CptS 428/528: Advanced Cyber Security

Fall 2022

Course credits: 3
Meeting time: Tuesday, Thursday, 1:30 pm – 2:45 pm, August 22 – December 09
Location: Carpenter 101
Course webpage: http://www.eecs.wsu.edu/~hcai/cpts4528

Instructor: Haipeng Cai
Office locations:
- Physical - EME B47
- Online - Zoom (id: 427 060 7346 or https://wsu.zoom.us/my/hcaiwsu)

Email: haipeng.cai@wsu.edu Phone: 509-335-7114
Office hours: Tuesday, Thursday, 10:00 am – 11:00 am, or by appointments

---

Course Description

Cyber security concerns the systematic process of protecting systems, networks, and software from cyber threats and attacks which may compromise their security properties including confidentiality, integrity, or availability. The core of this subject lies in the concepts and principles as well as methodologies and techniques for achieving those security properties for computer systems, networks, and software. The state of the art and practice of cyber security defenses, including practical defense tools, will also be covered in this course. This is an advanced version in our cyber security course series. Of particular importance, learning of the cyber security principles from this course will be complemented and enhanced by applying the principles to cyber security practice through diverse course projects and managed team collaborations.

Course Content Overview

This advanced course on cyber security addresses key aspects of cyber security with an emphasis on software and systems security. Accordingly, the core content includes concepts, principles, methodologies, and techniques on measuring and defending the various security properties of both the operating systems and application software. The technical approaches will cover source code analysis, binary analysis, dynamic random testing (fuzzing), and reverse engineering techniques, as applied in the context of vulnerability discovery, malware analysis, risk mitigation, and digital forensics. The central focus is on how to systematically assess, prevent, and contain security risks, threats, and attacks at all levels of the computer system (from architecture all the way up to application code).

Specifically, the key topics to be covered include the following:

- Operating system security (architectures, mechanisms, hardening)
- Distributed & fault tolerant systems security (transactions, communication, scalability)
- Forensics and anti-forensics (OS, wireless, memory, network, IoT, cloud)
- Machine learning systems security (adversarial robustness, transferability, poisoning)
- Reverse engineering (embedded systems, SCADA/ICS, malware analysis)
- Binary analysis (kernel, firmware, polymorphism, symbolic differencing)
- Source code analysis (source, static, dynamic, testing, malware, exploits)
- Vulnerability discovery (fuzzing, crash dumps, side channels, equities, mitigations)

In particular, the first four focus on concepts and principles of key facets of the cyber security landscape, while the last four focus on practical techniques and tools for assuring cyber security.

Student Learning Objectives (SLOs)

Students will gain knowledge and expertise on the core content of this course, which are to be embodied through their ability to define appropriate, specific security goals and develop actionable plans to realize the goals. Students will learn techniques that enable and empower software and systems security measurement, diagnoses, and improvement. In addition, students will also sharpen valuable skills necessary for cyber security defense practices, including the use of modern cyber security tools, collaborating in a security defense team, and technical communication and peer evaluation. Students will participate in a semester-long group project to gain hands-on experiences applying the principles and techniques learned.

Specifically, this course will help students acquire the ability to (with associated unified EECS SLOs and performance indicators in parentheses):

1. Describe cyber security practice using correct technical terms along with concrete examples (1b, 1c, 2c, 2d).
2. Interpret key concepts and terminologies in cyber security defense and attacks, and differentiate among similar ones (1b, 1c, 2c, 3a, 3c).
3. Identify countermeasures against common cyber security risks, threats, and attacks (1a, 1d, 1e, 2a, 2b, 2e, 2f, 3a, 3b).
4. Employ mitigating strategies and relevant tools to detect, assess, and diagnose cyber security breaches (2g, 3c, 3e, 6a, 6b, 6c, 6d).
5. Explain the criticality and challenges in systematic assurance of cyber security, especially software/system security across the full stack (4a, 4b, 4c, 4d, 4f).

6. Combine different techniques and tools to systematically evaluate and counteract common types of cyber security threats (6a, 6b, 7a, 7b, 7c, 7d, 7e, 7f, 7g).
7. Describe the strengths and limitations of existing cyber security strategies, as well as future cyber security needs with respect to cyber space dynamics (6c, 6d).

Prerequisites

Students taking this course are expected to have taken undergraduate/introductory courses on cyber/computer/software security (e.g.,*CptS 327 Introduction to Cyber Security*) that cover the general and basic security concepts. Students should also have gained a solid background in data structures and programming (C/C++, C#, or Java) through relevant courses to prepare them for realizing implementation and testing tasks.

Textbook Required

- No textbook is required; the lectures serve as the textbook

Suggested Books/Readings

- Mitnick, Kevin. *The art of invisibility: The world's most famous hacker teaches you how to be safe in the age of big brother and big data*. Little, Brown, ISBN: 9780316380492. 2017.
- Hubbard, Douglas W., and Richard Seiersen. *How to measure anything in cybersecurity risk*. Wiley, ISBN: 9781119085294. (2016).

Topics Outline and *Tentative* Lecture Schedule

Week	Lecture no.: Topics
1	1: Course logistics, project description, and content overview 2: security landscape across the full stack: arch, OS, runtime, user code
2	1: OS security - architecture-level side channels, kernel vulnerabilities 2: OS security - authentication and access control in Windows/Linux
3	1: OS security - logging, monitoring, auditing 2: OS security - hardening, firewalls
4	1: system-level security: intrusion detection, distributed info flow control 2: system-level security: denial of service (DoS), distributed DoS (DDoS)
5	1: system-level security: distributed fault tolerance 2: machine learning (ML) security: attacks (poisoning, backdooring)
6	1: machine learning (ML) security: defenses (adversarial robustness) 2: cyber forensics: database, memory, network, emails

7	1: cyber forensics: anti-forensics and mitigations *2: Midterm exam: 10/4, Tuesday (1:30 - 2:45 pm)*
8	1: reverse engineering: decompilation, specification recovery 2: reverse engineering: static/dynamic instrumentation
9	1: reverse engineering: application in malware analysis 2: binary analysis: disassembly, binary rewriting
10	1: binary analysis: model (e.g., call graph, CFG) construction 2: binary analysis: application in threat assessment
11	1: source code analysis: static analysis 2: source code analysis: testing, test generation
12	1: source code analysis: symbolic execution 2: source code analysis: taint analysis
13	1: vulnerability discovery: common vulnerabilities and exploits 2: vulnerability discovery: with random testing
14	Thanksgiving vacation
15	1: vulnerability discovery: with greybox fuzzing 2: vulnerability discovery: with symbolic execution
16	*Final review* *Project presentations*
17	*Final exam: 12/14, Wednesday (4:30 - 6:30 pm)*

Grading

The final course grade will be calculated using the following breakdown and be converted from numeric numbers to letter grades using the scale mapping as follows.

Breakdown *Scale mapping*

Coursework	Weights		Score	*Grade*	Score	*Grade*	Score	*Grade*
Participation	5%		>=93	*A*	[80,83)	*B-*	[66,70)	*D+*
Project	60%		[90,93)	*A-*	[77,80)	*C+*	[60,66)	*D*
Midterm exam	15%		[87,90)	*B+*	[73,77)	*C*	<60	*F*
Final exam	20%		[83,87)	*B*	[70,73)	*C-*		

Course Project

A key component of the coursework is a semester-long group project. The progress of this group project will be measured by deliverables. The objectives, requirements, and due date of each deliverable will be communicated well prior to the due date such that each group will have reasonably enough time to complete the tasks required for the deliverable. For each deliverable, each group will be required to submit a written report and/or code (along with test cases) to demonstrate the progress of the group. Each member of the group will initially receive the same credit based on the quality and timeliness of group submissions, and will be later adjusted according to in-group peer evaluation by the end of the project period. A list of sample project topics along with the concrete details on the deliverables will be given in a separate document (e.g., *project description*). Students are encouraged to choose different topics of their own, but should be approved by the instruction before starting the project.

Unless specified otherwise, each project deliverable shall be created and submitted electronically *as a single PDF* on Canvas prior to the deadline which is 11:59 pm of the posted due date. Any late submission will receive a zero if no notice is sent to the instructor about the expected delay ***prior to*** the deadline; if a notice is sent to the instructor prior to the deadline, then the penalty of the late submission is a flat *10% point deduction* for every day after the original due date until the submission is received or the point left becomes zero. Note that by the end of the semester, missing any project deliverable will lead to *an "I" (incomplete) grade* except for extenuating cases communicated to the instructor in advance -- the *I* grade for a student means the student does not complete the course. Students missing an exam by the end of the semester will also receive an 'I' grade for this course.

Expectations for 428 versus 528 students

This is a conjoined course for both undergraduate (428) and graduate (528) students. Coursework and learning objectives are common between these two student groups except for the following (mainly, the additional work 528 students are expected of):

- SLOs 6 and 7 are expected from 528 students but not from 428 students
- Topics on ML security and binary analysis mainly target 528 students
- 428 students are not expected to take on complex systems security topics for course projects like MLAdversary, which 528 students are expected to take
- 528 students are expected to give a technical presentation in addition to live demo during project reporting, while 428 students are not
- 428 students may work in groups of 4-6 members while 528 student groups should typically not be larger than 4 members in size

Communication

We will communicate announcements, assignments, lecture materials and other learning resources all on Canvas. In particular, we will host off-class Q&A through the *Discussion Board* on *Canvas*. Canvas is also the portal to be used for project deliverables submission and grading. For questions on course materials, lectures, and course project milestones, contact the instructor on the Discussion Board by sending posts instead of by emails, so as to facilitate communication. You have options for sending *private (anonymous)* posts. Make sure you **subscribe to each** of the forums there so that you won't be missing important information about the course logistics and extended lecture discussions initiated by questions raised by other students.

Participation

Class attendance is required at all lectures. Although lecture slides and other supplementary learning materials will be posted online, these materials as well as the suggested reading materials are only used as references by the instructor in developing the lectures. Thus, studying these materials serves the purpose of getting better prepared for attending in-class lectures, but would by no means substitute for class attendance. Also, the course project requires each team member to be responsible and collaborative as well as to contribute equally; thus, missing lectures without justifiable reasons and then relying on other team members to catch up missed topics is not acceptable. You are also expected to participate in class discussions, which aids learning and provides valuable feedback on the lecture. If you know you will miss a lecture for a justifiable reason such as a university activity or a medical appointment, notify the instructor by email at least 12 hours before the lecture. While attendance will not be taken in every class, it will be sampled randomly at the discretion of the instructor. The basic participation credit that accounts for 5% of the final grade will be calculated using the sampled attendance records (in addition to active participation in classroom discussion).

In addition, students are expected to maintain a professional and respectful classroom environment, for which students are suggested to:

- silence personal electronics (non-disruptive ones may be used during class)
- arrive on time and attend the entire class session

Late Submission Policy

Late penalty is a flat 10% deduction per day. Late assignments may be turned up to one week after the original due date. An advanced notice must be given to the instructor via email at least 24 hours before the deadline for a late submission. The instructor may allow for late submissions without penalty if extenuating cases are explained in the notice email sent to the instructor.

Expected Effort
Beyond the time for lecture attendance, students in this class are expected to invest a minimum of 1-2 hours outside class for each lecture equivalent (or 2-4 hours per week), including the time for working on the course project.

COVID-19 Policy
During the Covid-19 pandemic, necessary accommodations will be offered as well on a case-by-case basis according to the specific personal requests from students and the world/nation/state-wide pandemic development and orders. All current COVID-19 related university policies and public health directives are located at https://wsu.edu/covid-19/.

Academic Integrity / Honor Code
Academic integrity is the cornerstone of higher education. As such, all members of the university community share responsibility for maintaining and promoting the principles of integrity in all activities, including academic integrity and honest scholarship. Academic integrity will be strongly enforced in this course. Students who violate WSU's Academic Integrity Policy (identified in Washington Administrative Code (WAC) 504-26-010(4) will receive a *fail* grade for the course, will not have the option to withdraw from the course pending an appeal, and will be reported to the Center for Community Standards.

Cheating includes, but is not limited to, plagiarism and unauthorized collaboration as defined in the Standards of Conduct for Students, WAC 504-26-010(3). You need to read and understand all of the definitions of cheating. If you have any questions about what is and is not allowed in this course, you should ask course instructors before proceeding. If you wish to appeal a faculty member's decision relating to academic integrity, please use the form available at communitystandards.wsu.edu. Make sure you submit your appeal within 21 calendar days of the faculty member's decision.

In particular, the fundamental requirement for all student work in this class is: Unless otherwise explicitly permitted by the instructor, all work you turn in must be your own. It is dishonest not only to copy another student's work, but to permit another student to copy yours. Nevertheless, realizing that students can assist each other in understanding general course material, there are limited ways in which student collaboration is permitted:

1) You may communicate verbally with another student, as long as you do not communicate the answer or the content of what you are going to turn in, whether it be code or text. A good way to work in this regard is for the student providing help to ask guiding questions of the student needing help, letting them arrive at the answer themselves.

2) You may draw diagrams and such on a whiteboard, chalkboard, or piece of blank paper to illustrate the verbal points made in 1), as long as you do not write what you are going to turn in.

It will be up to the discretion of the grader (if applicable) and instructor to determine if any assignment shows evidence of collaboration beyond these limits. Any attempt to circumvent the spirit of these rules will be treated as a violation of the fundamental requirement. If you are in doubt, do not give help to or request it from another student: That's what office hours are set for. Information on WSU Academic Integrity can be found at www.academicintegrity.wsu.edu/ and conduct.wsu.edu/, and the WSU Honor code is on https://provost.wsu.edu/tag/wsu-honor-code/. Please also read the EECS Academic Integrity Policy carefully. Use these resources to ensure that you do not inadvertently violate WSU's standard of conduct.

Students with Disabilities

Reasonable accommodations are available for students with documented disabilities or chronic medical or psychological conditions. If you have a disability and need accommodations to fully participate in this class, please visit your campus' Access Center/Services website to follow published procedures to request accommodations. Students may also contact their campus offices to schedule an appointment with a Disability Specialist. All disability related accommodations are to be approved through the Access Center/Services on your campus. It is a university expectation that students visit with instructors (via email, Zoom, or in person) to discuss logistics within two weeks after they have officially requested their accommodations.

For more information contact a Disability Specialist on your home campus:

- Pullman, WSU Global Campus, Everett, Bremerton, and Puyallup: 509-335-3417 Access Center (https://www.accesscenter.wsu.edu) or email at access.center@wsu.edu
- Spokane: 509-358-7816 Access Services (https://spokane.wsu.edu/studentaffairs/access-resources/) or email j.schneider@wsu.edu
- Tri-Cities: Access Services (http://www.tricity.wsu.edu/disability/) or email g.hormel@wsu.edu
- Vancouver: 360-546-9238 Access Center (https://studentaffairs.vancouver.wsu.edu/student-wellness-center/access-center) or email van.access.center@wsu.edu

Accommodation for Religious Observances or Activities

Washington State University reasonably accommodates absences allowing for students to take holidays for reasons of faith or conscience or organized activities conducted under the auspices of a religious denomination, church, or religious organization. Reasonable accommodation requires the student to coordinate with the instructor on scheduling examinations or other activities necessary for course completion. Students requesting accommodation must provide written notification within the first two weeks of the beginning of the course and include specific dates for absences. Approved accommodations for absences will not adversely impact student grades. Absence from classes or examinations for religious reasons does not relieve students from responsibility for any part of the course work required during the period of absence. Students who feel they have been treated unfairly in terms of this accommodation may refer to Academic Regulation 104 – Academic Complaint Procedures.

Safety and Emergency Information

The Campus Safety Plan (http://safetyplan.wsu.edu) contains a comprehensive listing of university policies, procedures, statistics, and information relating to campus safety. The University emergency management website (http://oem.wsu.edu/) provides campus safety and emergency information. The emergency alternative site (http://alert.wsu.edu) provides information about emergencies and communication resources WSU will use to provide warning and notification during emergencies.

Classroom safety is also of paramount importance at Washington State University, and is the shared responsibility of the entire campus population. WSU urges students to follow the "Alert, Assess, Act" protocol for all types of emergencies and the "Run, Hide, Fight" response for an active shooter incident. Remain ALERT (through direct observation or emergency notification), ASSESS your specific situation, and act in the most appropriate way to assure your own safety (and the safety of others if you are able). Please sign up for emergency alerts on your account at MyWSU.