Com Sci CS M138 - Multiple-Cross Listed Course Proposal Syllabus

Course number: ECE 117 – cross listed with **Com Sci as CS M138**
Course Catalog Title: Computer System Security
Short Title: Computer System Security
Units: 4
Grading basis: Letter
Format:
4 hours lecture and other contact-activity
8 hours self-study

Requisites: Prerequisites for this class include CS33, recommended: CS111.
In addition, students should feel comfortable programming in a desktop environment such as Java, C, and Python.

Description:
Computing systems are advancing and providing exceptional benefits to society. However, the more society relies on computing systems, the greater the potential disruption and destruction that adversaries can create via malicious cyber activities. Thus, security is critical for computing systems. Are you interested in working on cutting-edge security research? Are you interested in how security practitioners protect systems against millions of attacks daily? This course will introduce students to the fundamental knowledge of computer system security. The goal of the course is to: (1) understand the exploit techniques, (2) learn to use the security tools, (3) learn to design and implement secure systems. Students will learn the concepts of computer security, including software vulnerability analysis and defense, web security, mobile security, and network security. In addition, the course will cover the latest security topics in practice (e.g., cryptocurrency), and in research (e.g., state-of-the-art fuzzing techniques and machine-learning-based security analysis). Students will also get hands-on experience in analyzing and designing secure systems. In addition, this course will include a course project for cutting-edge security research.

Learning Objectives/Competencies for Computer System Security Class

Knowledge outcomes:
Students will learn the core concepts in software vulnerabilities analysis and defenses, web security vulnerabilities and defenses, mobile security and privacy, network security and privacy, as well as emerging topics in computer security. The students will also learn security principles and threat modeling so that they will be able to use them in different kinds of cybersecurity problems.

Skills outcomes:

- Understanding Exploit Techniques: Students will gain knowledge and skills in understanding various exploit techniques used by adversaries to compromise computer systems.
- Using Security Tools: Students will learn how to use a variety of security tools and software to assess and enhance the security of computer systems.
- Designing and Implementing Secure Systems: Students will develop the ability to design and implement secure computer systems, considering best practices and security principles.
- Effective Communication: Students will effectively communicate security concepts, findings, and recommendations both in writing and verbally, demonstrating their ability to convey complex technical information to various audiences.
- Responsible Collaboration: Students will collaborate with peers on security projects, fostering teamwork and shared responsibility for security outcomes.

Attitudes and Values outcomes:

- Ethical Awareness: Students will develop a strong sense of ethical principles and values related to computer security, emphasizing the importance of responsible and lawful behavior in the field.
- Commitment to Security: Students will develop a commitment to ensuring the security and integrity of computing systema and recognize the broader societall implications of their work.

Behavioral Outcomes:

- Application of Knowledge and Skills: Students will apply their knowledge and skills in real-world scenarios, demonstrating their ability to assess, enhance, and maintain the security of computing systems.
- Participation in Research: Through the course project on cutting-edge security research, students will contribute to the field by addressing relevant security issues and advancing knowledge in the domain.
- Continuous Learning: Students will recognize the need for ongoing learning and adaptation in the ever-evolving field of computer security, showing a commitment to staying current with the latest developments and threats.

Justification for cross-listing with Computer Science:
This class should be cross-listed with computer science because it provides essential knowledge and skills for students in the rapidly advancing field of computing systems. When the class was offered last year, 50% of the students are from the computer science major. The course evaluations from the students are also very positive. Cross-listing the class will make it easier for more computer science students to take and benefit from the class. As society increasingly relies on computing systems, the threat of cyberattacks becomes more significant, making security critical in system design. This course offers students an opportunity to gain a comprehensive understanding of the basic concepts of computer security, including vulnerability analysis and defense, web, mobile, and network security. It also covers the latest security topics such as

cryptocurrency and machine-learning-based security analysis, ensuring that students are up-to-date on the most recent trends in the field. Furthermore, the course provides hands-on experience in analyzing and designing secure systems, which is crucial in preparing students for future employment in the field. Graduates with knowledge of computer system security are highly sought after in today's job market. Offering this course to computer science students ensures they are well-prepared for careers in the cybersecurity industry, which is expected to continue growing. Next, the course project offers students an opportunity to engage in cutting-edge security research, which is an essential aspect of the field and help to promote

interests in research. Thus, the course's content and approach justify to cross-list it with computer science, allowing students to gain the skills and knowledge necessary for success in the field of computer security.

Supplemental Information: please find the slides, course syllabus, assignments and handouts, course evaluations, and enrollment details in the folder.

Grading structure:
Homework assignments (30%)
Literature review (5%)
Participation in feedback to others' work (5%)
Course project (50%)

- Three presentations
    - Introduction Presentation (5%)
    - Midterm (5%)
    - Final (15% from Yuan's and peer's evaluation)
- Two reports
    - Midterm report (5%)
    - Final report (10%)
    - Quiz (10%)

Effective Date: Winter 2024
Fall/Winter/Spring: any
Overlap with existing classes:
The closest class is CS 136, which is offered by Peter Reiher. Peter and I looked at each other's syllabus last year and agrees that there is sufficient unique material in both classes to allow students to take both for credit. In particular, CS 136 covers more in crypto, malware, Intrusion Detection Systems, and privacy, while ECE 188 focuses more on system security, and include new topics such as mobile security, Cryptocurrency, IoT security, and machine learning security.

Instructors: Yuan Tian, Nader Sehatbakhsh

Offerings: Once a year