

Curricula in Information Security & Forensics

IIT School of Applied Technology Information Security & Forensics Courses

Department Web site: www.itm.iit.edu

IIT's School of Applied Technology offers a broad range of topics in the areas of information system security and computer and network forensics as undergraduate, graduate and continuing education courses. Course

offerings are listed below; some courses are offered at both the undergraduate and graduate levels, indicated by both 4xx and 5xx course numbers. Continuing education courses will have the same course numbers with an "IT" prefix.

Information Security & Forensics Courses within the Information Technology & Management Curricula

ITM 518 Coding Security

This course examines security architecture elements within modern object-oriented programming languages that create the framework for secure programming. Analysis of components and services with their inherent strength and weaknesses give rise to common coding security challenges. An exploration of identity management, encryption services and common hacking techniques will enable the student to evaluate the level of a systems data exposure. Coding Standards, best practices, guidelines and style will further enhance the student's ability to develop secure code. Homework assignments and a final project will reinforce the theories taught. A final project involves design and implementation of a secure product. Prerequisite: ITM 411 (3-0-3)

ITM 428 & ITM 528 Database Security

Students will engage in an in-depth examination of topics in data security including security considerations in applications & systems development, encryption methods, cryptography law and security architecture & models. Prerequisite: ITM 421 (3-0-3)

ITM 538 Computer & Network Forensics

This course will address methods to properly conduct a computer and/or network forensics investigation including digital evidence collection and evaluation and legal issues involved in network forensics. Technical issues in acquiring court-admissible chains-of-evidence using various forensic tools that reconstruct criminally liable actions at the physical and logical levels are also addressed. Technical topics covered include detailed analysis of hard disks, files systems (including FAT, NTFS and EXT) and removable storage media; mechanisms for hiding and detecting hidden information; and the hands-on use of powerful forensic analysis tools. (2-2-3)

ITM 539 Steganography

Digital steganography is the science of hiding covert information in otherwise innocent carrier files so that the observer is unaware that hidden information exists. This course studies both digital steganography and digital steganalysis (the science of discovering the existence of and extracting the covert information). In addition to understanding the science and the pathologies of specific carriers and hiding algorithms, students will have hands-on experience with tools to both hide and extract information. Carrier files such as image, audio and video files will be investigated. Prerequisite: ITM 538 (2-2-3)

ITM 443 & ITM 543 Vulnerability Analysis and Control

This course addresses hands-on ethical hacking, penetration testing, detection of malicious probes and their prevention. It provides students with in-depth theoretical and practical knowledge of the vulnerabilities of networks of computers including the networks themselves, operating systems and important applications. Integrated with the lectures are laboratories focusing on use of open source and freeware tools; students will learn in a closed environment to probe, penetrate and hack other networks. Prerequisite: ITM 440 (2-2-3)

ITM 448 & ITM 548 System and Network Security

Prepares students for a role as a network security administrator and analyst. Topics include viruses, worms, other attack mechanisms, vulnerabilities and countermeasures, network security protocols, encryption, identity and authentication, scanning, firewalls, security tools, and organizations addressing security. A key component of this course is a self-contained team project. Prerequisite: ITM 440 (2-2-3)

ITM 549 System and Network Security: Projects & Advanced Methods

Prepares students for a role as a network security analyst and developer and give the student experience in developing a production security system. Topics may include computer and network forensics, advances in cryptography and security protocols and systems; operating system security, analysis of recent security attacks, vulnerability and intrusion detection, incident analysis, and the design and development of secure networks. This course includes a significant real world team project the results in a fully operational security system. Students should have previous experience with object-oriented and/or scripting languages. Prerequisite: ITM 448 or ITM 548 (2-2-3)

ITM 458 & ITM 558 Operating System Security

This course will address theoretical concepts of operating system security, security architectures of current operating systems, and details of security implementation using best practices to configure operating systems to industry security standards. Server configuration, system-level firewalls, file system security, logging, anti-virus and anti-spyware measures and other operating system security strategies will be examined. Prerequisite: ITM 301 or ITM 302 (2-2-3)

ITM 478 & ITM 578 Information System Security Management

In-depth examination of topics in the management of information technology security including access control systems and methodology, business continuity and disaster recovery planning, legal issues in information system security, ethics, computer operations security, physical security and security architecture and models using current standards and models. (3-0-3)

ITM 579 Topics in Information Security: Compliance

In-depth examination of topics in security compliance, to include HIPAA, GLBA, NERC, SOX, PCI and compliance issues related to these requirements. Each successful student will demonstrate foundation knowledge and application of management, operational, technical and physical security concepts as they to apply to compliance in the organizational environment. Students will describe and identify best practices in information security compliance. (3-0-3)

ITM 579 Topics in Information Security: Risk Analysis

In-depth examination of industry-recognized methodologies used in the assessment of organizational risk. These methods will be discussed in detail during the course, and include the National Security Agency Information Assurance Methodology (NSA IAM), the OCTAVE method, risk assessment as detailed by the National Institute of Standards and Technology (NIST) and others. Each successful student will demonstrate foundation knowledge and application of risk assessment methodologies and best practices as they are implemented in an organizational environment. Students will describe and identify risk assessment frameworks, legal implications, and best practices in risk analysis. (3-0-3)

ITM 588 Incident Response, Disaster Recovery and Business Continuity

Students learn to design and manage key business information security functions including incident response plans and incident response teams; disaster recovery plans; business continuity plans; and crisis management teams and plans. Reporting, response planning and budgeting are all addressed. Students working in teams will prepare an incident response, disaster recovery, business continuity, or crisis management plan for a real-world organization such as a business or a government body or agency. (3-0-3)

Master of Information Technology & Management with a Specialization in Computer and Information Security

This degree requires completion of 30 credit hours with a GPA of 3.0/4.0 or better. Courses may be selected from 400- and 500-level courses, but a minimum of 18 credit hours must be at the 500-level or higher.

Students whose undergraduate degree is not in a computer-related area or who do not have significant experience or certifications in the information technology field may be required to complete prerequisite requirements and will be required to complete core courses, or may demonstrate their knowledge through equivalent coursework, certification or experience. Current prerequisite requirements include hardware and operating system literacy (ITM 301 or ITM 302). The core courses will ensure

an ability to program at a competent level using a contemporary programming language (ITM 411); basic knowledge of networking concepts, protocols and methods (ITM 540); knowledge of the Internet, including the ability to build Web sites and deliver them on a server (ITM 461); and the ability to create and administer databases using a modern database management system (ITM 421). Courses beyond the core courses and computer and information security offerings may be drawn from any course offered in the Information Technology & Management curriculum; see the current bulletin for full details. For additional information on this degree program, please contact Ray Trygstad at trygstad@iit.edu or 630.682.6032.

Core Courses (9 hours)

Required courses

ITM 411 Intermediate Software Development
and 6 hours chosen from the following:
 ITM 421 Data Modeling and Applications
 ITM 461 Internet Technologies & Web Design
 ITM 540 Introduction to Data Networks and the Internet

Note: Core courses may be waived upon presentation of evidence of equivalent coursework, certification or experience or successful completion of the placement examination. Approval of waivers will be made by the student's adviser or the ITM Associate Director. If any one core course is waived, students must still complete nine hours of core course content.

Specialization in Computer and Information Security Courses (18 hours)

Recommended courses (9 hours)

ITM 548 System and Network Security
 ITM 578 Information Systems Security Management
and 3 hours chosen from the following:
 ITM 518 Coding Security
 ITM 528 Database Security
 ITM 538 Computer & Network Forensics
 ITM 539 Steganography
 ITM 543 Vulnerability Analysis and Control
 ITM 549 System and Network Security: Projects & Advanced Methods
 ITM 558 Operating System Security
 ITM 588 Incident Response, Disaster Recovery and Business Continuity

Plus 9 hours chosen from the following:

ITM 518 Coding Security
 ITM 528 Database Security
 ITM 538 Computer & Network Forensics
 ITM 539 Steganography
 ITM 543 Vulnerability Analysis and Control
 ITM 549 System and Network Security: Projects & Advanced Methods
 ITM 551 Distributed Workstation System Administration
OR
 ITM 552 Client-Server System Administration
 ITM 558 Operating System Security
 ITM 579 Topics in Information Security
 ITM 586 Information Technology Auditing
 ITM 588 Incident Response, Disaster Recovery and Business Continuity

Computer and Network Security Technologies Graduate Certificate Program

This program is designed for students seeking knowledge that will prepare them for careers in computer and network security technologies and to deal with the challenging computer and network security problems facing society.

Complete the following two courses:

ITM 543 Vulnerability Analysis and Control
 ITM 548 System and Network Security

And any two of the following six courses:

ITM 518 Coding Security
 ITM 528 Database Security
 ITM 538 Computer & Network Forensics
 ITM 539 Steganography
 ITM 549 System and Network Security: Projects & Advanced Methods
 ITM 558 Operating System Security

Information Security Management Graduate Certificate Program

This program is designed for students seeking knowledge that will prepare them for careers in the management of information security.

Complete the following two courses:

ITM 548 System and Network Security
 ITM 578 Information System Security Management

And any two of the following four courses:

ITM 543 Vulnerability Analysis and Control
 ITM 579 Topics in Information Security
 ITM 586 Information Technology Auditing
 ITM 588 Incident Response, Disaster Recovery & Business Continuity
 ITM 579 Topics in Information Security may be applied to this certificate twice.

About Illinois Institute of Technology's School of Applied Technology

Illinois Institute of Technology's School of Applied Technology offers technology-oriented education and training for working professionals. The School of Applied Technology draws on Illinois Institute of Technology's (IIT) extensive experience in adult education. Courses are taught by Illinois Institute of Technology professors and industry professionals with significant working, teaching and research experience in their fields. The School of Applied Technology offers working professionals degree, non-degree, certificate, credit, non-credit programs, corporate training, short courses and seminars ranging from a few hours to several days in length. Both Bachelors and Masters Degrees are offered in Information Technology & Management and Industrial Technology & Management, as well as a Computer and Network Security Technologies Graduate Certificate and adult education/ CEU courses in all fields.

Illinois Institute of Technology is a private, Ph.D. granting university founded in Chicago in 1890, offering programs in engineering, science, technology, architecture, design, psychology, public administration, technical communication, business and law.