Course number and name:	**CS 03570: Cyber Defense of Operating Systems and Networks**
Credits and contact hours:	3 credits / 3 contact hours
Instructor's or course coordinator's name:	H. Alex Alborzfard
Text book, title, author, and year:	None

.

Specific course information

Catalog description: This course covers an in depth look on the role of operating system security, its basic functions, and the services it provides related to cyberattacks. Students will become familiar with typical network cyberattacks and their defenses as well as how these attacks can influence the behavior of an operating system. Students will also learn how to assess the security capabilities of a computing system using some standard evaluation criteria (such as the Trusted Computer System Evaluation Criteria used by the Department of Defense). Students will then learn to improve the robustness of an operating system by applying methods related to managing applications, services and network ports to harden an operating system. At least one open source operating system's capabilities will be studied as it relates to the chosen standard evaluation criteria.

Prerequisites: None

Type of Course: ☒ Required (MSCybSec) ☒ Elective (MSCS) ☐ Selected Elective

Specific goals for the course:

1. Become familiar with typical network cyberattacks and their defenses as well as how these attacks can influence the behavior of an operating system.

2. Learn how to assess the security capabilities of a computing system using some standard evaluation criteria (such as the Trusted Computer System Evaluation Criteria used by the Department of Defense).

3. Learn to improve the robustness of an operating system by applying methods related to managing applications, services and network ports to harden an operating system.

Required List of Topics to Be Covered:

1. Operating System Concepts
2. Operating System Hardening
3. Basic Networking
4. Network Defense Forensics