ITM SECURITY (ITMS)

ITMS 418
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's ability to develop secure code. Homework assignments and projects will reinforce theories taught.
Prerequisite(s): ITMD 411
Lecture: 3 **Lab:** 0 **Credits:** 3

ITMS 428
Database Security
Students will engage in an in-depth examination of topics in data security including security considerations in applications and systems development, encryption methods, cryptography law and security architecture and models.
Prerequisite(s): ITMD 421
Lecture: 3 **Lab:** 0 **Credits:** 3

ITMS 438
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.
Prerequisite(s): ITMS 448 and ITMO 456
Lecture: 3 **Lab:** 0 **Credits:** 3

ITMS 443
Vulnerability Analysis and Control
This course addresses hands-on ethical hacking, penetration testing, and 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 the use of open source and freeware tools; students will learn in a closed environment to probe, penetrate, and hack other networks.
Prerequisite(s): (ITMO 340 or ITMO 356) and (ITMO 440 or ITMO 456)
Lecture: 3 **Lab:** 0 **Credits:** 3

ITMS 446
Active Cyber Defense
This course covers the duties of cybersecurity analysts who are responsible for monitoring and detecting security incidents in information systems and networks, and for executing a proper response to such incidents. The course introduces tools and tactics to manage cybersecurity risks, identify various types of common threats, evaluate the organization's security, collect and analyze cybersecurity intelligence, and handle incidents as they occur.
Prerequisite(s): ITMO 340 or CS 542 with min. grade of C or CS 544 with min. grade of C or ECE 407 or ECE 408
Lecture: 2 **Lab:** 2 **Credits:** 3

ITMS 448
Cyber Security Technologies
Prepares students for a role as a network security analyst and administrator. Topics include viruses, worms, and other attack mechanisms, vulnerabilities, and countermeasures; network security protocols, encryption, identity and authentication, scanning, firewalls, security tools, and organizations addressing security. A component of this course is a self-contained team project that, if the student wishes, can be extended into a fully operational security system in a subsequent course.
Prerequisite(s): ITMO 340 or ITMO 540 with min. grade of C
Lecture: 2 **Lab:** 2 **Credits:** 3
Satisfies: Communications (C)

ITMS 458
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(s): ITMO 456 or Graduate standing
Lecture: 2 **Lab:** 2 **Credits:** 3

ITMS 478
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 & models using current standards and models.
Lecture: 3 **Lab:** 0 **Credits:** 3
Satisfies: Communications (C)

ITMS 479
Topics in Information Security
This course will cover a particular topic in Information Security, varying from semester to semester, in which there is particular student or staff interest. This course may be taken more than once but only 9 hours of ITMS 479/579 credit may be applied to a degree.
Credit: Variable

ITMS 483
Digital Evidence
In this course, students learn the fundamental principles and concepts in the conduct of investigations in the digital realm. Students will learn the process and methods of obtaining, preserving and presenting digital information for use as evidence in civil, criminal, or administrative cases. Topics include legal concepts and terminology, ethics, computer crime, investigative procedures, chain of custody, digital evidence controls, processing crime and incident scenes, data acquisition, e-mail Investigations, applicable case law, and appearance as an expert witness in a judicial or administrative proceeding.
Prerequisite(s): ITMS 438
Lecture: 3 **Lab:** 0 **Credits:** 3

ITMS 484
Governance, Risk, and Compliance
This course is an in-depth examination of topics in information technology/information security governance, risk, and compliance including information assurance policies, standards, and compliance as well as the examination of security risk analysis and the performance of systems certification and accreditation.
Lecture: 3 **Lab:** 0 **Credits:** 3

ITMS 514
Programming for Cybersecurity Analytics
This course will introduce essential programming concepts and techniques used in analytics. Students will learn and make use of industry standard programming languages widely used in application programming for data and statistical analysis in cybersecurity as well as other purposes. Students will understand and use various libraries for data manipulation, preparation, and analysis, and will be equipped to use the programming languages covered in real world scenarios and circumstances upon completion.
Lecture: 3 **Lab:** 0 **Credits:** 3

ITMS 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's ability to develop secure code. Homework assignments and projects will reinforce theories taught.
Prerequisite(s): ITMD 510 with min. grade of C or ITMD 512 with min. grade of C or ITMD 515 with min. grade of C
Lecture: 3 **Lab:** 0 **Credits:** 3

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.
Lecture: 3 **Lab:** 0 **Credits:** 3

ITMS 534
Human Factors in Cybersecurity
This course introduces the applied theories relevant to human factors in information security, digitalization, and sociotechnical environments. Examines the human element through a comprehensive approach that explores human errors, new technologies, and cybersecurity incidents. Investigates human-related aspects that have an impact on the practices, policies, and procedures that are in place in an organization to secure the firm's information. Topic areas include human behavior, ethics, psychology, social engineering, the culture of hacking, cybercrimes, security fatigue, and burnout. The analysis covers techniques to prevent intrusions and attacks that threaten organizational data and methods to identify potential insider threats.
Lecture: 3 **Lab:** 0 **Credits:** 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.
Lecture: 2 **Lab:** 2 **Credits:** 3

ITMS 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(s): ITMS 538 with min. grade of C or ITMS 548 with min. grade of C
Lecture: 2 **Lab:** 2 **Credits:** 3

ITMS 543
Vulnerability Analysis and Control
This course addresses hands-on ethical hacking, penetration testing, and 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 the use of open source and freeware tools; students will learn in a closed environment to probe, penetrate and hack other networks.
Prerequisite(s): ITMO 540 with min. grade of C
Lecture: 3 **Lab:** 0 **Credits:** 3

ITMS 546
Active Cyber Defense
This course covers the duties of cybersecurity analysts who are responsible for monitoring and detecting security incidents in information systems and networks, and for executing a proper response to such incidents. The course introduces tools and tactics to manage cybersecurity risks, identify various types of common threats, evaluate the organization's security, collect and analyze cybersecurity intelligence, and handle incidents as they occur.
Prerequisite(s): ITMO 340 or ITMS 540 with min. grade of C or CS 542 with min. grade of C or CS 544 with min. grade of C or ECE 407 or ECE 408
Lecture: 2 **Lab:** 2 **Credits:** 3

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 component of this course is a self-contained team project that, if the student wishes, can he extended into a full operational security system in a follow-course,
Prerequisite(s): ITMO 540 with min. grade of C
Lecture: 2 **Lab:** 2 **Credits:** 3

ITMS 549
Cyber Security Technologies: Projects & Advanced Methods
Prepares students for a role as a network security analyst and developer and gives 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 design and development of secure networks. This course includes a significant real world team project that results in an fully operational security system. Students should have previous experience with object-oriented and/or scripting languages.
Prerequisite(s): ITMS 539 with min. grade of C and ITMS 548 with min. grade of C
Lecture: 2 **Lab:** 2 **Credits:** 3

ITMS 555
Mobile Device Forensics
This course will address methods for recovering digital data or evidence and conducting forensic analysis of mobile devices such as smart phones and tablets. Various devices will be compared including iPhone, Android, and Blackberry. A brief review of Linux and related forensic tools. ANAND technology and mobile file systems will be discussed. Students will learn how to unlock and root mobile devices and recover data from actual mobile devices.
Lecture: 2 **Lab:** 2 **Credits:** 3

ITMS 557
Introduction to Cyber Warfare
Cyber warfare is defined as "warfare waged in cyberspace," which can include defending information and computer networks and deterring information attacks as well as denying an adversary's ability to do the same. It can include offensive information operations mounted against an adversary or even dominating information on the battlefield. Students participating in this discussion-based course will explore the current state of cyber security from national and international perspectives and consider cyber-based operations through the lens of a government pursuing strategic goals. How might their actions impact the industry's ability to conduct business operations? What does the current threat environment look like? The course will include extensive discussions and student presentations.
Lecture: 3 **Lab:** 0 **Credits:** 3

ITMS 558
Operating Systems 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.
Lecture: 2 **Lab:** 2 **Credits:** 3

ITMS 578
Cyber Security Management
In-depth examination of topics in the management of information technology security including access control systems & methodology, business continuity & disaster recovery planning, legal issues in information system security, ethics, computer operations security, physical security and security architecture & models using current standards and models.
Lecture: 3 **Lab:** 0 **Credits:** 3

ITMS 579
Topics in Information Security
This course will cover a particular topic in Information Security, varying from semester to semester, in which there is particular student or staff interest. This course may be taken more than once but only 9 hours of ITMS 579 credit may be applied to a degree.
Credit: Variable

ITMS 583
Digital Evidence
In this course, students learn the fundamental principles and concepts in the conduct of investigations in the digital realm. Students will learn the process and methods of obtaining, preserving and presenting digital information for use as evidence in civil, criminal, or administrative cases. Topics include legal concepts and terminology, ethics, computer crime, investigative procedures, chain of custody, digital evidence controls, processing crime and incident scenes, data acquisition, e-mail investigations, applicable case law, and appearance as an expert witness in a judicial or administrative proceeding.
Prerequisite(s): ITMS 538 with min. grade of C
Lecture: 3 **Lab:** 0 **Credits:** 3

ITMS 584
Governance, Risk, and Compliance
This course is an in-depth examination of topics in information technology/information security governance, risk, and compliance including information assurance policies, standards, and compliance as well as the examination of security risk analysis and the performance of systems certification and accreditation.
Prerequisite(s): ITMS 578 with min. grade of C
Lecture: 3 **Lab:** 0 **Credits:** 3

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; and business continuity plans. Reporting, response planning and budgeting are all addressed. Students working in reams will prepare an incident response, disaster recovery, or business continuity plan for a real-world organizations such as a business or a government body or agency.
Lecture: 3 **Lab:** 0 **Credits:** 3