CSC 682–Advanced Computer Security

Spring 2018
R 6:15-9:00

INSTRUCTOR INFORMATION

Name	James Walden
E-mail	*waldenj@nku.edu*
Office	GH 526
Phone	(859) 572-5571

Office Hours

MWR	2:00-3:00pm
T	2:30-3:00pm
T	4:30-5:00pm
also	by appt

SUMMARY

Description	:	A research-oriented seminar class focused on new and emerging areas in computer security. The goal of the class is to teach students how to read and analyze research papers in the field of cybersecurity, in order to enable them to advance their understanding to the current frontiers of the field. Topics may include but are not limited to the following areas: authentication and access control, cloud security, Internet of Things security, mobile security, network security, software security, and system security.
Prerequisites	:	CSC 582: Computer Security
Textbooks	:	None

STUDENT LEARNING OUTCOMES

By the end of the course, a successful student should be able to

1. Analyze and evaluate the quality of computer security papers.
2. Identify important techniques for solving computer security problems.
3. Evaluate proposed solutions to computer security problems.

CLASS STRUCTURE

Advanced Computer Security is a seminar style class, in which the participants collectively select current security topics that they wish to study. We will select and read two research papers each week. One student will be responsible for presenting each paper and leading the discussion in class. All students are required to read the papers and write a one page critical analysis of each paper. The analysis should include questions about the paper to be asked during the class discussion. Students must write their critiques independently, but it is likely that many students will have similar questions about the paper. There is no textbook for the

class. All readings come from the selected papers.

During the first week, we will discuss how to select topics, how to identify relevant materials on those topics, how to evaluate the materials we read or watch, and discuss the selection of discussion leaders. Each student will have a chance to serve as discussion leader multiple times. As the class meets once a week for three hours, there will be multiple discussion sessions in each meeting, usually on related topics.

Discussion leaders will be responsible for preparing to lead a one hour discussion, including checking references and reading related materials beyond the paper or other resource under discussion. Resources for discussion can include conference presentations, videos, and industry white papers in addition to academic papers. Discussion leaders are responsible for giving a 10-minute presentation on the paper and preparing a set of at least 10 questions for generating discussion. A copy of the presentation and the questions must be submitted to the instructor by the end of class. Presentations will be posted to the class web site after the discussion.

Topics can be chosen from any area of information and computer security, including but not limited to:

1. Cloud security
2. Contemporary cryptography
3. Defensive techniques
4. Electronic crime
5. Forensics
6. Hacking techniques
7. HTML5 security
8. Internet of Things security
9. Machine learning and security
10. Malware analysis
11. Privacy and anonymity
12. Ransomware
13. Secure software engineering
14. Security visualization
15. Social attacks and defenses
16. Steganography
17. Voting security
18. Web security

Class participation is essential in a seminar class. To help prepare for the discussion, students will write a short (approximately one page single spaced) review for each paper and bring it to class, where it can serve as notes for discussion and which must be submitted as hardcopy to the instructor at the end of the class period. The review consists of two parts. The first part is a critical response that must answer the following questions.

1. What problem does this work attempt to solve? What are the research questions?
2. What solution(s) does the work propose for the problem?
3. How does the work evaluate the proposed solution(s)? Is the evidence for the solution convincing?
4. What are the most important novel contributions described in the paper?
5. What modification would most significantly improve the research?

The instructor may add additional questions specific to individual papers when certain features of the papers need emphasis. Critical responses must be written in third person with well structured paragraphs and cor-

rect grammar and spelling, while avoiding excessive quoting or plagiarism. Critical responses must not be outlines, lists, or be formatted in question and answer style.

After the critical response, the second part of the review is a list of *a*t least 5 questions that can be asked during the class discussion.

Each student is responsible for asking or answering at least one question during the class discussion period. These questions may be from the list of questions in the review or may be original questions inspired by the class discussion. Students must add notes (handwritten is fine) to their reviews to indicate how they participated in the class discussion.

GRADING

Your grade in this course will be based on your analysis and discussion of selected research papers along with a term paper. The term paper may be a research paper or a systematic literature review of a particular area in the field of computer security. Research papers should be 8-12 pages single spaced, while systematic literature reviews should be 15-25 pages in length.

class participation	10%
paper responses	20%
discussion leadership	20%
term paper	40%
presentation	10%

Grade	Percent	Grade	Percent
A	93-100	C+	77-80
A-	90-93	C	73-77
B+	87-90	C-	70-73
B	83-87	F	0-70
B-	80-83		

You may miss one class period without receiving any penalty to your class participation grade.

While students may choose their own term paper topics, topics must be approved by the instructor. Term papers will be presented to the class during the last two weeks of the semester (including finals week).

COURSE CALENDAR

See the course web site, http://faculty.cs.nku.edu/~waldenj/classes/2018/spring/csc682/ for a current course schedule that will show which topics have been selected by the participants and who is responsible for each topic.

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 days x 150 min x 15 weeks)	37.5 hours
Reading papers (3 hours x 15 weeks)	45 hours
Term paper	45 hours
Presentation	10 hours
TOTAL	137.5 hours

STUDENTS WITH DISABILITIES

Students with disabilities who require accomodations (Academic adjustments, auxiliary aids or services) for this course must register with the Disability Services Office. Please contact the Disability Service Office immediately in the University Center, Suite 320 or visit the website at http://disability.nku.edu/ for more information. Verification of your disability is required in the Disability Services Office for you to receive reasonable academic accomodations.

HONOR CODE

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.

The purpose of the Honor Code is to establish standards of academic conduct for students at Northern Kentucky University and to provide a procedure that offers basic assurances of fundamental fairness to any person accused of violations of these rules. Each Northern Kentucky University student is bound by the provisions of the Honor Code and is presumed to be familiar with all of its provisions. Students also should aspire to conduct themselves in a manner that is consistent with the highest degree of ethical integrity in all matters, whether covered in the Honor Code or not. The success of this commitment begins in the diligence with which students uphold the letter and the spirit of the Honor Code. Students may view the complete honor code at http://deanofstudents.nku.edu/policies/student-rights.html#policies.

STUDENT EVALUATIONS

Northern Kentucky University takes Instructor and Course Evaluations very seriously as an important means of gathering information for the enhancement of learning opportunities for its students. It is an important

responsibility of NKU students as citizens of the University to participate in the instructor and course evaluation process. During the two weeks prior to the end of each semester's classes, you will be asked to reflect upon what you have learned in this course, the extent to which you have invested the necessary effort to maximize your learning, and the role your instructor has played in the learning process. It is very important that you complete the online evaluations with thoughtfully written comments.

Student evaluations of courses and instructors are regarded as strictly confidential. They are not available to the instructor until after final grades are submitted, and extensive precautions are taken to prevent your comments from being identified as coming from you. Students who complete an evaluation for a particular course (or opt out of doing so in the evaluation) will be rewarded for their participation by having access to their course grade as soon as that grade is submitted by the instructor. On the other hand, any student who does not complete the course evaluation (or opt out of doing so in the evaluation) should expect to incur a two week delay in access to his or her course grade beyond the university's official date for grade availability. To complete online evaluations go to http://eval.nku.edu/. Click on "student login" and use the same username and password as used on campus.

In addition, you should be aware that:

- Evaluations can effect change in courses. Evaluations without comments are less valuable and less credible than those filled out thoughtfully. Comments that are expressed well are more effective than those that are not.
- Positive feedback is just as important as criticism. Moreover, negative evaluations without any explanation and specifics are not especially useful.
- Once grades are submitted, all evaluations are read not only by the instructor, but also by the instructors department chairperson.
- Evaluations not only provide feedback to your instructor, but also provide information to the department chair for use in performance evaluations. This information affects reappointments, promotions, salaries, and teaching assignments.

The instructor reserves the right to alter this syllabus if he deems it to be necessary.