EECS 349/444: Computer Security
Fall 2019 (CRN: 10737/4911) - Credit Hours: 3

Instructor: **Prof. Yanfang (Fanny) Ye**
Office: Olin-610
Email: yanfang.ye@case.edu
URL: http://community.wvu.edu/~yaye/

Class Meets: T/R 10:00-11:15pm, in Bingham-103

Office Hours: R 12:00-2:00pm, in Olin-610

Why this Course?

- ***Cybersecurity is a national priority and critical to the well-being of all organizations***: from both the public and private sectors are creating new cyber jobs and hiring thousands of cyber professionals to protect networks and information systems.
- With a growing cyber threat landscape and the ***demand of cybersecurity professionals*** is expected to rise to 6 million globally by 2019, which ***is far outstrips the supply***.

This course is intended for undergraduate seniors and graduate who are interested in the field of cybersecurity and intend to gain practical experiences to become cybersecurity professionals.

Course Pre or Co Requisites:

Assembly Language*; **C Programming Language***.

Recommended Preparation: EECS 132, EECS 281, EECS 293, EECS 325 and EECS 338.

Course Description:

Cybersecurity knowledge and practices on security risk management. Current security trends and industrial practices on cybersecurity. Experiments on ethical hacking and practice of cyber defense.

Course Overview:

Cyberattack has been one of the most severe security threats to the world which becomes more networked and relies more on a complex but fragile cyberspace. To combat both immediate and growing cyberattacks, businesses and governments are spending billions of dollars on cybersecurity. This course equips students with cybersecurity knowledge and practices on security risk management. Through this course, students will explore existing cybersecurity issues, learn how to assess security risks, and conduct experiments on ethical hacking. They will practice system attack and defense strategies using security tools, so as to gain practical experience to become a cybersecurity professional.

Expected Learning Outcomes:

Upon successful completion of this course, the student shall be able to:

- Describe a range of current problems and tensions in modern cybersecurity.
- Recognize the vulnerabilities and threats to cyber infrastructure and assess the security risks.
- Conduct reverse engineering and static/dynamic code analysis of malicious software.
- Apply typical techniques for malware detection.
- Conduct cybersecurity attack and defense strategies using security tools.
- Apply the principles of risk and conduct a risk management exercise.

Course Resources:

No textbook is required. Course lectures, notes and other materials will be found under the course materials section on CWRU SIS (canvas) system.

Course Topics (Tentative):

- Introduction of Cybersecurity
- Software Security: Attacks & Defenses
- Reverse Engineering and Malware Analysis
- Mobile Security: Attacks & Defenses
- Web Security: Attacks & Defenses
- Network Security: Attacks & Defenses
- Advanced Topics in Cybersecurity

Evaluation/Grading:

- **Homework (60%)** Homework assignments may be discussed with other students, but each student must complete by your own. Any submitted work that it copied from any source or too similar to be an independent write-up will not be given credit. ***Note that additional question(s) will be given for EECS 444 for the homework assignments***.

- **Group project (40%)** You will be assigned one group project. Project topics will be related to cybersecurity practices. You will be required to use cutting-edge techniques to solve the proposed security problems.
  - 4 students per group
  - Select a seed idea for your group project
  - Fully motivate the problem (5%)
  - Survey related work (10%)
  - Develop your own solutions – substantial novel technique development and implementation are expected (20%)
  - A thorough empirical evaluation and comparing with baseline methods (20%)
  - A fully developed project report (25%):
    EECS 349: 8 pages in ACM SIG Tighter Alternate style
    EECS 444: 12 pages in ACM SIG Tighter Alternate style
    https://www.acm.org/publications/proceedings-template
  - Project presentation (20%): 12min presentation + 3min Q/A

Course Grading Scale:

90-100% = A
80-89.9% = B
70-79.9% = C
60-69.9% = D
Below 59% = F

* Bonus credits can be given according to the class performances.
* '+' and '-' grade may be reported if the score is near boundary.

Late Assignments:

Any assignment not submitted by the due date/time will receive an automatic 20% grade deduction. Any late assignment not submitted (generally 2 days after the original due date) will not be accepted and the grade will remain a 0. Please contact the instructor BEFORE the due date if you need to discuss an exception to an assignment due date. Note that absolutely no late assignments will be accepted for the Final Project.

Attendance Policy:

Students are expected to attend and participate in class lectures and discussions, and should note that students will be responsible for course material and information that may be conveyed through lectures and class discussion whether or not that material or information is contained in handouts, instructor provided notes, or assigned or optional readings. Students should also note that a significant portion of the course content will be conveyed through class lectures, in-class activities and class discussions. Students should also note that a portion of the student's grade will be based on course participation: after three noted absences, students will lose two points per absence; after three noted late arrivals, students will lose one point per late arrival.

CWRU Academic Policies and Procedures:

- Undergraduate Academic Policies and Procedures:
  http://bulletin.case.edu/undergraduatestudies/policies/

- Graduate Studies Academic Policies:
  http://bulletin.case.edu/schoolofgraduatestudies/academicpolicies/