachers" alias on canvas informing the teachers of your intended absence. The teacher or LA will get back to you in a timely manner and mark your attendance card accordingly.

Note: Any student who misses more than 10% of classes (Unexcused absences) over the course of the semester will receive a letter grade lower as a final grade, regardless of whether assignments are complete.

Course Grading Scale

Grade	A	A-	B+	B	B-	C+	C	D	F
Percent	93% to 100%	90% to 92.9%	87% to 89.9%	83% to 86.9%	80% to 82.9%	77% to 79.9%	70% to 76.9%	60% to 69.9%	<60%
Points	930 - 1000	900 - 929	870 - 899	830 - 869	800 - 829	770 - 799	700 - 769	600 - 699	0 - 599

Schedule

The following schedule outlines the topics covered in this course, along with the associated time frames, time frames, readings, activities, and assignments. All due dates reflect Eastern Time (ET). Specifying the time zone ensures that all students have the same deadlines, regardless of where they live.

All assignments are due at midnight **Sunday 11:59 PM (ET)** each week, unless otherwise stated.

Group Led Discussions

Each group will put together a brief 5 minute presentation for the class to hear that group's proposed topic. Dr. Hill's and I will be providing verbal feedback about your topic. Please make a submission in the forum with the link to your article the Thursday of the week of your presentation.

Discussion Activity Number	Group Number	Discussion Date
3	6	
4	3	
4	7	
5	5	
6	2	
7	9	
8	1	
9	4	
10	8	

Course Schedule

Week 1

Week 1 Topic(s) Introduction to Security Fundamentals

Time frame January 9 to January 15, 2017

Readings Syllabus
Chapter 1

Assignments Homework 1, Discussion #1

Week 2

Week 2 Topic(s) Cryptographic Tools

Time frame January 16 to January 22, 2017

Readings Chapter 2

Assignments Homework 2
Discussion #2

Week 3

Week 3 Topic(s) User Authentication

Time frame January 23 to January 29, 2017

Readings Chapter 3

Assignments Homework 3
Discussion Question #3

Week 4

Week 4 Topic(s) Access Control

Time frame January 30 to February 5, 2017

Readings Chapter 4

Assignments Discussion Question #4

Week 5

Week 5 Topic(s) Database Security

Time frame February 6 to February 12, 2017

Readings Chapter 5

Assignments Homework 4
Discussion Question #5

Week 6

Week 6 Topic(s) Malicious Software

Time frame February 13 to February 19, 2017

Readings None

Assignments Term Paper Milestone 1
Discussion Question # 6

Week 7

Week 7 Topic(s) Lab Week

Time frame February 20 to February 26, 2017

Readings None

Assignments Lab 1

Week 8

Week 8 Topic(s) Lab Week

Time frame February 27 to March 5, 2017

Readings None

Assignments Lab 2

Week 9

Week 9 Topic(s) No Class, Spring Break

Time frame March 5 to March 12, 2017

Readings None

Assignments
Take a break, have fun!

Week 9

Week 9 Topic(s) Denial of Service Attacks

Time frame March 13 to March 19, 2017

Readings Chapter 7

Assignments Homework 5
Class Discussion #7

Week 10

Week 10 Topic(s) Intrusion Detection

Time frame March 20 to March 26, 2017

Readings Chapter 8

Assignments Exam 1, Lab 3

Week 11

Week 11 Topic(s) Firewalls & Intrusion Prevention

Time frame March 27 to April 2, 2017

Readings Chapter 9

Assignments Lab 4

Week 12

Week 12 Topic(s) IT Security Controls, Plans and Procedures

Time frame April 3 to April 9, 2017

Readings Chapter 15

Assignments Term Paper Milestone 2
Class Discussion #8

Week 13

Time frame April 10 to April 16, 2017

Readings None

Assignments Exam 2
Class Discussion #9

Week 14

Time frame April 17 to April 23, 2017

Readings None

Assignments Term Paper Milestone 3
Class Discussion # 10

Week 15

Week 15 Topic Presentations

Time frame April 24 to April 28, 2017 (5 days)

Readings None

Assignments Term Paper Milestone 4
Team Briefings

Course Policies and Expectations

- Team work is encouraged in this course. Homework assignments are individual. Labs and term papers are team-based. You should credit persons that have helped by noting the names in the assignments, reports, or papers, and reference to the literature you read.
- Late penalty is 10% per day. Submissions late more than a week are generally not accepted. Requests for exceptions, with justifications, should be sent in advance to the *grader*.
- Logging into CANVAS- Students are expected to login regularly to check for course updates, announcements, emails, discussions, etc.
- Emailing through CANVAS- Students are expected to use CANVAS for all course email communication.
- Attending virtual meetings - Students are expected to use specified virtual meeting tool(s) for collaboration, meetings, presentations, etc., as needed.

Resources

Find extensive information and links to resources, including the Penn State library, web conferencing, course tools, writing help, and much more on the [Resources](#) page.

University Policies

Review current information regarding Penn State policies, including Academic Integrity, Disability Accommodations, Military Accommodations, and many others on the [University Policies](#) page.

Assignments Summary:

Date	Details
Sun Jan 22, 2017	Discussion Activity 1
	Homework 1 Dropbox
Sun Jan 29, 2017	Discussion Activity 2
	Homework 2 Dropbox
Sun Feb 5, 2017	Discussion Activity 3
	Homework 3 Dropbox
Sun Feb 12, 2017	Discussion Activity 4
Sun Feb 19, 2017	Discussion Activity 5
	Homework 4 Dropbox
Sun Feb 26, 2017	Discussion Activity 6
	Term Paper: Milestone 1 Dropbox
Sun Mar 5, 2017	Lab 1 Dropbox - Nmap/Nessus Scanning Lab
Sun Mar 12, 2017	Lab 2 Dropbox - Network Vulnerability
Sun Mar 26, 2017	Discussion Activity 7

Date	Details
	Homework 5 Dropbox
Sun Apr 2, 2017	Exam 1 Drop Box
	Exam 1 Scenario
	Lab 3 Dropbox Intrusion Detection
Sun Apr 9, 2017	Lab 4 Dropbox - Network Security Monitoring
Sun Apr 16, 2017	Discussion Activity 8
	Term Paper: Milestone 2 Dropbox
Sun Apr 23, 2017	Discussion Activity 9
	Term Paper: Milestone 3 Dropbox
Fri Apr 28, 2017	Term Paper: Presentation Dropbox
Sun Apr 30, 2017	Discussion Activity 10
	Additional Nmap Information
	Anti-censorship survey paper
	Chapter 15 Slides
	Exam 2
	Getting Started with VHOL
	Lab 1 Instructions
	Lab 2 Instructions
	Lab 3 Instructions
	Lab 4 Instructions
	Lecture Five

Date

Details

[Lecture Four](#)

[Lecture One](#)

[Lecture Overview](#)

[Lecture Three](#)

[Lecture Two](#)

[Roll Call Attendance](#)

January 2017

