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 544 with min. grade of C or ITMO 540 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 456 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
Satisfies: Communications (C)

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