CYBER SECURITY MINOR

The minor is intended for students studying computer engineering, computer science, software engineering, or management information systems with the goal of enabling them to work in cyber security. The minor consists of a series of lab based courses that are designed to provide students with both the technical background and the hands-on experiences along with the theoretical background to allow them to compete for jobs in cyber security.

The minor requires 15 credits, including no more than 6 credits used to meet any other department, college, or university requirement. Below is the list of courses used in the minor.

Core		
CPR E 230	Cyber Security Fundamentals	3
CPR E 231	Cyber Security Concepts and Tools	3
CPR E 431	Basics of Information System Security	3
Plus one of the following (3-4 cr.)		3
CPR E 308	Operating Systems: Principles and Practice	
COM S 252	Linux Operating System Essentials	
COM S 352	Introduction to Operating Systems	
Electives-one of the following:		3
CPR E 419	Software Tools for Large Scale Data Analysis	
CPR E 430	Network Protocols and Security	
Total Credits		15

Objectives

The minor in cyber security is designed to prepare students with the technical skills for entry into cybersecurity positions in industry or government agencies.

A few years after graduation, students completing the cyber security minor should be:

1. Contributing to their communities and society in the area of cyber security technology and applications and demonstrating an understanding of contemporary security issues, both technological and societal.
2. Advancing in their careers through application of their knowledge of cyber security
3. Working effectively as team members and demonstrating ethics and responsible behavior
4. Applying cyber security methods and concepts to the general area of their BS degree
5. Continuing their professional development through life-long learning

Learning Outcomes

After earning the minor in cyber security students will

1. Demonstrate the ability to apply knowledge of cyber security concepts, tools and technologies to computer systems.
2. Understand cyber security risks, threats and countermeasures and apply this understanding to develop cyber defense strategies.
3. Demonstrate the ability to design cyber security systems to meet organizational needs within realistic constraints such as economic, environmental, social, and ethical expectations.
4. Demonstrate the ability to function on teams.