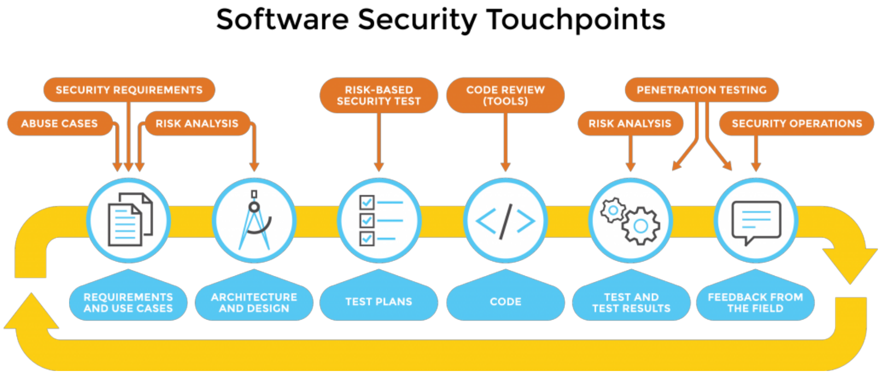
Welcome to
Secure Software Engineering!

CSC 666

Meets on Wednesday evenings 6:15-9:00 online



Dr. James Walden

waldenj@nku.edu (859) 572-5571

http://faculty.cs.nku.edu/~waldenj

Table of Contents

1 SUMMARY

Secure software engineering focuses on creating software that functions correctly even when attacked. Topics include common software vulnerabilities, risk analysis, misuse cases, secure design principles and patterns, secure programming techniques, code reviews, and security testing. Students need to have a basic level of understanding of both software engineering and information security before taking this course.

1.1 Prerequisites

- **CSC 540**. Students should understand the software development lifecycle from requirements through maintenance.
- **CSC 582**. Students should have a basic understanding of common vulnerabilities in software, such as buffer overflows and SQL injection.

1.2 Student Learning Outcomes

After successfully completing this course, you should be able to

1. Describe changes that can be made to the software development lifecycle to improve security.
2. Collect, analyze, and visualize software project data.
3. Appraise the efficacy of secure development techniques using empirical evidence.
4. Develop and compare predictive models for software engineering projects.

2 WHAT CAN I EXPECT TO HAPPEN DURING CLASS?

In order to learn, you will need to be actively engaged with the course content. The schedule on the class home page on Canvas provides a summary of what you need to do to prepare for each class meeting. Before each class meeting, complete the readings listed in the Readings column of the class schedule for that meeting, and read and review the research paper listed in the Paper column. Reviews are due the night before class, and we will discuss the research paper during class.

Class meetings will be divided into multiple segments, including mini-lectures, small group activities, discussions, and hands-on activities. Hands-on activities will often involve data analysis or modeling. Students will work on these activities in small groups in Zoom breakout rooms, with partners and groups chosen randomly each time. We will begin working on hands-on activities during class times, but these activites may require time outside of class to complete. Hands-on activities build the skills you need to complete the semester long research project.

3 TECHNOLOGY USED IN THIS CLASS

As a virtual class, class meetings will be held using Zoom, with breakout rooms being used for small group activities. Students will need a webcam and microphone to participate in class meetings. During class meetings, students can ask questions using Zoom's chat function. While I do not have regular office hours for online classes, I will schedule Zoom sessions to review course materials and provide additional help and I am available for one-on-one meetings by appointment.

Each student will have their own virtual machine running Ubuntu Linux 18.04. R 4.0, RStudio, and a suite of R packages that we will use for data analysis, modeling, and visualization. All of the software packages we use for software metrics and analytics are installed on the VM. Many class activities will be submitted in the form of R Markdown notebooks created using RStudio.

Student virtual machines are accessed through the NKU College of Informatics vSphere system. vSphere is available through a web interface at `https://coivcenter.hh.nku.edu`. NKU's vSphere system can only be accessed while using NKU's Virtual Private Network (VPN). If you have already installed and configured the NKU VPN, you can use your current installation. If you have not installed NKU's VPN yet, go to `https://vpn.nku.edu` to download and install the VPN software.

As all of the software used in this class is open source, students may install the software on their own systems. However, the instructor can only provide help for using the software on the provided virtual machine.

4 Available Help and Support

I am available to help you with the class via e-mail, discussion forums, scheduled Zoom sessions, and appointments. I will respond to questions within one business day, unless an emergency arises. Please see the Communication Policy below for how to best get answers to your questions.

Cybersecurity content resources specific to this course can be found via the Resources page on the class web site, while cybersecurity resources for the university and local area can be found on the web site for NKU's http://cis.nku.edu/.

NKU's tutoring program and writing center are both available online at `https://inside.nku.edu/plus/tutoring/online.html`. Help and resources for NKU's learning management system are available from `https://inside.nku.edu/cite/technologyresources/Canvas_student.html`. The student technology guide, including support for student services, can be found at `https://inside.nku.edu/it/student-tech-guide.html`.

5 Research Project

Students will replicate and extend an existing software engineering study in a semester long research project. Students will need to read the original analyses, import and process replication data, replicate the original analysis and visualizations, and extend the paper in one or more ways, such as adding research questions, data sources, or new analysis techniques.

Students may choose any software engineering paper desired for replication, with the exception of literature reviews and papers already used in class. The instructor is the final arbiter of whether a paper chosen for replication is acceptable. If the selected paper is not deemed acceptable, students will have a week to find a different paper to replicate.

It is recommended that students choose a study to replicate for which data is already available. The class resources page lists dozens of places where software engineering data can be found. Data may be publicly available or may be obtained by writing one of the authors of the study. Note that in past classes, fewer than half of authors responded to requests for data.

The replication must use the same data source and answer the same research questions as the original study. Student results may not be identical to the results of the original study for a variety of reasons, including errors by the student or the original researchers, but also because of different versions of data collection and analysis tools, different implementations of modeling algorithms, and different random seeds. While student results are not required to be identical to those of the original study, the paper must include an explanation of why the results are different. Small differences can arise from small tool changes or different random seeds and require little explanation, but large differences of a standard deviation or more are more likely to result from student error and so require substantial investigation and explanation.

To extend the study, students may add an additional research question, use additional data (such as attempting to replicate the results of a study on newer versions of the studied application or different applications of the same class), or use additional modeling techniques (would a paper be improved by using a different machine learning algorithm or feature selection technique.) Students may want to examine the future work section of the paper for ideas on how to extend the paper. In the writeup of the project, the student must clearly distinguish between the replication and the extended features in both their paper and presentation.

The project may be completed individually or as a group of up to three students. Group projects must have *one extension per student in the group*. For example, a group of three students could add a research question, use additional data, and use additional modeling techniques. Extensions must be described in the project proposal and must be approved by the instructor.

There are five deliverables for the research project with the following due dates:

1. **Project proposal** is due March 2.
2. **Data analysis check-in** is due March 31.
3. **Research paper** is due April 27.
4. **Replication package** is due April 27.
5. **Presentation** slides are due April 27.

The project proposal is a one to two page document describing the paper chosen for replication, the data sources to be used, and the extensions planned for the student research project. The data analysis check-in is an in-class meeting with the instructor, in which students demonstrate that they have obtained and cleaned the data to be used and that they have a prototype of the data analysis process. The research paper is an 8-page report in IEEE conference paper format. It is accompanied by a replication package, which includes the data used to write the research paper along with all code used to analyze, model, and visualize the model. The presentation is a 20-minute in class presentation of the research project, given during the last class period on April 28 or during the final exam period on May 5.

6 Participation Policy

You are expected to be an active participant in class discussions and other in-class activities. To do this, you must prepare by completing the readings and other learning activities specified on the class schedule before coming to class. Class activities have been designed to help prepared students achieve the class learning outcomes. Missing class, not actively participating, and not being prepared will negatively affect your ability to learn course content.

7 Late Work Policy

All students are expected to complete learning tasks on schedule. It is important to stay on track with your assignments. This is an important skill in the workplace and will help you feel less stressed. Being able to meet deadlines and juggle many tasks are important career and life skills. Thus, you will need to complete all paper reviews, research project components, and activities according to the class schedule. However, I recognize that personal circumstances may at times make it difficult or impossible to complete a learning task on schedule. If you have a personal situation that prevents you from completing a task on time, you will need to discuss this with me prior to the due date if possible, or as soon as it becomes possible, so that we can develop a plan. Extensions are at my discretion. If an extension is provided, it is important to know that the format or content of an assignment may be modified.

8 Grading

Your grade in this course will be based on the following classes of assessments, each of which counts for the specified percentage of your semester grade. There are no exams, and the majority of your grade will be determined by your final project.

Paper Reviews (16%) Students will review one paper from the secure software engineering literature each week during the first part of the semester, for a total of eight paper reviews. The review should be approximately one page in length and must follow a format specified by the instructor on the class web site. Reviews are due on the day before the class during which we will discuss the paper. Students will be expected to use their review as a reference during class discussions. During the first week of class, we will read a paper during class and discuss how to review papers. Paper reviews are not accepted late unless a prior arrangement is made with the instructor.

Activities (14%) During each class, hands-on activities will help you understand the practical aspects of security engineering. Activities include both data analysis and software engineering exercises, some of which will be completed in small groups. Some activities will be completed during class, while others will require time outside of class to complete. Activities will be graded on effort rather than correctness, and each week's activities are worth approximately 1% of your semester grade. There will be no hands-on activities during presentation days, so there are 14 activities that will be graded in total.

Research Project (70%) The semester long research project described above is worth 70% of your semester grade. This grade is based on five deliverables, each of which counts for the specified percentage of your semester grade below.

1. **Project proposal** (2%)
2. **Data analysis check-in** (3%)
3. **Research paper** (35%)
4. **Replication package** (15%)
5. **Presentation** (15%)

Your letter grade in this course will be computed using the table below.

Graduate Students			
Grade	**Percent**	**Grade**	**Percent**
A	93-100	C+	77-80
A-	90-93	C	73-77
B+	87-90	F	0-73
B	83-87		
B-	80-83		

9 Communication Policy

I'm here to help you learn, and I have a few communication guidelines to make the course run as smoothly as possible. Questions about course content or technology should be asked in the General Questions & Answers forum, so that other students can provide and benefit from posted answers. Personal matters should be discussed with me by contacting my NKU e-mail address. We can either address the issue by e-mail or by scheduling a Zoom meeting.

When asking questions on a discussion forum or by e-mail, be sure to include:

- A subject that provides a summary of your question. Include the class number at the beginning of the subject for e-mail messages.
- A detailed description of the problem. Specify precisely on which assignment, virtual machine, user account, and software the problem occurred and provide a detailed list of steps needed to reproduce the problem. Include the full text of any error messages.
- The message should close with your full name.

I will answer forum questions within one business day unless a student has already provided a correct answers. I will respond to e-mail messages within one business day except in the event of an emergency. Note that I do not use the Canvas e-mail feature. E-mail always refers to my NKU e-mail address given at the top of this syllabus.

Students should check the class web site and NKU e-mail accounts for university-wide and class-specific announcements 24 hours before each class period.

10 Registrar Withdrawal Information

Students sometimes need to withdraw from a course for personal or academic reasons. If you do encounter difficulties with the course, please contact me prior to withdrawing. NKU's Spring 2021 Academic Calendar includes deadlines for withdrawing for a course.

11 Academic Integrity Policy

Academic integrity benefits everyone in our community. It not only helps you reach the real goal of this class–learning–but also allows for the university and degree program to be perceived positively by others, including your future colleagues and employers. When students are dishonest, they lose out on valuable learning that will help them perform well in their career. Academic dishonesty is any attempt by a student to gain academic advantage through dishonest means or to help another student in gaining an unfair advantage. Academic integrity is important whether the work is graded or ungraded, group or individual, written or oral.

The Student Honor Code is a commitment by students of Northern Kentucky University, through their matriculation or continued enrollment at the University, to adhere to the highest degree of ethical integrity in academic conduct. It is a commitment individually and collectively that the students of Northern Kentucky University will not lie, cheat, or plagiarize to gain an academic advantage over fellow students or avoid academic requirements.

Students, faculty, staff, and administrators at NKU strive to achieve the highest standards of scholarship and integrity. Any violation of the Student or Graduate Student Honor Codes is a potentially serious offense because it threatens the quality of scholarship and undermines the integrity of the community. All NKU faculty members are asked to report incidents of academic misconduct to the office of Student Conduct Rights and Advocacy. While academic in scope, a violation of the NKU Honor Code may be considered a violation of the NKU Code of Student Rights and Responsibilities and will follow the adjudication processes described therein.

Through the NKU Honor Code, students who are responsible for academic dishonesty may receive sanctions, including, but not limited to, a final grade of F, or removal from the course in which the violation occurs. Repeated violations of the NKU Honor Code, or when suspension or expulsion from NKU may be a possible outcome of the violation, the incident will be referred to the office of Student Conduct, Rights and Advocacy.

12 Credit Hour Policy

In accordance with federal policy, NKU defines a credit hour as the amount of work represented in the achievement of student learning outcomes (verified by evidence of student achievement) that reasonably approximates one hour (50 minutes) of classroom instruction and a minimum of two hours of out-of-class student work. For every course credit hour, a typical student should expect to spend at least three hours per week of concentrated attention on course-related work including, but not limited to, class meeting time, reading, reviewing, organizing notes, studying and completing assignments. At least an equivalent amount of time is expected for other academic activities such as online courses, laboratory work, internships, practica, studio work and other academic work leading to the award of credit hours.

Estimates of the time required for a typical student to complete course expectations are:

In-Class (1 day x 150 min x 15 weeks)	37.5 hours
Paper readings and reviews Class readings and quizzes (150 min x 15 weeks)	37.5 hours
TOTAL	145 hours

13 NKU Policies

13.1 Accomodations Due to Disability

The University is committed to making reasonable efforts to assist individuals with disabilities in their efforts to avail themselves of services and programs offered by the University. To this end, Northern Kentucky University will provide reasonable accommodations for persons with documented qualifying disabilities. If you have a disability and feel you need accommodations in this course, you must present me a letter from the Office for Student Accessibility (OSA, SU 303) indicating the existence of a disability and the suggested accommodations. More information on OSA can be found at https://inside.nku.edu/osa.html.

13.2 Changes in the Syllabus

The syllabus is a projection of what the instructor anticipates for the course. The instructor has the right to modify the syllabus in order to adjust to changing circumstances.

13.3 Other Information

For information on university-wide policies governing students, please see the University Common Syllabus on your course Canvas site.