Master of Science in Information Systems & Security Management

Courses Descriptions

Security Related Courses

ISSM 530. Information Security. 1st Semester. Lect. 3, 3 credits. This is an introductory course in information security which presents the students an overview of the fundamental principles, the security problems, risk analysis, and policies. Topics include basic concepts, access control, security policies, authentication, assurance and trust, information flow, vulnerabilities analysis, incident response, and legal and ethical issues. Prerequisite: Graduate standing or administrative approval.

ISSM 531. Network Security and Management. 1st Semester. Lect. 3, 3 credits. This course introduces the fundamentals of network security, security vulnerabilities, attack methods, and mitigation approaches. A comprehensive list of security issues related to networking design and development will be discussed. Topics include ethics in network security, basic cryptography, Firewalls, threats and security measures at different TCP/IP layers. SSH protocol, E-mail security, and Web security. Prerequisite: CSCI 0370 or equivalent (with administrative approval)

ISSM 532. Information Security Policy and Risk Analysis. 2nd Semester. Lect. 3, 3 credits. Analytical tools for calculating the costs and benefits of investment security decisions, and how to calculate the return on investments, in a hands-on setting. Additional topics covered include a brief introduction to commercially available tools for risk management, an introduction to vulnerability management, risk aversion and insurance. Prerequisite: ISSM 530 or equivalent (with administrative approval)

ISSM 533. Information Assurance Management. 1st Semester. Lect. 3, 3 credits. Students learn how to operate an information system at a specified level of trust. Further, they learn how to analyze and judge the information for validity and reliability to ensure the system will operate at the proposed level of trust. The course contents include understanding of information system architecture, system security measures, systems operations policy, system security management plan, legal and ethical considerations and provision for system operator and end user training. This is a multi-discipline computer security course. Prerequisite: ISSM 530 or equivalent (with administrative approval)

ISSM 534. Software Security. 2nd Semester. Lect. 3, 3 credits. Most reported security incidents are the result of defects that are unintentionally introduced during the design and development of the application. To reduce software vulnerabilities, the occurrence of flaws and the threat of attack on applications, the defect content of software needs to be significantly reduced. The purpose of the course, secure software development, is to address the issues of security practices within the software development lifecycle. Software Security is the study of various security practices within the context of the software development lifecycle. The course will address security practices that can be used to reduce defects in software as well as reduce the vulnerabilities in software. The course will also expose students to current research topics in the field. Prerequisite: CSCI 0430 or equivalent (with administrative approval)
ISSM 535. Incidence Response and Recovery. 1st Semester. Lect. 3, 3 credits. This course teaches the theory and principles of incident response through a hands-on and practical approach. Students will see common network attacks first hand, and then learn the specific steps and methodology necessary to resolve the incident. They will learn how a particular attack leaves a signature, and will be given the tools to identify those signatures. Students will then use those tools to identify unknown attacks, both in lab settings and projects. The entire lifecycle of incident response is covered, from pre-incident preparation through notification, initial response, and recovery. Real world case studies will provide insight into the computer crime cases that corporations and government are currently facing. Prerequisite: ISSM 530 or equivalent (with administrative approval)

ISSM 536. Mobile Security. 2nd Semester. 3 credits. Mobile devices continue to evolve and penetrate our everyday lives, leading to increased importance of mobile security - a topic living in the intersection of wireless communication, mobile computing, and computer security. This course focuses on aspects of information and network security that arise in this challenging and ever-evolving space of mobile communication systems, including mobile/cellular telephony, wireless Internet, and mobile ad hoc and sensor networks. Material will cover standards and research challenges in both deployed systems and future systems. Possible topics of study include (but are not limited to) telecom vulnerabilities; smart phone security; mobile Internet security; mobile location privacy; and ad hoc, mesh, and sensor network security. The course will involve an intensive group research project focusing on protocols/algorithms, vulnerabilities, and attacks as well as several individual homework and programming tasks. Groups will perform a sequence of cumulative tasks (literature review, analysis, simulation, design, implementation) to address aspects of their chosen topic, occasionally reporting their results to the class through brief presentations, leading to a final report. Prerequisites: CSCI 0370 or equivalent (with administrative approval)

ISSM 537. Computer Forensics. 1st Semester, Lect. 3, 3 credits. This course will introduce collecting, examining, and preserving digital evidence in support of criminal investigations, civil investigations, and sensitive business matters. The laws, regulations, and international standards governing sound forensics processes at cyber crime scene will be discussed. The course examines the issues, tools, techniques, and processes needed to successfully prepare for, respond to, and investigate such matters. The student will be also be introduced to some of the advanced computer forensics topics such as encryption, password cracking tools, data hiding techniques, stenography, anti-forensic tools and their effect on investigation, forensic problem solving (reconstruction of web pages from web cache, reverse engineering of P2P networks, images, etc.) hidden partitions, advanced MAC (modified, accessed, created) time discussion, metadata, etc. The student will be expected to take a case study from beginning to the end of investigation and course process. The student will receive a case study problem, and will be expected to write incident reports, collect evidence, acquire digital evidence, and perform the forensic investigation of several types of digital evidence, write reports regarding the forensic examinations, participate in trial preparation and courtroom testimony. Prerequisites: ISSM 530 or equivalent (with administrative approval)

ISSM 538. Web Application Security. 2nd Semester, Lect. 3, 3 credits. This course will introduce methods of exploiting the vulnerabilities of web applications, such as SQL injection, cross-site scripting, remoting frameworks, HTML5, cross-domain integration techniques, UI redress, and buffer overflows in the application layer. The student will examine the procedures
and technologies that are essential to developing, penetration testing and releasing a secure web application. The course will emphasize that web application security should be addressed earlier in the lifecycle in development and quality assurance, and how it differs from other types of Internet security. Through a review of recent web application breaches, the student will be exposed to the prolific methods hackers use to execute web attacks using common vulnerabilities. Some open source tools will be used to provide to the student an opportunity to exploit vulnerabilities of some web applications and how to secure the web applications. *Prerequisite: CSCI 0370 or equivalent (with administrative approval)*

**ISSM 599. Information Systems and Security Management Project.** 1st and 2nd Semesters. 3 credits. The ISSM project course provides students an exciting opportunity to apply skills they develop in the classroom to a problem from a real world context. In doing so, students begin to make the transition from their academic world to the environments in which they will work once they graduate. In these environments, the challenges of team building, resource development, client relations, limited information and pressing deadlines are as real and important as the technical and managerial components of any task.

A major feature of the project is integrating information systems and security knowledge into a group project. Students may focus on any of the areas constituting information security, such as privacy and confidentiality, network security, information assurance, application security, survivable systems, cyber security, or information security policy. *Prerequisite: Graduate standing, permission of the research supervisor.*

**ISSM 600. Master’s Thesis.** 1st and 2nd Semesters. 6 credits. *Prerequisite: Graduate standing, permission of the research supervisor.*

**Business and Information Systems Related Courses**

**BUSN 504. Information Security Economics.** Lect. 3, 3 credits This course applies tools of economic analysis to evaluate the evolving role of information security in the United States and world economies. Network security and privacy depends not only on technological, but also economic, behavioral, and legal factors. The course addresses theories of firm conduct and performance in the information systems; the role of information and e-commerce intermediaries; the economics of Internet advertising; intellectual property rights of digital products; national and international public-policy issues of information security; the financial and monetary implications of electronic trading; and the broader implications of e- Economics for U.S. and world economic activity. *Prerequisite: ECON 0201 or equivalent (with administrative approval)*

**BUSN 505. Information Security Operations Management.** Lect. 3, 3 credits. This course examines current and historical perspectives of business processes role in organizational information security. Topics will address process identification, process mapping and information security strategies. Additional topics will address challenges of information security in the areas of business integration and outsourcing. The course will focus on investigating present and simulated methods of operations in the management and protection of information related to current business processes. The course includes an information operations project. *Prerequisite: BUSN 406 or equivalent (with administrative approval)*
BUSN 506. Financial Security Systems. Lect. 3, 3 credits The purpose of this course is to study the analysis, design, development and implementation of accounting and financial systems. The course is intended to prepare students with the accounting and financial technological skills to be able to bridge the gap between management and technology. Topics addressed include: analysis, design, development and implementation of accounting systems; flows of funds and financial intermediation; financial systems and organizations; financial markets on fixed income and equity markets; management of accounting and financial risk; current and emerging trends in accounting and financial systems. Prerequisite: BUSN 0301 or equivalents (with administrative approval)

BUSN 507. Supply Chain Information Security Management. Lect. 3, 3 credits. This course examines the concepts, practices, and applications of all aspects of Supply Chain Management. Students learn about the impact of data on the strategic importance of demand forecasting, procurement, warehousing and distribution center operations, the critical role of all modes of transportation, and the vital contributions of information technology and communications. Deeply embedded in all phases of this course is the essential role of security of proprietary information within supply chains applications such as enterprise resource systems, warehouse management systems and transportation management systems. The course includes a supply chain information security project. Prerequisite: BUSN 0310 or equivalents (with administrative approval)

BUSN 508. Information Resource Management. 1st Semester. Lect. 3, 3 credits. Is a popular concept of viewing information systems resources from a strategic resource and security perspective. Discuss the IRM concept as well as provide pragmatic tools for implementing this approach within the organization including methods of securing the information. Topics will include: IS outsourcing, total cost of ownership, IS planning and strategic analysis, justification for IT investment, management of IT human resources, traditional project management theory, and project management techniques derived from the Theory of Constraints (TOC) all in the context of information security. Prerequisite: BUSN 0351 or equivalent (with administrative approval)

BUSN 509. Legal and Social Informatics of Security. 1st Semester. Lect. 3, 3 credits. Security technologies make explicit organizational choices that allocate power. Security implementations allocate risk, determine authority, reify or alter relationships, and determine trust extended to organizational participants. The course begins with an introduction to relevant definitions (security, privacy, trust) and then moves to a series of timely case studies of security technologies. The course also requires a project, including a work plan, a timeline, peer evaluations, and professional presentations. Prerequisite: PHIL 0348 or equivalent (with administrative approval)

BUSN 599. Information Systems and Security Management Project. 1st and 2nd semesters. 3 credits. The ISSM project course provides students an exciting opportunity to apply skills they develop in the classroom to a problem from a real world context. In doing so, students begin to make the transition from their academic world to the environments in which they will work once they graduate. In these environments, the challenges of team building, resource development, client relations, limited information and pressing deadlines are as real and important as the technical and managerial components of any task.
The project is a semester long, intensive team-based experience focusing on one of the specialization areas available in the MISM program. A typical project course includes design and development of an information system for an external client - often a corporation or public agency. Each project results in a final report/document as well a demonstration, a prototype, a significant portion of a larger system, or a finished system. Prerequisite: Graduate standing, permission of the research supervisor.

**BUSN 600. Master’s Thesis.** 1st and 2nd Semesters. 6 credits. Prerequisite: Graduate standing, permission of the research supervisor.