CYBS-CYBERSECURITY

CYBS 3113 Operating Systems Fundamentals 3 Credit Hours
Prerequisite: CYBS 3123. This course introduces major concepts and techniques for designing and implementing operating systems, including memory management, process management, information management, and computer security. Principles of performance evaluation. Class projects require the design and implementation of software systems. A UNIX family operating system will be used. (Sp)

CYBS 3123 Introduction to Unix Systems 3 Credit Hours
Prerequisite: C S 2413 and MATH 1914; and C S 2813 or MATH 2513. This course provides an introduction to the UNIX operating system. Topics include files and directories, electronic mail, security, advanced file systems, network utilities, network file sharing, text utilities, shell programming, regular expressions, UNIX internals, UNIX system administration, UNIX variations, and systems programming. Programming assignments involve the UNIX shell script language. (F)

CYBS 3213 Foundations of Cybersecurity 3 Credit Hours
Prerequisite: C S 2413, MATH 1914 and either C S 2813 or MATH 2513. This course introduces cybersecurity, principles, and technologies. It deals with security issues related to systems and software. Topics include cyber threats and vulnerabilities, information security frameworks and policies, cryptography, penetration testing, and in-depth defense. The goal is to develop a foundation for further study in cybersecurity. (F)

CYBS 3223 Applied Statistics for Computing 3 Credit Hours
Prerequisite: MATH 2423, course is not open to freshmen. This course is an introduction to basic statistical concepts and techniques with an emphasis on application to applied computing. Topics include basic properties of probability, a review of descriptive statistics, common discrete and continuous distributions of data, visualization of real data, hypothesis testing, parametric versus nonparametric tests, supervised and unsupervised learning methods, the bias-variance tradeoff, use of statistical packages. (F)

CYBS 3313 Introduction to Cyber Ethics and Law 3 Credit Hours
Prerequisite: Junior Standing. Legal and ethical issues with networked IT, including privacy, surveillance, digital piracy, and military use. First unit introduces ethical frameworks applicable to cybersecurity, sources of applicable law and regulation. Second unit introduces issues relating to cybercrime: intellectual property, user privacy, information assurance, and harmful online content. Third unit introduces issues with IT in government operations. (Sp)

CYBS 3323 Hardware Security 3 Credit Hours
Prerequisite: CYBS 3123 or concurrent enrollment in CYBS 3123. This course focuses on hardware (HW) security and covers security and trust from the HW perspective. It introduces students to HW components, including SoC and PCB, and examines security and trust issues in such HW components. Topics include digital lock, circuit theory, ASICs and FPGAs, HW security threats, malware, and attacks, along with specific countermeasures against HW attacks. (F)

CYBS 3440 Mentored Research Experience 3 Credit Hours
0 to 3 hours. Prerequisites: ENGL 1113 or equivalent, and permission of instructor. May be repeated; maximum credit 12 hours. For the inquisitive student to apply the scholarly processes of the discipline to a research or creative project under the mentorship of a faculty member. Student and instructor should complete an Undergraduate Research & Creative Projects (URCP) Mentoring Agreement and file it the with the URCP office. Not for honors credit. (F, Sp, Su)

CYBS 3743 Cyberforensics Fundamentals 3 Credit Hours
Prerequisite: CYBS 3213. This course introduces students to cyber forensics and cyber-crime scene analysis fundamentals. The various laws and regulations dealing with computer forensic analysis are discussed. Students are introduced to the emerging international standards for cyber forensic analysis and a formal methodology for conducting computer forensic investigations. (Sp)

CYBS 3813 Network Fundamentals 3 Credit Hours
Prerequisite: C S 2413, MATH 1914, and either C S 2813 or MATH 2513. Introduces the fundamentals of computer networks, including network architectures, network topologies, network protocols, layering concepts (for example, ISO/OSI, TCP/IP reference models), wired and wireless network protocols, communication paradigms (point-to-point vs. multicast/broadcast, connectionless vs. connection-oriented), and networking APIs (sockets). Protocols in all layers will be introduced. In this course, socket programming is also introduced. (Sp)

CYBS 3913 Database Fundamentals 3 Credit Hours
Prerequisite: C S 2413, MATH 1914, and either C S 2813 or MATH 2513. Introduction to the concepts behind relational database systems, modeling with Entity-Relationship diagrams and how these are used for data design. SQL to define, manipulate, and test the database, programmatic access, and practical issues. Strong foundation in database security, auditing principles, practices and methodologies. Topics: application security models, security architecture, access controls, auditing, trust management, privacy, threat vectors, and attack methods. (Sp)

CYBS 3990 Independent Study 1-3 Credit Hours
1 to 3 hours. Prerequisite: permission of instructor and junior standing. May be repeated once with change of content. Independent study may be arranged to study a subject not available through regular course offerings. (F, Sp, Su)

CYBS 4103 Engineering Secure Software 3 Credit Hours
Prerequisite: CYBS 3813 and CYBS 3913. This course covers topics at the intersection of security and software engineering. This course introduces software engineering processes and standards for building secure software applications. It discusses secure software life cycle development principles to include security in every phase. It also explores security issues and vulnerabilities in software applications due to a lack of secure software engineering processes. (F)

CYBS 4123 System Administration 3 Credit Hours
Prerequisite: CYBS 3123. This course provides a comprehensive introduction to system administration. Topics include virtualization, authentication and authorization, directory services, system management, and system security and to set up modern compute and storage clouds, networking systems, file systems, logging and analysis, and networking. Includes topics related to scripting for all administrative functions. Emphasis is placed on enterprise-level systems. (F, Sp)

CYBS 4133 Ethical Hacking and Penetration Testing 3 Credit Hours
Prerequisite: CYBS 3113. This course covers concepts related to ethical hacking and penetration testing methods to assess, exploit, and report security vulnerabilities on systems and their resources. The course will emphasize the ethical application of penetration testing methods and hacking tools. (F, Sp)

CYBS 4203 Cybersecurity Risk Management and Assessment 3 Credit Hours
Prerequisite: CYBS 3213. This course develops competency in information security policies and plans, including controls for physical, software, and networks. The course introduces security risk detection strategies, countermeasures, damage assessment, and control. The course introduces the students to performing information system risk analysis and management audits. Tools for analyzing log files of various kinds will also be introduced. (F)

CYBS 4293 Introduction to Cloud Computing and Security 3 Credit Hours
Prerequisite: CYBS 3113. Course covers the concepts behind cloud computing, including storage and computing. We will also learn about virtualization, software as a service, and deployment models. We will learn about cybersecurity risks on cloud infrastructure and countermeasures using access policies, distributed access control, key management, and others. Cover topics in the cloud computing security guidelines set forth in international standards organizations. (Sp)

CYBS 4323 IoT Security and Privacy 3 Credit Hours
Prerequisite: CYBS 3323. This course prepares students to securely develop and operate Internet of Things (IoT) devices considering security and privacy. The course covers concepts of IoT architectures with a focus on security and privacy issues. (F, Sp)

CYBS 4333 Incidence Response Management 3 Credit Hours
Prerequisite: CYBS 3123. This course provides a comprehensive treatment of cyber incidents and how to manage them, including understanding attacker motivation, attack methods, and the anatomy of the attacks. Additionally, topics related to incidence readiness, remote triage tools, memory analysis, malware analysis, disk forensics, network intrusion detection tools, and others will be discussed. (F, Sp)

CYBS 4473 Network Security 3 Credit Hours
Prerequisite: CYBS 3113. The course deals with understanding all aspects of cybersecurity that involve the network. Topics will include network transport-level security, wireless network security, electronic mail security, IP security, firewalls, VPNs, Secure HTTP, person-in-the-middle attack scenarios, and SSL/TLS and SSH (SP). Learn about various tools for analyzing network data at various levels of the TCP/IP stack and operating security operations centers. (F)

CYBS 4583 Machine Learning for Cybersecurity 3 Credit Hours
Prerequisite: CYBS 3213 and CYBS 3223. Various machine learning concepts, deep learning, time-series analysis, data mining, and other machine-learning concepts. Tools and libraries to analyze data sets, build predictive models, and evaluate the fit of the models. Common learning algorithms, including dimensionality reduction, classification, principal-component analysis, k-NN, k-means clustering, gradient descent, regression, logistic regression, regularization, multiclass data, algorithms, boosting and decision trees. Applies concepts to problems. (F, Sp)

CYBS 4883 Cryptography Fundamentals 3 Credit Hours
Prerequisite: CYBS 3213. This course introduces cryptography and its related tools. Specifically, in this course, cryptographic algorithms, protocols, and techniques will be introduced. The course will also introduce students to public key encryption, key exchange protocols, digital signatures, hashing-based encryption, and Data Encryption Standards. This course will also introduce cryptographic implementation in software and web application programming. (F)

CYBS 4953 Operating and Maintaining Cyber Ranges 3 Credit Hours
Prerequisite: CYBS 4473. Students will learn to use and build a cyber range for various assessments of threats and exploits. They will learn to build configurations for different business operations and the formation of red and blue team exercises. Students will have real-world experiences in handling situations without the real-world risk associated with practicing on live production equipment and systems. (Sp)

CYBS 4963 Cybersecurity Capstone 3 Credit Hours
Prerequisite: CYBS 4103 and Senior Standing. Provides the students with an experience to exhibit their knowledge and skills in all areas of cybersecurity. Students will work in small groups to identify and scope a cybersecurity problem and/or challenges. Required to write a proposal about their project and asked to create a work plan to develop solution to solve the problem/challenge. Create a final report and presentation. (Sp)