GRADUATE COMPUTER SCIENCE CYBERSECURITY CERTIFICATE

Certificate Requirements

The School of Computing is responding to its industry need for a skilled workforce in Cybersecurity.

Cybersecurity requirements for critical infrastructure continues to be vital for the US national defense and health of our national economy. Continued attacks, such as ransomware, against these systems requires advanced educational training to stay ahead of such threats. The goal of the graduate computer science cybersecurity certificate is to ensure educational relevancy in the identification and defense of current cyber threats to critical infrastructure. The certificate includes course options in Artificial Intelligence (AI) and Machine Learning (ML) as these have been deemed critical to the advancement of cybersecurity, to include using AI/ML for cybersecurity as well as the security of the AI/ML systems themselves. The included courses delve into the theory and mathematical foundations as well as hands-on components focused on security at both a software and hardware level.

This certificate can be completed by both graduate-level degree and non-degree seeking students that have completed an appropriate computer science or computer engineering undergraduate degree. We provide a choose five-of-eight approach as some of these courses may have be previously taken as cross-listed undergraduate courses and the proposed graduate certificate requires 15 graduate credits.

Code	Title	Hours
Choose 5 of the following courses		15
CSC 510	Compiler Design-Construction	
CSC 516	AI Theory and Programming	
CSC 526	Data Mining	
CSC 550	Surreptitious Software	
CSC 560	Security of HW Implementations	
CSC 582	Network Security	
CSC 585	Cyber-Physical Security	
MA 581	Cryptography	
or CSC 580	Data Security	
Total Hours		**15**