M.S. with a Major in Security Engineering

Candidates must satisfy a total of 30 credit hours (CH) with a minimum G.P.A. of 3.000 on a 4.000 scale.

All students must complete 12 credit hours (CH) of the core curriculum.

CSE 7339 Computer System Security

Investigates a broad selection of contemporary issues in computer security, including an assessment of state-of-the-art technology used to address security problems. Includes sources for computer security threats and appropriate reactions, basic encryption and decryption, secure encryption systems, program security, trusted operating systems, database security, network and distributed systems security, administering security, and legal and ethical issues. *Prerequisite*: CSE 5343 or equivalent.

CSE 7343 Operating Systems and System Software

Theoretical and practical aspects of operating systems, including an overview of system software, time-sharing, and multiprogramming operating systems. Also, network operating systems and the Internet, virtual memory management, interprocess communication and synchronization, file organization, and case studies. *Prerequisite*: CSE 2341.

CSE 7349 Data and Network Security

Covers conventional and state-of-the-art methods for achieving data and network security. Private key and public key encryption approaches are discussed in detail, with coverage of popular algorithms such as DES, Blowfish, and RSA. In the network security area, the course covers authentication protocols, IP security, Web security, and system-level security. *Prerequisite*: CSE 7339 or equivalent with instructor permission.

CSE 7359 Software Security

As software is delivered across network and Web-based environments, security is critical to successful software deployment. This course focuses on software security issues that pertain to the network application layer in the classic OSI model. At the application network layer, issues related to encryption, validation, and authentication are handled programmatically rather than at the network level. Students work with APIs for cryptography, digital signatures, and third-party certificate authorities. The course also explores issues related to XML and Web services security by examining standards and technologies for securing data and programs across collaborative networks.
Prerequisite: C- or better in CSE 7339.

All students must complete 9 credit hours (CH) of advanced elective courses.

CSE 7314 Software Testing and Quality Assurance

The relationship of software testing to quality is examined with an emphasis on testing techniques and the role of testing in the validation of system requirements. Topics include module and unit testing, integration, code inspection, peer reviews, verification and validation, statistical testing methods, preventing and detecting errors, selecting and implementing project metrics, and defining test plans and strategies that map to system requirements. Testing principles, formal models of testing, performance monitoring, and measurement also are examined.

CSE 7331 Introduction to Data Mining and Related Topics

Introduces data mining topics, with an emphasis on understanding concepts through an applied, hands-on approach. Includes other related topics such as data warehousing and dimensional modeling. All material covered is reinforced through hands-on implementation exercises.
Prerequisite: CSE 2341.

CSE 7338 Security Economics

Introduces economics as a tool for understanding and managing information security. Reviews key information security challenges and technologies in order to reason about the topics economically. Students are introduced to techniques of analytic and empirical modeling. Economic concepts reviewed include rationality, markets, and information. Presents models and metrics of security investment, along with cost-benefit analysis techniques, and techniques for empirical investigation and measurement of cybercrime. Security games are designed to capture the strategic interaction between defenders, as well as between attacker and defenders. Implications for public policy are discussed.

CSE 7369 Hardware Security and Trojan Detection

Introduces several contemporary topics in hardware security, with a particular emphasis on hardware Trojans. Other topics include physically unclonable functions, the problem of counterfeiting, security implications of design for testability in hardware, intellectual property protection, and secure coprocessors and smart cards.

CSE 8317 Software Reliability and Safety

In-depth study of techniques for ensuring software reliability and safety. Topics include software reliability engineering, software safety engineering, and recent developments in those areas. Reliability concepts applied to the software domain and safety concepts applied to computer-intensive systems will be discussed. Specific techniques such as software reliability models and analysis methods, operational profiles, safety and hazard analysis using fault trees and event trees, and formal verification for safety-critical software systems will be covered.

CSE 8331 Advanced Data Mining

Examines advanced data mining topics, including temporal mining. Web mining, spatial mining and text mining. Case studies and projects. *Prerequisite*: CSE 7331.

CSE 8349 Advanced Network and System Security

In-depth analysis of secure networks and systems, security audit, intrusion detection and prevention, storage security, firewall configurations, security log analysis, DMZs, honeypots, malicious codes, and mobile and grid computing security. *Prerequisite*: CSE 7349.

CSE 8352 (EE 8372) Cryptography and Data Security

Cryptography is the study of mathematical systems for solving two kinds of security problems on public channels: privacy and authentication. Covers the theory and practice of both classical and modern cryptographic systems. The fundamental issues involved in the analysis and design of a modern cryptographic system will be identified or studied. *Prerequisite*: EE/STAT/CSE 4340 or equivalent.

CSE 8353 Digital Forensics

Collection and analysis of evidence from electronic storage media or active systems. Methods to preserve, document, and present evidence in a court of law.

CSE 8356 Border and Transportation Security

Legal, political, and economic challenges of border and transportation security. Specific technologies include power solutions, wireless communications, sensor networks, sensing devices, screening devices, image acquisition, and image processing.

CSE 8359 Advanced Software Security

Advanced software security architectural patterns, software reverse engineering, and malware analysis. Advanced software exploitation techniques including shell coding, return-oriented programming, ASLR, and DEP bypassing. Advanced Web application security and secure coding principles/practices. Security testing techniques, fuzzing, operating system security, and root kits. *Prerequisite*: CSE 5359, CSE 7359, or equivalent.

CSE 8377 Fault-Tolerant Computing

Faults, errors, and failures, hardware fault tolerance, reliability, availability, reliable distributed systems, check-pointing and recovery, atomic actions data and process resiliency, software fault tolerance, case studies. *Prerequisite*: Permission of instructor.

EMIS 7313 Integrated Logistics Support

An introduction to concepts, methods and techniques for engineering and development of logistics systems associated with product production/manufacturing, product order and service fulfillment, and product/service/ customer support, utilizing system engineering principles and analyses. Specific topics include logistics systems requirements, logistics systems design and engineering concurrently with product and service development, transportation and distribution, supply/material support, supply Web design and management and product/service/customer support. *Prerequisites*: EMIS 7300 and EMIS 7301 or permission of instructor.

All students must complete 9 credit hours (CH) of elective courses. For a full listing, please refer to the graduate catalog.