CYBERSECURITY (CYB)

CYB 500. Special Topics Cyber Security. 3 Credits.
Offered: Every year, Fall

CYB 501. Security I (Intro to Security Design). 1 Credit.
This course introduces students to fundamental security principles and good security design. Students discuss information assurance and cyber defense and gain an understanding of their role in providing system security.
Prerequisites: Take CYB 550.

CYB 502. Security II (Intro to Cyber Threats). 1 Credit.
This course introduces students to the analysis of cyber threats. Students learn to identify bad actors in cyberspace and compare and contrast their resources, capabilities/techniques, motivations and aversion to risk. Students learn to describe different types of attacks and their characteristics.
Prerequisites: Take CYB 501.

CYB 503. Security III (Intro to Cyber Defense). 1 Credit.
Students learn about potential system attacks and the actors that might perform them. Students learn to describe cyber defense tools, methods and components, and apply cyber defense methods to prepare a system to repel attacks.
Prerequisites: Take CYB 502.

CYB 504. Systems I (Systems Administration). 1 Credit.
This course introduces students to the configuration, installation and maintenance of a computer system. Strategies for successful administration from user management to auditing to backup strategies and processes are covered.

CYB 505. Systems II (IT Infrastructure). 1 Credit.
Students study the hardware components of modern computing environments and their individual functions. They learn about the types of hardware, and their interconnection, in a modern data center.
Prerequisites: Take CYB 504.

CYB 506. Systems III (Systems Programming). 1 Credit.
This course introduces students to various aspects of the design and implementation of a computer system. The final part of this three-course sequence focuses on systems-level programming. Topics include advanced shell scripting, the C programming language and the C system libraries.
Prerequisites: Take CYB 505.

CYB 509. Operating Systems Security (Processes). 1 Credit.
This course introduces students to operating systems, the software to support these systems and best practices to secure them. Topics include processes, storage and fundamental security design principles, rootkits, evasion techniques, in-memory attacks, persistence, process injection, and privilege escalation.

CYB 510. Operating Systems II (Storage). 1 Credit.
This course introduces students to operating systems and the software to support these systems. The second part of this four-course sequence focuses on memory and storage management. Topics include virtual memory, algorithms for page swapping, paging systems, file systems, directories and the handling of input and output on various devices.
Prerequisites: Take CYB 509.

CYB 511. Operating Systems III (Performance). 1 Credit.
This course introduces students to operating systems and the software to support these systems. The third part of this four-course sequence focuses on performance issues. Topics include virtualization, cloud-based computing, multiple-core systems, distributed processing and load balancing.
Prerequisites: Take CYB 510.

CYB 514. Theory of Computation I (Automata). 1 Credit.
This course introduces the classical theory of computer science. The aim is to develop a mathematical understanding of the nature of computing by trying to answer one overarching question: "What are the fundamental capabilities and limitations of computers?" The first part of this three-course sequence deals with finite automata and formal languages, answering the question: "How do we define a model of computation?

CYB 515. Theory of Computation II (Computability). 1 Credit.
This course introduces the classical theory of computer science. The aim is to develop a mathematical understanding of the nature of computing by trying to answer one overarching question: "What are the fundamental capabilities and limitations of computers?" The second part of this three-course sequence deals with computability, answering the question: "How do we prove that something cannot be computed?
Prerequisites: Take CYB 514.

CYB 516. Theory of Computation III (Compexity). 1 Credit.
This course introduces the classical theory of computer science. The aim is to develop a mathematical understanding of the nature of computing by trying to answer one overarching question: "What are the fundamental capabilities and limitations of computers?" The final part of this three-course sequence deals with complexity, answering the question: "What makes some problems so much harder than others to solve?
Prerequisites: Take CYB 515.

CYB 517. Cryptography I (Symmetric-Key Systems). 1 Credit.
This course introduces the methods of transmitting information securely in the face of a malicious adversary deliberately trying to read or alter it. The first part of this three-course sequence deals with classic cryptosystems, basic number theory, and modern symmetric-key systems such as the Data Encryption Standard (DES) and the Advanced Encryption Standard (AES).

CYB 518. Cryptography II (Public-Key Systems and Digital Signatures). 1 Credit.
This course introduces the methods of transmitting information securely in the face of a malicious adversary deliberately trying to read or alter it. The second part of this three-course sequence deals with public-key systems such as the RSA algorithm and discrete logarithm techniques, cryptographic hashing and digital signatures.
Prerequisites: Take CYB 517.

CYB 519. Cryptography III (Security Protocols and Advanced Topics). 1 Credit.
This course introduces the methods of transmitting information securely in the face of a malicious adversary deliberately trying to read or alter it. The final part of this three-course sequence deals with security protocols, cryptocurrencies, information theory, elliptic curves and error-correcting codes.
Prerequisites: Take CYB 518.

CYB 524. Database I (Relational Databases). 1 Credit.
This course introduces students to the theory, application and securing of database systems. The first part of this four-course sequence focuses on the relational database model. Topics include data modeling, relational database schema, the structured query language (SQL), and relational algebra and calculus.

CYB 525. Database II (Database Management Systems). 1 Credit.
This course introduces students to the theory, application and securing of database systems. The second part of this four-course sequence focuses on (relational) database management systems. Topics include the entity-relationship model, relational database design, database storage, database indexing and hashing and the processing and optimization of queries.
Prerequisites: Take CYB 524.

CYB 526. Non-relational Database Security. 1 Credit.
This course introduces students to the theory, application and security of non-relational database systems. It will focus on data management, query and security aspects of non-relational databases. Topics include a comparison between relational and nonrelational database models, NoSQL storage types for different databases such as MongoDB, Hadoop, Amazon DynamoDB, document-based databases and graph databases.
Prerequisites: Take CYB 524.

CYB 540. Networking I (Intro to Networking). 1 Credit.
This course introduces students to the theoretical and practical aspects of designing, creating, using and defending computer networks. The first part of this four-course sequence focuses on a basic introduction to networking and network layers. Topics include network models, network layers, programming at the application layer, the TCP/IP layer, routing algorithms, socket programming and packet sniffing.

CYB 541. Networking II (Networking Infrastructure). 1 Credit.
This course introduces students to the theoretical and practical aspects of designing, creating, using and defending computer networks. The second part of this four-course sequence focuses on the physical and data link layers. Topics include basic signal processing, wired/wireless transmission, multiplexing, the data link layer, error detection and correction, medium access control (MAC) sublayer, Ethernet, 802.11 wireless LANs, Bluetooth and RFIDs.
Prerequisites: Take CYB 540.

CYB 550. Cyber Policy. 3 Credits.
Students learn about the applicable laws and policies related to cyber defense and describe the major components of each pertaining to the storage and transmission of data. This course also covers responsibilities related to the handling of information about vulnerabilities, and how the type of legal dispute (civil, criminal, private) affects the evidence used to resolve it.

CYB 610. Operating Systems IV (Security). 1 Credit.
This course introduces students to operating systems and the software to support these systems. The final part of this four-course sequence focuses on OS security. Topics include threats and attacks on an OS, access control, use of cryptography in an OS, authentication, basic computer forensics, firewalls and other OS defenses.
Prerequisites: Take CYB 503 CYB 511 CYB 550.

CYB 625. Database IV (Database Security). 1 Credit.
This course introduces students to the theory, application and securing of database systems. The final part of this four-course sequence focuses on security issues involving database systems. Topics include database access controls, assessing access control, SQL injections, database inferences and database auditing.
Prerequisites: Take CYB 525 CYB 550.

CYB 640. Networking III (Intro to Network Defense). 1 Credit.
This course introduces students to the theoretical and practical aspects of designing, creating, using and defending computer networks. The third part of this four-course sequence focuses on basic network vulnerabilities and defense. Topics include network attacks such as man-in-the-middle, denial-of-service, and packet injections, message encryption, digital signatures and certificates, authentication, email with PGP, and remote access with SSH.
Prerequisites: Take CYB 541 CYB 550.

CYB 641. Networking IV (Advanced Networking Defense). 1 Credit.
This course introduces students to the theoretical and practical aspects of designing, creating, using and defending computer networks. The final part of this four-course sequence focuses on advanced network vulnerabilities and defense. Topics include firewall configuration, intrusion detection and prevention, port mapping, snort configuration rules, VPNs, e-commerce using SSL, and wireless network security (WEP, WPA, WPA2).
Prerequisites: Take CYB 640.

CYB 650. Cyber Operations. 1 Credit.
Students study the phases of a well-organized cyber operation and describe the goals and objectives of each phase. Emphasis is placed on identifying specific phases of a cyber operation in network traffic, and understanding potential motivations that might prompt an entity to perform a cyber operation.
Prerequisites: Take CYB 503 CYB 506.

CYB 660. Scripting for Investigations. 1 Credit.
This course covers the command line as a tool for data analysis for cyber investigations. Emphasis is placed on a basic set of tools that can be used individually or together to analyze and visualize data.
Prerequisites: Take BAN 610.

CYB 661. Programming for Security Automation. 1 Credit.
This course focuses on programming methods that are applicable to security automation. Students gain experience in automation using Python and Cloud native CLI to facilitate such tasks as automated code scanning; automated application scanning in testing and staging; automated network, server, container configuration checks; and continuous monitoring of development pipeline components and job scheduling.
Prerequisites: Take CYB 506.
Offered: Every year, Summer

CYB 662. Secure Web Applications Design. 1 Credit.
This course covers the design and architecture of secure web applications, such as: traditional three-tier architectures, SOA, microservices, FaaS; application protocols; authentication and session management; client and server-side controls; input-based vulnerabilities and web application attack trends.
Prerequisites: Take CYB 661.
Offered: Every year, Fall and Summer

CYB 663. Secure Web Application Engineering. 1 Credit.
In this course, students learn processes and practices needed to secure applications within the Software Development Life Cycle (SDLC). The course covers traditional SDLC processes and methods to secure modern Cloud native development processes and using concepts of DevSecOps.
Prerequisites: Take CYB 662.
Offered: Every year, Fall and Summer

CYB 664. Web Applications Security Testing. **1 Credit.**
This course will introduce students to web application security testing. Topics covered include application security metrics, selecting the right testing tool and integrating the results into the development life cycle. Students will gain hands-on experience using these tools in practical settings
Prerequisites: Take CYB 663;
Offered: Every year, Fall and Summer

CYB 665. Workforce Access Security. **1 Credit.**
This course focuses on authentication and user access technologies and practices within the enterprise. Topics include Active Directory services and architecture, and enterprise network access protocols.
Prerequisites: Take CYB 517.
Offered: Every year, Fall

CYB 667. B2C Access Security. **1 Credit.**
This course focuses on authentication and user access technologies and practices within B2C access. Topics include standards-based B2C authentication and access management protocols.
Prerequisites: Take CYB 665.
Offered: Every year, Fall

CYB 669. B2B Access Security. **1 Credit.**
This course will cover access concepts based on B2B communication APIs, such as standard-based protocols and B2B on-boarding, for mobile, social and IoT applications.
Prerequisites: Take CYB 667.
Offered: Every year, Fall

CYB 670. Embedded Device Security. **1 Credit.**
This course covers security as it pertains to the explosion of embedded devices embodied by the growth of the Internet of Things (IoT). Students learn about the specific security issues related to embedded devices.

CYB 680. Introduction to Cloud Security. **1 Credit.**
In this course, students learn fundamentals of Cloud computing and Cloud security. This course covers topics such as shared responsibility models for IaaS, PaaS, SaaS and FaaS, and Cloud Security Alliance CCM. Students will get hands-on experience creating secure systems within a commercial Cloud vendor environment.
Prerequisites: Take CYB 669.
Offered: Every year, Fall

CYB 681. Securing Workloads in AWS. **1 Credit.**
This course covers concepts and practices for securing AWS workloads. Students will be introduced to security controls, such as access controls using IAM, logging and auditing, and other AWS security services.
Prerequisites: Take CYB 680.
Offered: Every year, Fall

CYB 682. Securing Workloads in Azure. **1 Credit.**
This course covers concepts and practices for securing Azure workloads. Students will be introduced to security controls, such as access controls using IAM, logging and auditing, and other AWS security services.
Prerequisites: Take CYB 681.
Offered: Every year, Fall

CYB 683. Resilient System Design and Development. **1 Credit.**
This course introduces students to the concepts of secure system design and cyber resilience. The content of this course includes best security processes recommended in NIST 800-160 and techniques and technologies needed for secure system design and development.
Prerequisites: Take CYB 682.
Offered: Every year, Spring

CYB 684. Resilient System Testing. **1 Credit.**
This course introduces students to state-of-the-art concepts and methods to evaluate cyber resiliency. Topics include breach and attack simulation, configuration assessment and compliance. Hands-on experience with systems testing tools will be part of this course.
Prerequisites: Take CYB 683.
Offered: Every year, Spring

CYB 685. Operating Resilient Systems. **1 Credit.**
This course includes hands-on experience with tools for security activities such as intrusion detection and cloud security monitoring. Other topics this course covers include Site Reliability Engineering (SRE), maintaining situational awareness and dynamic threat.
Prerequisites: Take CYB 684.
Offered: Every year, Spring

CYB 691. Capstone I. **1 Credit.**
This course enables students to explore the computer security profession by working independently or in teams, under the guidance of a mentor, on a significant security-related project. In the first part of this two-course sequence, students review professional literature and explore security ethics, as they work to develop and present a capstone project proposal in written and oral form.
Prerequisites: By permission of director only.

CYB 692. Capstone II. **2 Credits.**
This course enables students to explore the computer security profession by working independently or in teams, under the guidance of a mentor, on a significant security-related project. In the second part of this two-course sequence, students complete work on their project and create an appropriate formal presentation of their results.
Prerequisites: Take CYB 691.