WEST VIRGINIA UNIVERSITY
College of Engineering and Mineral Resources
Lane Department of Computer Science and Electrical Engineering

CS 465 Cybersecurity Principles and Practice

Spring 2020 Semester
3 credit hours

Class time: Tuesday & Thursday – 12:30 pm - 1:45 pm
Location: AER 137

Instructor: Dr. Katerina Goseva-Popstojanova
Office: 261 AER
E-mail: Katerina.Goseva@mail.wvu.edu
Phone: 304-293-9691
URL: http://community.wvu.edu/~kagoseva/
Office hours: Tuesday & Thursday 2:00 pm – 3:00 pm or by appointment

Graduate Teaching Assistant: Michael Austin
Office: 302 AER
E-mail: maa0075@mix.wvu.edu
Office hours: Monday & Wednesday 9:30 am – 10:30 am or by appointment

Prerequisites: Knowledge of computer system concepts (CS350 at WVU or equivalent) or Instructor consent.

Course Materials:

- *Required textbook:* Charles P. Pfleeger, Shari Lawrence Pfleeger, and Jonathan Margulies, *Security in Computing*, Prentice Hall, Fifth edition, 2015. (Available online at WVU Libraries.)
- *Optional textbook:* Yuri Diogenes and Erdal Ozkaya, *Cybersecurity: Attack and Defense Strategies*, Packt Publishing, 2018. (Available online at WVU Libraries.)
- *Required and optional papers selected from technical magazines, journals, and relevant conferences.*

Course Description and Objectives: This course covers the principles and practice of cybersecurity. It addresses different areas of cybersecurity such as encryption; malicious code, spyware, and spam; authentication and access control; network security; and social engineering. The objective of this course is to provide students with a comprehensive overview of the cybersecurity threats, technologies for information assurance, and engineering approaches to build and maintain secure cyber systems and networks.

Learning Outcomes: Upon successful completion of CS 465, students will be able to:

- Use encryption algorithms and secure protocols
- Use appropriate protection measures against malicious code
- Apply the principles of physical security, authentication, and access control
- Plan, implement, and assess security protection mechanisms in computer systems and networks
- Recognize and protect from social engineering attacks

Tentative Lectures Schedule:

1) *Security Threats and Vulnerabilities* [1 week]. Threats and vulnerabilities. Attributes of cybersecurity.
2) *Encryption* [3 weeks]. What is encryption and how it protects both stored data and communications. Secret key cryptography, public key cryptography, digital signatures. Secure protocols (e.g., SSL, SSH, SFTP).
3) *Malicious Code, Spyware, and Spam* [2 weeks]. Malicious code, including viruses, worms, and Trojan horses. Spyware. Spam.
4) *Social Engineering and Human Aspects of Cybersecurity* [1 week]. Social engineering attacks (e.g., Pretexting, Phishing, Baiting, Quid pro quo, Tailgating).
5) *User authentication* [1.5 week]. Password authentication, including password selection criteria and attacks on passwords. Authentication with biometric devices.
6) *System and data access controls*. [1 week]. Principles of access control. Modern OS access control.
7) *Network Security* [5.5 weeks]. Network security topics such as message confidentiality and integrity violations, and denial of service attacks. Web security. Wireless network security. Types and examples of firewalls.

RULES OF OPERATION

Attendance: Students are expected to regularly attend lectures. Students are responsible for all material covered in the course, keeping track of assignments and examination dates.

Homework and Programming Assignments: Homework assignments will be due at the beginning of the class on the scheduled date. Programming assignments will be due at midnight on the scheduled date. Please make sure that you have an active account on LDCSEE Linux shell servers. You will need it for developing and testing your programming assignments. In cases when late assignments are allowed, unexcused late assignments will be penalized 10% for each day late. All work submitted for the homework and programming assignments must be your own work. Evidence to the contrary will be dealt with in accordance with the WVU Student Conduct Code.

Exams: There will be a midterm exam and a final exam. The midterm exam will be administered during the seventh or eighth week of the semester. The final exam will be given according to the Registrar's exam schedule. Collaboration is not permitted on any part of the midterm and final exams. Evidence to the contrary will be dealt with in accordance with the WVU Student Conduct Code. Make-up exams will be given only by prior arrangement and only *under truly extraordinary circumstances*. Consistent with WVU guidelines, students absent from regularly scheduled examinations because of authorized University activities will have the opportunity to take them at an alternate time.

Grading: Semester grades will be computed roughly as follows:

Homework assignments 25%
Programming assignments 30%
Midterm exam 22%
Final exam 23%

Passing grade (more than 60%) must be obtained in both homework/programming assignments and exams in order to pass the course. Grades will be A = 90-100%, B = 80-89%, C = 70-79%, D = 60-69%, and F = 0-59%.
'+' and '-' grade may be reported if the score is near boundary.

Communication: All course material, assignments, announcements, etc. will be provided using the eCampus features. Please check eCampus and your e-mail regularly.

Academic Policies and Syllabus Statements (including the Academic Integrity Statement and Inclusivity Statement) can be found at https://tlcommons.wvu.edu/syllabus-policies-and-statements.

Students must adhere to the West Virginia University standards for academic integrity and avoid academic dishonesty in all its forms, including (but not limited to) collaboration with peers beyond that authorized by the instructor, receiving/ giving unauthorized personal assistance, and utilizing unauthorized physical or technological resources (e.g., https://www.chegg.com/). Details on what constitutes academic dishonesty are given at the Academic Standards web site.

Other Policies: In this class we will discuss vulnerabilities in widely deployed computer systems and networks. This is not intended as an invitation to go exploit those vulnerabilities. It is important that we discuss real-world experiences in class; students are expected to behave responsibly. WVU's policy (and our policy) on this is clear: you may not break into machines that are not your own; you may not attempt to attack or subvert any system security. Unauthorized access, use, modification, destruction, or disclosure of any computer system or computer network or any computer software, program, documentation, or data contained in such computer system or computer network is computer crime.