CS 499/579
EMPIRICAL COMPUTER SECURITY

Overview

Empirical security research seeks to understand how computer security concerns manifest in practice. For instance, in 2017 NIST (National Institute of Standards and Technology) reversed their password recommendations after empirical research showed that their requirements actually led to more easily guessable passwords! This course explores recent research developments in applied security research across a wide range of computer security areas: computer networks, the web, social engineering, misinformation, malware, botnets, usable security, and emerging applications such as Internet of Things, smart cars, etc. This also a project-based course that will concurrently introduce students to the basics of security research. The instructor will work with students to identify a research problem (e.g., identifying new threats, developing security defenses), design experiments, collect data, and communicate findings through writing and presentation. In addition to teaching modern computer security, this course aims to prepare students for successful research careers, either in graduate school or industry.

Course Info

Instructor: Zane Ma (zane.ma@oregonstate.edu)

Credits: 4

Prerequisites: CS 370 (Intro to Security) or CS 373 (Def. Against the Dark Arts).

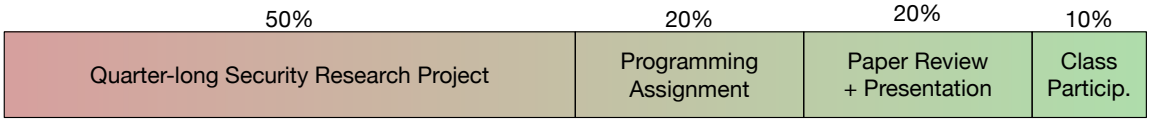
Exceptions may be permitted if you email the instructor.

Course materials: All materials will be provided electronically at no cost.

Syllabus

Week 1: Measurement 101 + Ethics
Week 2: Security 101
Week 3: Network Security + DNS
Week 4: Web: TLS + HTTPS
Week 5: User Auth + Usable Security
Week 6: Social Engineering + Misinformation
Week 7: IoT + Cyber-Physical Systems
Week 8: Malware + DDoS
Week 9: Underground Ecosystems
Week 10: Project Presentation

Grading



If you have any questions, please don't hesitate to reach out to zane.ma@oregonstate.edu!