CYBERSECURITY (CYBR)

Courses and Descriptions

CYBR 500 Beyond Code: Cybersecurity in Context 3 Credits
At its core, cybersecurity is a technical, computing-based discipline. This course explores the most important non-technical elements that shape the landscape upon which cybersecurity problems emerge and are managed. Students will assume different lenses — legal, economic, political, societal, and ethical — to better understand how different forces enable and constrain security technologies and policies. Specific topics include ethical and societal issues, policy-making, business models, legal frameworks, national security considerations, and the roles of users, industry, and government which includes the military.

CYBR 510 Cryptography for Cybersecurity 3 Credits
This course focuses on both mathematical foundations and practical applications of cryptography. The course discusses asymmetric and symmetric cryptography, Kerchkoff's Principle, chosen and known plaintext attacks, public key infrastructure, authentication protocols. The course includes a close examination of various cryptosystems including the RSA, DES, AES, Elliptic Curve, and SHA family cryptosystems. Topics include a brief history of cryptography, ciphers, digital signatures, hash functions, message authentication codes, secure e-commerce, and digital cash.

CYBR 520 Managing Cyber Risks 3 Credits
In the context of risk management, this course examines the motivating reasons behind cyber attacks and data breaches. Various risk management frameworks to measure organizational cybersecurity threats and vulnerabilities are presented. Further, students will model cybersecurity risks, using both qualitative and quantitative risk assessment methods. Students also will articulate the organizational consequences of the assessed risks along with mitigating strategies to reduce or eliminate the cyber risks.

CYBR 530 Mobile Computing and Wireless Security 3 Credits
This course examines the cybersecurity of mobile computing and wireless networking, especially the vulnerabilities, threats, and mitigation techniques. Topics include: mobile malware, wireless communications infrastructure vulnerabilities and associated mitigation techniques, mobile platform vulnerabilities and associated mitigation techniques, mobile app vulnerabilities and associated mitigation techniques, mobile device vulnerabilities and associated mitigation techniques, and organizational policies for mobile computing and wireless networking.
Prerequisite(s): CYBR 510.

CYBR 540 Secure Coding for Cyber Defense 3 Credits
This combined course of lecture and hands-on labs follows the philosophy and principles of secure and robust programming, using the Java language. The eight design principles that govern secure and robust coding will be emphasized with follow-on coding labs to apply these design methods to real-world problems. Design choices, good or bad, drive implementation in coding, so designing software security from the beginning will be practiced. Common software vulnerabilities and static analysis of code will be examined, as well as informal, formal, and ad hoc coding methods will be differentiated. Prior experience with the Java programming language is highly recommended.

CYBR 550 Cybercrime and Digital Forensics Analysis 3 Credits
Digital forensics is a hybrid science that offers a systematic approach for conducting comprehensive investigations to solve cybercrimes. In this course, students will learn the principles and techniques of digital forensics investigations to ensure court admissibility of electronic evidence, including the legal and ethical implications. Students also will also gain hands-on experience with performing proper forensic investigations with different file systems (e.g., Unix/Linux, Mac, Windows, Android) and writing appropriate forensics analysis reports.

CYBR 560 Usable Privacy and Security 3 Credits
There is growing recognition that technology alone cannot provide all of the solutions to security and privacy problems. Human factors play an important role, and it is important for security and privacy experts to have an understanding of how people might interact with the systems they develop. This course explores a variety of usability and user interface pitfalls related to privacy and security and provides experiences in designing studies aimed at helping to evaluate usability issues in security and privacy systems.
Prerequisite(s): CYBR 500.

CYBR 570 Special Topics in Cybersecurity 3 Credits
This course is used as a general placeholder for one time offerings and new courses that have not been assigned a permanent designation. The course will cover advanced and emerging topics of current interest in cybersecurity. This course code may be taken more than once as long as the topic offered is different each time.
Prerequisite(s): Permission of instructor.

CYBR 590 Independent Research and Study 1-4 Credits
Provides students with an opportunity to design and carry out original research in an area of their choice. Students designate a faculty supervisor and work closely with him/her during the semester. Permission of instructor.

CYBR 591 M.S. in Cybersecurity Internship 3 Credits
The course is part of the capstone requirement for the M.S. in Cybersecurity. The course will have students complete an internship, self-evaluation, and a project related to their experience working in a cybersecurity related position. Permission of instructor.

CYBR 600 Software Vulnerability and Malware Analysis 3 Credits
This combined course of lecture and hands-on labs covers both the art and science of discovering software vulnerabilities and malware. Beginning with the foundational techniques used to analyze both source and binary code, this course will examine current threats and evaluate the actions needed to prevent attackers from taking advantage of both known and unknown vulnerabilities. The course will cover passive and active reverse engineering techniques in order to discover and categorize software vulnerabilities and malware, create workarounds to better secure the system, and demonstrate security solutions that provide protection from an adversary attempting to exploit the vulnerabilities. Techniques covered include the use of static analysis, dynamic reverse engineering tools, and fault injection to better understand and improve the security of software. Prior exposure to Intel assembly is helpful, though not required.
Prerequisite(s): CYBR 540.

CYBR 610 Cloud Computing Security and Privacy 3 Credits
This course focuses on the security and privacy issues in Cloud Computing. While the Cloud Computing paradigm gains in popularity, there are many unresolved cybersecurity issues related to confidentiality, integrity, and availability of data and computations involving the Cloud. This course examines Cloud Computing models and the associated risks, threats and vulnerabilities; focuses on sound architectural design for secure and private computing; and explores practical applications of cloud computing and the Internet of Things (IoT).
Prerequisite(s): CYBR 530.

CYBR 620 Blockchains and Cryptocurrencies 3 Credits
This combined Lecture-Lab course covers the mathematical, computational, and economic foundations of Blockchain technology, and exposes students to the societal and legal implications of a decentralized monetary system based on consensus. Students learn what cryptocurrencies are, why it is possible to make money using cryptocurrencies such as bitcoins, and why it is so volatile. Through hands-on practice with the bitcoin and Ethereum-based software platforms, students will program secure decentralized applications (Dapps), develop an understanding of cryptographic principles, and reexamine critical economic questions.
Prerequisite(s): CYBR 510.