

CYBERSECURITY ENGINEERING, MASTER OF ENGINEERING (M.ENG.)

Non-thesis only: 30 credits

The student must complete 30 credits of approved coursework with an average grade of B. The coursework, which allows up to 12 credits at the 400-level, must be approved by the program's departmental faculty advisor.

All Professional Master of Engineering Programs consist of 10 courses/30 credits. All students are expected to complete a preliminary course plan for their intended degree program. Degree planning worksheets can be found here: <https://advancedengineering.umd.edu/degree-planning-sheets> (<https://advancedengineering.umd.edu/degree-planning-sheets/>)

Course	Title	Credits
Required course:		3
ENPM691	Hacking of C programs and Unix Binaries (Programming in C for Cybersecurity Applications)	
Choose three of the following core courses:		9
ENPM685	Security Tools for Information Security	
ENPM686	Information Assurance	
ENPM693	Network Security	
ENPM694	Networks and Protocols	
ENPM695	Secure Operating Systems	
Choose at least two of the following electives:		6
ENPM687	Digital Forensics and Incident Response	
ENPM697	Secure Software Testing and Construction	
ENPM809	Special Topics in Engineering (ENPM809A - Applied Cryptography)	
ENPM809	Special Topics in Engineering (ENPM809I - Embedded Systems Hacking and Security)	
ENPM809	Special Topics in Engineering (ENPM809J - Cloud Security)	
ENPM809	Special Topics in Engineering (ENPM809K - Fundamentals for Artificial Intelligence and Deep Learning Framework)	
ENPM809	Special Topics in Engineering (ENPM809V - Bitcoin and Cryptocurrency Technologies)	
ENPM808	Advanced Topics in Engineering (ENPM8080 - Intrusion Detection: From Theory to Practice)	
Remainder of electives chosen with advisor		12
Total Credits		30