CYBER SECURITY ENGINEERING (CYB E)

Courses primarily for undergraduates:

CYB E 230: Cyber Security Fundamentals
(Cross-listed with CPR E). (2-2) Cr. 3. F.
Prereq: COM S 227 or E E 285 or MIS 207.
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.

CYB E 231: Cyber Security Concepts and Tools
(Cross-listed with CPR E). (2-2) Cr. 3. S.
Prereq: CPR E 230 or CYB E 230
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.

CYB E 234: Legal, Professional, and Ethical Issues in Cyber Systems
(Cross-listed with CPR E). (3-0) Cr. 3. S.
Prereq: COM S 227, or E E 285, or MIS 207
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.

CYB E 331: Application of Cryptographic Concepts to Cyber Security
(Cross-listed with CPR E). Cr. 3. F.S.
Prereq: CPR E 231 or CYB E 231
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.