ALL COURSES

CYBERSECURITY

CSEC 1113: Introduction to Networking

Offered: Fall

Computer and communications networks are the very environment in which cyber operations are conducted. An understanding of these networks is essential to any discussion of cyber operations activities.

Specific topics to be covered to satisfy this knowledge unit must minimally include: Routing, network, and application protocols (TCP/IP (versions 4 and 6), ARP, BGP, SLL/TLS, DNS, SMTP, HTTP), network architectures, network security, wireless network technologies, network traffic analysis, protocol analysis (examining component-to-component communication to determine the protocol being used and what it is doing), and network mapping techniques (active and passive).

CSEC 1213: Wireless and Cellular Security

Offered: Spring

Prerequisite: CSEC 1113 Introduction to Networking

An overview of wireless and mobile security providing students with practical and theoretical experiences. Topics include threat analysis, security infrastructure, security services, wireless network security components. Topics include, but not limited to: overview of smart phone technologies, overview of embedded operating systems (e.g., iOS, Android), Wireless technologies (mobile: GSM, WCDMA, CDMA2000, LTE; and Internet: 802.00b/g/n), Infrastructure components (e.g., fiber optic network, evolved packet core, PLMN), Mobile protocols (SS7, RR, MM, CC), Mobile logical channel descriptions (BCCH, SDCH, RACH, AGCH, etch.), Mobile registration procedures, mobile encryptions standards, Mobile identifiers (IMSI, IMEI, MSIDN, ESN, Global Title, E.164), and Mobile and Location-based services.

CSEC 2113: Introduction to Information Systems

Offered: Fall

Prerequisite: CSEC 1113 Introduction to Networking

Introduction to the infrastructure of information technology and systems. Topics include computer hardware and software, communication and networks, databases, e-commerce technology, design and development of information systems, Cloud computing, information security, privacy, ethics, and social impact.

CSEC 2213: Network Forensics and Incident Response

Offered: Spring

Pre-requisite: CSEC 1113 Introduction to Networking

This course teaches the fundamentals of incident response and network forensics. An overview of operating systems will then lead to a systematic approach to incident response will be reviewed, focusing on a six step process (Preparation, Identification, Containment, Eradication, Recovery, Lessons Learned.) Network Forensics (tcpdump, Wireshark, nfsen,) and legal aspects of both investigation and preservation will be discussed.

CSEC 2223: Virtualization

Offered: Spring

Prerequisites: CSEC 1113 Introduction to Networking

Virtualization technology has rapidly spread to encompass workstations, servers, infrastructure devices, storage, and networks, and such has become critical to cyber operations. Specific topics to be covered in this knowledge unit must minimally include, but are not limited to: Virtualization techniques, Virtual machine architectures, uses of virtualization for: security, efficiency, simplicity, and resource savings (space, admin overhead).

CSEC 3113: Assembly Programming

Offered: Fall

Prerequisites: COMS 2104 and COMS 2903 Discrete Structures for Technical Majors

An introduction to the study of the basic structure and language of machines. Topics include basic concepts of Boolean algebra, number systems, language, addressing techniques, data representation, file organization, symbolic coding and assembly systems, using of macros, batch operation and job handling.

CSEC 3123: Cyber Defense I

Offered: Fall

Prerequisites:CSEC 2213 Network Forensics and Incident Response and CSEC 2223 Virtualization

This course introduces the fundamental principles of cyber defense. Topics covered include: security fundamental principles, vulnerability assessment, intrusion detection, cryptography protocols, network defense, trust relationships, and legal and ethical issues in computer security. A balance between theory and current practice will be presented. Topics to be covered include, but are not limited to: identification of reconnaissance operations, anomaly/intrusion detection, anomaly identification, identification of command and control operations, identification of data exfiltration activities, identifying malicious code based on signatures, behavior, and artifacts, networking security techniques and components (e.g., firewalls, IDS, etc.), cryptography (include PKI cryptography) and its uses in cybersecurity, malicious activity detection, system security architectures and concepts, defense in depth, and virtualization.

CSEC 3223: Programming Embedded Systems

Offered: Spring

Prerequisites: COMS 2213 Data Structures and CSEC 2223 Virtualization

The course involves the design, coding, debugging, and implementation of programs for securing embedded systems. Embedded software vulnerabilities and secure programming methods are introduced through hands-on projects. Buffer overflow attacks are discussed.

After completing the course content mapped to this knowledge unit, students will be able to develop programs that can be embedded into an OS kernel, such as a device driver, with the required complexity and sophistication to implement exploits for discovered vulnerabilities. Students will be able to write a program that implements a network stack to manage network communications.

CSEC 3233: Cyber Defense II

Offered: Spring

Prerequisite: CSEC 3123 Cyber Defense I

This course introduces penetration testing for the purposes of learning about cyber security vulnerabilities. Topics include: vulnerability taxonomies, buffer overflow attacks, password attacks, trust relationship exploitation, race condition exploitations, and local vs remote exploitations. The topics will be enhanced with hands-on examples using Linux.

CSEC 3243: Computer Architecture

Offered: Spring

Prerequisites: COMS 3703 Advanced Operating Systems, ELEG 2130 Digital Logic Design Lab, and ELEG 2134 Digital Logic Design.

Introduction to computer architecture. Aspects of computer systems, such as pipelining, memory hierarchy, and input/output systems. Performance metrics. Examines each component of a complicated computer system. Topics include: performance evaluation, instruction set architecture, machine arithmetic, data paths and pipelining, memory hierarchy, branch prediction, scheduling techniques, multiprocessors.

CSEC 4123: Applied Cryptography

Offered: Fall

Prerequisite: CSEC 3243 Computer Architecture

This course covers multiple cryptography protocols and their application to cybersecurity. Techniques in modern cryptography will be presented such as stream ciphers, DES, AES, block ciphers, etc. The course will discuss the level of security that various protocols provide and how to select an appropriate protocol for a specific application with an understanding of the limitations of key management systems, such as symmetric and asymmetric encryption, will be presented. Select protocols will be implemented in appropriate programming languages or systems.

CSEC 4133: Large Scale Distributed Systems

Offered: Fall

Prerequisite: CSEC 2223 Virtualization and junior standing in CSEC.

This course will provide an overview to large scale distributed systems. Topics include: concepts of distributed systems (threads, concurrency, dead/live lock, consistency, scalability, fault tolerant, etc.), design and development of large scale distributed systems (TCP/IP, UDP, networking data transfer, synchronization, threads, distributed locking, etc.), basic distributed algorithms that can be applied in practical systems, different kinds of cloud computing architecture models, services, and security issues, components (logical and physical) of cloud architecture, data paths within a given cloud design.

CSEC 4143: Building Secure Software

Offered: Fall

Prerequisite: CSEC 3243 Computer Architecture

This course introduces reverse engineering techniques in general and reverse engineering for software specification recovery, malware analysis, and communications in particular. Tools and hands-on lab exercises will be applied to safely perform static and dynamic analysis of software of unknown origin to fully understand the software's functionality, recover the software specification, and discover data used by the software.

CSEC 4153: Human Factors in Cybersecurity

Prerequisite: CSEC 3223 Programming Embedded Systems

This course will address the interaction of human behavior, cybersecurity controls, and the resulting security and privacy concerns. Topics covered in the class include: development and analysis of information security policies for user governance, ethical considerations of the impact of security policies on employee privacy, and security training and compliance for employees.

CSEC 4213: Information Systems Risk Management

Offered: Spring

Prerequisites: CSEC 2113 Introduction to Information Systems and CSEC 3233 Cyber Defense II

This course provides an overview for Information Security and Assurance to allow students to understand the key issues associated with protecting information assets, determining the levels of protection and response to security incidents, and designing a consistent, reasonable information security system, with appropriate intrusion detection and reporting features. Topics include but are not limited to: inspection and protection of information assets, detection of and reaction to threats to information assets, and examination of pre- and post- incident procedures.

CSEC 4233: Legal Issues in Cybersecurity

Offered: Spring

Prerequisite: Junior Standing in CS, IS, IT, or Cybersecurity
This course will provide a high-level explanation of the legal issues governing the authorized conduct of cyber operations and the use of related tools, techniques, technology and data. Both international and U.S. laws that operations in cyberspace must be in compliance, will be introduced. Specific topics to be covered in this knowledge unit must minimally include:
International Law: Jus ad bellum, United Nations Charter; Jus in bello, Hague and Geneva Conventions.
U.S. Laws: Constitution, Article I (Legislative Branch), Article II (Presidency), Article III (Judiciary), Amendment 4 (Search and Seizure), and Article 14 (Due Process); Statutory Laws: Title 10 (Armed Forces), Title 50 (Espionage and Covert Action), and Title 18 (Crimes) 18 USC 1030 (Computer Fraud and Abuse Act), 18 USC 2510-22 Electronic Communications Privacy Act, 18 USC 2701-12 Stored Communications Act, 18 USC 1831-32 Economic Espionage Acts.

CSEC 4240: Software Security Analysis and Reverse Engineering Lab

Offered: Spring
Co-requisite: CSEC 4243 Software Security Analysis and Reverse Engineering
This is a lab designed to support CSEC 4243 Software Security Analysis and Reverse Engineering.

CSEC 4243: Software Security Analysis and Reverse Engineering

Offered: Spring
Prerequisite: COMS 2213 Data Structures and CSEC 4143 Building Secure Software
To learn code analysis techniques and apply testing methodologies to detect the presence of loopholes or weaknesses of software and to determine the effectiveness of security controls that are implemented in the software.

CSEC 4293: Cybersecurity Capstone Project

Offered: Spring
Prerequisite: Departmental Approval
An integrative and intensive learning project which culminates the cyber security program during the senior year. Student will build on program course work to develop a strategic evaluation and plan for the management of secure information systems in an organization, either real or hypothetical. Student may use a start-up project as well. At the end of the project, the student will present their proposals or finding and recommendations to a panel of faculty and fellow students.