CMPSC 443 Introduction to Computer and Network Security (SP2016)
Lecture: M W 11:15 AM - 12:05 PM, Room: 107 Burke
Lab: R noon - 1:50 PM, Room: 147 Burke

Instructor: Dr. Zhifeng Xiao, Assistant Professor of CSSE
Contact: zux2@psu.edu, 814-898-6252, 157 Burke
Office Hours: 3:30 pm - 5 pm, Mon & Wed, and by appointment.
Prerequisites: Operating system, Computer networks.

Addressed ABET Computer Science Outcomes:

- (c) An ability to design, implement, and evaluate a computer-based system, process, component, or program to meet desired needs.
- (d) An ability to function effectively on teams to accomplish a common goal.
- (e) An understanding of professional, ethical, legal, security and social issues and responsibilities.
- (f) An ability to communicate effectively with a range of audiences.
- (g) An ability to analyze the local and global impact of computing on individuals, organizations, and society.
- (i) An ability to use current techniques, skills, and tools necessary for computing practice.

Course Overview: The course covers principles of computer systems and network security. We will discuss various attack techniques and how to defend against them. Topics include network attacks and defenses, software security, web security, malware, and applied cryptography, etc. Course projects will focus on building reliable code and understanding attacks.

Course Outline:

- Introduction and course overview: security requirements, attack models, etc.
- Cryptography: symmetric & public cryptography, pseudo-random number generator, message authentication code, hash function, digital signature.
- Software security: buffer overflow attack, return-to-lib, return-oriented programming; security testing; secure programming.
- Web application offense techniques: SQL injection, cross-site scripting (XSS), etc.; Session management and user authentication; Penetration testing.
- Network security: Network protocols and vulnerabilities; Network defense tools: Secure protocols, Firewalls, VPNs, Intrusion Detection; Botnet.
- Malware analysis.

Textbook Information This is NO required textbook for this course. A recommended reference: Michael Goodrich and Roberto Tamassia, "Introduction to Computer Security", ISBN-10: 0321512944 ISBN-13: 9780321512949, 2011 Addison-Wesley

Course Grade: Your grade will be based on the following distribution of points:

- Course project (40%)
- Labs (40%)
- Take-home final (10%)
- Attendance (10%)
- Bonus for CTF participation (2%)

Grading Scale:

Grade	A	A-	B+	B	B-	C+	C	D	F
Upper	100	92	89	86	82	79	76	69	59
Lower	93	90	87	83	80	77	70	60	0

Course Project

- The course project is a team work. Each team consists of 3 students.
- Each team needs to choose a project from a list of projects provided by the instructor. There is one chance to change projects within the first 4 weeks.
- Project timeline:
  - Team formation and Project selection ..... Jan 15
  - Presentation I ..... Feb 22 - Feb 26
    Each team does a 7-min presentation (3-min Q&A)
  - Midterm report submission ..... Mar 2
    Both midterm report and final report should follow the given template report_template.doc, which is available on Angel. Midterm report should be no less than **2000 words** in length. All writing should be in your own words; no copy-paste is allowed. If you cite other papers or resources, a reference is always required.
  - Presentation II ..... Apr 25 - Apr 29
    Each team does a 10-min presentation (3-min Q&A)
  - Project submission and warp up ..... May 4
    A team needs to submit the following material: 1) Slides for both presentations, 2) All source code, experiment data, figures, etc, 3) Midterm report (no less than **2000** words) and final report (no less than **4000** words).
- Project repository: we will be using Github for project management.
- Weekly updates - The instructor will hold a meeting for each team in the lab session. Every team member needs to report to the instructor by answering three questions:
  - What did you accomplish last week?
  - What is your current task?
  - What are you planning to do next week?

- Project grades: project selection (5%), weekly updates (15%), presentation I (20%), midterm report (20%), presentation II (20%), project package (20%)

Lab Policy:

- All labs are hands on experiments.
- Most labs are individual work.
- A lab is due within a week since it is given.
- A submission of a lab includes the following: 1) source code / script (if any), 2) a lab report.
- Late submissions incur a 10% penalty on the same day, 30% penalty on the second day, 50% penalty on the third day. Beyond that, no credit will be given.

Final Exam Policy:

- There is a take-home final exam.
- The exam is comprehensive.
- The instructor will distribute the final exam sometime in the final week via email. Students have 12 hours to complete the final.
- Late submissions incur a 10% penalty.

Attendance: Attending and participating in class are essential elements of the learning experience. Students are encouraged to participate in every class through taking notes, asking questions, and engaging in discussions. Regular attendance will be taken throughout the semester. Each absence incurs 1% of point loss. There will be NO unexcused absence.

Emails and Angel Access: The instructor may need to contact the entire class or an individual student via e-mail. The default email address for every student is the PSU account. If you do not use your PSU account, you need to forward the e-mail from this account to an address that you do check on a regular basis. All course material (syllabus, schedule, slides, solution to homework/exam, etc.) will be available on Angel. In addition, you will need to upload your programming homework via Angel. Details will be given in class.

Academic Integrity: Academic integrity is the pursuit of scholarly activity free from fraud and deception and is an educational objective of this institution. Academic dishonesty includes and is not limited to: cheating, copying the work of others, plagiarism, acts of aiding and abetting others, unauthorized possession of examinations, submitting previous work, tampering with work, ghosting or misrepresentation, altering examinations, and computer theft. Acts of academic dishonesty will initiate action according the University academic integrity processes.

Note to students with disabilities: Penn State welcomes students with disabilities into the University's educational programs. If you have a disability-related need for modifications or reasonable accommodations in this course, contact the Disability Specialist in the Office of Student Affairs, Room 115 Reed Union Building, 898-7101.

Electronic Devices: Out of respect for fellow students, please silence all electronic devices during class. Laptops are permitted, but they should be used for note taking purposes only.