Master of Science in Cybersecurity

Syllabus for CYB770 Security Architecture

NOTE: This syllabus document contains the basic information of this course. The most current syllabus is available in the full course.

Course Description

Focuses on security architectures for the protection of information systems and data. Students completing this course can identify potential vulnerabilities in system architectures and design secure architectures. Topics include common enterprise and security architectures and their key design elements, such as secure cloud computing and virtualization infrastructures.

Prerequisite(s)

CYB 703

Course Materials

Program Outcomes

This course addresses the following competencies and program outcomes of the Masters of Science in Cybersecurity:

- Program Outcome 2: Interpret and analyze network protocols
- Program Outcome 3: Design, evaluate, and test systems including networks, computers, and hardware for security requirements
- Program Outcome 4: Implement best practices in secure software development
- Program Outcome 6: Assess security implications for emerging software technologies

Course Outcomes

Upon completing this course, you will be able to do the following:

1. Articulate the fundamentals of enterprise security architectures
2. Identify security requirements for an organization via business attribute profiling
3. Assess existing designs for security flaws and suggest improvements
4. Evaluate security implications for common system infrastructures, including cloud computing, IoT, and wireless networks
5. Define and apply security principles to security architecture design

Course Components

Discussions

Each module includes a discussion for students to explore an intriguing topic relevant to the module's central theme. Students are expected to address the discussion prompts completely by presenting multiple points of view, making connections with course materials, personal experiences, or external references, and contributing to meaningful conversation.

Labs

Three labs are designed for students to gain hands-on experiences in cloud computing, the Internet of Things (IoT), and wireless networks. To be specific, Lab 1 allows students to learn how to create and secure an AWS account and experiment with the different services AWS has to offer, For Lab 2, students will play with a (virtual) IoT device, configure it to access the cloud services provided by AWS, and dive deep into MQTT, a lightweight and widely adopted messaging protocol in IoT. For Lab 3, students will examine how a Wi-Fi device connects to a wireless network and how TLS sessions are negotiated.

Assignments

The assignments are given in modules 4 to 7 for students to reflect on security architecture and security architecture frameworks and apply the SABSA model to the design of a security architecture. For module 5, students will be writing an essay comparing different security architecture frameworks. For modules 4, 6, and 7, students will be working on a fictitious scenario to define security-related architecture principles, identify security requirements, and determine security services and security mechanisms that align with the business security requirements.

Grading

The following grading scale will be used to evaluate all course requirements and to determine your final grade:

Assignment	Points
7 Discussions @ 10pts	70
3 Labs (30, 50, 100)	180
4 Assignments (50, 50, 50, 100)	250
Total Points	500

Grade	Percentage Range
A	>94%
A-	>90%
B+	>87.5%
B	>85%
B-	>80%
C+	>77.5%
C	>70%
C-	>65%
F	<65%