RIT | Department of Cybersecurity

CSEC MS Course Descriptions

CSEC 600 - Introduction to Computing Security (Bridge)
This is a graduate-level introduction to the field of cybersecurity An extensive overview of various branches of computing security areas will be presented including concepts, issues, and tools that are critical in solving problems in the cybersecurity domain. Students will have the opportunity to learn essential techniques in protecting systems and network infrastructures, analyzing and monitoring potential threats and attacks, and devising and implementing security solutions for organizations large or small. (This is a bridge course, and cannot be taken as an elective course)

CSEC 603 - Enterprise Security (AE)
This course is designed to provide students with the advanced concepts needed to establish network security strategies to ensure adequate protection for the corporate environment and yet provide accessibility for the corporate community.

CSEC 604 - Cryptography and Authentication (Core)
In this course, students will gain in-depth knowledge of cryptography and authentication. Students will explore various cryptographic algorithms and authentication protocols, focusing on their design and implementation. Students will also work on a research or implementation project, based on cryptographic algorithms and/or authentication protocols. The applications of cryptography and authentication in the areas of computer networks and systems will also be investigated. This course requires prior knowledge in Discrete Mathematics.

CSEC 620 - Cyber Analytics and Machine Learning (AE)
The course provides students an opportunity to explore methods and applications in cyber analytics with advanced machine learning algorithms including deep learning. Students will learn how to use machine learning methods to solve cybersecurity problems such as network security, anomaly detection, malware analysis, etc. Students will also learn basic concepts and algorithms in machine learning such as clustering, neural networks, adversarial machine learning, etc. A key component of the course will be an independent exploratory project to solve a security program with machine learning algorithms. Students taking this course should have knowledge in Discrete Math, Probability and Statistics, and Linear Algebra. Students should also be able to program in Python.

CSEC- 622 - Side Channel Analysis (AE)
Side-channel analysis (SCA) is an offensive security technique that targets not the formal description of a security-critical system, but the implementation of it. Examples of side channels include—but are not limited to—latency measurements, power consumption, electro-magnetic radiation, and acoustic emanations. This is a young but very active field within applied computer security. Modern processors are equipped with numerous features to improve the average performance of software, including—but not limited to—low-latency execution pipelines, various caches, prediction, speculative execution, and multi-layered parallelism. These mechanisms can often be used as side channels to attack implementations of security-critical systems by using leakage to recover critical data or state that should remain secret. This course provides an overview of these modern SCA concepts, explains how to establish and construct these channels, demonstrates how to apply SCA techniques, and furthermore basic methods to prevent them. Students will also be exposed to current literature covering research in side-channel analysis. Students will program in C and need a strong understanding of the design of modern computer architectures.

CSEC 630 – Trusted Computing (AE)
This course covers some of the foundational technologies for establishing trust in modern computing systems, including classic methods (e.g., boot chain-of-trust, secure boot, exception/privilege levels, and Trusted Platform Modules – TPMs) and more recent trusted computing architectures such as ARM TrustZone and Intel Secure Guard eXtensions (SGX), which are increasingly popular and widely adopted in both academic research and industry. The latter part of the course will touch upon more advanced and research-oriented aspects in the intersection of trusted computing and various realms of Computing Security & Privacy. A key component of the course will be an exploratory research project aiming to use trusted computing technologies to address a security/privacy problem. To be successful in this course students should be knowledgeable in applied cryptography and basic security technologies.

CSEC 635 - Open-Source Software Security (AE)
The Free and Open-Source Software (FOSS) movement promotes the principles of software freedom, collaboration, and innovation, allowing users to access, modify, and share software without restrictions. FOSS is good for software security because it promotes transparency, allowing anyone to review the source code for vulnerabilities and ensuring that security flaws are more likely to be discovered and fixed quickly: "given enough eyeballs, all bugs are shallow" –Eric S. Raymond (Linus's law). In this course, we use OpenSSL—one of the most security-critical FOSS projects of our time—as a case study on the evolution of an FOSS project in response to vulnerabilities reported by security researchers. We study, discuss, and present their discovery, potential exploitation, mitigation, and disclosure. We also learn how to effectively contribute to FOSS projects.

RIT | Department of Cybersecurity

CSEC 659 – Offensive Security Engineering (AE)
A hands-on, in-depth approach to building offensive cyber capabilities on Windows 10 (x64). We will cover Windows architecture, OS primitives, PE file format, process injection, shellcode, and building extendable/modular software. This course includes a strong technical focus in C/C++ programming. We will also cover the ethics of developing offensive capabilities and why understanding how to build cyber capabilities will prepare students for a career in the security industry.

CSEC 659 – Blockchains and Smart Contracts (AE)
Humans are a critical element in security and privacy, yet they and their interactions with systems are often not considered. This course will investigate privacy and security from a user-centered point of view. In what ways do people think about privacy and security? How do they interact with current applications and solutions? What are the key considerations when designing user-friendly security systems? Usability and user-interface issues related to privacy and security are introduced, as well as an examination of potential designs and solutions. *This is a Research Elective*

CSEC 659 – Open-Source Intelligence (AE)
The Free and Open-Source Software (FOSS) movement promotes the principles of software freedom, collaboration, and innovation, allowing users to access, modify, and share software without restrictions. FOSS is good for software security because it promotes transparency, allowing anyone to review the source code for vulnerabilities and ensuring that security flaws are more likely to be discovered and fixed quickly: "given enough eyeballs, all bugs are shallow" –Eric S. Raymond (Linus's law)

CSEC 659 – Generative AI in Cybersecurity (AE)
Generative AI and large language models (LLMs) such as ChatGPT have taken the cybersecurity world by storm, with Microsoft introducing Security CoPilot and Google launching the Google Cloud Security AI Workbench. In this project-based course, we invite students who are already proficient in cybersecurity to delve into the application of Generative AI through real-world case studies.

CSEC 659 - Social Engineering (AE)
Depending on who you ask, you will get a different version of the same statistic: 90+% of cybersecurity breaches start with social engineering. But statistics, like people, are prone to manipulation. This course will explore both the ethics and the tactics of social engineering at the micro and macro levels—from influencing a single bad action (clicking a phishing link) to influencing an entire population (information warfare, troll farms, and fake news). Students will receive practical instruction in social-engineering focused pentesting that incorporates vishing, phishing, creating payloads, applying advanced OSINT, and physical security considerations for on-prem engagements. Students will select a recent case in social engineering and perform a case study paper/project. Prerequisites: CSEC 101, or 102, or 140, or 600.

CSEC 669 – Wireless Security (AE)
The goal of this course is to provide the students with an understanding of wireless communication concepts and principles of wireless networks along with their vulnerabilities and security protocols. In addition, the students will gain practical experience via a series of wireless system administration and attack/defense lab activities, and a software-defined radio project to explore mechanisms for analyzing and/or securing modern wireless networks. The course begins with a primer on wireless security concepts from a physical-layer perspective. It then covers and discusses various generations of security protocols for IEEE 802.11 (Wi-Fi) systems, security of cellular networks, security of wireless protocols for Internet-of-Things (IoT), and other selected trending topics (e.g., connected vehicles security).

CSEC 677 – Disaster Recovery (AE)
Cybersecurity professionals are increasingly being called upon to apply their knowledge to the development of disaster recovery and business continuity plans. This course will explore disaster recovery planning and business continuity in depth using current tools and techniques. Business requirements will be analyzed from the budget, business needs and risk management perspective. Students will examine the principles and best practices for developing and implementing effective disaster recovery plans using emerging technologies to ensure organizational resilience in the face of natural and man-made disasters.

CSEC 720 – Deep Learning Security (RE)
This course covers the intersection of cybersecurity and deep learning technologies such as CNNs, LSTMs, and GANs. Topics include the application of deep learning to traffic analysis, Deepfake detection, malware classification, fooling deep learning classifiers with adversarial examples, network attack prediction and modeling, poisoning attacks, and privacy attacks like model inversion and membership inference. Students will present research papers, perform several exercises to apply attack and defense techniques, and complete a final research project. Prior experience with machine learning concepts and implementation is required, but necessary details on deep learning will be covered. *This is a Research Elective*

CSEC 730 - Advanced Computer Forensics (AE)
This course provides students with the latest techniques and methods needed for extracting, preserving and analyzing volatile and nonvolatile information from digital devices. Students will gain exposure to the spectrum of available computer forensics tools along with developing their own tools for “special need” situations. The core forensics procedures necessary for ensuring the admissibility of evidence in court, as well as the legal and ethical implications of the process, will be covered on both Unix and Windows platforms, under multiple file systems. Therefore, students must possess a knowledge of available file systems on both platforms.

CSEC 731 - Web Server and Application Security Audits (AE)
This course discusses the processes and procedures to perform a technical security audit of web servers and web based applications. Students will not only explore Web Servers and Applications/Services threats, but also apply the latest auditing techniques to identify vulnerabilities existing in or stemming from web servers and applications. Students will write and present their findings and recommendations in audit reports on web servers and application vulnerabilities. To be successful in this course students should be knowledgeable in a scripting language and comfortable with the administration of both Linux and Windows platforms.

CSEC 733 - Information Security Risk Management (AE)
This course will provide students with an introduction to the principle of risk management and its three key elements: risk analysis, risk assessment and vulnerability assessment. Students will also learn the differences between quantitative and qualitative risk assessment, and details of how security metrics can be modeled/monitored/controlled and how various types of qualitative risk assessment can be applied to the overall assessment process. Several industry case studies will be studied and discussed. Students will work together in teams to conduct risk assessments based on selected case studies or hypothetical scenarios. Finally, they will write and present their risk assessment reports and findings.

CSEC 741 – IoT Security (RE)
This course is designed to provide students with knowledge of sensor network security with respect to practical implementations. In particular, secure sensor network design for Supervisor Control and Data Acquisition (SCADA) is discussed. SCADA encompasses technologies that manage and control much of the infrastructure that we depend on every day without realizing it. The failure or corruption of SCADA systems can not only be inconvenient but also hazardous when the resource is critical or life-threatening. Securing SCADA systems is of great strategic importance. The role of sensor networks in SCADA is discussed and sensor security protocols for SCADA applications are evaluated and studied. To be successful in this course students should be knowledgeable in basic networking, systems, and security technologies. *This class is a Research Elective.*

CSEC 742 - Computer System Security (Core)
The importance of effective security policies and procedures coupled with experience and practice is emphasized and reinforced through research and practical assignments. Organization and management of security discipline and response to threats is studied. Case studies of effective and failed security planning and implementation will be examined and analyzed. The issues influencing proper and appropriate planning for security and response to attacks will be studied. To be successful in this course students should be knowledgeable in networking, systems, and security technologies.

CSEC 743 - Computer Viruses and Malicious Software (AE)
Computer malware is a computer program with malicious intent. In this course, students will study the history of computer malware, categorizations of malware such as computer viruses, worms, Trojan horses, spyware, etc. Other topics include, but are not limited to, basic structures and functions of malware, malware delivery mechanism, propagation models, anti-malware software, its methods and applications, and reverse engineering techniques. Students will conduct research to understand the current state of computer malware defense and offense.

CSEC 744 - Network Security (AE)
Students will examine the areas of intrusion detection, evidence collection, network auditing, network security policy design and implementation as well as preparation for and defense against attacks. The issues and facilities available to both the intruder and data network administrator will be examined and evaluated with appropriate laboratory exercises to illustrate their effect. The students will be provided with an understanding of the principles and concepts of wired and wireless data network security. Students will perform a series of laboratory or homework experiments in order to explore various mechanisms for securing data networks including physical layer mechanisms, filters, applications and encryption. Students will engage in attack/defend scenarios to test their deployments against other teams. Students should be knowledgeable in networking technologies

CSEC 750 - Covert Communications (RE)
Students will be introduced to the history, theory, methodology and implementation of various kinds of covert communications. Students will explore future techniques and uses of covert communications. More specifically students will explore possible uses of covert communications in the management of botnets. To be successful in this course students should be knowledgeable in networking, systems, and security technologies. *This class is a Research Elective.*

CSEC 751 - Information Security Policy and Law (AE)
This course explores Information Security Policy development and deployment as well as laws (US and International) that impact information security. Students in this class will develop policies and analyze how policy impacts an organization. Students will also determine how federal, state, and international laws impact the information security policies of an organization.

.

CSEC-759 - Advanced Networking and Distributed Systems Security (RE)
This course focuses on security and privacy issues in computer and mobile networks. Topics include cryptographic primitives, privacy enhancing technologies, anonymous communications, and security and privacy issues in mobile crowdsourcing, social networks, Internet of Things, cloud computing, and blockchain & cryptocurrency. Students will learn fundamental cryptographic and privacy enhancing techniques, read and present research papers, and complete a final term paper that involves identifying and formulating a research problem, choosing appropriate techniques or developing new solutions to solve the problem, and reporting finds. Knowledge on computer networks is required.

CSEC 759 - Advanced Malware Forensics (RE)
In this course, students will gain in-depth knowledge on analysis approaches that reveal malware behavior on infected machines and techniques used by malware to evade analysis. Furthermore, students will explore current research in the malware domain to gain perspective on the different problems being discussed in the literature and the solutions being proposed. Students will also learn to use three tools for malware analysis and incident response, namely Cuckoo Sandbox, Volatility, and Google Rapid Response. This is a research-oriented course where students are encouraged to explore current research in the malware domain in addition to the required readings. Furthermore, the tools discussed in this course are open-sourced, which allows students to study the tools' source code in-depth. Although studying the source code is not required, it is highly recommended.

CSEC 759 - Advanced Software Security Analysis (RE)
This research seminar is designed to encapsulate the latest developments and challenges in software security, focusing primarily on program analysis for vulnerability detection. The course offers an in-depth understand-ing of the technical aspects of software security and covers a range of topics including static and dynamic analysis, software reverse engineering, and fuzzing techniques for vulnerability detection. By the end of this research seminar, participants will be able to identify potential vulnerabilities and implement strategies to prevent exploitations. Prerequisites: CSEC 600

CSEC 759 - Human Factors in Security (RE)
Human factors play an essential role in the overall security and privacy a system can provide to its users, and it is important for security and privacy experts to have an understanding of how people will interact with the systems they develop. This course will investigate privacy and security from a user-centered point of view. In what ways do people think about privacy and security? How do they interact with current applications and solutions? What are the key considerations when designing user-friendly security systems? Usability and user-interface issues related to privacy and security are introduced, as well as methods to evaluate potential designs and solutions. Students taking the class would be expected to be comfortable with reading scholarly articles published in academic journals/conferences and complete commentary assignments on them, regularly participate in-class discussions and complete a group project on designing and/or evaluating a security system for usability.

CSEC 769 - Emerging Topics in Wireless Security (RE)
This course focuses on security in current and emerging systems and protocols of the modern wireless ecosystems, aiming at advancing students' understanding of these systems while providing an insight into state-of-the-art wireless security research trends. The course covers a primer on wireless communications and introduces prominent wireless systems and their security protocols. Along with reviewing research approaches in wireless security, students then study and discuss several recent papers on current topics, including Wi-Fi and cellular networks security; physical-layer security; security of wireless protocols for IoT, connected vehicles, and GPS; and other selected topics. Students will also practice the steps of a research process by completing a small project, from critically reviewing the literature to evaluating a novel idea on a hardware testbed, and finally presenting their findings.

CSEC 790 - MS Thesis
This course is a capstone course in the MS in computing security program. It offers students the opportunity to investigate a selected topic and make an original contribution which extends knowledge within the computing security domain. As part of their original work students will write and submit for publication an article to a peer reviewed journal or conference. Students must submit an acceptable proposal to a thesis committee (chair, reader, and observer) before they may be registered by the department for the MS Thesis. Students must defend their work in an open thesis defense and complete a written report of their work before a pass/fail grade is awarded

CSEC 791 - MS Project
This course is a capstone course in the MS in computing security program. It offers students the opportunity to investigate a selected topic within the computing security domain. The student may complete a project for real world application or in a laboratory environment. Students must submit an acceptable proposal to a project committee (chair, and reader) before they may be registered by the department for the MS project. Students must defend their work in an open project defense and complete a written report of their work before a letter grade is awarded

CSEC 793 - Capstone for Computing Security
Students will apply their knowledge learned through the program to solve real world problems various areas of computing security. Large size projects will be defined for students to work on throughout the semester. At the end of semester students will present their results and demonstrate their knowledge and skills in problem solving and critical thinking in a setting open to the public

RIT | Department of Cybersecurity

Approved Electives from Other Departments

CMPE 661 – Hardware and Software Design for Cryptographic Applications (AE)
The objective of this course is to build knowledge and skills necessary for efficient implementations of cryptographic primitives on reconfigurable hardware. The implementation platform will be a field programmable gate array (FPGA) containing a general-purpose processor and additional reconfigurable fabric for implementations of custom hardware accelerators. In the studio format, team projects require design of selected cryptographic primitives followed by comparison and contrast of various implementation alternatives, such as software, custom FPGA hardware, and hybrid hardware-software co-design. Project teams are ideally composed of one Computer Engineering student and one Software Engineering or Computer Science student. Computer Engineering students lead the hardware design portions of each project, and Software Engineering and Computer Science students lead the software development portions. Topics may include binary finite field arithmetic, block ciphers, hash functions, counter mode of operation for block ciphers, public key cryptosystems, hardware/software co-design methodologies with FPGAs, software development and profiling, high level synthesis, on-chip buses, hardware/software interfaces, custom hardware accelerators and side channel attacks

CSCI 620 – Introduction to Big Data (AE)
This course provides a broad introduction to the exploration and management of large datasets being generated and used in the modern world. First, practical techniques used in exploratory data analysis and mining are introduced; topics include data preparation, visualization, statistics for understanding data, and grouping and prediction techniques. Second, approaches used to store, retrieve, and manage data in the real world are presented; topics include traditional database systems, query languages, and data integrity and quality. Case studies will examine issues in data capture, organization, storage, retrieval, visualization, and analysis in diverse settings such as urban crime, drug research, census data, social networking, and space exploration. Big data exploration and management projects, a term paper and a presentation are required. Sufficient background in database systems and statistics is recommended

CSCI 622 – Data Security and Privacy (AE)
This course examines policies, methods and mechanisms for securing enterprise and personal data and ensuring data privacy. Topics include data integrity and confidentiality; access control models; secure database architectures; secure transaction processing; information flow, aggregation, and inference controls; auditing; securing data in contemporary (relational, XML and other NO SQL) database systems; data privacy; and legal and ethical issues in data protection. Programming projects are required.

CSCI 642 – Secure Coding (AE)
This course introduces secure coding including topics such as principles of secure coding, security architectures and design, operational practices and testing, programmatic use of cryptography, and defenses against software exploitation. Other topics include software-based fault isolation, type-safe languages, certifying compilers; proof-carrying code, and automated program analysis and program rewriting. Programming projects, presentations, and a term paper will be required

CSCI 655 - Foundations in Cybersecurity (AE)
This course provides a graduate-level introduction to cybersecurity principles and practices, and emphasizes policies and mechanisms for building secure and trusted computer systems. It will cover cybersecurity principles, policies and mechanisms; core knowledge areas of data, software, component, connection, system, human, organizational and societal security; and crosscutting concepts of confidentiality, integrity, availability, risk, adversarial thinking, and systems thinking. Topics in privacy, and legal and ethical aspects will also be emphasized. The course also explores the current research in cybersecurity. Presentations, reports and projects are required.

CSCI 662 – Foundations of Cryptography (AE)
This course introduces cryptography, its mathematical foundations, and its relation to security. It covers classical cryptosystems, private-key cryptosystems (including DES and AES), hashing and public-key cryptosystems (including RSA). The course also introduces data integrity and authentication. Note: students who complete CSCI-462 or CSEC 604 may not take CSCI-662 for credit.

CSCI 720 – Big Data Analytics (AE)
This course provides a graduate-level introduction to the concepts and techniques used in data mining. Topics include the knowledge discovery process; prototype development and building data mining models; current issues and application domains for data mining; and legal and ethical issues involved in collecting and mining data. Both algorithmic and application issues are emphasized to permit students to gain the knowledge needed to conduct research in data mining and apply data mining techniques in practical applications. Data mining projects, a term paper, and presentations are required

CSCI 735 – Foundations of Intelligent Security Systems (AE)
The course will introduce students to the application of intelligent methodologies applications in computer security and information assurance system design. It will review different application areas such as intrusion detection and monitoring systems, access control and biological authentication, firewall structure and design. The students will be required to implement a course project on design of a particular security tool with an application of an artificial intelligence methodology and to undertake research and analysis of artificial intelligence applications in computer security.

CSCI 764 - Quantum-Resistant Cryptography (AE)
Quantum-Resistant Cryptography (QRC) refers to cryptographic systems that are secure against attacks from both quantum and classical computers. Such systems may be achieved through classical (i.e. non-quantum) means. The security of many commonly used cryptographic protocols (especially Public Key cryptosystems and Digital Signatures) would be compromised if general-purpose, large-scale, fault-tolerant quantum computers became a reality. This course covers the consequences of Quantum Computing and why it poses a threat to currently used cryptographic systems, and then discusses cryptosystems designed to be resistant to such attacks. Students will describe and utilize the designs recommended by NIST for Quantum-Resistant encryption algorithms and explain their security advantages over classical cryptosystems.

ISTE 721 - Information Assurance Fundamentals (AE)
This course introduces the topic of information assurance as it pertains to an awareness of the risks inherent in protecting digital content in today's networked computing environments. Topics in secure data and information access will be explored from the perspectives of software development, software implementation, data storage, and system administration and network communications. The application of computing technologies, procedures and policies and the activities necessary to detect, document, and counter unauthorized data and system access will be explored. Effective implementation will be discussed and include topics from other fields such as management science, security engineering and criminology. A broad understanding of this subject is important for computing students who are involved in the architecting and creation of information and will include current software exploitation issues and techniques for information assurance.

ISTE 730 – Foundations of IoT (AE)
Internet of Things (IoT) refers to physical and virtual objects that are connected to the Internet to provide intelligent services for energy management, logistics, retail, agriculture and many other domains. IoT leverages sensors, wireless communication, mobile devices, networking and cloud technologies to create many smart applications. In this course, the students learn about IoT design and development methodologies that enable the development of IoT applications. The students have hands-on opportunities to program and build IoT prototypes through lab assignments and a course project. The students should have some programming knowledge and required to purchase an IoT kit.

RIT | Department of Cybersecurity

PUBL 705.01 – Advanced Methods: Cryptocurrency/Blockchain Analytics (AE)
This course is designed to provide an introduction to statistical tools, specifically those used for analyses of cryptocurrency transactions on the blockchain and the development of related policies. Students will have the opportunity to work with software from private industry and gain knowledge and understanding on blockchain analytics and other related digital forensics used for investigations of illicit activity, as well as the development of policy and regulations concerning proprietary software and algorithms. At the end of the course, students will earn an official certification from Chainalysis and opportunities for employment recruitment. (Registration is restricted: while there are no prerequisites for this class, permission of the instructor is required. Contact the instructor with the following information: degree you are enrolled in, prior coursework in statistics or analytics, and why you are interested in this class.