BS Course Descriptions

CSEC-99 – Cooperative Education Seminar – Offered Fall & Spring
This course helps students prepare for co-operative education employment ("co-op") by developing job search strategies and material. Students will explore current and emerging aspects of the Computing Security field with employers, alumni and current students who have already been on co-op. Students are introduced to RIT's Office of Career Services and Cooperative Education and learn about professional and ethical responsibilities for their co-op and subsequent professional experiences. Students will work collaboratively to build résumés and to prepare for interviews.

CSEC-140 – Introduction to Cybersecurity – Offered Fall & Spring
This course will introduce many fundamental cybersecurity concepts. The course will teach students to think about information systems using an adversarial mindset, evaluate risk to information systems, and introduce controls that can be implemented to reduce risk. Topics will include authentication systems, data security and encryption, risk management and security regulatory frameworks, networking and system security, application security, organizational and human security considerations, and societal implications of cybersecurity issues. These topics will be discussed at an introductory level with a focus on applied learning through hands-on virtual lab exercises.

CSEC-201 – Programming for Information Security – Offered Fall & Spring
This course builds upon basic programming skills to give students the programming knowledge necessary to study computing security. Students will be introduced to network programming, memory management, and operating system calls along with associated security concepts. Specific focus will placed on understanding the compilation process and on the relation between high-level programming concepts and low-level programming concepts, culminating in identifying and exploiting memory corruption vulnerabilities.

CSEC-202 – Reverse Engineering Fundamentals – Offered Fall & Spring
This course will teach students the core concepts needed to analyze unknown source code. Students will study a variety of low-level programming languages and how high-level programming language structures relate to low-level programming languages. Students will learn study tools and techniques used for both static and dynamic analysis of unknown binaries, providing the foundation for further study in malware analysis.

CSEC-380 – Principles of Web Application Security – Offered Fall, Spring, & Summer
This course is designed to give students a foundation in the theories and practice relating to web application security. The course will introduce students to the concepts associated with deploying and securing a typical HTTP environment as well as defensive techniques they may employ.

CSEC-461 – Computer System Security – Offered Spring

This course will discuss the areas of liability, exposure, opportunity, ability and function of various weaknesses in computer security. The course will cover forms of attack and the methods to detect and defend against them. The issues and facilities available to both the intruder and administrator will be examined and evaluated with appropriate out-of-class laboratory exercises to illustrate their effect.

CSEC-462 – Network Security and Forensics – Offered Fall & Spring
This course investigates the many facets of network security and forensics. 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.

CSEC-464 – Computer System Forensics – Offered Fall & Spring
An investigation of the tasks of incident response and computer system forensics will be pursued. Students will learn the basic procedure for incident response as well as the tools needed to uncover the activities of computer users (deleted and hidden files, cryptographic steganography, illegal software, etc). Students will also learn to employ the activities needed to gather and preserve this evidence to ensure admissibility in court.

CSEC-465 –Network and System Security Audit – Offered Fall & Spring
This course will provide students with an introduction to the processes and procedures for performing a technical security audit of systems and networks. Students will explore state-of-the-art auditing techniques and apply appropriate tools to audit systems and network infrastructure components. In addition, students will write and present their audit reports on vulnerabilities as well as recommendations to fix any problems discovered.

CSEC-467 – Mobile Device Security and Forensics – Offered Fall
This course will be an in-depth study of security, incident response, and forensics as applied to the hardening and protection of mobile devices. Students will learn issues specific to the security of and vulnerabilities of mobile devices as well as forensics tools and incident response techniques used to reveal activities and information related to mobile devices.

CSEC-468 – Risk Management for Information Security – Offered Fall
The three key elements of risk management will be introduced and explored. These are risk analysis, risk assessment, and vulnerability assessment. Both quantitative and qualitative methodologies will be discussed as well as how security metrics can be modeled, monitored, and controlled. Several case studies will be used to demonstrate the risk management principles featured throughout the course. Students will work in teams to conduct risk assessments on the selected case study scenarios. They will develop mitigation plans and present the results of their analysis both in written reports and oral presentations.

CSEC-470 – Covert Communications – Offered every other Fall
Covert communications have been employed in the past in traditional information warfare. Today with huge amounts of digital information exchanged in our cyber space and covert communication will become a potential tool for information warfare inside the

space. 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. Students will conduct research in this topic area and will write a research paper on their research. Students will be required to submit their paper for publication in a peer-reviewed venue. *Writing Intensive Elective*

CSEC-471 – Penetration Testing Frameworks & Methodologies – Offered Fall & Spring
The process and methodologies employed in negotiating a contract, performing a penetration test, and presenting the results will be examined and exercised. Students will be exposed to tools and techniques employed in penetration testing. Assignments will explore the difficulties and challenges in planning for and conducting an assessment exposing potential vulnerabilities. Students will develop a metric used to evaluate the security posture of a given network and will develop a coherent and comprehensive report of their findings to present to their client. Particular attention will be paid to the ramifications of the findings toward the security of the targets.

CSEC-472 – Authentication and Security Models – Offered Fall & Spring
Access control and authentication systems are some of the most critical components of cybersecurity ecosystems. This course covers the theory, design, and implementation of systems used in identification, authentication, authorization, and accountability processes with a focus on trust at each layer. Students will examine formal models of access control systems and approaches to system accreditation, the application of cryptography to authentication systems, and the implementation of IAAA principles in modern operating systems. A special focus will be placed on preparing students to research and write about future topics in this area.

CSEC-473 – Cyber Defense Techniques – Offered Fall & Spring
Students will study, build, defend and test the security of computer systems and networking infrastructure while potentially under attack. Students will gain an understanding of standard business operations, timelines and the value of risk and project management. Techniques as related to security guidelines and goals will be studied. Aspects of legal requirements, inheriting existing infrastructure, techniques for backup and recovery of data and systems will be examined.

CSEC-476 – Malware Reverse Engineering – Offered Spring
This course provides an overview of basic concepts, techniques, and tools of malware reverse engineering. Students will learn how to perform reverse engineering to discover hidden software functions and hidden network communication techniques and protocols. Students will also learn techniques to protect against software reverse engineering.

CSEC-477 – Disaster Recovery – Offered Spring
Security and network professionals are increasingly being called upon to apply their knowledge to the development of disaster recovery and business continuity plans. This course will explore DRP/BC in depth using current tools and techniques. Business requirements will be analyzed from the budget, business needs and risk management perspective. Experience gained from at least one co-op is required.

CSEC-490 – Capstone in Computing Security – Offered Fall & Spring
This is a capstone course for students in the information security and forensics program. Students will apply knowledge and skills learned and work on real world projects in various areas of computing security. Projects may require performing security analysis of systems, networks, and software, etc., devising and implementing security solutions in real world applications.
Department Required Writing Intensive

CSEC-520 – Cyber Analytics and Machine Learning – Offered Fall
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. Students taking this course should have the 4th year status and completed MATH-190 Discrete Math, MATH-251 Probability and Statistics I, and MATH-241 Linear Algebra.

CSEC-559 – Hacking for Defense – Offered Fall & Spring
Student participates in multidisciplinary team to solve real problems for the United States government through Hacking for Defense initiative. Students will develop expertise conducting semi-structured interviews for (cooperative constructive preference elicitation), and learn the process of business model generation for technology and service commercialization. In addition, graduate students will conduct literature review in support of future technology research and development options.

CSEC-559 – Offensive Security Engineering – Offered Spring
This course will provide students with the technical foundations necessary to construct custom tooling needed to perform offensive cyber operations or adversary emulation projects. Students will study, analyze, and implement access, persistence, and evasion techniques used by real advanced persistent threat actors. The design and implementation of malicious implants, command and control frameworks, and custom access will all be studied. This is a programming intensive course and students are expected to have familiarity with writing buffer overflow exploits.

CSEC-559 – Usable Security and Privacy – Offered Fall
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.

CSEC-569 – Wireless Security – Offered Spring
The goal of this course is to provide the students with an understanding of the principles and concepts of wireless communications and networks, as well as their security vulnerabilities and security protocols. In addition, the students will gain practical experience via a series of

attack/defense lab activities, and a software 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 various generations of security protocols for IEEE 802.11 (Wi-Fi) systems, security of cellular networks, security of Internet-of-Things (IoT) communication protocols, security standards for connected vehicles communications, and other selected trending topics.

CSEC-731 – Web Server and Application Security Audits (Graduate course)
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.

Non-CSEC Courses

CSCI-455 – Principles of Cybersecurity
This course provides a broad 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. Presentations, reports and projects are required. This course requires the knowledge of computer science theory and concepts of computer systems.

CSCI-462 – Introduction to Cryptography
This course provides an introduction to 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 provides an introduction to data integrity and authentication.

CSCI-464 – Xtreme Theory
A fast paced, informal look at current trends in the theory of computing. Each week is dedicated to a different topic and will explore some of the underlying theory as well as the practical applications of the theory. Sample topics may include: quantum cryptography, networks and complex systems, social welfare and game theory, zero knowledge protocols. Students will be evaluated on homework assignments and a final presentation. Offered every other year.

CSCI-531 – Introduction to Security Measurement
The course will introduce students into the algorithmic foundations and modern methods used for security evaluation and tools design. It will combine a theoretical revision of the methods and models currently applied for computer security evaluation and an investigation of computer

security through the study of user's practice. The students will be required to complete a few homework assignments, to deliver a class presentation and to implement a team project.

CSCI-532 – Introduction to Intelligent Security Systems
The course will introduce students to the application of intelligent methodologies in computer security and information assurance systems 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 its performance analysis.

CSCI-622 – Data Security and Privacy (Graduate course)
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 (Graduate course)
This course provides an introduction to 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-762 – Advanced Cryptography (Graduate course)
This course investigates advanced topics in cryptography. It begins with an overview of necessary background in algebra and number theory, private- and public-key cryptosystems, and basic signature schemes. The course will cover number theory and basic theory of Galois fields used in cryptography; history of primality algorithms and the polynomial-time test of primality; discrete logarithm based cryptosystems including those based on elliptic curves; interactive protocols including the role of zero-knowledge proofs in authentication; construction of untraceable electronic cash on the net; and quantum cryptography, and one or more of digital watermarking, fingerprinting and stenography. Programming will be required.

GCIS-123 – Software Development and Problem Solving I – Offered Fall & Spring
A first course introducing students to the fundamentals of computational problem solving. Students will learn a systematic approach to problem solving, including how to frame a problem in computational terms, how to decompose larger problems into smaller components, how to implement innovative software solutions using a contemporary programming language, how to critically debug their solutions, and how to assess the adequacy of the software solution. Additional topics include an introduction to object-oriented programming and data structures such as arrays and stacks. Students will complete both in-class and out-of-class assignments.

This course is co-listed as SWEN-123, CSEC-123 and ISTE-123; therefore students may only receive credit for one of these courses.

GCIS-124 – Software Development and Problem Solving II – Offered Fall & Spring
A second course that delves further into computational problem solving, now with a focus on an object-oriented perspective. There is a continued emphasis on basic software design, testing & verification, and incremental development. Key topics include theoretical abstractions such as classes, objects, encapsulation, inheritance, interfaces, polymorphism, software design comprising multiple classes with UML, data structures (e.g. lists, trees, sets, maps, and graphs), exception/error handling, I/O including files and networking, concurrency, and graphical user interfaces. Additional topics include basic software design principles (coupling, cohesion, information expert, open-closed principle, etc.), test driven development, design patterns, data integrity, and data security. This course is co-listed as SWEN-124, CSEC-124 and ISTE-124; therefore students may only receive credit for one of these courses.

ISTE-230 – Introduction to Database and Data Modeling
A presentation of the fundamental concepts and theories used in organizing and structuring data. Coverage includes the data modeling process, basic relational model, normalization theory, relational algebra, and mapping a data model into a database schema. Structured Query Language is used to illustrate the translation of a data model to physical data organization. Modeling and programming assignments will be required. Note: students should have one course in object-oriented programming.

NSSA-221 – Systems Administration I
This course is designed to give students an understanding of the role of the system administrator in large organizations. This will be accomplished through a discussion of many of the tasks and tools of system administration. Students will participate in both a lecture section and a separate lab section. The technologies discussed in this class include: operating systems, system security, and service deployment strategies.

NSSA-241 – Intro to Routing and Switching
This course provides an introduction to wired network infrastructures, topologies, technologies, and the protocols required for effective end-to-end communication. Basic security concepts for TCP/IP based technologies are introduced. Networking layers 1, 2, and 3 are examined in-depth using the International Standards Organization's Open Systems Interconnection and TCP/IP models as reference. Course topics focus on the TCP/IP protocol suite, the Ethernet LAN protocol, switching technology, and routed and routing protocols common in TCP/IP networks. The lab assignments mirror the lecture content, providing an experiential learning component for each topic covered.

NSSA-245 – Network Services
This course will investigate the protocols used to support network based services and the tasks involved in configuring and administering those services in virtualized Linux and Windows internetworking environments. Topics include an overview of the TCP/IP protocol suite, in-depth discussions of the transport layer protocols, TCP and UDP, administration of network based services including the Dynamic Host Configuration Protocol (DHCP), Domain Name

Service (DNS), Secure Shell (SSH), and Voice Over IP (VoIP). Students completing this course will have thorough theoretical knowledge of the Internet Protocol (IP), the Transport Control Protocol (TCP), and the User Datagram Protocol (UDP), as well as experience in administering, monitoring, securing and troubleshooting an internet work of computer systems running these protocols and services.

PUBL-363 – Cyber Security Policy and Law

Why are we still so bad at protecting computer systems? Is it because we don't have good enough technology? Or because we lack sufficient economic incentives to implement that technology? Or because we implement technologies but then fail to use them correctly? Or because the laws governing computer security are so outdated? Or because our legal frameworks are ill-equipped to deal with an international threat landscape? All these reasons—and others—have been offered to explain why we seem to see more and more large-scale cybersecurity incidents and show no signs of getting better at preventing them. This course will examine the non-technical dimensions of this problem—the laws and other policy measures that govern computer security threats and incidents. We will focus primarily on U.S. policy but will also discuss relevant policies in the E.U. and China, as well as international tensions and norms. The central themes of the course will be the ways in which technical challenges in security can be influenced by the social, political, economic, and legal landscapes, and what it means to protect against cybersecurity threats not just by writing better code but also by writing better policies and laws.

SWEN-261 – Introduction to Software Engineering

An introductory course in software engineering, emphasizing the organizational aspects of software development and software design and implementation by individuals and small teams within a process/product framework. Topics include the software lifecycle, software design, user interface issues, specification and implementation of components, assessing design quality, design reviews and code inspections, software testing, basic support tools, technical communications and system documentation, team-based development. A term-long, team-based project done in a studio format is used to reinforce concepts presented in class.

SWEN-331 – Engineering Secure Software

Principles and practices forming the foundation for developing secure software systems. Coverage ranges across the entire development lifecycle: requirements, design, implementation and testing. Emphasis is on practices and patterns that reduce or eliminate security breaches in software intensive systems, and on testing systems to expose security weaknesses.