CYBERSECURITY (CYBR)

Cybersecurity Graduate Courses

CYBR 8080 SPECIAL TOPICS IN INFORMATION ASSURANCE (1-6 credits)
The course provides a format for exploring advanced research areas for graduate students in Information Assurance and related fields. Specific topics vary, in keeping with 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 Information Assurance research.
Prerequisite(s): Instructor Permission.

CYBR 8366 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 4360, CSCI 8366)

CYBR 8396 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 4390).

CYBR 8410 DISTRIBUTED SYSTEMS AND NETWORK SECURITY (3 credits)
The course aims at understanding the issues surrounding data security, integrity, confidentiality and availability in distributed systems. Further, we will discuss various network security issues, threats that exist and strategies to mitigate them. This course will cover topics in cryptography, public key infrastructure, authentication, hashing, digital signatures, ARP protection, IP and IPSEC, IP Tables, SSL/TLS, firewalls, etc. (Cross-listed with CSCI 8410)
Prerequisite(s): IASC 8366 or equivalent(s); or instructor permission. Not open to non-degree graduate students.

CYBR 8420 SOFTWARE ASSURANCE (3 credits)
Software assurance is a reasoned, auditable argument created to support the belief that the software will operate as expected. This course is an intersection of knowledge areas necessary to perform engineering activities or aspects of activities relevant for promoting software assurance. This course takes on a software development lifecycle perspective for the prevention of flaws. (Cross-listed with CSCI 8420)
Prerequisite(s): CSCI 8836 OR by permission of the Instructor. Not open to non-degree graduate students.

CYBR 8436 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 4430, CSCI 4430).

CYBR 8446 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 4440)

CYBR 8450 APPLIED CRYPTOGRAPHY (3 credits)
In this course we will implement stream and block ciphers in different modes, public key algorithms, hash functions, message authentication codes, random number generators, etc. Along the way we will also explore weaknesses of these algorithms and implement well-known attacks on them. We will also solve crypto challenges and puzzles. This is a hand-on course and will require programming proficiency. The preferred language will be Python; you can, however, use other object oriented languages.
Prerequisite(s): CSCI 8410 or CYBR 8410

CYBR 8456 HOST-BASED VULNERABILITY DISCOVERY (3 credits)
The class will cover security issues at an implementation and hardware level. The students will learn assembly language and the use of a reverse assembler and debugger. This will allow the student to analyze various "packing" algorithms for computer viruses, the viruses themselves, operating system "hooking", "fuzzing", and other machine code, host-based exploits. The class will be using both Windows and Linux as operating systems. (Cross-listed with CYBR 4450.)
Prerequisite(s): CSCI 3710 and CYBR 2250.

CYBR 8466 NETWORK-BASED VULNERABILITY DISCOVERY (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 4460)
Prerequisite(s): CSCI 3550

CYBR 8470 SECURE WEB APPLICATION DEVELOPMENT (3 credits)
Web applications are pervasive fixtures of 21st century culture. Web application security is an inclusive, amorphous, term that spans application level security, i.e. ensuring high level code cannot be exploited, server level security, i.e. ensuring server resources such as databases and file systems cannot be exploited, and network security, i.e. ensuring unauthorized parties cannot access a server or tamper with user sessions. This course cross-cuts the web application security concepts across the different categories above and takes a heavily hands-on approach to introduce students to the world of secure web app. design and development.

CYBR 8480 SECURE MOBILE DEVELOPMENT (3 credits)
Mobile devices are already pervasive fixtures of 21st century culture and increasingly the internet of things (IoT) and wearables are proliferating throughout the world. As this proliferation occurs, numerous vendor-centric and third-party mobile, wearable, and internet of things apps are being created by developers and downloaded by end-users with little to no thought about the security and privacy of the information used and collected by the apps. This course examines this issue from a development point of view to a) introduce mobile/wearable/IoT architectures and technologies, b) increase student application development competencies with these technologies, and c) integrate secure design principles into the ideation, design, and testing phases during development.
Prerequisite(s): CYBR 8470 or Instructor Permission

CYBR 8490 CYBER INVESTIGATIONS (3 credits)
Security incidents and cybercrimes detected by organizations are escalating in both scale and complexity. As a result, cyber investigation capabilities have become a critical mechanism for organizations in an effort to minimize the damage from incidents and cybercrimes. These investigations often involve the preservation, identification, extraction, analysis and documentation of digital data (evidence) stored on a variety of electronic devices. The aim of this course is to introduce graduate students to acceptable approaches for collecting, analyzing and reporting data from a cyber investigation. Topics include but are not limited to: an introduction to cyber investigations, cyber investigations and the law, incident response and first responder actions, investigation techniques, operating system analysis, and network investigations Students will be required to perform several analyses in a controlled lab environment.
Prerequisite(s): CYBR 8366 or equivalent. CSCI 3550 or ISQA 3400, or equivalent. CYBR 3370 or equivalent. Alternatively, instructor permission can be sought before enrolling into the class for students who have not met all of the above requirements.

CYBR 8546 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 4540, ISQA 8546)
Prerequisite(s): CYBR 4360 or permission of the instructor.

CYBR 8570 INFORMATION SECURITY POLICY AND ETHICS (3 credits)
The course will cover the development and need for information security policies, issues regarding privacy, and the application of computer ethics. (Cross-listed with ISQA 8570)
Prerequisite(s): CIST 2100 or BSAD 8030, or permission of instructor.

CYBR 8900 INDEPENDENT STUDY IN INFORMATION ASSURANCE (1-3 credits)
The course provides a format for exploring advanced research areas for graduate students in Information Assurance and related fields. The class is designed for students that would like to explore specific Information Assurance topics at a greater depth, or topics that are not currently a part of the IA curriculum. The class is proposed and organized by the student, with participating faculty mentoring.
Prerequisite(s): Instructor Permission

CYBR 8910 INTERNSHIP (1-3 credits)
The purpose of this course is to provide the students with an opportunity for practical application and further development of knowledge and skills acquired in the MS in CyberSecurity (CYBR) program. The internship gives students professional work experience and exposure to the challenges and opportunities faced by IT professionals in the workplace.
Prerequisite(s): Students must have completed a minimum of 12 credit hours towards the MS in CYBR program. Instructor permission is required to register. Not open to non-degree graduate students.

CYBR 8950 CYBERSECURITY GRADUATE CAPSTONE (3 credits)
The graduate capstone course challenges students to prove their mastery of the skills and domain knowledge they have gathered throughout their program of study. The course begins with a module on project management and research best practices. The majority of course is structured around facilitating a non-trivial semester-long project, often in service to a third-party project sponsor, such as a community, industry, or government partner. The course is intended for students that have selected the coursework option, not thesis, and that are close to graduation (see prerequisites). The course is considered summative and replaces the MS in CYBR comprehensive examination requirement.
Prerequisite(s): Students must have 9 credit hours or fewer left in the program. Students must have completed CYBR 8366, CYBR 8410, and CYBR 8420. Not open to non-degree graduate students.

CYBR 8986 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 4980)
Prerequisite(s): Instructor Permission.

CYBR 8990 THESIS IN INFORMATION ASSURANCE (1-6 credits)
A research project, designed and executed under the supervision of the chair and approval by members of the graduate student's thesis advisory committee. In this project the student will develop and perfect a number of skills including the ability to design, conduct, analyze and report the results in writing (i.e., thesis) of an original, independent scientific investigation.
Prerequisite(s): Instructor Permission.

CYBR 9460 SECURITY OF EMBEDDED SYSTEMS (3 credits)
An embedded system is some combination of computer hardware and software, either fixed in capability or programmable, which is specifically designed for a particular function. Industrial machines, automobile electronic systems, medical equipment, cameras, household appliances, airplanes, and vending machines, are among the myriad possible hosts of an embedded system. This course covers forward-looking topics in the security of embedded systems, including topics such as logic circuit obfuscation, hardware security methods, network setup exploits, and other "lower level" computer architecture subjects with respect to cybersecurity.
Prerequisite(s): CYBR 8366 - Foundations of Information Assurance