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

CYBE 366 – Secure Software Development
3 credit hours

Class time: Tuesday & Thursday – 11: 00 am – 12:15 pm
Location: AER 135

Instructor: TBD

Prerequisites: CS 230 and CS 350 both with a grade of C- or better

Course Materials:
Required texts:
Secure Coding in C and C++ (2nd Edition) (SEI Series in Software Engineering) (ISBN-13: 978-0321822130 ISBN-10: 0321822137), 2013, Pearson Education Inc.

Java Coding Guidelines: 75 Recommendations for Reliable and Secure Programs (SEI Series in Software Engineering), (ISBN-13: 978-0321933157; ISBN-10: 032193315X), 2014, Pearson Education Inc.

Course Description: Covers the design, implementation, and testing of secure software. The topics include the role of security in the software development lifecycle, designing secure software, best security programming practices, and verification and validation of software applications' security.

Learning Outcomes: Upon successful completion of CS 366, students will be able to:
- Incorporate security into software development process
- Design and implement secure software applications
- Use appropriate techniques and tools to analyze and test software applications for weaknesses and vulnerabilities
- Fix software security bugs using secure coding techniques

Topics Covered and Tentative Lectures Schedule:
1. *Secure software development lifecycle* [0.5 weeks]
2. *Specification of security and privacy requirements* [1 week]
3. *Design principles of secure programming* [1.5 weeks], including Separation (of domains), Isolation, Encapsulation, Modularity, Layering, Least Privilege, Fail Safe Defaults, Fail Secure, End-to-End Security, Defense in Depth Simplicity of design, Minimization of implementation
4. *Defensive/Secure software programming practices & Secure coding standards* [8 weeks]
   - Input validation and sanitization
   - Type checking
   - String management
   - Memory and resource management
   - Exception handling
   - Overflows (buffer, integer, other)
   - File I/O vulnerabilities, including race conditions
   - Protecting sensitive data
   - Java Platform and API Security
5. *Web application security* [1 week]
   - SQL injection, Cross-site scripting (XSS), and Cross-site request forgery (CSRF)
   - Secure Web session management
6. *Secure software verification and validation* [3 weeks]
   - Static source code analysis
   - Penetration testing
   - Fuzz testing

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.

Programming Assignments and Project: The individual mini-programming assignments will be due at the beginning of the class on the scheduled date. The group project will be due at midnight on the scheduled date. Unexcused late assignments will be penalized 10% for each day late. All work submitted for the programming assignments and group project must be students' 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 eight 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 as follows:

Individual mini-programming assignments on secure software programming 35%
Group project on secure software verification 25%
Midterm exam 20%
Final exam 20%

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/qualitymatters/syllabus-policies-and-statements.

Other Policies: In this class we will discuss software weaknesses and vulnerabilities. This is not intended as an invitation to go exploit those weaknesses and 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 software application, data, documentation, computer system or network are computer crimes.