CYBER SECURITY (CYBSC)

Courses primarily for undergraduates:

CYBSC 1310: Introduction to Computer Security Literacy
(Cross-listed with CPRE 1310).
Credits: 1. Contact Hours: Lecture 1.
Basic concepts of practical computer and Internet security: passwords, firewalls, antivirus software, malware, social networking, surfing the Internet, phishing, and wireless networks. This class is intended for students with little or no background in information technology or security. Basic knowledge of word processing required. Offered on a satisfactory-fail basis only.

CYBSC 3320: Cyber Defense Competition
(Cross-listed with CPRE 3320).
Credits: 1. Contact Hours: Laboratory 2.
Repeatable.
Participation in cyber defense competition driven by scenario-based network design. Includes computer system setup, risk assessment and implementation of security systems, as well as defense of computer and network systems against trained attackers. Team based. Offered on a satisfactory-fail basis only. (Typically Offered: Spring)

CYBSC 4300: Network Protocols and Security
(Dual-listed with CPRE 5300/ CYBSC 5300). (Cross-listed with CPRE 4300).
Credits: 3. Contact Hours: Lecture 3.
*Prereq: (*CPRE 3080 *or* COMS 2520 *or* COMS 3520*) OR* CPRE 2880
Detailed examination of networking standards, protocols, and their implementation. TCP/IP protocol suite, network application protocols. Network security issues, attack and mitigation techniques. Emphasis on laboratory experiments.

Courses primarily for graduate students, open to qualified undergraduates:

CYBSC 5300: Network Protocols and Security
(Dual-listed with CPRE 4300/ CYBSC 4300). (Cross-listed with CPRE 5300).
Credits: 3. Contact Hours: Lecture 3.
Detailed examination of networking standards, protocols, and their implementation. TCP/IP protocol suite, network application protocols. Network security issues, attack and mitigation techniques. Emphasis on laboratory experiments.

CYBSC 5310: Information System Security
(Cross-listed with CPRE 5310).
Credits: 3. Contact Hours: Lecture 3.
Computer, software, and data security: basic cryptography, security policies, multilevel security models, attack and protection mechanisms, legal and ethical issues.

CYBSC 5320: Information Warfare
(Cross-listed with CPRE 5320).
Credits: 3. Contact Hours: Lecture 3.
Computer system and network security: implementation, configuration, testing of security software and hardware, network monitoring. Authentication, firewalls, vulnerabilities, exploits, countermeasures. Study and use of attack tools. Ethics in cyber security. Emphasis on laboratory experiments. (Typically Offered: Spring)

CYBSC 5330: Cryptography
(Cross-listed with CPRE 5330/ MATH 5330).
Credits: 3. Contact Hours: Lecture 3.
Basic concepts of secure communication, DES and AES, public-key cryptosystems, elliptic curves, hash algorithms, digital signatures, applications. Relevant material on number theory and finite fields. (Typically Offered: Spring)

CYBSC 5340: Legal and Ethical Issues in Cyber Security
(Cross-listed with CPRE 5340/ POLS 5340).
Credits: 3. Contact Hours: Lecture 3.
Legal and ethical issues in computer security. State and local codes and regulations. Privacy issues. (Typically Offered: Spring)

CYBSC 5350: Steganography and Digital Image Forensics
(Cross-listed with CPRE 5350/ MATH 5350).
Credits: 3. Contact Hours: Lecture 3.
Basic principles of covert communication, steganalysis, and forensic analysis for digital images. Steganographic security and capacity, matrix embedding, blind attacks, image forensic detection and device identification techniques. Related material on coding theory, statistics, image processing, pattern recognition. (Typically Offered: Spring)

CYBSC 5360: Computer and Network Forensics
(Cross-listed with CPRE 5360).
Credits: 3. Contact Hours: Lecture 3.
Fundamentals of computer and network forensics, forensic duplication and analysis, network surveillance, intrusion detection and response, incident response, anonymity and pseudonymity, privacy-protection techniques, cyber law, computer security policies and guidelines, court testimony and report writing, and case studies. Emphasis on hands-on experiments.

CYBSC 5380: Reverse Engineering and Security Testing
(Cross-listed with CPRE 5380).
Credits: 3. Contact Hours: Lecture 3.
Techniques and tools for understanding the behavior of software/hardware systems based on reverse engineering. Flaw hypothesis, black, grey, and white box testing as well as other methods for testing the security of software systems. Discussion of counter-reverse engineering techniques. (Typically Offered: Spring)

CYBSC 5600: Data-Driven Security and Privacy
(Cross-listed with COMS 5600/ CPRE 5600).
Credits: 3. Contact Hours: Lecture 3.
Examination of applications of machine learning and big data techniques to various security and privacy problems, as well as secure and privacy-preserving machine learning algorithms. Offered irregularly. (Typically Offered: Spring)

CYBSC 5920: Seminar in Cyber Security
Credits: 1-3. Contact Hours: Lecture 3.
Repeatable.
Projects or seminar in Cyber Security. (Typically Offered: Fall, Spring, Summer)

Courses for graduate students:

CYBSC 6310: Cyber Security Operations Practicum
(Cross-listed with CPRE 6310).
Credits: 3. Contact Hours: Lecture 1.
Repeatable.
Practical experience in cyber operations. Cyber security threat analysis, malware analysis, and intrusion detection management. Cyber security data analysis methods. Pen testing tools and techniques. Weekly threat analysis briefings. Offered on a satisfactory-fail basis only.

CYBSC 6320: Cyber Security Capstone Design
(Cross-listed with CPRE 6320).
Credits: 3. Contact Hours: Lecture 3.
Capstone design course which integrates the security design process. Design of a security policy. Creation of a security plan. Implementation of the security plan. The students will attack each other’s secure environments in an effort to defeat the security systems. Students evaluate the security plans and the performance of the plans. Social, political and ethics issues. Student self-evaluation, journaling, final written report.

CYBSC 6340: Current Research Problems in Cyber Security
Credits: 3. Contact Hours: Lecture 3.
Repeatable.
Discussion of complex cyber security problems. Students will learn how to apply research techniques, think clearly about these issues, formulate and analyze potential solutions, and communicate their results. Working in small groups under the mentorship of technical clients from government and industry, each student will formulate, carry out, and present original research on complex current cybersecurity problems of interest to the nation. This course will be run in a synchronized distance fashion, coordinating some activities with our partner schools and our technical clients. (Typically Offered: Fall, Spring)

CYBSC 6970: Cyber Security Summer Internship
Credits: Required.
One semester and one summer maximum per academic year professional work period. Offered on a satisfactory-fail basis only.