Master Course Syllabus
School of Engineering and Computer Science
Washington State University Vancouver
CS 425
Digital Forensics
3 Semester Hours
(3 lecture hours)

Catalog Description

Use of computers in the investigation of criminal and civil incidents in which computers or computer technology play a significant or interesting role.

Prerequisite Courses

- CS 360 with a C or better, or concurrent enrollment

Prerequisite Topics

- Proficiency with C/C++ programming language.
- Knowledge of assembly language concepts, including procedure calling conventions
- Understanding of computer memory and I/O architecture
- Experience with the Linux environment for coding, compilation, debugging, and testing

Measured Course Outcomes

Students taking this course will:

1) Recognize insecure programming patterns and know how to replace them with secure alternatives (Contributes to performance criterion 1-c.)
2) Use standard digital forensic tools and assess their capabilities/limitations (Contributes to performance criterion 2-c.)
3) Deliver a well-organized project presentation and effectively communicate the severity of a security vulnerability and its potential mitigations (Contributes to performance criterion 3-b.)

Required Textbooks

No textbook required

Reference Material

- Casey, Digital Evidence and Computer Crime, Academic Press.
- Howard, M., LeBlanc, D., & Viega, J., 24 deadly sins of software security, McGraw-Hill.
- Taylor, Unix in 24 Hours, Sams Publishing.
- Altheide & Carvey, Digital Forensics with Open Source Tools, Syngress.
- Carrier, File System Forensic Analysis, Addison-Wesley.
- Russinovich & Solomon, Windows Internals, Microsoft Press.
- Anley et al. The Shellcoders Handbook, J. Wiley Publishing

Major Topics Covered in the Course

- Evidence collection, preservation, and analysis
- Disk Forensics
- Network Forensics (Cybercrime)
- Source-Code Forensics
- Volatile Data Forensics (Live Forensics)
- Anti-Forensics (Encryption, Steganography)
- Privacy and Ethics

Projects

Programming Project Area	Weeks

Design, Implementation and Analysis

Students learn the digital forensic process of collecting, preserving, and analyzing data. Standard open source digital forensics tools are introduced where students examine each tool to both understand their capabilities and determine their limitations. In addition, students investigate a variety of systems/applications for the presence of malicious activity. Finally, students learn defensive programming best practices and how various system protection techniques are designed and implemented.

CS2013

This course provides coverage of CS2013 knowledge areas. Values listed are minimum course hours dedicated to the topic, percentages indicate the fraction of CS2013 knowledge area topics covered (acceptable values are: <25%, 25-75%, >75%, or 100%).

Area	Tier 1	Tier 2	Elective
IAS/Foundational Concepts in Security	1(25-75%)		
IAS/Principles of Secure Design	2(100%)	2(100%)	
IAS/Defensive Programming	5(100%)	1(25%-75%)	2(25-75%)
IAS/Threats and Attacks		2(>75%)	2(100%)
IAS/Network Security		5(>75%)	
IAS/Digital Forensics			7(>75%)

Course Coordinator:	Anna Wisniewska
Last Updated:	January 24, 2022
Syllabus Version Number:	2.1