

CYBERSECURITY, ADVANCED CERTIFICATE

Program Director: Dr. Huihui Wang

Phone:

Email: hwang@sbu.edu

Code	Title	Credits
CYB-500A	COMPUTERS & CYBER WORLD	3
CYB-500B	INTRODUCTION TO PROGRAMMING	3
CYB-500C	INTRODUCTION TO DATABASES	3
CYB-500	COMPUTER NETWORKS	3
CYB-501	FOUNDATIONS OF CYBERSECURITY, ETHICAL HACKING, PENETRATION TESTING	3
Total Credits		15

CYB-500 COMPUTER NETWORKS (3 Credits)

A study of computer networks based on the OSI model of a layered network architecture. The TCP/IP protocol suite is used to illustrate network protocols. The course includes an overview of local area networks, routing algorithms, and network applications. The course consists of three lecture hours and one two-hour laboratory per week. The laboratory component provides experience in network programming using sockets.

Restrictions: RGP.123

CYB-500A COMPUTERS & CYBER WORLD (3 Credits)

Computer hardware and organization, number Systems, types of data, discrete mathematics and logic, algorithms, files and data structures, operating systems and compilers, virtual machines, Linux, security, privacy, threats, identity, introduction to technical, legal & policy issues in cybersecurity.

CYB-500B INTRODUCTION TO PROGRAMMING (3 Credits)

The course introduces the object-oriented approach to software design using a programming language such as Python, R or Java. The programming language is used to implement software designs. No previous programming experience is presupposed.

CYB-500C INTRODUCTION TO DATABASES (3 Credits)

An introduction to database management systems, including database design and application development. Different database models are introduced, with emphasis on the relational model. The theoretical principles underlying the design of a database and the physical storage of data and its integrity are covered. Other conceptual points are covered such as relations in mathematics that form the bases of a relational model. Along with designing and implementing databases using Sequel Server, the student will create a GUI interface to a database using JDBC and JavaFX.

CYB-501 FOUNDATIONS OF CYBERSECURITY, ETHICAL HACKING, PENETRATION TESTING (3 Credits)

To provide students with a fundamental understanding of cybersecurity and an in-depth understanding of penetration testing and ethical hacking. This course will include intelligence gathering, assessment of software vulnerabilities and weaknesses, cross platform penetration testing, learning ethical hacking requirements, and data protection.

Restrictions: RGP.123

CYB-502 ADVANCED CYBERSECURITY (3 Credits)

This course will expand on previous cybersecurity courses and delve deeper into its topics. Combining topics from computer science and cybersecurity, students will delve into system and network analysis, Diverse DDoS, DDoS and advanced persistent attacks, intrusion detection system development and control system. Students will be able to use quantitative and qualitative reasoning to solve problems with an array of different system vulnerabilities. Students will need knowledge of operating systems and advanced algebra before taking this course.

Restrictions: RGP.123

CYB-503 Enterprise Security (3 Credits)

This course will expand on previous cybersecurity courses and introduce business and enterprise topics. This will be done through analysis of real-world business examples of cyberattacks and the needs businesses have in the areas of cybersecurity. This course will emphasize real-world developmental practices and aim to improve students' ability to work in a professional cybersecurity environment.

Restrictions: RGP.123

CYB-504 CYBERSECURITY FORENSICS (3 Credits)

This course will give an in-depth look into the world of cybercrime and digital evidence. Throughout this course, students will use industry tools to perform forensic analysis of crimes to learn about how to prevent, detect, and respond to cyber-crime, cyber-terrorism, and cyber-predators. This course aims to both inform students of the types of crimes that exist as well as ways to catch those responsible even through virtual anonymity.

Restrictions: RGP.123

CYB-505 SECURE SOFTWARE DESIGN (3 Credits)

This course aims to establish an understanding of proper software design for a secure product. This course will do so by comparing both secure and insecure design structures to ensure that similarly made software programs are not vulnerable to known forms of cyberattacks or cybercrimes.

Restrictions: RGP.123

CYB-506 ENTERPRISE NETWORKS (3 Credits)

This course will build an understanding of how networks function within a business environment and the threats that face networks if they are not properly protected. Networks are a cornerstone of a modern business of any size, and thus these networks must be made to be secure in order to ensure that these companies can function properly.

CYB-507 APPLIED CRYPTOGRAPHY (3 Credits)

This course will help students understand the fundamentals of cryptography as well as the applications that it holds in modern technology. Cryptographic methods and tools, such as encryption and digital signatures, will be studied to understand how to protect information within a program. This course will also explore the differences between symmetric and asymmetric cryptography and the benefits to both.

Restrictions: RGP.123

CYB-508 APPLIED DATA MINING WITH APPLICATIONS IN CYBERSECURITY (3 Credits)

This course will help students understand the importance of data mining in the cybersecurity field and how to apply various data mining techniques. Students will learn about the fundamentals to data mining in general, growing their skills until they are able to later integrate data mining into cybersecurity applications and topics.

Restrictions: RGP.123

**CYB-509 MACHINE LEARNING WITH APPLICATIONS IN CYBERSECURITY
(3 Credits)**

This course will aim to enhance students' knowledge of the fundamentals of machine learning and how said technologies can be applied to cybersecurity. Different types of machine learning will be explored in the realms of cybercrime and cybercrime prevention.

Restrictions: RGP.123

CYB-510 Risk Management & System Hardening & PROTECTION (3 Credits)

This course will aim to teach students skills required to perform cyber risk management for organizations as well as how to prevent systems from being breached to begin with. There are risks that accompany all forms of system, this course will both give students the tools to identify possible risks that can be impactful in the future and how to manage breaches once they occur.

Restrictions: RGP.123

CYB-511 BLOCKCHAIN TECHNOLOGIES (3 Credits)

This course will aim to teach students skills required to understand the fundamentals of Blockchain technologies, common applications of the Blockchain technology, and the current state of blockchain technology as well as its future potential. This course will also help students gain a deep understanding of blockchain technology and mining of cryptocurrency.

Prerequisite(s): Take CYB-501

CYB-512 CLOUD SECURITY (3 Credits)

This course provides a practical explanation of both the principles and practice of cloud security by describing the cloud security architecture and exploring the guiding security design principles from the threat and CIA model viewpoint. In order to gain a thorough understanding of the design and development of secure cloud services we will examine industry standards and applied technologies for delivering and managing secure cloud-based services specially Google Cloud Platform (GCP). This course also covers protection and isolation of physical and logical infrastructures, identity management, access control, monitoring and auditing processes. Students also learn mitigation techniques for attacks at many points in a GCP-based infrastructure, including Distributed Denial-of-Service attacks, phishing attacks, and threats involving content classification and use.

Prerequisite(s): Take CYB-501