ESOF 422 Spring 2025
Advanced Software Engineering: Secure Software Practices

Lecture Time and Location: M,W,F 14:10 – 15:00 in AIH 166

Instructor: Dr. Clem Izurieta and Mr. Reese Pearsall
Contact: clemente.izurieta@montana.edu
reese.pearsall@montana.edu
Office Hours: Dr. Izurieta: MWF 11:00 – 12:00, or by appointment
Office Location: NAH 253D

Office Hours: Mr. Pearsall: TWF 12:00 PM – 1:00 PM, or by appointment
Office Location: Barnard 361

Course and Lab Assistant: Sarker Mahmud
Contact email: sarkersafat.mahmud@student.montana.edu
Office Hours: M 17:10 – 18:10
Office Location: Barnard 348

Textbooks:

1. Warmer and Kleppe, "The Object Constraint Language Second Edition," Addison Wesley 2003. ISBN 0-321-17936-6
    - *This is out of print but you can find old copies on the net and it is a good book to have. I will provide handouts in class.*

Any textbook or resource that will help you with UML. This is your choice.

Prerequisites:
ESOF 322 – Software Engineering
Strong grasp of UML diagrams and design patterns

Course Description:
This course focuses on the early phases of the software lifecycle, extending the knowledge developed in ESOF 322 around UML specifications to formulate precise requirements. We rely heavily on UML and Design Patterns. We will focus on advanced software modeling and specification techniques. We will discuss model-driven engineering through model-driven software development and its support tools, such as UML, USE, and OCL. We then turn our attention to the cybersecurity aspects of software engineering. We will discuss cloud computing, digital forensics, the security lifecycle of software, and security analysis techniques.

Course Objectives:

- Build expertise in modeling techniques
- Introduce software design through the use of rigorous UML
- Introduce constraint-based modeling
- Learn relevant and pragmatic topics in cybersecurity. Specifically the Security Lifecycle and analysis techniques
- Learn many relevant cybersecurity tools
- Learn advanced testing techniques also applied in cybersecurity
- Learn relevant digital forensics

Course Outcomes

- Articulate what formal methods are.
- Be able to read and write formal specifications written in UML and OCL.
- Write and analyze specification constraints using OCL.

- Write SOIL to extend UML diagrams.
- Form informed opinions about model-driven techniques.
- Use a constraint solving tool –USE
- Cybersecurity Knowledge Units (KUs):
    - Describe the Security lifecycle (KU: LCS)
    - Understand and perform simple software forensics and software analysis (KU: DFS)
    - Software Security Analysis (KU: SSA)
    - Penetration Testing (KU: QAT)

Software and Additional Reference Material
The following is a list of the software and relevant downloads that we will use throughout this course:

Modeling
We will use the USE framework (v6.0) to do modeling.
Download here: https://sourceforge.net/projects/useocl/

Cybersecurity
We will need access to a Linux machine, which we will use Kali Linux VM. You will also need virtualization software, such as VirtualBox or VMWare.
Download here: https://www.kali.org/get-kali/#kali-platforms

Grading Policy:
HWs, exams, attendance and class participation.
3 Exams: 40%
HW: 60%

The final exam is optional. If you decide not to take it, the average of your first two exams will be used as your final exam grade.

Instruction:
New HW is assigned every fortnight. We will typically load the HW to D2L on Mondays, and they will be due on Friday of the subsequent week. The TA will be available during his/her office hours. There will be **no makeup Labs or HWs (strictly enforced).**

Attendance and Participation:
Class attendance and participation are highly encouraged, as they will be taken into consideration for final grades. Attendance can be worth (5% - 10%) of your grade. You are responsible for all the material covered in class. Prepare in advance for class by reading and studying the assigned text and ensuring you understand the previous lecture.

Student Help:
A student who desires accommodation for a disability needs to speak to the instructor prior to the graded event.

Academic Integrity:
Honesty and integrity is expected in all class work. The standards set by MSU's academic integrity and student conduct guidelines apply to this class. Academic misconduct is unacceptable. It is the responsibility of all students to adhere to strict standards of integrity in their professional and scholarly activities. **Misconduct will be treated swiftly and harshly**. It is a breach of academic integrity to present the ideas or works of another as one's own work, or to permit another to present one's work without customary and proper acknowledgment of authorship.

Students are responsible for the honest completion and representation of their work, the appropriate citation of sources and the respect and recognition of others' academic endeavors. According to MSU's Conduct Guidelines and Grievance Procedures for Students, academic misconduct includes cheating,

plagiarism, forgery, falsification, facilitation or aiding academic dishonesty; multiple submission, theft of instructional materials or tests; unauthorized access to, manipulation of or tampering with laboratory equipment, experiments, or computer programs, without proper authorization; alteration of grades or scores; misuse of research data in reporting results; use of personal relationships to gain grades or favors, or otherwise attempting to obtain grades or credit through fraudulent means.

Syllabus (this can and will change… please monitor)

Advanced Software Engineering – Lectures
Spring 2025

W	Date	Topic	Resources	Events/Readings
1	Jan 15, 17	Introduction, UML review Model driven development USE: https://sourceforge.net/projects/useocl/	IntroToUML, MDSE Handout	Start of classes
2	Jan 20, 22, 24 **No class Jan 20**	OCL Inheritance Liskov's rules	OCL	OCL Book (Ch 2) **HW1 due 1/31**
3	Jan 27 **No class** Jan 29, 30 **Clem at conference**	Aggregation, Composition	OCL	OCL Book (Ch 2, 3)
4	Feb 3, 5, 7	Component diagrams Security design patterns		**HW2 due 2/14**
5	Feb 10, 12, 14	2/10: Exam 1 Lifecycle Security, Software Assurance maturity model (SAMM), Software Architecture https://owasp.org/www-project-samm/		**Feb 10: Exam 1**
6	Feb 17, 19, 21 **No class Feb 17**	Testing Introduction Graph Coverage Criteria Graph coverage with paths		**HW3 due 2/28**
7	Feb 24, 26, 28	Predicate Logic Coverage		
8	Mar 3, 5, 7 **No class Mar 3**	3/7: Exam 2 Input space partitioning		**Mar 7: Exam 2**
9	Mar 10, 12, 14 **No class Mar 14**	Secure by Design		
10	Mar 18, 20, 22	**No Class**		**Spring Break**
11	Mar 24, 26, 28	Vulnerability Analysis		
12	Mar 31, Apr 2, 4	Penetration Testing		**HW 4 due 4/2**
13	Apr 7, 9, 11	Digital Forensics Introduction Principles of Digital Forensics Incident Management Investigation Models Capturing Digital Evidence		
14	Apr 14, 16, 18 **No class Apr 18**	Memory Forensics System Architecture Review Operating System Fundamentals Volatility		**HW 5 due 4/16**
15	Apr 21, 23, 25 **No class Apr 21**	Digital Forensics Volatility		
16	Apr 28, 30 May 2	Digital Forensics, Course Conclusion		**HW6 due 5/4**
F	Wednesday May 7th 2:00 – 3:50 PM	Final Exam (in our normal classroom)		**May 7: Exam 3**