CYBR - CYBERSECURITY

CYBR 2159 Fundamentals of Computer Networks (3-0-3)
This course provides students with a comprehensive overview of the technologies and standards that make the modern connected world a reality. Requiring no previous knowledge of computer networking, this course takes students on a tour of the building blocks of modern-day networks. Major concepts, such as OSI and TCP/IP models, network media specifications and functions, LAN/WAN protocols, topologies, and capabilities, are covered in detail. Industry standards and a brief historical development of major networking technologies are surveyed in conjunction with basic awareness of software and hardware components used in typical networking and internetworking environments.
Prerequisite(s): CPSC 1301 with a minimum grade of C or CPSC 1301H with a minimum grade of C or CPSC 1301K with a minimum grade of C or CPSC 1301I with a minimum grade of C or CSCI 1301 with a minimum grade of C or CSCI 1301K with a minimum grade of C

CYBR 2160 Intro to Information Security (3-0-3)
This course introduces the main hardware and software components of a modern computer system, investigates the vulnerabilities and threats associated with each component, and suggests prudent measures to defend against these threats
Prerequisite(s): CYBR 2159 (may be taken concurrently) with a minimum grade of C

CYBR 3106 Cybersecurity Risk Management (3-0-3)
This course provides an overview of the management of information systems security and its implications on IT infrastructures and compliance. From risk identification to mitigation, it covers the main steps in risk management with a focus on security and introduces students to the National Institute of Standards and Technology's (NIST) risk management and security frameworks. It includes the topics of business continuity plan, disaster recovery plan, and computer incident response plan as ways of mitigating security risks in a business.
Prerequisite(s): CYBR 2106 with a minimum grade of C or CYBR 2160 with a minimum grade of C or CPSC 2106 with a minimum grade of C

CYBR 3108 Defensive Programming (3-0-3)
This course provides a study of basic security practices in hardening a system and programming through hands-on activities. The course emphasizes secure design principles and applying additional controls and measures to prevent development of vulnerable systems and code.
Prerequisite(s): (CPSC 2106 with a minimum grade of C or CYBR 2106 with a minimum grade of C) and CPSC 2108 with a minimum grade of C

CYBR 3115 Programming for Data Science (3-0-3)
This course provides an introduction to using programming to manipulate data, a fundamental skill in both computer science and data science. Students will learn to write and modify scripts and programs to import data from local files and the Internet from a variety of storage formats such as csv files, text files, XML files, and relational databases and manipulate the data programmatically using a variety of data structures. Students will learn introductory data visualization techniques as well as get an introduction on how to use AI and statistics to analyze data.
Prerequisite(s): CPSC 1301 with a minimum grade of C or CPSC 1301H with a minimum grade of C or CPSC 1301K with a minimum grade of C

CYBR 3119 Fundamentals of Digital Forensics (3-0-3)
An introduction to various Computer Forensics tools and analysis methodologies in a variety of standalone and networked computer environments with Windows Operating System
Prerequisite(s): (CYBR 2106 with a minimum grade of C or CYBR 2160 with a minimum grade of C) or CPSC 2106 with a minimum grade of C

CYBR 3126 Client / Server Security (3-0-3)
This course explores the concept of controlling access to information systems and applications. Topics include access, authentication and accounting for end-users and system administrators, and security controls for access control including tokens and public key infrastructures (PKIs).
Prerequisite(s): CYBR 3135 with a minimum grade of C

CYBR 3128 Cybersecurity Management (3-0-3)
This course provides an overview of the management of information systems security including access control systems and methodology, business continuity and disaster recovery planning, legal issues in information systems security, ethics, computer operations security, physical security and security architecture models using current standards and models. The course also explores network infrastructure, cryptography, assessments and audits, and organizational security.
Prerequisite(s): MISM 3115 with a minimum grade of C or MISM 3109 with a minimum grade of C or (CPSC 2115 with a minimum grade of C and CYBR 2159 with a minimum grade of C)

CYBR 3135 Infrastructure Security (3-0-3)
Security challenges encountered on backbone networks in an information and communications infrastructure. Topics include methods of tightening infrastructure security, a variety of tools for monitoring and managing infrastructure security and commonly-used technologies, such as firewalls, IDS, IPS and VPNs
Prerequisite(s): CYBR 2159 with a minimum grade of C and (CYBR 2160 with a minimum grade of C or CYBR 2106 with a minimum grade of C)

CYBR 3136 Wireless, IoT and Mobile Security (3-0-3)
This course explores the world of wireless and mobile devices that is evolving day-to-day, with many individuals relying solely on their wireless devices in the workplace and in the home. This course provides step-by-step real-life, advanced scenarios of performing security assessments of wireless networks and how to perform security posture assessments of Internet of Things (IoT) technologies and solutions. The student will learn how to perform security posture assessments of mobile devices, such as smartphones,
Prerequisite(s): CYBR 2159 with a minimum grade of C and (CYBR 2160 with a minimum grade of C or CYBR 2106 with a minimum grade of C)

CYBR 4125 Global Perspectives on Cybersecurity (3-0-3)
This course is designed to prepare students to think broadly on the nature of international relations and national security aspects of cyberspace. This includes, but is not limited to, cyber warfare and intelligence gathering activities, international agreements and domestic policies pertaining to cyberspace, the difference between cyber terrorism and cybercrime, data privacy, location, protection, ownership and retrieval issues in the US versus abroad, and how governments respond to cyberattacks. Students should take away from the
Restriction(s):
Freshman, Sophomore or Junior students may **not** enroll.

CYBR 4127 Computer and Network Security (3-0-3)
This course is a basic introduction to the issues of software security with a focus on raising the students' awareness of the difficulties of maintaining a secure software environment. It reviews traditional security techniques and discusses the vulnerabilities of such methods. The course emphasizes well-written software as a prerequisite to network security and highlights security implications of common programming mistakes.
Prerequisite(s): (CYBR 2160 with a minimum grade of C or CYBR 2106 with a minimum grade of C) and CYBR 2159 with a minimum grade of C

CYBR 4128 Penetration Testing and Countermeasures (3-0-3)
This course explores hacking techniques and countermeasures. Topics include network systems penetration tools and techniques for identifying vulnerabilities and security holes in operating systems and software applications. Students will practice ethical hacking procedures to attempt unauthorized access to target systems and data, and incident handling procedures in the case of an information security compromise.
Prerequisite(s): CYBR 2160 with a minimum grade of C or CPSC 2106 with a minimum grade of C

CYBR 4137 Security Policies & Implementation Security (3-0-3)
This course explores security policies that protect and maintain an organization's network and information systems assets. Topics include the effects of organizational culture, behavior and communications styles on generating, enforcing and maintaining security policies.
Prerequisite(s): CYBR 2160 with a minimum grade of C or CYBR 2106 with a minimum grade of C

CYBR 4138 Security Auditing for Compliance (3-0-3)
This course examines principles, approaches and methodology used in auditing information systems security to ensure processes and procedures are in compliance with pertinent laws and regulatory provisions.
Prerequisite(s): CYBR 2160 with a minimum grade of C or CYBR 2106 with a minimum grade of C

CYBR 4139 Security Issues in Legal Context (3-0-3)
This course will provide students exposure to the current key legal and policy issues related to cybersecurity, including the legal authorities and obligations of both the government and the private sector with respect to protecting computer systems and networks, as well as the national security aspects of the cyber domain including authorities related to offensive activities in cyberspace.
Prerequisite(s): CYBR 2160 with a minimum grade of C or CYBR 2106 with a minimum grade of C

CYBR 4145 Security for Web Applications & Social Networking (3-0-3)
In this course, students will analyze security implications of information exchange on the Internet and via Web-based applications. Topics include methods and techniques to identify and countermeasure risks, threats and vulnerabilities for Web-based applications, and to mitigate risks associated with Web applications and social networking.
Prerequisite(s): CYBR 3135 with a minimum grade of C

CYBR 4146 Network, Virtualization & Cloud Communication Infrastructure (3-0-3)
This course explores the convergence of computer networking, telecommunications technologies, virtualization, cloud and the Internet of Things (IoT). Capabilities and limitations of converged networking infrastructure are analyzed through voice, data, video, cloud and IoT applications in relation to performance, management and security challenges.
Prerequisite(s): CYBR 2160 with a minimum grade of C or CYBR 2106 with a minimum grade of C

CYBR 4160 Applied Cryptography (3-0-3)
This course features a rigorous introduction to modern cryptography, with an emphasis on the fundamental cryptographic primitives of symmetric and public-key encryption, basic cryptanalysis, hash functions, and digital signatures.
Prerequisite(s): CPSC 2108 with a minimum grade of C and (CYBR 2160 with a minimum grade of C or CYBR 2106 with a minimum grade of C)

CYBR 4166 Intrusion Detection and Prevention (3-0-3)
The capstone course delivers the tenets of intrusion detection and prevention, specifically focus on stepping-stone intrusion detection and prevention. Intrusion detection focuses on the methods to detect attempts (attacks or intrusions) to compromise the confidentiality, integrity or availability of an information system. Intrusion prevention focuses on the techniques to block such intrusions. It includes host-based intrusion detection, network-based intrusion detection, network traffic sniffing tools, stepping-stone intrusion detection, packet round-trip time, detection performance management, hackers' evasion techniques, and attacks via The Onion Router (TOR).
Prerequisite(s): CYBR 4127 with a minimum grade of C or CPSC 4127 with a minimum grade of C

CYBR 4416 Cybersecurity Practicum (0-2-1)
This course engages students in experiential opportunities to enhance their knowledge of current topics and job opportunities in the fast changing field of cybersecurity. The course will require students to participate in a variety of activities to obtain a broader perspective of the cybersecurity landscape.
Repeatability: Repeatable for credit up to 2 times or 3 hours.
Restriction(s):
Freshman or Sophomore students may **not** enroll.

CYBR 6000 Graduate Exit Examination (0-0-0)
This is a zero-credit hour course that should be taken in the last semester prior to graduation. It is designed to prepare MS Cybersecurity students for graduation. (S/U grading).
Restriction(s):
Enrollment is limited to Graduate Level level students.

CYBR 6126 Introduction to Cybersecurity (3-0-3)
This course focuses on the protection of information systems against cyber threats whether data is in transit, at rest, or in processing. Topics include an overview of cyber threats, measures necessary to detect, assess, and counter such threats, network security basics, symmetric and public key encryption, basic cryptologic analysis, access control, authentication, malware, vulnerability assessment, digital forensics, security policies, privacy, and ethics. This course builds knowledge, skills and abilities (KSAs) of principles and practices in cybersecurity.
Restriction(s):
Undergraduate Level level students may **not** enroll.

CYBR 6128 Network Security (3-0-3)
This course covers the fundamentals of application and Web security, computer and network security, attacking and defending mechanisms. After completing this course, students will understand the issues of application and Web security, computer and network security. Students should be able to explain the underlying security protocols and techniques, such as IPsec and SSL/TLS. Students will also examine the methods and tools to attack and defend a computer network, including network reconnaissance, exploits, firewalls, and IDS. Some advanced topics such as wireless security, switch security, router security, and IPv6 security are covered as well.
Prerequisite(s): (CPSC 6126 with a minimum grade of C or CYBR 6126 with a minimum grade of C) and CPSC 6157 with a minimum grade of C

CYBR 6136 Human Aspects of Cybersecurity (3-0-3)
This course examines the human behavioral and psychological aspects that create a complex system of cybercrimes and ethical and moral violations in the Internet. Students analyze various cybercrimes and cyber incidents that impact human life, and discuss how the human factor can be controlled or manipulated in order to create a more secure cyberspace.
Prerequisite(s): CPSC 6126 with a minimum grade of C or CYBR 6126 with a minimum grade of C

CYBR 6159 Digital Forensics (3-0-3)
The course focuses on the role of computer forensics and the methods used in the investigation of computer crimes. The course explains the need for proper investigation and illustrates the process of locating, handling, and processing computer evidence.
Prerequisite(s): CPSC 6126 with a minimum grade of C or CYBR 6126 with a minimum grade of C

CYBR 6167 Cybersecurity Risk Management (3-0-3)
This course focuses on the risk analysis component of cybersecurity management. It provides detailed coverage of contemporary frameworks and processes related to managing risk. Also, it involves enumerating organizations' resources and prioritizing their protection based on probability of threat and subsequent damage. Reporting security breaches to management, and providing steps to mitigate threats and implement future controls will be an integral part of this course.
Prerequisite(s): CPSC 6126 with a minimum grade of C or CYBR 6126 with a minimum grade of C

CYBR 6222 Foundation of Cybersecurity Policy and Management (3-0-3)
This course provides students with an introduction to information security policies. Students will be introduced to sociological and psychological issues in policy implementation in general and then provided a focused dialogue on information security specific policies. The class discusses the entire lifecycle of policy creation and enactment and presents the students with issue specific policies in different domains of security. The structure of the policy is also discussed to assist the students to design and modify policies. Several examples from different domains are incorporated in the curriculum to assist the students learn in context of real life situations.
Restriction(s):
Enrollment is limited to Graduate Level level students.

CYBR 6226 Cloud Computing Security (3-0-3)
This course focuses on the security concerns and countermeasures in a cloud environment. Topics include an overview of cloud computing and virtualization, the critical technology underpinning cloud computing, necessary foundation for threats in cloud computing, access control, identity management, account and service hijacking, secure APIs, malware, regulatory compliance, forensics, and secure computing in the cloud.
Prerequisite(s): CPSC 6157 with a minimum grade of C

CYBR 6228 Global Cybersecurity (3-0-3)
This course provides an in-depth study of cybersecurity from a global perspective. Topics include cyber-terrorism, cybercrime, and cyber-warfare; the international legal environment; nation- and region-specific norms regarding privacy and intellectual property; international standard setting; effects on trade (including offshore outsourcing); and opportunities for international cooperation.
Prerequisite(s): CPSC 6126 with a minimum grade of C or CYBR 6126 with a minimum grade of C

CYBR 6299 Capstone in Cybersecurity Policy and Management (0-0-3)
This course will provide students with the opportunity to integrate concepts and competencies learned in the Cybersecurity Management (MS) program into a single project. The student will propose, research and produce a deliverable as part of a comprehensive project. With instructor approval, the project may be undertaken as an internship/co-op at a company, including the student's workplace, under a mentor within the company, provided it goes beyond the scope of the student's normal work duties. Students should have successfully completed at least 9-credit hours in the program to enroll in the course.
Repeatability: Repeatable for credit up to 1 times or 6 hours.

CYBR 6985 Cybersecurity Research and Thesis (0-0-(1-3))
This course involves the completion of a research project in adherence to the School of Computer Science MS thesis policy. The project is to be designed in consultation with a thesis advisor who is a member of the graduate faculty of the School of Computer Science. (S/U grading)
Restriction(s):
Enrollment is limited to Graduate Level level students.

CYBR 6986 Thesis Defense (0-0-0)
Department approval required. A satisfactory grade in the course indicates a successful oral defense of the thesis, the completion of edits and approval by the advisor or committee, and submission to the library. Degree candidates must be enrolled during the semester of their defense. S/U grading.
Restriction(s):
Enrollment is limited to Graduate Level level students.