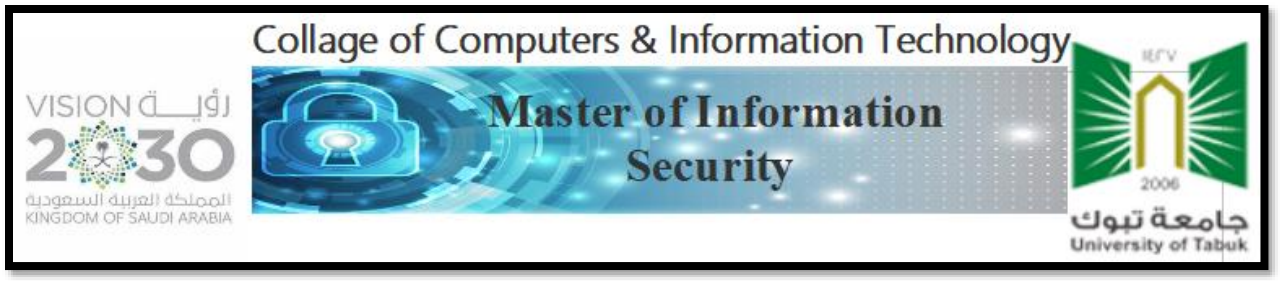


Mission

The mission of the Master of Information Security program is to qualify individuals to expand their knowledge of information technology security and scrutinize IT ethics in a group-based setting and prepare students to compete for jobs in high-demand information security industry.

Educational Objectives

The MIS program prepared students:

- To be qualified for planning and designing a suitable security policy and services for an organization.
- To develop into experienced and spirited professionals in information technology, particularly information security.
- To plan and apply valuable security method for organizations using modern equipment.
- To train students to implement security strategies in order to protect information and meet the IT industry's increase in demand.
- To predestine substantially trained specialists in information security for Saudi industry.
- To help students to proceed their responsibilities in professional and ethical manners.

Learning Outcomes

At the end of the program, graduates should be able to:

1. Exemplify advanced IT security topics in an efficient manner in the areas of: network security and communications, risk Management, and security policies.
2. Identify, investigate, and define information security problems related to hacking and protection methods and propose efficient solutions.
3. Obtain the skills to develop solutions for security problem.
4. Obtain efficient communication skills and written proficiencies to be able to work with professionals in a team environment.

Program Design

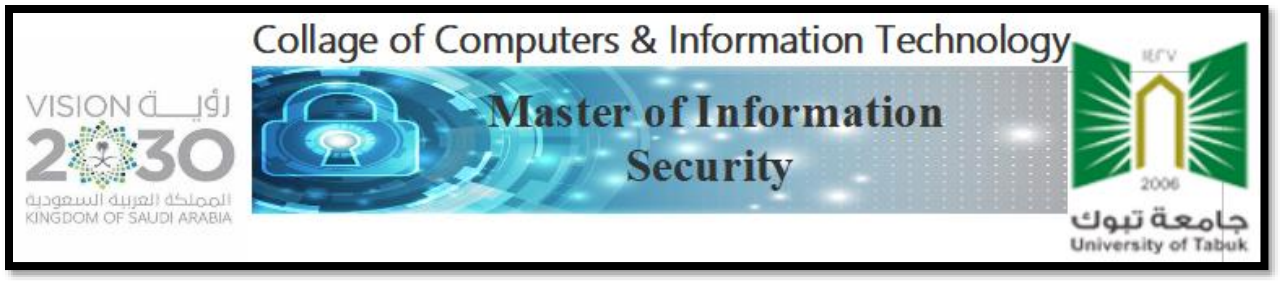
The program is course based along with a capstone project. Students are required to complete a minimum of 43 credit hours by both courses and capstone project.

Detailed Program Design

With the approval of a supervising professor, qualified students may be admitted to the program. Master of Information Security students must complete CIT 608 Graduate Seminar, 9 information security courses and 2 capstone projects 1 and 2

Master of Information Security students must complete minimum 43 credit hours, including:

1. At least 38 course credits that include:
   - 3 course credits of CIT 608Graduate Seminar.
   - 35 course credit of 8 Information Security Courses.
2. 5 Project credits: Capstone Project 1 (2 credits) and Capstone Project 2 (3 credits).



Master of Information Security: Study Plan

First Semester		
Course	**Credit Hours**	**Pre-requisite**
CIT 603 Database Security	4	
CIT 601 Applied Cryptography	4	
CIT 606 Security Policies and Risk Management	3	
CIT 608 Master of Information Security Seminar	3	
TOTAL	14	

2nd Semester		
Course	**Credit Hours**	**Pre-requisite**
CIT 602 Network Security	4	
CIT 605 Operating System Security	4	
CIT 604 Secure Software Systems	4	
TOTAL	12	

3rd Semester		
Course	**Credit Hours**	**Pre-requisite**
CIT 607 Biometrics and Access Control	4	
CIT 610 Selected Topics in Computer Security	4	
CIT 611 IT Security Capstone Research Project I	2	22 hrs in MIS program
TOTAL	10	

4th Semester		
Course	**Credit Hours**	**Pre-requisite**
CIT 609 Penetration Testing and Ethical Hacking	4	CIT602, CIT605, CIT601
CIT 612 IT Security Capstone Research Project II	3	CIT 611
TOTAL	7	

Courses

Code	Course Title	Credits	Prerequisite
CIT 603	Database Security	4	None

Description

This subject focuses on security issues related to databases. In particular, the subject reviews practical security mechanisms and solutions, such as identity and access management (ex: grant/revoke model; security by views; auditing in databases; multi-level database security). It also focuses on vulnerabilities, threats, and attacks that exist within various database environments or that have been used to attack databases, as well as the control measures that used to protect databases against these types of threats.

Code	Course Title	Credits	Prerequisite
CIT 601	Applied Cryptography	4	None

Description

This course will introduce students to the fundamental knowledge of applied cryptography and describes algorithms, systems, and their interactions. Topics include Overview of Cryptography, Mathematics Background, Classical Cryptography, Steam ciphers, Block Ciphers, Hash functions and data integrity، Public Key encryption, Private Key Encryption, Identification and Entity Authentication, Digital Signatures, Key Establishment Protocols, Key Management Techniques and Efficient implementation.

Code	Course Title	Credits	Prerequisite
CIT 606	Security Policies and Risk Management	3	None

Description

This course covers the role and importance of risk management and security policies. It describes how attackers exploit interactions between computer systems and their environment in order to learn how to prevent, detect and respond to such attacks. It will also discuss broader security issues related to business such as business continuity, incident recovery, legal issues related to security policies and risk management. Current techniques will be discussed throughout the course to assist in the implementation of security policies and risk management plans.

Code	Course Title	Credits	Prerequisite
CIT 607	Biometrics and Access Control	4	None

Description

This course discusses the theoretical constructs around Access Control in detail and provides an overview of the fundamental background. Traditionally, most security systems authenticate you based on something you know, i.e., a password. However, where security really matters, it makes sense to add a second layer, which could be something you have (e.g., a smartcard). Also, as a third option, probably the most authentic method, it could be something you are, something that, at least Theoretically, would be virtually impossible to forge. To this end, this course is about biometric controls, where biometrics is generally the study of measurable physical characteristics and behavioral patterns. This course deals with various authentication techniques their effectiveness, cost, intrusiveness, and accuracy.

Code	Course Title	Credits	Prerequisite
CIT 609	Penetration Testing and Ethical Hacking	4	CIT 602, CIT 605, CIT 601

Description

This course discusses the penetration testing steps including reconnaissance, scanning, exploitation, maintaining access, covering tracks and reporting. Students will gain hands on experience using various tools including metasploit to perform a professional penetration testing. Students will understand the difference between vulnerability assessment and penetration testing, the get-out-of-jail free card, the fundamentals of web application penetration testing, wireless network hacking, password attacks, and more. This course deals with various attacking techniques, their effectiveness, cost, intrusiveness, and accuracy.

Code	Course Title	Credits	Prerequisite
CIT 608	Seminar	3	None

Description

Students will learn how to prepare a professional seminar and are expected to participate in a series of seminars on current IT security issues. All students will be required to attend all seminars and provide a seminar on their research projects culminating upon completion and attending Capstone seminars as presented by other MIS students. The students will be evaluated based on the Seminar they provide.

Code	Course Title	Credits	Prerequisite
CIT 602	Network Security	4	None

Description

This course is concerned with the use of cryptographic algorithms and security protocols with the aim of providing protection for data/information transferred over networks and Internet. The module commences with a brief overview of Cryptography and Information Security perceptions. Then, deeply study and discussion are considered for Network Security topics. Topics include User Authentication, Network Access Control and Cloud Security, Transport-Level Security, Wireless Network Security, Electronic Mail Security, IP security, Network Intrusion Detection Systems, Mobile Communications Security, Firewalls, Honey Pot Systems, and other Network Defences.

Code	Course Title	Credits	Prerequisite
CIT 605	Operating System Security	4	None

Description

This course discusses advanced theory and concepts behind operating system security. Topics includes OS level mechanisms and policies, access control fundamentals, generalized security architectures, virtual machine introspection, and capability system will be discussed. Recent advanced techniques such as host-based intrusion detections, system randomization, vulnerability fingerprinting, and virtualization will also be introduced.

Code	Course Title	Credits	Prerequisite
CIT 604	Secure Software Systems	4	None

Description

This course examines approaches, mechanisms, and tools used to make software systems more secure. It focuses on creating software that functions correctly even when attacked. Topics include common software vulnerabilities, risk analysis, misuse cases, secure design principles and patterns, secure programming techniques, code reviews, and security testing.

Code	Course Title	Credits	Prerequisite
CIT 611	Capstone Project I	2	22 hrs in MIS program

Description

This course provides students with an opportunity to gather the knowledge and skills learned from the program coursework and conduct a research project with industrial applications. Students are expected to conduct a review of research literature and develop a set of hypotheses for a research project in IT security. A research proposal explaining the hypotheses and alternative remedies to the problem must be submitted to the faculty advisor at the end of the semester. Students are evaluated based on the research proposal and oral presentation.

Code	Course Title	Credits	Prerequisite
CIT 610	Selected Topics in Computer Security	4	None

Description

To highlights the up to date issues in Information Security field. The main purpose of this course is to highlight and investigate selected "special topics" in computer security that are not covered in the other offered courses. Such topics might be interrelated to one or more security disciplines.

Code	Course Title	Credits	Prerequisite
CIT 612	Capstone Project II	3	CIT 611

Description

The research outlined in the MIS 611 proposal must be completed during this course. The final report of the research findings and recommendations should be submitted to the advisor and the results presented. The results should have direct practical applications and / or be available for publication in refereed publications. Students are evaluated based on the submitted research and oral presentation.