MS Course Descriptions

CMPE 661 – Hardware and Software Design for Cryptographic Applications
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
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 – Secure Data Management
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
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 662 – Foundations of 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. Note: students who complete CSCI-462 or CSEC 604 may not take CSCI-662 for credit.

CSCI 720 – Big Data Analytics
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 734 – Foundations of Security Measurement and Evaluation
The course will introduce students into the algorithmic foundations and modern methods used for security evaluation. It will combine a theoretical revision of the methods and models currently applied for computer security evaluation and an investigation of computer security through study of user's practice. The students will be required to complete a few home assignments, to deliver a class presentation, to implement a team project, to lead the team's work and to undertake research on the topic assigned.

CSCI 735 – Foundations of Intelligent Security Systems
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 736 – Neural Networks and Machine Learning
The course will introduce students into the current state of artificial neural networks. It will review different application areas such as intrusion detection and monitoring systems, pattern recognition, access control and biological authentication, and their design. The students will be required to conduct research and analysis of existing applications and tools as well as to implement a course programming project on design of a specified application based on neural networks and/or fuzzy rules systems.

CSCI 762 - Advanced Cryptography
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.

CSEC 600 - Introduction to Computing Security
This is a graduate level introduction to the field of computing security. 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 computing security domain. Students will have opportunities to learn essential techniques in protecting systems and network infrastructures, analyzing and monitoring potential threats and attacks, 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
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
In this course, students will learn in depth knowledge of cryptography and authentication. Students will explore various cryptography algorithms, authentication protocols, and their design and implementation. Students will work on a project to implement a cryptographic algorithm and/or an authentication protocol. The applications of cryptography and authentications in the areas of computer networks and systems and information assurance will also be investigated.

CSEC 659 - Cyber Analytics and Machine Learning
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 in machine learning such as clustering, neural networks, adversarial machine learning, etc. This class is a research elective.

CSEC 659 – Hacking for Defense
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 659 - Trusted Computing and Trusted Execution
This course is designed to provide students with knowledge of secure, trusted, and trustworthy computing with respect to practical implementations and real-world systems. In particular, Trusted Platform Modules, Intel SGX, or ARM TrustZone are discussed. Trusted computing and trusted execution systems are of great strategic importance for server, network, cloud, or embedded devices. Prerequisites: (Operating system knowledge, or permission of the instructor). This class is a research elective.

CSEC 659 – Usable Security and Privacy
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 730 - Advanced Computer Forensics
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
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 732 - Mobile Device Forensics
Techniques and limitations related to the seizure and interrogation of a variety of digital devices will be explored. Various mobile phone and tablet platforms will be interrogated with the intent of gaining better access and understanding of the organization of data in the devices. The infusion of digital storage and identification devices such as MP3 players, RFID and tokens into our everyday lives requires the study of their weaknesses and forensic exploit-ability. As personal information is frequently gathered and stored on these devices, the loss of a device could adversely affect individuals and organizations. The examination, collection, and removal of such information will be studied. To be successful in this course students should be knowledgeable in basic networking, systems, and security technologies.

CSEC 733 - Information Security Risk Management
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 - Sensor and SCADA Security
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
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
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, reverse engineering techniques. Students will conduct research to understand the current state of the computer malware defense and offense.

CSEC 744 - Network Security
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
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
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 Wireless Security
Motivated by the fast growth of wireless ecosystem, this course focuses on vulnerabilities and attacks in wireless systems, and the security protocols for such systems. Topics include wireless networks fundamentals, physical-layer security, smart jamming, friendly jamming, and security issues in 802.11 networks, Internet of Things, wearable devices, vehicle-to-vehicle communications, and dynamic spectrum access networks. Students will present research papers, perform simulation exercises, and do a final project that involves implementing a security protocol on a software-defined radio platform. Programming and networking knowledge are required. This class is a research elective.

CSEC 759 - Adv. Malware Forensics and Anti-Forensics
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.

CSEC 759 - Deep Learning and Security Course
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 do a final research project.

Prior experience with machine learning is required, but necessary details on deep learning will be covered.

CSEC 759 - Internet Security and Privacy
This course provides training in research in computer and network security, with a special focus on usable security and anonymity and censorship circumvention on the Internet. Students will present research papers, perform a simulation exercise, write critically about research papers, and conduct a semester-long research project. Programming is required.

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

ISTE 721 - Information Assurance Fundamentals
This course provides an introduction to 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