Curricula in Cyber Security & Forensics

IIT School of Applied Technology Cyber 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-S" prefix.

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

ITMS 518 Coding Security
This course examines security architecture elements within modern object-oriented programming languages that create the framework for secure pro-gramming. 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: ITMO 411 (3-0-3)

ITMS 428 & ITMS 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: ITMD 421 (3-0-3)

ITMS 538 Cyber 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)

ITMS 539 Stegnography
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: ITMS 538 (2-2-3)

ITMS 443 & ITMS 543 Vulnerability Analysis & 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: ITMO 440 (2-2-3)

ITMS 448 & ITMS 548 Cyber Security Technologies
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: ITMO 440 (2-2-3)

ITMS 549 Cyber Security Technologies: 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: ITMS 448 or ITMS 548 (2-2-3)

ITMS 458 & ITMS 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: ITMO 456 (2-2-3)

ITMS 478 & ITMS 578 Cyber 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)

ITMS 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)

ITMS 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)

ITMS 579 Topics in Information Security
Additional topics may vary each term.

ITMS 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 Cyber Forensics and 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: a minimum of 18 credit hours must be at the 500-level or higher. Law courses count as 500-level courses toward this total).

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. Current prerequisites for the Master of Cyber Forensics and Security include computer hardware and operating system literacy (ITMO 301 or ITMO 302 or equivalent coursework certification or experience); an ability to program at a competent level using a contemporary programming language (ITMD 411); basic knowledge of networking concepts, protocols, methods, and the Internet (ITMO 440), and the ability to create and administer databases using a modern database management system (ITMD 421). Students enrolled in undergraduate postbaccalaureate studies may take these courses as part of that program. For additional information on this degree program, please contact Ray Trygstad at trygstad@iit.edu or 630.682.6032.

Core Courses (15 hours)

Required courses

ITMS 538 Cyber Forensics
ITMS 543 Vulnerability Analysis and Control
ITMS 548 Cyber Security Technologies
ITMS 578 Cyber Security Management
LAW 273 Evidence

Note: Core course requirements may be waived upon presentation of evidence of equivalent coursework, certification, or experience. Approval of waivers will be made by the student's advisor or the ITM Associate Director.

Elective Courses (15 hours)

Select at least 12 hours from the following:

ITMS 518 Coding Security
ITMS 528 Database Security
ITMS 539 Steganography
ITMS 549 Cyber Security Technologies: Projects and Advanced Methods
ITMS 555 Mobile Device Forensics
ITMS 558 Cyber Forensics
ITMS 579 Topics in Information Security
ITMS 588 Incident Response, Disaster Recovery, and Business Continuity
ITMM 585 Legal and Ethical Issues in Information Technology
ITMM 586 Information Technology Auditing
ITMO 456 Introduction to Open Source Operating Systems
ITMT 594 Special Projects in Information Technology

Plus 3 or more hours from the following:

LAW 240 National Security Law
LAW 478 Computer and Network Privacy and Security: Ethical, Legal, and Technical Considerations
LAW 495 Electronic Discovery

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 course-work, 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

ITMD 411 Intermediate Software Development

and 6 hours chosen from the following:

ITMD 421 Data Modeling and Applications
ITMD 461 Internet Technologies & Web Design
ITMO 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 (21 hours)

Recommended courses (12 hours)

ITMO 456 Introduction to Open Source Operating Systems
ITMS 548 Cyber Security Technologies
ITMS 549 Cyber Security Technologies: Projects and Advanced Methods
ITMS 578 Cyber Security Management

and 6 hours from the following:

Any 500-level ITMS elective (ITMS 579 may only be taken once as part of this requirement)

Plus 3 or more hours from the following:

Any 500 level ITMS elective
ITMO 551 Distributed Workstation System Administration
OR
ITMO 552 Client-Server System Administration
ITMM 586 Information Technology Auditing

Curricula in Cyber Security & Forensics

Cyber 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:

ITMO 543 Vulnerability Analysis and Control
ITMS 548 Cyber Security Technologies

And any two of the following courses:

ITMS 518 Coding Security
ITMS 528 Database Security
ITMS 538 Cyber Forensics
ITMS 539 Steganography
ITMS 549 Cyber Security Technologies: Projects & Advanced Methods
ITMS 558 Operating System Security

Cyber 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:

ITMO 543 Vulnerability Analysis and Control
ITMS 548 Cyber Security Technologies

And any two of the following courses:

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

Undergraduate Specialization in Systems Security

As a part of our undergraduate degree in Information Technology and Management, this program focuses on application, data, and network security and the management of information technology security, and is intended for working information technology professionals who desire to complete a baccalaureate degree in their field with a particular focus on cyber security. In addition to required courses for the degree, the specialization includes:

ITMS 478 Cyber Security Management

AND one course from the following:
ITMO 451 Distributed Workstation System Administration
ITMO 452 Client-Server System Administration
ITMO 456 Introduction to Open Source Operating Systems

AND any two ITMS electives

For more on the Bachelor of Information Technology and Management degree, see the Undergraduate Bulletin at http://www.itm.iit.edu/data/undergraduatebulletin/ or contact Ray Trygstad at trygstad@iit.edu or 630.682.6032.

About Illinois Institute of Technology's Degree Programs in Information Technology and Management

Courses in our program are available at IIT's Rice Campus in Wheaton, at our Chicago Main Campus live or on the Internet, and at remote locations via the Internet. As some courses in the Cyber Security curricula must be completed in a live laboratory environment, degrees and certificates in this area of study cannot be completed entirely online. Courses are offered on a semester basis with the fall semester beginning in late August and the Spring semester beginning in mid-January. As this is a program originally structured for working professionals, most course offerings are in the evening or on Saturday morning. To meet the needs of our full-time students, we do offer daytime classes as well, but in most cases these courses will be available online for part-time students. Courses with laboratories normally run from 5:30pm to 9:30pm one evening a week; lecture-only courses normally run 6:25pm to 9:05pm one evening a week. Because of the strong hands-on emphasis of these programs, many courses will include a laboratory. Bus transportation is provided from IIT's Main Campus for courses that are only taught in our specialized labs at the Rice Campus. Daytime courses normally will meet two days a week for 75 minutes each session, but may meet once a week for 150 minutes.

Information Technology & Management courses are a careful blend of theory and practical application.

Applications: A core goal of the Information Technology & Management degree programs is to teach you practical, hands-on, applied knowledge that can lead to immediate employment in the IT field. To this end, ITM courses will teach the latest applications and tools used in the field, maximizing your opportunities to make hands-on use of these application and tools. In many instances courses will be tracked to existing industry certification requirements, giving immediate employment credibility to course content. Course tracking will be to vendor-neutral certifications to the greatest extent possible but this does not preclude the teaching of vendor-specific material when appropriate.

Theory: While the stress of courses in the Information Technology & Management degree programs is principally practical, given the scope and rapidity of change within the IT industry a solid grounding in theory is necessary to equip you to cope with the emergence of new technologies and to advance in your career in the field. A good grounding in theory is necessary to meet the goals of a university education, equipping you with critical thinking skills and the ability to see beyond "plug-and-chug" solutions all too commonly found in information technology training courses. This allows you to reason out solutions to problems rather than relying on canned solutions and blind adherence to procedure.

About Illinois Institute of Technology's School of Applied Technology

Illinois Institute of Technology's School of Applied Technology offers hands-on, project-based technology-oriented education and training for both full-time students and working professionals. Courses are taught by IIT professors and industry professionals with significant working, teaching and research experience in their fields. The School of Applied Technology offers 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 Graduate Certificates in Information Technology & Management topics and adult education/CEU courses in all fields. Graduate degrees are also offered in Food Safety & Technology and Food Process Engineering. Our Information Technology & Management and Food Safety & Technology curricula are supported by extensive dedicated laboratory and research facilities.

Illinois Institute of Technology (IIT) 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.