CYBER SECURITY ENGINEERING (CYBE)

Courses primarily for undergraduates:

CYBE 2300: Cyber Security Fundamentals
(Cross-listed with CPRE 2300).
Credits: 3. Contact Hours: Lecture 2, Laboratory 2.
Prereq: COMS 2270 *or EE 2850 or* MIS 2070
Introduction to computer and network infrastructures used to support cyber security. Basic concepts of computer and network configuration used to secure environments. Computer virtualization, network routing and address translation, computer installation and configuration, network monitoring, in a virtual environment. Laboratory experiments and exercises including secure computer and network configuration and management. (Typically Offered: Fall)

CYBE 2310: Cyber Security Concepts and Tools
(Cross-listed with CPRE 2310).
Credits: 3. Contact Hours: Lecture 2, Laboratory 2.
Prereq: CPRE 2300 *or* CYBE 2300
Basic concepts of practical computer and Internet security and the tools used to protect and attack systems and networks. Computer and network security methods including: user authentication, access control, firewalls, intrusion detection, use of vulnerability assessment tools and methods, and penetration testing. Ethics and legal issues in cyber security will also be covered. Laboratory experiments and exercises including evaluating systems for vulnerabilities, understanding potential exploits of the systems, and defenses for the systems. (Typically Offered: Spring)

CYBE 2340: Legal, Professional, and Ethical Issues in Cyber Systems
(Cross-listed with CPRE 2340).
Credits: 3. Contact Hours: Lecture 3.
Prereq: COMS 2270 *or EE 2850 or* MIS 2070
Emphasizes legal, ethical, and professional issues in cyber systems. Other topics include privacy, government regulation, and compliance as applied to professional practice. Guest lecturer from government and industry, as well as discussions including current legal and ethical issues found in the main stream. (Typically Offered: Spring)

CYBE 3310: Application of Cryptographic Concepts to Cyber Security
(Cross-listed with CPRE 3310).
Credits: 3. Contact Hours: Lecture 2, Laboratory 2.
Prereq: CPRE 2310 *or* CYBE 2310
Basic cryptographic underpinnings used in modern cyber security encryption suites. Encryption benefits to cyber security and its use in protocols. Topics include cryptographically secure hash functions and pseudorandom numbers, key distribution techniques, secure authentication including single sign on. Detection and prevention of security threats such as covert communication, malicious code, and other security threats in protocols are included. In addition to laboratory experiments and exercises, students complete a project focused on cyber security problem and solution. Graduation Restriction: Only one of CPRE/CYBE 3310 and CPRE 4310 may count towards graduation. (Typically Offered: Fall, Spring)

CYBE 4370X: Introduction to Wireless Security
(Cross-listed with CPRE 4370X).
Credits: 3. Contact Hours: Lecture 3.
With communication and network services and applications increasingly leveraging wireless media, the importance of information and network security in the wireless domain continues to grow. The challenges of providing secure communication and network services are considerably more difficult in wireless environments than in traditional wired systems (e.g., the Internet), so the focus of the course will be purely wireless covering both networking issues and security aspects of modern wireless environments. Fundamentals of mobile LANs and WANs, ad hoc, sensor networks/internet of things and cloud, mobile IP/TCP, confidentiality, key establishment, authentication, broadcasting, RFIDs, and rogue attacks.

CYBE 4400: Operating System Security
(Cross-listed with CPRE 4400).
Credits: 3. Contact Hours: Lecture 3.
Prereq: COMS 3520 *or* CPRE 3080
Focus on fundamentals and advanced topics in operating system (OS) security. Design issues, principles, mechanisms, and good practice for design and implementation of secure computer/OS systems. Threat models, vulnerabilities, attacks compromise security, and advanced OS-level techniques for achieving security. Topics include OS security concepts and principles, seminal security in Multics, vulnerabilities in ordinary systems, secure capability systems, information flow control, mandatory access control, security kernels, memory protection, file system, virtual machine systems, hardware/architecture support (e.g., Intel SGX) for OS security, secure microkernel OSes (e.g., seL4, QNX), modern mobile operating systems (e.g., Android and iOS), and security from end-user perspective. Assignments include labs exploring and implementing the technologies in the context of the Linux, Android, and seL4 systems (some involving kernel programming). (Typically Offered: Spring)