CYBERSECURITY

(Department of Computer Science)

Cybersecurity is a computing-based discipline that involves the creation, operation, analysis, and testing of secure systems, networks, and applications to protect against a variety of digital threats. The cybersecurity curriculum is based on national standards and builds on a computer science foundation. The curriculum emphasizes four main areas of cybersecurity: information security, software security, network security, and system security. Mindful of the rapid changes in technology, the curriculum seeks to prepare students for lifelong learning to enable them to meet future challenges. A student expecting to major in cybersecurity should complete CSCI 111 and CSCI 112 in the first year.

Capstone experiences offered by the Department of Computer Science include CSCI 401, CSCI 403, and CSCI 485, all of which are available to majors in cybersecurity.

- Cybersecurity Major (https://catalog.rmc.edu/programs/cybersecurity/cybersecurity-major/)
- Cybersecurity Minor (https://catalog.rmc.edu/programs/cybersecurity/cybersecurity-minor/)

CSEC 121 - Privacy and Security (3 Hours)
This course explores how the concepts of privacy and security have changed with the emergence of personal computers, tablets, and smartphones. Students will learn to leverage the benefits of emerging technologies and applications while understanding the impacts on their personal security and privacy. Students will also develop a working knowledge of the ethical issues related to emerging technologies and social media applications and research issues related to personal privacy, freedom of expression, and respecting and protecting intellectual property. C21:CL,NS,WA.
Curriculum: CL,NS,WA

CSEC 222 - Computer and Data Security (3 Hours)
This course introduces the fundamental security principles and techniques for securing both computers and data to protect against unauthorized access and malicious attacks. Topics include data integrity and availability, identification and authentication, authorization and access control, encryption and cryptanalysis, cryptographic tools, database security, log files and auditing, and malware. Prerequisities: CSCI 111 and CSEC 121.

CSEC 238 - Security Policy (3 Hours)
This course provides an introduction and overview of computer security policy topics, with a focus on understanding the fundamental concepts of policy development, risk assessment, and incident response. Topics will include cybersecurity policy and governance, risk management, asset management and loss prevention, operations security, incident response, business continuity management, regulatory compliance, and the acquisition and maintenance of software and hardware systems.
Prerequisite(s): CSEC 121

CSEC 322 - System Security and Defense (3 Hours)
This course explores the principles and techniques for securing hardware and software systems and detecting and recovering from malicious software and network attacks. Topics include an in-depth study of network and malware attacks, the techniques used to defend against attacks, intrusion detection, penetration testing, system recovery, and tools for assessing system vulnerabilities. A closed sandbox computer and network lab is used to simulate and study various network attacks.
Prerequisite(s): CSCI 330 and CSEC 121

CSEC 323 - Software Security (3 Hours)
This course introduces the fundamentals of designing and developing secure software that reliably protects the information it stores and the systems on which it is used. Topics include open design, least privilege, static and dynamic testing, integration testing, specification of security requirements, validating input, use of security features, patching, and assurance documentation.
Prerequisite(s): CSEC 222 and either CSCI 212 or CSCI 213

CSEC 353 - Cryptography (3 Hours)
Cryptography is the study of secure communication and has become essential to protecting sensitive information in a world with constant data transfer. This course covers classical cryptography which focuses on encryption, and modern cryptography which relies on computationally difficult problems to make systems unbreakable in practice. Topics include stream and block ciphers, the Advanced Encryption Standard, public-key cryptosystems, digital signatures, and known attacks for the algorithms covered. C21:CC.
Prerequisite(s): ENGL 185 and either CSCI 212 or CSCI 213

Curriculum: CC

CSEC 381 - Special Topics in Cybersecurity (3 Hours)

CSEC 382 - Special Topics in Cybersecurity (3 Hours)

CSEC 457 - Internship in Cybersecurity (Paid) (3 Hours)
With prior approval students may earn Experiential Cross Area Requirement (CAR) credit and transcript notation for three credit hours for a paid internship. To qualify for experiential credit a student must have completed 48 semester hours of work prior to the beginning of the internship and be in good academic standing (not on academic probation) at the time of application and at the start of the internship. Registration and application procedures are similar to those for academic internship courses. Satisfactory completion of a paid internship requires at a minimum 130 hours (160 recommended) working at the host site, a reflective daily journal, final written report, and satisfactory evaluation from the site supervisor. C21:EL .
Curriculum: EL