CYBERSECURITY (CYBR)

Cybersecurity Undergraduate Courses

CYBR 1100 INTRODUCTION TO INFORMATION SECURITY (3 credits)

This course emphasizes our current dependence on information technology and how its security in cyberspace (or lack thereof) is shaping the global landscape. Several historical and contemporary global events that have been influenced by the exploitation of information technology motivates topics on cyber crime, malware, intrusion detection, cryptography, among others, and how to secure one's own data and computer system. Several aspects of this course are geared towards developing an understanding of the "cyberspace" as a new medium that breaks all geographical boundaries, while highlighting noticeable influences on it from social, political, economic and cultural factors of a geographical region. (Cross-listed with ACMP 1100).
Distribution: Global Diversity General Education course

CYBR 2250 LOW-LEVEL PROGRAMMING (3 credits)

This course will teach the cybersecurity (CYBR) students low-level programming in the 'C' and assembly languages, and the interrelationship between these two programming paradigms. The student will learn the various control structures in 'C' and how they are implemented in machine code, memory allocation and management, and the basics of allocation classes such as static versus automatic variables. The students will also learn assembly language in the 'C' environment and will be able to write useful, functional, stand-alone assembly language programs with no help from external libraries.
Prerequisite(s): CSCI 1620. Not open to non-degree graduate students.

CYBR 2600 SYSTEM ADMINISTRATION (3 credits)

This course covers topics a system administrator would encounter in their profession. The student will learn how a system administrator fulfills various computer management requirements using both Windows and Linux operating systems on both physical and virtual machines. Topics include installation, creating and maintaining file systems, user and group administration, backup and restore processes, network configuration, system services, virtualization, and security administration.
Prerequisite(s): CIST 1400 or CIST 1600 or Instructor Permission

CYBR 2980 SPECIAL TOPICS IN CYBERSECURITY (3 credits)

The course provides a format for exploring subject areas in Cybersecurity and related fields for sophomore undergraduate students. Specific topics vary, in keeping with research interests of faculty and students. Examples include network configuration, network security, forensics, regulatory compliance, web services and applications, vulnerability assessments, cloud computing security, and other issues in Cybersecurity.
Prerequisite(s): Instructor permission required. Not open to non-degree graduate students.

CYBR 3050 PRINCIPLES OF CYBER OPERATIONS AND DEFENSE (3 credits)

An overview of cyber-defense involves examining strategies, tools, and practices designed to protect digital systems, networks, and data from cyber threats and attacks. This includes learning about the technologies and strategies used to protect systems and networks, developing a comprehensive understanding of the core principles of cybersecurity, understanding different types of vulnerabilities and their causes, and describing the legal frameworks that exist within the cybersecurity discipline.
Prerequisite(s): CYBR 1100, CIST 1400 OR CIST 1600

CYBR 3450 NATURAL LANGUAGE PROCESSING (3 credits)

The course will provide overview of the topics in natural language processing such as word and sentence tokenization, syntactic parsing, semantic role labeling, text classification. We will discuss fundamental algorithms and mathematical models for processing natural language, and how these can be used to solve practical problems. We will touch on such applications of natural language processing technology as information extraction and sentiment analysis. (Cross-listed with CSCI 3450).
Prerequisite(s): Prereq: CSCI 2030 with C- or better; Co-req: CSCI 3320 with C- or better; Students should be comfortable w/ scripting (Python is the language extensively used in natural language processing tools including NLTK). Not open to non-degree graduate students.

CYBR 3570 CRYPTOGRAPHY (3 credits)

The course will provide a broad overview of the concepts, fundamental ideas, vocabulary, and literature base central to the study and development of cryptography and cryptanalysis. This course will explore historical development of cryptography, as well as methods used to defeat it.
In addition, the course will cover the mathematical foundations of cryptography today, as well as some current uses of such cryptography, such as public key infrastructures, the Internet Key Exchange protocol, and more.
Prerequisite(s): CSCI 3320 or ISQA 3300. Not open to non-degree graduate students.

CYBR 3600 CYBERSECURITY POLICY AND AWARENESS (3 credits)

This course will cover the planning and development for information governance, security policies and procedures, and security awareness.
Prerequisite(s): CIST 3110, which may be taken concurrently.

CYBR 4360 PRINCIPLES OF SECURE SYSTEM DESIGN (3 credits)

Contemporary issues in computer security, including sources for computer security threats and appropriate reactions; basic encryption and decryption; secure encryption systems; program security, trusted operating systems; database security, network and distributed systems security, administering security; legal and ethical issues. (Cross-listed with CYBR 8366, CSCI 8366).
Prerequisite(s): CSCI 3320 or CSCI 8325 OR ISQA 3400 OR By instructor permission

CYBR 4380 DIGITAL FORENSICS (3 credits)

Digital forensics involves the preservation, identification, extraction, analysis and documentation of digital evidence stored on a variety of electronic devices. The aim of this course is to introduce students to acceptable approaches for collecting, analyzing and reporting data from a forensics investigation. Topics include: an introduction to digital forensics, data acquisition, first response, memory forensics, operating system forensics, and network forensics. Students will be required to perform several forensics analyses in a controlled lab environment, including acquiring forensically sound hard drive images, memory images and analyzing these using industry standard tools, such as Forensic Toolkit (FTK). The Digital Forensics class is designed for Cybersecurity, Computer Science and other qualified students to learn what actions are both appropriate and required for preserving, collecting and analyzing digital evidence in cases of intrusion, data theft or other cybercrimes. (Cross-listed with CSCI 4380).
Prerequisite(s): CYBR 3600 or CIST 3600; CSCI 3550 or ISQA 3400; CYBR 2600 or CYBR 3350 or CYBR 3370.

CYBR 4390 MOBILE DEVICE FORENSICS (3 credits)

Mobile device forensics is the science of recovering digital evidence from a mobile device under forensically sound conditions using accepted methods. The aim of this course is to introduce students to acceptable approaches for collecting, analyzing and reporting data from a mobile device forensics investigation. Topics include: an introduction to digital and mobile device forensics, mobile forensics standards, acquisition methods (manual, logical, physical and provider-side), Android and iOS filesystem analysis, decoding approaches, application data analysis, and report writing. Students will be required to perform several investigations in a controlled lab environment, including acquiring forensically sound evidence and analyzing these using industry standard tools. (Cross-listed with CYBR 8396).

Prerequisite(s): CYBR 4380/8386 - Computer and Network Forensics or Instructors Permission

CYBR 4430 QUANTUM COMPUTING AND CRYPTOGRAPHY (3 credits)

The course builds an understanding of exciting concepts behind quantum computing and quantum cryptography. In doing so it will introduce the principles of qubits, superposition, entanglement, teleportation, measurement, quantum error correction, quantum algorithms such as quantum Fourier transformation, Shor's algorithm and Grover's algorithm, quantum key exchange, quantum encryption, and secure quantum channels that are built using these principles. It will also discuss advantages of quantum computing and cryptography over classical computing and cryptography and limitations thereof. The students will come out with a working understanding of the field of quantum computing and quantum cryptography. During the course, students will also implement several of the quantum algorithms. (Cross-listed with CYBR 8436, CSCI 4430).

Prerequisite(s): Co-requisites: CYBR 3570 or CSCI 4560; or Instructor permission.

CYBR 4440 INDUSTRIAL CONTROL SYSTEM SECURITY (3 credits)

The objective of this course is to research vulnerabilities into, and provide guidance for securing, industrial control systems (ICS). ICS is a general term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system items such as Programmable Logic Controllers (PLC). The student will learn to identify network and device vulnerabilities and potential countermeasures to these weaknesses. (Cross-listed with CYBR 8446)

Prerequisite(s): CSCI 3550.

CYBR 4450 ETHICAL HACKING - MALWARE ANALYSIS (3 credits)

Malware analysis is the study of computer viruses and how they operate. A heavy emphasis in the class is learning and using reverse engineering tools for analyzing executable computer software at an assembly-language level, particularly using the x86 instruction set. Students will learn about "packing", "hooking", and other low-level ploys that malware utilizes to make itself stealthy, persistent, and to thwart reverse engineering efforts. (Cross-listed with CYBR 8456.)

Prerequisite(s): CSCI 3710 and CYBR 2250

CYBR 4460 ETHICAL HACKING - NETWORK ANALYSIS (3 credits)

The course is an advanced class in which the students learn various techniques for testing for and identifying security flaws in network software and web applications. Internet technologies such as HTTP, DNS, DHCP, and others are examined in the context of cyber security. Students are expected to participate in numerous hands-on experiments related to Information Assurance with respect to web technologies. (Cross-listed with CYBR 8466)

Prerequisite(s): CSCI 3550

CYBR 4540 COMPUTER SECURITY MANAGEMENT (3 credits)

The purpose of this course is to integrate concepts and techniques from security assessment, risk mitigation, disaster planning, and auditing to identify, understand, and propose solutions to problems of computer security and security administration. (Cross-listed with CIST 4540, CYBR 8546, ISQA 8546)

Prerequisite(s): CYBR 4360 or permission of the instructor.

CYBR 4580 CAPSTONE (3 credits)

This capstone course serves as the culminating experience for students in Cybersecurity or Applied Computing and Informatics. Students choose among three pathways: the Security Maker Path, where they design, build, and secure a new system or significant component, producing artifacts such as design documentation, code, and testing results; the Security Breaker Path, where they rigorously evaluate an existing product or system using system, network, and/or software testing methods, generating artifacts such as reversed design documents, vulnerability analyses, test cases, scans, and an overall systems posture analysis report; and the Applied Computing Path, focusing on design, development, and innovation artifacts in areas such as software development, data analytics, informatics solutions, and/or biomedical areas. Most projects will include a community-engaged component, enabling students to tackle real-world challenges and contribute positively to the community. This course is ideally taken in the final semester of your degree. (Cross-listed with ACMP 4580).

Prerequisite(s): Senior standing in Cybersecurity or Applied Computing and Informatics. Not open to non-degree graduate students.

CYBR 4950 INTERNSHIP IN CYBERSECURITY (1-3 credits)

The course provides a format for a student to work with a local or national industry partner in a cyber-security oriented position, and to receive credit for this practical experience. The internship may or may not be a paid position, but will definitely be directly related to the Cybersecurity degree program. The class is proposed and organized by the student, with participating faculty supervising and input provided by the industry partner.

Prerequisite(s): Instructor Permission

CYBR 4980 SPECIAL TOPICS IN CYBERSECURITY (3 credits)

The course provides a format for exploring advanced research areas for undergraduate and graduate students in Cybersecurity and related fields. Specific topics vary, in keeping with the research interests of faculty and students. Examples include applied data mining, mobile security, web services and applications, vulnerability assessments, cloud computing security, and other issues in Cybersecurity research. (Cross-listed with CYBR 8986)

Prerequisite(s): Instructor Permission.

CYBR 4990 INDEPENDENT STUDY IN CYBERSECURITY (1-3 credits)

The course provides a format for exploring advanced research areas for undergraduate students in Cybersecurity and related fields. The class is designed for students that would like to explore specific Cybersecurity topics at a greater depth, or topics which are not currently a part of the CYBR curriculum. The class is proposed and organized by the student, with participating faculty mentoring.

Prerequisite(s): Instructor Permission