CYSE - Cybersecurity

CYBERSECURITY Courses

CYSE 100. Cyber Explorers and University Orientation. 1 Credit.
This course provides an introduction to cyber hygiene and orientation to university life.

CYSE 200T. Cybersecurity, Technology, and Society. 3 Credits.
Students will explore how technology is related to cybersecurity from an interdisciplinary orientation. Attention is given to the way that technologically-driven cybersecurity issues are connected to cultural, political, legal, ethical, and business domains.

CYSE 250. Basic Cybersecurity Programming and Networking. 3 Credits.
This course introduces the cybersecurity-centric programming and networking concepts. Students will develop problem solving skills by using low-level programming languages (including C and assembly) and learn fundamentals of network protocols. This course is the technical base for students to take cybersecurity major courses. No prior knowledge of programming and networking is assumed. Prerequisite: MATH 162M or higher.

CYSE 270. Linux System for Cybersecurity. 3 Credits.
This course introduces the basic operations in major Linux distros for cybersecurity using both graphical interface and command line interface. Students will learn about the basic installation and configuration, file systems management, shell scripts, and user authentication in Linux systems. This course is the technical base for students to take cybersecurity major courses.

CYSE 300. Introduction to Cybersecurity. 3 Credits.
This course provides an overview of the field of cybersecurity. It covers core cybersecurity topics including computer system architectures, critical infrastructures, cyber threats and vulnerabilities, cryptography, information assurance, network security, and risk assessment and management. Students are expected to become familiar with fundamental security concepts, technologies and practices, and develop a foundation for further study in cybersecurity. Prerequisite: MATH 162M or permission of the instructor.

CYSE 301. Cybersecurity Techniques and Operations. 3 Credits.
This course introduces tools and techniques used to secure and analyze large computer networks and systems. Students will explore and map networks using a variety of diagnostic software tools, learn advanced packet analysis, configure firewalls, write intrusion detection rules, perform forensic investigation, and practice techniques for penetration testing. Prerequisite: MATH 162M or permission of the instructor.

CYSE 368. Cybersecurity Internship. 1-6 Credits.
This course allows students to volunteer to work in an agency related to cybersecurity. Students must volunteer for 50 hours per course credit and complete course assignments. Prerequisite: approval by the Director of the Center for Cybersecurity Education and Research.

CYSE 395. Topics in Cybersecurity. 1-3 Credits.
Study of selected topics in cybersecurity. Prerequisites: junior standing.

CYSE 404. Law and Digital Forensics. 3 Credits.
This course will focus on the intersection of digital forensics and the criminal justice system, namely how digital forensics is understood and applied to key criminal justice, constitutional and statutory considerations within the criminal justice system. Students will explore such topics as the nature and types of cybercrime; search and seizure principles in the digital world; finding, handling and maintaining chain of custody of digital evidence; interviewing individuals relating to digital evidence and related activities; and testifying in court about digital evidence matters. Prerequisites: Junior standing or permission of instructor.

CYSE 406. Cyber Law. 3 Credits.
This course tackles two major cyber law subjects. The first part of the course examines various U.S. laws and legal considerations that impact the digital and cyberspace worlds from traditional civil, and to a lesser extent, traditional criminal perspectives. The second part will familiarize cyber operations professionals about the extent of and limitations on their authorities to ensure operations in cyberspace are in compliance with U.S. law, regulations, directives and policies. The course will also introduce students to miscellaneous cybersecurity topics such as the Federal Acquisition Requirements. Prerequisite: junior standing.

CYSE 407. Digital Forensics. 3 Credits.
This course introduces the basic concepts and technologies of digital forensics. Students will learn the fundamental techniques and tools utilized for collecting, processing, and preserving digital evidence on computers, mobile devices, networks, and cloud computing environments. Students will also engage in oral and written communication to report digital forensic findings and prepare court presentation materials. Prerequisites: declared major and junior standing.

CYSE 409. Crime and Computer Applications. 3 Credits.
The purpose of this interdisciplinary course is to introduce students to the ways in which computers are involved in the commission and the investigation of crime. Students will learn the fundamentals of cryptography and steganography and the tools used to perform these activities. Students will also use forensic software to identify, gather, and verify relevant digital evidence. Cross-listed with CRJS 409. Prerequisite: CRJS 310 or permission of instructor.

CYSE 416/516. Cyber Defense Fundamentals. 3 Credits.
This course focuses on cybersecurity theory, information protection and assurance, and computer systems and networks security. The objectives are to understand the basic security models and concepts, learn fundamental knowledge and tools for building, analyzing, and attacking modern security systems, and gain hands-on experience in cryptographic algorithms, security fundamental principles, and Internet security protocol and standards. Prerequisite: ECE 355 or equivalent or permission of the instructor.

CYSE 417. Digital Leadership. 3 Credits.
This course explores technology as it relates to leadership experiences. Theories, case studies and real world examples are analyzed to show both successful and unsuccessful uses of online and digital approaches that inform leaders' communication strategies. Students will explore how their own digital identities may impact their futures as leaders. They will also learn how to create digital identities that will shape their professional identities throughout their careers. Prerequisites: Junior standing or permission of instructor.

CYSE 419/519. Cyber Physical System Security. 3 Credits.
Cyber Physical Systems (CPS) integrate computing, networking, and physical processes. The objectives of this course are to learn the basic concepts, technologies and applications of CPS, understand the fundamental CPS security challenges and national security impact, and gain hands-on experience in CPS infrastructures, critical vulnerabilities, and practical countermeasures. Prerequisite: ECE 355 or permission of the instructor.

CYSE 425W. Cybersecurity Strategy and Policy. 3 Credits.
This writing intensive course explores cybersecurity policy and strategy and introduces students to the essentials of strategy development and policy making in cybersecurity. Topics considered include planning principles in cyber strategy; risk management and cybersecurity policy; the connections between cybersecurity policies, businesses, and governmental institutions; the knowledge, skills, and abilities needed to develop and implement cybersecurity policy; the social, political and ethical implications that arise in cybersecurity policies and strategies; strategies to assess cybersecurity policy; and the ties between national security and cybersecurity policy. Prerequisites: ENGL 110C and ENGL 211C or ENGL 221C or ENGL 231C with a grade of C or better and CYSE 200T or POLS 101S.
This course explores the national security dimensions of cybersecurity and examines cyber war in international relations. Exploration of cyber war begins with an examination of cybersecurity as a component of national security and investigates the topics of U.S National Cybersecurity and other national approaches to cyber war. The topics of cyber deterrence, cyber as a military domain, the roles of international organizations in cyber war, cyber terrorism, the role of social media, and information warfare will be discussed. The international dimension of cybersecurity is also discussed. Prerequisites: CYSE 200T or POLS 101S or permission of the instructor.

This course introduces the basic terminologies used in ethical hacking and useful tools in relation to penetration testing on Kali Linux. Students will learn to explore the vulnerabilities in various systems and operate the industry-leading tools and framework to perform the penetration testing on different target systems. Prerequisites: CYSE 270 and CYSE 301 or permission of the instructor.

This course is designed to help students enhance their personal and professional development through innovation guided by faculty members and professionals. It offers students an opportunity to integrate disciplinary theory and knowledge through developing a nonprofit program, product, business, or other initiative. The real-world experiences that entrepreneurship provides will help students understand how academic knowledge leads to transformations, innovations, and solutions to different types of problems. The course can be delivered either as an independent project for individual students or as group projects similar to those sometimes offered in topics courses. Prerequisite: Approval by the Director of the Center for Cybersecurity Education and Research.

The advanced study of selected cybersecurity topics designed to permit small groups of qualified students to work on subjects of mutual interest. These courses will appear in the course schedule, and will be more fully described in information distributed to academic advisors. Prerequisite: permission of the instructor.

The advanced study of selected cybersecurity topics designed to permit small groups of qualified students to work on subjects of mutual interest. These courses will appear in the course schedule, and will be more fully described in information distributed to academic advisors. Prerequisite: permission of the instructor.

Independent reading and study on a topic to be selected under the direction of an instructor. Conferences and papers as appropriate. Prerequisite: approval of the Director of the Center for Cybersecurity Education and Research.

Independent reading and study on a topic to be selected under the direction of an instructor. Conferences and papers as appropriate. Prerequisite: approval of the Director of the Center for Cybersecurity Education and Research.

This course provides an overview of the field of cybersecurity. It covers core cybersecurity topics including computer system architectures, critical infrastructures, cyber threats and vulnerabilities, cryptography, cryptographic protocol design, information assurance, network security, and risk assessment and management. Students are expected to become familiar with fundamental security concepts, technologies and practices, and develop a foundation for further study in cybersecurity.

This course introduces tools and techniques used to secure and analyze large computer networks and systems. It will include significant hands-on lab work. Students will explore and map networks using a variety of diagnostic software tools, learn advanced packet analysis, configure firewalls, write intrusion detection rules, perform malware detection, forensic investigation, and practice techniques for penetration testing.

This course addresses two major cyber law subject matters. The first part of the course examines various U.S. laws and legal considerations that impact the digital and cyberspace worlds from civil and criminal perspectives. The second part, which builds upon the first, will familiarize cyber operations professionals about the extent of and limitations on their authorities to ensure operations in cyberspace are in compliance with U.S. law, regulations, directives and policies.

This course focuses on cybersecurity theory, information protection and assurance, and computer systems and networks security. The objectives are to understand the basic security models and concepts, learn fundamental knowledge and tools for building, analyzing, and attacking modern security systems, and gain hands-on experience in cryptographic algorithms, security fundamental principles, and Internet security protocol and standards. Prerequisites: ECE 355 or equivalent or permission of the instructor.

This course focuses on cybersecurity techniques and operations. 3 Credits.

This course introduces skills to manage technical professionals and lead strategic change in their organization. Based on the basic operations and functionality of cybersecurity systems, students will learn the management of cybersecurity technical professionals, including how to effectively lead and manage teams, how to launch and assess organizational change initiatives, and how to work effectively within an interdependent group to achieve common goals.
CYSE 607. Advanced Digital Forensics, 3 Credits.
This course introduces the concepts and technologies of digital forensics. Students will learn the advanced techniques and tools utilized for collecting, processing, and preserving digital evidence on computers, mobile devices, networks, and cloud computing environments. Students will also engage in oral and written communication to report digital forensic findings and prepare court presentation materials.

CYSE 615. Mobile and Wireless Security, 3 Credits.
An overview of wireless and mobile security providing students with practical and theoretical experiences. Topics include smartphone security, mobile Internet security, mobile location privacy, and wireless ad hoc, mesh, and sensor network security.

CYSE 625. Advanced Ethical Hacking and Penetration Testing, 3 Credits.
This course teaches students the underlying principles and many of the techniques associated with the cybersecurity practice known as penetration testing or ethical hacking. The course covers planning, reconnaissance, scanning, exploitation, post-exploitation, and result reporting. Students will discover how system vulnerabilities can be exploited and learn to avoid such problems.

CYSE 697. Independent Study in Cybersecurity, 3 Credits.
This course allows students to develop specialized expertise by independent study (supervised by a faculty member).

CYSE 698. Master's Project, 3 Credits.
This capstone course provides opportunities to synthesize and apply the knowledge and skills to solve real-world cyber security problems.