CYBR 435: Cyber Risk, Spring 2022
Department of Computer Sciences and Electrical Engineering
Marshall University

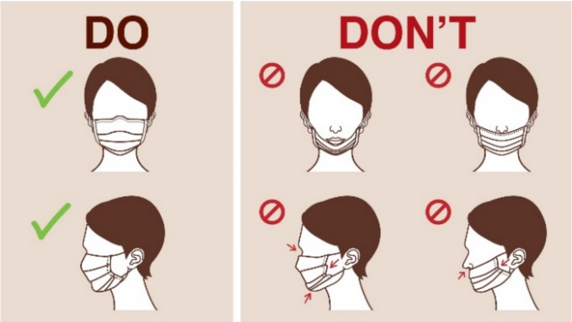
Course Information:

- Instructor: Dr. Cong Pu (Ph.D., Assistant Professor)
- Office: Weisberg Applied Engineering Complex (WAEC) 3109
- Office Phone: (304) 696-6204
- Email: puc@marshall.edu
- Course meetings: Tue/Thu, 2:00 p.m. – 3:15 p.m., WAEC 3245
- Virtual office hours:
  - Important: All office hours will be held virtually during the COVID-19 pandemic.
  - Tentative office hours:

    Tue, 7:00 a.m. – 11:30 a.m.
    Thu, 7:00 a.m. – 11:30 a.m., 3:30 p.m. – 4:30 p.m.
    Or by appointment through email.
  - Students are expected to communicate with instructor to set up video meetings via Microsoft Teams.
- Course web page: MU Online (Blackboard) http://www.marshall.edu/muonline/.
  - It is important to visit MU Online (Blackboard) regularly for up-to-date course information.

COVID-19 Related Information: From University

- Marshall's official COVID-19 protocols are online at https://www.marshall.edu/coronavirus . Policies and protocols may change over time as we respond to changing conditions. The website will always contain the most recent information.
- Key policies at the start of the Fall 2021 semester include the following:
  - **Masks are required for everyone in all public indoor spaces on university property, regardless of one's vaccination status.** These spaces include classrooms, labs, office suites, hallways, lobbies, stairwells, etc. Instructors may choose to teach either while wearing a mask or face shield or while standing behind the plexiglass barrier in the classroom.



  - **In order to remain in in-person classes, students must sign the Marshall Return to Campus Student Agreement** that outlines public health expectations and University COVID-19 policies: https://bit.ly/2VP3Naa.
  - **In order to remain in in-person classes for the Fall 2021 semester, students must submit their current vaccination status** in the online Student Vaccination Registry here: https://mubert.marshall.edu/vaccinerecord.php. The registry offers several possible responses, including an option to not disclose vaccination status.

    - **Students will disinfect their personal workspaces and virtual learning hubs with** disinfectant wipes provided nearby.
    - **Students who are unable to follow University requirements due to a disability** should seek reasonable accommodations from the Office of Disability Services (ODS) during the first week of class.

Course Description:

- This advanced course will expand the practical knowledge of cybersecurity technologies as applied to an industrial setting. The course covers the functions and purposes of the key elements used to analyze, create, secure, and protect an industrial cyber infrastructure from cyber threats. Students will familiarize themselves with the latest developments in cybersecurity, including practical guides to design, implementation, and testing industrial networks and applications to ensure their security and reliability in an industrial production environment. (From Catalog)
- The course is expected to follow National Security Telecommunications and Systems Security Instruction (NSTISSI) 4011 and 4013 standards. It will also help prepare students to obtain a variety of industry certifications, including the Computing Technology Industry Association's (CompTIA) A+, Network+ and Security+ certifications; Cisco's Certified Network Associate (CCNA) certification, and the Security Certified Network Professional certification.
- Prerequisite: CS 430
    - Students are expected to have a good knowledge in programming, data structures, discrete level mathematics background, networking and cybersecurity concepts.

By Enrolling In This Course, You Are Agreeing To The Following:

- In a nutshell, though, if you access any computer without its owner’s permission, and obtain any information from it or cause any damage (even accidentally), you have broken the law. See 18 U.S.C. § 1030, https://www.law.cornell.edu/uscode/text/18/1030
- Any material in this course contains topics that, outside the context of this course, may be considered unethical and even illegal if used an offensive or proactive manner. Although you reserve the right to employ the use of the techniques and tools you learn in this course to defend your own network(s), you agree and promise not to apply them in a fashion that may be perceived as being aggressive in any way nor to use them on any network(s) you do not own or maintain.
- you understand that you are personally responsible for any consequences that may occur as a result of the unauthorized use of the material you learn in this course. You will not hold Marshall University nor any of its staff/faculty/course instructor responsible if you are charged or convicted with any crime related to the material learned in this event. You acknowledge that you must be familiar with and fully abide by Marshall University Computing Services’ Acceptable Use Policy.

Course Student Learning Outcomes: The table below shows the following relationships: How each student learning outcomes will be practiced and accessed in the course.

Course Student Learning Outcomes	How students will practice each outcome in this course	How student achievement of each outcome will be assessed in this course
Design, develop and implement a secure Cyber-infrastructure and Security Operation Center.	• Lecture • Example discussion • In-class exercise	• Assignment • Project • Exam
Assess network defenses and computer system's security vulnerabilities and detect attempted security breaches using appropriate tools and resources.	• Lecture • Example discussion • In-class exercise	• Assignment • Project • Exam
Utilize security technologies such as firewalls, VPNs, virtualization, virus scanning, intrusion protection and patches to industrially harden a cyber-infrastructure.	• Lecture • Example discussion • In-class exercise	• Assignment • Project • Exam

Preferred Communication Method and Expected Response Time:

- You can always meet with instructor via Microsoft Teams during virtual office hours, no appointment is required.
- Outside virtual office hours, 6 hours advance notice is required when scheduling an appointment. If you ask instructor to meet you on Microsoft Teams immediately, the answer will probably be "No".
- You can generally expect an email response within 6 hours. If you do not get a response within 6 hours, please forward your previous email to instructor.
- You can generally expect the feedback on assignment and exam in one week after submission. If you do not receive the feedback in two weeks, please send an email to instructor.

Required Textbooks, Additional Reading, and Other Materials:

- Wenliang Du. Computer & Internet Security: A Hands-on Approach. 2nd Edition. ISBN-13: 978-1733003933, ISBN-10: 1733003932.

Course Requirements and Grading Policy:

- **1st Exam: 10%**, Feb 10 (Thursday), 2:00 p.m. – 3:15 p.m., MU Online (Blackboard), WAEC 3245
- **2nd Exam: 10%**, Mar 22 (Tuesday), 2:00 p.m. – 3:15 p.m., MU Online (Blackboard), WAEC 3245
- **3rd Exam: 10%**, Apr 28 (Thursday), 12:45 p.m. – 2:45 p.m., MU Online (Blackboard), WAEC 3245
  - All three (non-cumulative) exams are computer-based exams.
  - All three exams should be taken in the classroom (WAEC 3245). However, you can

start exam wherever you want during exam time and submit on Blackboard.
    - Open book and notes; Internet resources are allowed.
    - There will be NO make-up for missing exam. Only university excused absences with appropriate and official DOCUMENTATION will be accepted for make-up exam. Please contact Student Affairs (https://www.marshall.edu/student-affairs/) for university excused absence documentation first, and then schedule make-up exam with instructor.
        - The make-up exam must be taken within two days after the scheduled exam.
    - If you take a conflict exam, you must talk to instructor and provide a valid document at least two weeks before the scheduled exam.
        - The conflict exam must be taken within two days after the scheduled exam.
- **Assignment: 50%**
    - Assignment should be SUBMITTED on Blackboard before Due Date. *Other submission methods* (i.e., email) *will NOT be accepted.*
    - LATE Submission will NOT Be Accepted on Blackboard since the submission link will be closed automatically after due date.
    - There will be NO re-submission for missing assignment. Only university excused absences with appropriate and official DOCUMENTATION will be accepted for assignment re-submission*. Please contact Student Affairs (https://www.marshall.edu/student-affairs/) for university excused absence documentation first, and then contact instructor for re-submission.
        - *The re-submission will be provided *if and only if* the duration of university excused absences is ***equal to*** or ***longer than*** the half of the time limit on the assignment.
    - Each student has unlimited submission attempts on Blackboard before due date. However, instructor only grades the final submission attempt.
    - There will be NO re-submission if the student submitted the wrong assignment.
- **Team Project: 20%**
    - Each team comprises 2-3 students
        - Building a new secure system
        - Improving an existing security technique
    - Project Proposal (two-page): **5%**
        - Title and Authors
        - Problem Statement
            - Describe what the problem is and why it is important
        - Related Work
            - Present and analyze state-of-the-art solutions to the problem
        - Proposed New Solution
            - Describe the plan of your proposed approach and use diagrams and figures if necessary
        - Evaluation Plan
            - Describe your evaluation plan
                - Effectiveness and performance
                - What tools/benchmarks/attacks/experiments?
                - What deliverables?

        - Project proposal should follow IEEE publication format
            - https://www.ieee.org/conferences/publishing/templates.html
    - Project Report (eight-page): **10%**
        - Project report should contain the following sections:
            - Title and Authors
            - Abstract
            - Introduction
            - Related Work
            - Background
            - System Architecture/System Design/Technical Approach
            - Implementation
            - Evaluation Results
            - Discussion (e.g., design features, limitation, improvement)
            - Conclusion
            - References
        - Project report should follow IEEE publication format
            - https://www.ieee.org/conferences/publishing/templates.html
    - Project Presentation: **5%**
        - Each team is expected to present and demonstrate the project at the end of semester.
    - Project should be SUBMITTED on Blackboard before Due Date. *Other submission methods* (i.e., email) *will NOT be accepted.*
    - LATE Submission will NOT Be Accepted on Blackboard since the submission link will be closed automatically after due date.
- Plagiarism:
    - Plagiarism or cheating will not be tolerated in the class.
        - 1st plagiarism will result in zero point in the suspected work.
        - 2nd plagiarism will result in immediate dismissal (F grade).
- All grades will be posted on Blackboard:
    - *You are highly suggested to check your grade on Blackboard frequently and notify instructor immediately if there is any grading error*.
    - Mid-term grade will be posted around March 21 (Monday)
        - March 25 (Friday), last day to drop an individual course.
        - Spring 2022 calendar: https://www.marshall.edu/academic-calendar/spring-2022-semester/
- Grade Scale:
    - Actual points received in each category should be converted into category percentage.
    - For example, if you got 40/50 for 5 assignments, the percentage of assignment category will be (40 / 50) * 40 = 32 (%).
    - A (100 - 90), B (89 - 80), C (79 - 70), D (69 - 60), and F (59 - 0)
- Excuses
    - Because there is a degree of flexibility in completing items, it is your responsibility to keep track of dates and give yourself enough time for completion. If you wait until the last minute, there is no one to blame but yourself. With that said, I am also not heartless. If there is something that occurs which prevents your access to the course for a significant length of time (e.g., serious illness, death in the

family, or personal tragedy) please contact me as soon as possible and we may be able to work something out. In this case, I will need verification, and it will be left to my discretion on its acceptability.

Attendance and Classroom Policy:

- Students are expected to attend punctually all class meetings, from the beginning of the semester until the end of the semester. **However, you don't have to inform me of your absence or explain reasons for absence in advance.**
- If a student needs self-quarantine for 14 days due to COVID-19, make-up will be provided for exam or assignment that is due during self-quarantine period when the self-quarantine is over.
- If a student misses a class without university excused absence documentation, the student should not expect individualized instruction on what was missed. This will be effective from the beginning of semester.
- Students are expected to assist in maintaining a classroom environment that is conducive to learning. In order to assure that all students have the opportunity to gain from time spent in class, unless otherwise approved by the instructor, students are prohibited from engaging in any other form of distraction. Inappropriate behavior in the classroom shall result, minimally, in a request to leave class.

Marshall University Policy: By enrolling in this course, you agree to the University Policies. Please read the full text of each policy (listed below) by going to Academic Affairs: Marshall University Policies. (URL: http://www.marshall.edu/academic-affairs/policies/)

- Academic Dishonesty Policy
- Academic Dismissal Policy
- Academic Forgiveness Policy
- Academic Probation and Suspension Policy
- Affirmative Action Policy
- Dead Week Policy
- D/F Repeat Rule
- Excused Absence Policy for Undergraduates
- Inclement Weather Policy
- Sexual Harassment Policy
- Students with Disabilities (Policies and Procedures)
- University Computing Services Acceptable Use Policy

Course Schedule and Important Dates: Topics and/or dates may be changed during the semester at the instructor's discretion because of scheduling issues, developments in the discipline, or other contingencies.

- Jan 11: Welcome & Course Introduction
  - Form Your Project Team
- Jan 13: Packet Sniffing
- Jan 18: Lab 1
- Jan 20: Secure Coding and Buffer Overflow Attack

- Jan 25: Buffer Overflow Attack and Defenses
- Jan 27: Lab 2
- Feb 01: Team Project Proposal Presentation
- Feb 03: Penetration Testing
- Feb 08: Lab 3
- **Feb 10: 1st Exam. Thursday, 2:00 p.m. – 3:15 p.m.**
- Feb 15: Internet of Things Security and Privacy
- Feb 17: Lab 4
- Feb 22: Firewalls
- Feb 24: Lab 5
- Mar 01: Dirty COW
- Mar 03: Lab 6
- Mar 08: Format String Vulnerability and Countermeasures
- Mar 10: Lab 7
- **Mar 15: Spring Break – Classes Dismissed**
- **Mar 17: Spring Break – Classes Dismissed**
- **Mar 22: 2nd Exam. Tuesday, 2:00 p.m. – 3:15 p.m.**
- Mar 24: Web Security
- Mar 29: Lab 8
- Mar 31: Return-to-libc Attack and ROP
- Apr 05: Lab 9
- Apr 07: Wireless Exploitation and Defenses
- Apr 12: Lab 10
- Apr 14: Team Project Presentation
- Apr 19: “Dead Week” – Self Review; No Class
    - Team Project Presentation if Necessary
- Apr 21: “Dead Week” – Self Review; No Class
    - Team Project Due
- **Apr 28: 3rd Exam. Thursday, 12:45 p.m. – 2:45 p.m.**