NEW YORK CITY COLLEGE OF TECHNOLOGY/CUNY
Computer Systems Technology Department

CST 2410 - Computer Security
-WAC version-

Instructor:

Prof. Yu-Wen Chen
Lecture: Mon., Wed. 12:00 pm - 1:40 pm, at N-904
Office hours: Mon., Wed. 2-3 pm, at N-913
Email: YWChen@citytech.cuny.edu

Course Description:
This course is an introduction to security issues facing computer professionals today. Students will acquire the knowledge and skills on how to maintain the integrity, authenticity, availability and privacy of data. It covers computer viruses, authentication models, certificates, group policy, cryptography, and access control. It also introduces the fundamental security issues of programming, database and web server. Other topics include how to monitor the system for suspicious activity and fend off attacks, to keep spies and Spam out of the e-mail, to take control of security by encrypting data, to design Active directory, blocking ports, and locking down the registry.

City Tech designates this course as "Writing Intensive." This course provides you with the opportunity to write frequently, learn how to write through multiple modes of writing and in online forums. The WI requirement includes both formal (graded) and informal (non-graded) writing assignments. The majority of your grade in this course will be based on the completion and quality of these assignments. You will have the opportunity to build on some of your written assignments and receive feedback from your instructor and the tutors at the Learning Center. You can expect to write each week.

Objective:
This is the first course of the information security module. It equips students and computing professionals with the basic information security knowledge and operating system security skills needed to implement and maintain modern information infrastructure and systems.

Learning Outcomes:
At the end of the course, students should be able to:

- Demonstrate understanding of the risks and vulnerabilities associated with computer programs.
- Maintain the integrity, authenticity, availability and privacy of data.
- Demonstrate understanding of how to protect privacy by using cryptography.
- Demonstrate understanding of network protocols and the risks and vulnerabilities associated with computer networks.
- Demonstrate understanding of the risks and vulnerabilities associated with operating systems.
- Secure the Windows and LINUX/UNIX operating system.

Prerequisites:
CST1215 and CST2307

Required textbook:
M. Whitman and H. Mattord, *Principles of Information Security*, (4th, 5th or 6th Ed.), ISBN 978-1111138219

Reference book and sites:
Pfleeger, Charles P, and Shari Lawrence Pfleeger. *Security in Computing.*Prentice Hall, 2003.

D. Liu, R. Wisselink, *Securing Windows Server 2008 Prevent Attacks from Outside and Inside Your Organization*, Syngress

Assignments:
Assignments will be based on chapter questions and based on other related readings assigned by the instructor.

Project:
Students should work in groups to finish and demonstrate the project. Project must be submitted on the due date.

Grade Requirement:
Students must complete all project assignments and participate in all tests.

Course grading formula:

Assignments	20%
Quizzes & Participation	15%
Term Project	10%
On-line Certificate	15%
Midterm Exam	20%
Final Exam	20%
	100%

All assignments and on-line certificate should be submitted to Blackboard. Emailing them to me is unacceptable, and hand-written papers are unacceptable.

Any late assignment is subject to 5% penalty for each late day.
No late assignment is accepted after 2 days of the due date.

Letter Grade	A	A-	B+	B	B-	C+	C	D	F
Numerical Grade	93-100	90-92.9	87-89.9	83-86.9	80-82.9	77-79.9	70-76.9	60-69.9	<=59.9

Academic Integrity Standards:
The instructor of the course has the authority to give a grade of **F** if the student submits the work of another person in a manner that represents his/her work, or knowingly permits one's work to be submitted by another person without the instructor's permission (see College Catalog).

Progression Requirements:
Students majoring in CST department must earn a grade of "C" or better in this course in order to progress to the next level courses (CST3610 and CST4710). If grade earned is less than "C", the course must be repeated.

Topics and Schedule:

Week 1:	Introduction to Information Security
Week 2:	The Need for Security
Weeks 3-4:	Legal, Ethical, and Professional Issues in Information Security.
Weeks 5-6:	Risk Management, Physical Security
Week 7:	Review & Midterm
Weeks 8-9:	Planning for Security
Weeks 10-11:	Cryptography I
Weeks 12-13:	Cryptography II & III
Week 14:	Selective Security Topics (E.g., Microsoft Windows Server 2008)

Week 15: Review and FINAL

Class rules:

* Individual-effort assignments must be individual efforts. Students who submit identical or highly similar assignments will receive an F as the letter grade of this course.
* Student who plagiarizes other work (including people outside of the class) in any part of assignments/tests will receive an F.
* Student who cheats on the quizzes and exam will receive an F.
* You are welcome to discuss your graded assignments and exams with the instructor. However, the discussion must be done within two weeks after you receive your graded assignment/exam back.
* Please mute or turn off your cell phone during the class.
* No headphone on your head in the class.
* Be on time for class.

Learning Center:

The College Learning Center, through its extensive computer labs, workshops and tutoring, offers assistance to students across the entire college population. The Learning Center is located in room G18.

Counseling Service Center

The Counseling Services Center provides individual counseling services that address personal concerns, crisis intervention, educational planning and referral services to assist students in achieving their academic goals. Student privacy is respected. The Counseling Center is located in Namm Hall (N-108),

Americans with Disabilities Act: Any student who believes he/she is eligible for accommodations in the classroom and/or during testing due to a documented disability is encouraged to contact the Director of Student Support Services at (718) 355-5081.

Appendix I: Writing Related Work

1. ***In-Class Discussion Notes for the review session of each class meeting (Informal)****:*

   Every class starts with a brief review session for the materials and concepts from the previous lecture. During the review session, students will bring discussion notes (at least 50 words) to class as part of their participation grades.

   a. What did you learn from the previous class session?
   b. Were there any confusing points from the previous class which need clarification?
   c. Any security related news or articles that you want to share with the class?

2. In-Class Writing related Activities and Discussions (Informal):

Feb. 4 - In-class activities for chapter 1: Introduction to Information Security

- Discuss the following scenario with your classmates for 10 minutes and write the ideas on the board to share with the class. If you are working for an origination, and would like to initiate a new project, what would you do in steps?

Feb. 6 - In-class activities for chapter 1: Introduction to Information Security

- Form five teams of students. Each team spends 10 minutes to read through the example from "The Role of Chief Security Officer is More Vital than Ever" http://www.govtech.com/security/The-Role-of-Chief-Security-Officer-is-More-Vital-than-Ever.html
- Have a representative from each group provide a brief summary from the example to the whole class.

Feb. 20- In-class activities for chapter 2: The Need for Security

- Read the following articles, and write down your thoughts. Tesla Offers a Model 3 as 'Bug Bounty' for Anyone Who Can Hack Into It https://www.bloomberg.com/news/articles/2019-01-14/tesla-offers-model-3-as-bug-bounty-for-cybersecurity-researchers

Feb. 25 - In-class activities for chapter 3: Legal, Ethical, and Professional Issues in Information Security

- Write down what is private and what is not private to you.

Feb. 27 - In-class activities for chapter 3: Legal, Ethical, and Professional Issues in Information Security

- There is a file named "Computer Ethics Studies Exercise" in Blackboard and in the textbook on page ___. Discuss with another student, and complete the survey for the first five scenarios. Please also include your thoughts on the selection.

March 6 - In-class activities for chapter 4: Risk Management

- Brainstorm questions that you would ask to help develop criteria for asset valuation. (e.g., Is it most critical to the organization's success?) Write at least two questions and share with classmates.

3. Writing questions in the assignments (Formal):

Please see the attached 5 assignments as the references.

4. ***Term Project Report (Formal):*** The term project requires student to conduct a thoughtful study on the specific course-related topic (selected by students and needs to be approved by the instructor). Students have to present in class with PowerPoint slides for 15 minutes and submit a formal project report at the end of the semester. Details can be found in Appendix II below.

Appendix II: Term Project

Requirements:

- At least 10 pages
- Letter size, font size 12, and single space
- Do not copy & paste from the article. The Internet-based plagiarism detection tool "Turnitin" will be used.
- Proper citation to indicate the source is important and required.

Guidelines and grading scale:

I. **(5 points) Title:**

II. **(10 points) Abstract:**

III. **(10 points) Introduction:**
- Why this topic?
- What are the related parts in the covered articles?

IV. **(10 points) Methodology:** (from the non-survey paper)
- What are the approaches in those articles?

V. **(10 points) Performance Evaluation:** (from the non-survey paper)
- What are their results?

VI. **(25 points) Critical thinking:**
- What do you think they fail to discuss, or what can be improved?

VII. **(20 points) Summary:**
- What did you learn from those articles and this project?

VIII. **(10 points) References:**
- IEEE format citation is required for every referenced article.

The grading for each section follows the rubric in Appendix III.

Timeline:

- 03/04: Propose the project title

- 03/05: Feedback for the project title will be available. Revise the title if needed. The topic selection needs to be approved by 03/10.
- 03/20: Submit the proposed articles with the IEEE format citations.
- 03/21: Feedback for the selected articles will be available. Research the articles, or resubmit the citation if needed. Articles need to be approved by 03/25.
- 04/15: Submit the first draft of the slides outline and sections III, IV, and V of the report.
- 04/18: Feedback will be available. Modify the draft if needed.
- 05/01: Submit the second draft of the slides and sections VI and VII of the report.
- 05/06: Feedback will be available. Modify the draft if needed.
- 05/15 & 05/20: In-class presentation. Submit the finalized slides.
- 05/22: Submit the final report.

Appendix III: Rubric

	Strong	**Proficient**	**Satisfactory**	**Weak**	**Unsatisfactory**
	Full credit	80% credit	60% credit	40% credit	20% credit
	Sufficiently address the question with complete sentences and correct grammar	Clearly address the question; consistent and concise; no more than 2 errors	Clearly address the question with no more than 5 errors	Lacks clarity; numerous spelling and grammatical errors	Inappropriate and lacks clarity of components; no answer is provided
5 pt activity	5	4	3	2	1
10 pt activity	10	8	6	4	2
15 pt activity	15	12	9	6	3
20 pt activity	20	16	12	8	4
25 pt activity	25	20	15	10	5

* This rubric is an adaptation of examples offered by the Information Technology Department at Montclair State University.

CST2410 Introduction to Computer Security, Spring 2019
Assignment 1

Total points: 100
< The grading for this assignment follows the rubric in Appendix III >

1. (15 points) What type of security was dominant in the early years of computing?

2. (15 points) What is the difference between vulnerability and exposure?

3. (15 points) What is the difference between a threat agent and a threat?

4. (15 points) Pick one sub-cube from the McCumber cube (e.g., Availability – Policy – Processing). Explain the meaning and think a daily example for this sub-cube.

5. (20 points) Search on the Internet and find a data breaches news in 2018. Provide a brief summary in your own words on that incident. Include the information such as which company, how many records breached, when is this happened, etc. Cite your sources.

6. (20 points) Read the section 2 “software development” from the article “Software Engineering at Google” (https://arxiv.org/ftp/arxiv/papers/1702/1702.01715.pdf). Provide a summary and address your thoughts on this section.

CST2410 Introduction to Computer Security, Spring 2019
Assignment 2

Total points: 100
< The grading for this assignment follows the rubric in Appendix III >

1. (10 points) What is the difference between a denial-of-service attack and a distributed denial-of-service attack? Which is more dangerous? Why?

2. (10 points) For a sniffer attack to succeed, what must the attacker do? How can an attacker gain access to a network to use the sniffer system?

3. (5 points) Find at least 2 **websites** dedicated to hacking (cannot be the one introduced in the class).

4. (10 points) Locate two **software tools** you think would be useful to hackers and provide a brief description of the tools and their potential danger

5. With the provided link below, study the 2018 Data Breach Investigations Report from Verizon and answer the following questions. (https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf)
    a. (10 points) Which industry is facing the greater threat from inside than from outside, and what is the common cause?

    b. (5 points) Which threat actions is the highest across from 2013 to 2016?

    c. (15 points) The report suggests several things that we can do to prevent the data breach. Pick one thing and provide a brief description on how you can adopt it in the daily life or what would be the tools that you would choose for doing it.

6. (20 points) Among the several cybersecurity concerns that modern businesses have to deal with, zero-day attacks are calling for more and more attention. Organizations are witnessing increasing difficulties in detecting such attacks, let alone preventing them. Please search from the online resource and find one potential solution for this type of attack. (remember to cite your source)

7. (15 points) Search **two** Microsoft (as the vendor) vulnerabilities from the SecurityFocus (https://www.securityfocus.com/). Provide **a brief description** and **the URL** for each vulnerability.

CST2410 Introduction to Computer Security, Spring 2019
Assignment 3

Total points: 100
< The grading for this assignment follows the rubric in Appendix III >

1. (10 points) If you work for a financial services organization such as a bank or credit union, which 1999 law affects your use of customer data? What other effects does it have?

2. (10 points) What is PCI DSS and why is it important for information security?

3. (10 points) Of the information security organizations listed in this chapter that have codes of ethics, which has been established for the longest time? When was it founded?

4. (15 points) Visit the National Conference of State Legislatures Web site at www.ncsl.org and use the search box to find the security breach notification law, data disposal laws, and identity theft statutes for the New York State. Screen-shot or copy-paste your search result.

5. (10 points) Find 2 **web-sites** dedicated to **computer security**

6. (20 points) Locate two **software tools** you think would be useful to help **defend against an attack**. Provide your brief explanations on those two tools.

7. (25 points) To have a safer online communication, Electronic Frontier Foundation provides several tips and tool guides. Please select one guide (e.g., How to: XXX) from the list of tool guides in https://ssd.eff.org/module-categories/tool-guides. Provide a brief summary for the selected guide and address your thoughts.

CST2410 Introduction to Computer Security, Spring 2019
Assignment 4

Total points: 100
< The grading for problem 1 to problem 3 follows the rubric in Appendix III >

1. (5 points) Why do networking components need more examination from an information security perspective than from a systems development perspective?

2. (5 points) What's the difference between an asset's ability to generate revenue and its ability to generate profit?

3. (10 points) What five strategies for controlling risk are described in this chapter? Please think a daily example for using **each** strategy.

4. (8 points) Calculate the weighted score for the asset 1 and asset 2. Which asset is more important?

Information Asset	Criterion 1	Criterion 2
Criterion weight	**60**	**40**
Asset 1	**0.7**	**0.8**
Asset 2	**0.8**	**0.7**

5. (24 points) Suppose XYZ Software Company has a new application development project. Using the following table, calculate the **ARO** and **ALE** for each threat category the company faces for this project.

Threat Category	**Cost per Incident (SLE)**	**Frequency of Occurrence**	**ARO**	**ALE**
Programmer mistakes	$5,000	2 per weeks		
Loss of intellectual property	$25,000	2 per year		
Software piracy	$500	1 per 2 weeks		
Theft of information (hacker)	$1,500	5 per quarter		

6. (48 points) Assume that a year has passed and XYZ has improved security by applying several controls. Using the information from problem 5 and the following table, calculate the **post-control ARO** and **ALE** for each threat category listed. Calculate the **CBA** for the planned risk control approach in each threat category. For each threat category, **determine whether the proposed control is worth the costs**.

Threat Category	**Cost per Incident**	**Frequency of Occurrence**	**Cost of Control**	**Type of Control**
Programmer mistakes	$5,000	3 per month	$20,000	Training
Loss of intellectual property	$25,000	1 per 2 years	$20,000	Firewall/IDS
Software piracy	$500	1 per 2 months	$9,000	Firewall/IDS
Theft of information (hacker)	$1,500	2 per 6 months	$20,000	Firewall/IDS

CST2410 Introduction to Computer Security, Spring 2019
Assignment 5

Total: 100 points
< The grading for problem 1 to problem 4 follows the rubric in Appendix III >

1. (10 points) What is steganography, and what can it be used for?

2. (10 points) If you were setting up an encryption-based network, what key size would you choose and why?

3. (10 points) What are the most popular encryption systems used over the Web?

4. (10 points) What encryption standard is currently recommended by NIST?

5. (20 points) Use the Caesar cipher with the shift equals to 6, find the plaintext from the cipher.
   Cipher: COTZKX_OY_NKX

6. (20 points) Use the 5-bits block size transposition Cipher to encode the plaintext: " N B A P L A Y O F F " with the following key pattern. Include your procedure and the final answer for the ciphertext.
   Key pattern: 5 -> 1, 4 -> 5, 3 -> 2, 2 -> 3, 1 -> 4.

7. (20 points) Using the Vigenere square and the following information, find out the ciphertext.
   Plaintext = "HappySpring", Key = "Recess"

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Table 8-2 The Vigenère Square