UMBC UGC New Course Request: IS 479: Cybersecurity Project

Date Submitted: 12/15/15 Proposed Effective Date: Fall 2016

	Name	Email	Phone	Dept
Dept Chair or UPD	Carolyn Seaman	cseaman@umbc.edu	53937	IS
Other Contact	Vandana Janeja	vjaneja@umbc.edu	56238	IS

COURSE INFORMATION:

Course Number(s)	IS 479
Formal Title	Cybersecurity Project
Transcript Title (≤30c)	Cybersecurity Project
Recommended Course Preparation	
Prerequisite **NOTE:** Unless otherwise indicated, a prerequisite is assumed to be passed with a "D" or better.	
Credits	3
Repeatable?	☐ Yes ☒ No
Max. Total Credits	3 This should be equal to the number of credits for courses that cannot be repeated for credit. For courses that may be repeated for credit, enter the maximum total number of credits a student can receive from this course. E.g., enter 6 credits for a 3 credit course that may be taken a second time for credit, but not for a third time. Please note that this does NOT refer to how many times a class may be retaken for a higher grade.
Grading Method(s)	☒ Reg (A-F) ☐ Audit ☐ Pass-Fail

PROPOSED CATALOG DESCRIPTION (no longer than 75 words**):**

This course provides the opportunity for IS majors, particularly those enrolled in the Cybersecurity Informatics certificate program, to synthesize material learned in previous coursework by applying it to a cybersecurity-related project related to the student's interests. It is open to IS majors by permission of the department. It consists of an independent study/research project, either individual or in a small group, directed by a faculty member. Department permission required.

RATIONALE FOR NEW COURSE:

a) Why is there a need for this course at this time?
The IS department already has a similar senior project course, IS 469. The rationale for a second one for cybersecurity is to simplify administration of the proposed Cybersecurity Informatics certificate, for which a cybersecurity-related project fulfills one of the requirements. The new course, IS 479, will be similar in structure to our current senior project course.

b) How often is the course likely to be taught?
Every semester

c) How does this course fit into your department's curriculum?
This course is one of two that fulfills the cybersecurity "experience" requirement.

d) What primary student population will the course serve?
Undergraduate IS majors declare the Cybersecurity Informatics certificate.

e) Why is the course offered at the level (ie. 100, 200, 300, or 400 level) chosen?
It is upper-level, as is our current project course, and is numbered to be in sequence with other courses related to the Cybersecurity Informatics certificate.

f) Explain the appropriateness of the recommended course preparation(s) and prerequisite(s).

The appropriate prerequisites for the course would depend on the particular project that a student engages in. Therefore, the course will be permission required with no specific prerequisites listed.

g) Explain the reasoning behind the P/F or regular grading method.
This course is regular graded, as it is expected to have significant academic content.

h) Provide a justification for the repeatability of the course.
This course is not repeatable.

ATTACH COURSE OUTLINE (mandatory):

No syllabus exists for this course, as its nature and structure changes with each project.

Information Systems Department
University of Maryland Baltimore County
Baltimore Maryland 21250

IS 479: Cybersecurity Project

Instructor: Faculty in the IS department

Meeting Times: By Arrangement

Textbook:
There is no single textbook for the course. Material will be selected from relevant readings available through the ACM and Digital Libraries for key conference and journal papers in the area of Cybersecurity.

Course Description: This course provides the opportunity for IS majors, particularly those enrolled in the Cybersecurity Informatics certificate program, to synthesize material learned in previous coursework by applying it to a cybersecurity-related project related to the student's interests. It is open to IS majors by permission of the department. It consists of an independent study/research project, either individual or in a small group, directed by a faculty member.

Instructional Methods: Discussion, Readings and Project development

Course Requirements:

Review Related readings
Design and Develop Project in the area of cybersecurity

Grading:

IS instructors are expected to have exams and evaluations consisting of a mix of class work, test, homework and programming projects, which result in a reasonable distribution of grades. Students will be tested on research and development of projects in the area of CyberSecurity for this course. The break up for this class is as follows:

Literature Survey: 20 Points
Project Design and development: 50 points

Project Writeup: 30 points

Project Deliverables:

- Deliverable 1 : One page write-up and potential datasets list in case of analytics or list of key sources to be surveyed (must include each members role)
- Deliverable 2 : Analytics project-preprocessed Datasets uploaded to blackboard –along with details of the data and source information. Survey project– document with Key sources and detailed field information to be reviewed
- Deliverable 3 : Introduction and motivation
- Deliverable 4 : Remainder of the term paper - Methodology and Experimental results, abstract, conclusions, related work and lessons learned

Sample Topics:

The students can explore a wide range of research interests in cybersecurity across the department, we outline a few sample projects here:

Security of Electronic Voting Systems: Students can investigate into the trustworthiness of electronic voting systems. Example projects can include reliability (are votes recorded as cast and counted as recorded?), lack of standard protocols such as 2PL in voting machines and their impacts. Students can get access to e-voting systems such as Diebold, ScytlPnyx.DRE, and VoteHere through our connections with vendors from previous studies.

Security and Privacy in EMR: The Health Information Technology for Economic and Clinical Health (HITECH) Act mandates that every American have access to their electronic medical records (EMR) by 2014. In addition, personal health records (PHRs) are also becoming a reality. Students can investigate: How can patients create fine-grained and dynamic access control policy on their health data where the access is all or nothing? How can sensitive health information such as history, drug-use, and sexual orientation be stored in a third-party server without any authority over the access control mechanisms established by the third party host?

Powergrid: With more aspects of the United States infrastructure moving to the cyber world, many new threats have emerged. As a result the protection against attacks on power grids has become a huge area of concern. In this project using graph mining, students can analyze the Western United States power grid data (public sample data available)and locate areas in the grid where attacks may cause the most damage.

Software Vulnerability analysis: A software vulnerability is a defect in the system, which allows an attacker to exploit the system and potentially pose a security threat. Students can investigate and discover trends in various operating systems to determine levels of vulnerability. Using the National Vulnerability Database, trends can be analyzed for the last ten years and across major releases for operating systems.

Event Log Mining: Log files are an excellent source for determining the health of the system, many systems employ centralized logging and log file monitoring infrastructure, through Intrusion Detection Systems (IDSs). Students can investigate data mining methods to preprocess and mine event logs such as from Snort logs to identify hidden patterns.

Grading criteria: With respect to final letter grades, the University's Undergraduate Catalogue states that, "A, indicates superior achievement; B, good performance; C, adequate performance; D, minimal

performance; F, failure" There is specifically no mention of any numerical scores associated with these letter grades. Final letter grades in this course conform to the University's officially published definitions of the respective letter grades. In accordance with the published University grading policy, it is important to understand that final letter grades reflect academic achievement and not effort. While mistakes in the arithmetic computation of grades and grade recording errors will always be corrected, it is important to understand that in all other situations final letter grades are not negotiable and challenges to final letter grades are not entertained.

Academic Integrity: By enrolling in this course, each student assumes the responsibilities of an active participant in UMBC's scholarly community in which everyone's academic work and behavior are held to the highest standards of honesty. Cheating, fabricating, plagiarism, and helping others to commit these acts are all forms of academic dishonesty and they are wrong. Academic misconduct could result in disciplinary action that may include, but is not limited to, suspension or dismissal. Full policies on academic integrity should be available in the UMBC Student Handbook, Faculty Handbook, or the UMBC Directory.

Cheating in any form will not be tolerated in this class.*You may not copy other students' work or copy programs from the Internet. You will receive an F for any assignment found to be copied, from any source (this includes any collaboration on individual assignments), for the first time and any subsequent violations will result in immediate failure of the course. You may not reuse your own work from another class for the deliverables in this course.* **Any form of cheating will be reported and will stay on student's record for the rest of their term at UMBC with possible note on their transcripts.**

Accessibility in the classroom: If you have any special needs for technology or classroom accessibility please contact the student support Services and me as well if you like so that we can best accommodate your needs in a confidential and timely manner.

UMBC is committed to eliminating discriminatory obstacles that disadvantage students based on disability. Student Support Services (SSS) is the UMBC department designated to receive and maintain confidential files of disability-related documentation, certify eligibility for services, determine reasonable accommodations, develop with each student plans for the provision of such accommodations, and serve as a liaison between faculty members and students regarding disability-related issues. If you have a disability and want to request accommodations, contact SSS in the Math/Psych Bldg., room 213 or at 410-455-2459. SSS will require you to provide appropriate documentation of disability. If you require accommodations for this class, make an appointment to meet with me to discuss your SSS-approved accommodations.

TENTATIVE COURSE SCHEDULE
(Schedule subject to change)

Week	Topic	Deliverables
Week 1	Discussion of faculty research in cybersecurity Discussion of related projects done by students	
Week 2	Discuss potential Project ideas	
Week 3	Identify related readings	

Week 4	Prepare a bibliography and brief description of related work	
Week 5	Identify key questions to address	Project Deliverable 1: One page outline Due
Week 6	Prepare project design outline, select technology to use, datasets to be used	
Week 7	Prepare datasets	
Week 8-10	Project Development	Project Deliverable 2: Preprocessed Datasets / Key source doc Due
Week 11	Review Preliminary results	
Week 12	Review Preliminary results	Project Deliverable 3: Introduction and Motivation Due
Week 13	Develop Full paper outline	
Week 14-15	Paper Writeup	
Week 16		Project Deliverable 4: Project Final Writeup

Warning/Disclaimer: You will explore several Cybersecurity threats, software and potentially mal-intended websites. Please use utmost caution while learning and exploring these including visiting websites which may infect your computers. You may not use the packet sniffers to collect data without explicit permission from authorized personnel.

Safegaurds to follow to secure your own computer: http://www.fbi.gov/scams-safety/computer_protect