PETERS TOWNSHIP HIGH SCHOOL
COURSE SYLLABUS: CHS COMPUTER SECURITY (INF SCI 1074)

Course Overview and Essential Skills

This course covers the fundamental concepts in Computer security and privacy. The course is intended to expose the various security threats and vulnerabilities in computer systems and provide an understanding of the various defense and protection mechanisms. Primarily, the course will focus on models and mechanisms related to insuring confidentiality, integrity and availability related to computer and information systems. We will cover the basic concepts of cryptography including symmetric and public key encryption schemes. We then focus on program security issues such as buffer overflow attacks and discuss various control mechanisms to handle malicious code. The second half of the course will cover the topics of Database Security, general security issues in Operating Systems, and discuss various security and privacy issues in the context of emerging cloud computing systems. The last 9 weeks will be devoted to a computer security project covering concepts learned during the year and additional research in computer security. This class is an elective class for seniors. A programming class is strongly suggested as a pre-requisite for this class.

Course Textbook (Optional...students may elect to take home 1 classroom textbook for additional study)

- Title: *Security in Computing*, Fifth Edition, 2015, Charles Pfleeger, Shari Lawrence Pfleeger and Jonathan Marguiles
- Title: *Java Programming (Guided Learning with Early Objects)*, 2009, D.S. Malik & Robert P. Burton, ISBN-13: 978-1-4239-0162-4 and ISBN-10: 1-4239-0162-2
- Title*: Java Programming*, 1999, Joyce Farrell, ISBN#: 0-7600-1070-6
- Notes, sample programs, and programming assignments will be given in class and stored on the students H: drive

Course Outline of Material Covered:

Unit or Topic	Course Activities/Resources	Timeframe
Course Plan	- Students will develop, add, and maintain yearly plan for the end of year project to enhance and enrich education in computer security - The plan will be composed of 2 parts: Part 1 of the project choices could be: demonstration, video, showcase, manual, competition day between high schools or a computer security day at the high school - Part 2 of the project is completing a report in area of interest in the computer	1 week

	security such firewalls, cryptography, biometrics security, etc. • This project will be completed in the 4th 9 weeks	
Introduction	• Define/Describe/explain some key computer security terms • Distinguish between vulnerability, threat, and control • Describe/explain the importance of confidentiality, integrity and availability in the context of computer security • Research what security measures are used on your home computer, what security measures are used at school, and what security measures would be used at a business • Upon researching security measures taken, create a profile on who may want to attack the program • Explain the types of harm they want to cause, and vulnerabilities might they exploit to cause the harm	2 weeks
ToolBox: Authentication, Access Control, and Cryptography	• Explain and show how more factors mean less security • Recognize/explain and use the basic cryptographic techniques such as substitution and transposition ciphers • Recognize/compare the pros and cons of stream ciphers Vs block ciphers • Recognize/explain concepts related to public key encryption and concepts related to certificates • Recognize the basic access control mechanism in general purpose operating systems • Recognize the basic access in OS and use access control commands to manipulate permissions in OS	4 weeks

	• List 3 reasons people might be reluctant to use biometrics for authentication and can you demonstrate ways to counter those objections • Calculate the timing of password guessing contacts • Code a java program that would use to try to eliminate brute force attack to determine a password	
Programs and Programming	• Recognize, compare/contrast, and explain, different types of malicious code • Recognize, compare/contrast, explain buffer overflow attacks and TOCTOU attacks mechanisms • Recognize, compare/contrast, and explain different types of virus programs • Recognize, compare/contrast, and explain different types of software vulnerabilities and defense mechanisms for viruses • Calculate the timing of password guessing contacts • Code a java program that would use to try to eliminate brute force attack to determine a password • Code a java program that would determine the amount of time between secure and insecure passwords • State and justify your assumptions for the vulnerability of finding a password and the amount of time required	2 weeks
The Web – User Side	• Recognize and explain the attacks against browsers, against and from web sites, attacks seeking sensitive data and through email • List 5 types of Malicious Code that you know • Explain an summarize the what the malicious does and harm that it could provide	2 weeks

	• Research and summarize 3 malicious code infections with the year and the effect that they had on society	
Operating Systems	• Recognize and explain that the operating system is the fundamental controller of all system resources, which make it a primary target of attack as well • Discuss and show how the operating system is designed to protect objects • Explain and show how the operating system is designed for self-protection	2 weeks
Networks	• Recognize and explain the vulnerabilities and threats to networks through wiretapping, modification, and addressing • Discuss and show how protections can be provided through cryptography, firewalls, intrusion detection and protection systems	2 weeks
Databases	• Recognize and explain the basic security and privacy issues in database systems • Understand and explain security and privacy models and approaches	2 weeks
Cloud Computing	• Understand and explain Location Privacy, Cloud computing models, benefits and disadvantages • Recognize, explain the basic security issues in Cloud computing systems	2 weeks
Privacy	• Understand and explain the fundamental concepts in data and location privacy such as k-anonymity and l-diversity • Recognize and explain the aspect of security and confidentiality on personal or business privacy and the internet	2 weeks

Management and Incidents	• Discuss and explain how security planning, incident response and business continuity planning, risk analysis, and handling natural and human-caused disasters effect computer security	2 weeks
Emerging Topics, Legal Issues and Ethics	• Students will research and evaluate by comparing, analyzing, and predicting future threats and problems in computer security (locally, nationally, and throughout the world)	3 weeks
Speakers and Testing (throughout the year)	• Speakers will be introduced to students at least once a month (we will try) from the FBI, banks, financial firms, hospitals, armed forces and other types of companies discussing security measures and threats in computer security posed to their companies	2 weeks
Final Project	• Completion of their end of year project (see week 1 for more information)	8 weeks

*Depending on the needs of the class or changes in the school year, the course outline is subject to change.