جامعة الإمام محمد بن سعود الإسلامية
كلية علوم الحاسب والمعلومات

ماجستير العلوم في أمن المعلومات

M.Sc. in Information Security

دليل الدراسات العليا

Graduate Studies Guide

1445 هـ - 2023م

Version 1.0

Content

Program Overview

In alignment with Saudi Arabia's Vision 2030 and the National Transformation Program 2020, which aim to enhance the digital infrastructure, and recognizing that information security is a strategic matter and a crucial element of national security in its broad sense, the College of Computer and Information Sciences has been keen to contribute to this vital field. The college designed the Master of Science program in Information Security to prepare qualified national professionals in this domain. This program was developed after studying and analyzing numerous information security programs at Saudi and international universities, as well as conducting a comprehensive review of curricula to ensure that the program's plan covers various topics with depth and a broad scope within the information security specialization.

The university's esteemed council issued Decision No. 3169 for the academic year 1438/1439 AH, approving the establishment of the Master of Science in Information Security program. This decision followed the approval of the university council in its twelfth session on 16/06/1439 AH, based on the recommendations submitted by the Department of Computer Science and the College of Computer and Information Sciences in the same year.

Program Vision

To establish the Information Security program as a leading program locally and internationally in teaching and research in the field of Information Security.

Program mission

The Mission the of the Information Security master program is to produce highly skilled professionals and researchers equipped with appropriate computational knowledge and practices to handle challenges in a wide range of disciplines related to Information Security. To accomplish this, the program is significantly contributing to modern research, the development of new Information Security Systems and provide service to professional societies, the community, and the nation.

Program goals

1. Produce generations of skillful, and knowledgeable Information Security professionals.
2. Provide theoretical and practical skills to conduct advanced research in the field of Information Security.
3. Provide and maintain effective educational and research environment that can contribute in the building of a knowledge-based economy, and offer services to professional societies, the community, and the nation.

Career Opportunities for Program Graduates

1. Information Security Specialist
2. Information Security Consultant
3. Researcher in Information Security
4. Lecturer of Information Security
5. Information Security Manager/Director
6. Information Technology Manager
7. Lecturer
8. Teacher assistant
9. Academic Researcher
10. Computer Science Specialist
11. System Designer
12. Application developer
13. Database designer

Program Learning Outcomes

Knowledge and Understanding:	
K1	Possess in-depth knowledge of information security concepts, governance, operating system security and access control, as well as network security and cryptography.
K2	Recognize knowledge of computing and mathematics appropriately to conduct research and develop solutions for information security threats.
K3	Recognize information assurance requirements using standards and best practices
Skills:	
S1	Develop a computing-based solution for Operating Systems and Network Security threats and attacks in an efficient and proactive way
S2	Develop high-level practical skills over a broad range of information security related tools and techniques
S3	Communicate effectively with stakeholders using various communication tools to deliver knowledge and research outcomes
Values, Autonomy, and Responsibility:	
V1	Recognize the need for and an ability to engage in continuing professional development
V2	Work effectively on teams to accomplish a common goal
V3	Demonstrate compliance with ethical and professional responsibilities of researchers in the field of information security.

Admission Requirement

The general admission requirements for the program are as follows:

- A bachelor's degree in the field of Computer and Information Sciences. The department council may approve other specializations upon the announcement of admission.
- A minimum GPA of "Good" in the undergraduate degree for regular students.
- Achieving the required score on the General Aptitude Test for University Graduates (Qiyas) or the GRE test at the time of application.
- Achieving the required score on the English language proficiency test (STEP) or equivalent scores on the IELTS or TOEFL exams.
- Passing the written test or interview, if applicable.

The department and college councils have the authority to modify admission requirements and criteria for ranking applicants and to announce them in collaboration with the University's Deanship of Graduate Studies.

Study Plan

General Structure of the Program

The study plan for the Master of Science in Information Security (Academic Master's) consists of 49 credit hours distributed over six levels, including 10 core courses and 2 elective courses. Completing the program requires a minimum of two years (six semesters), along with the successful completion of a thesis.

Prerequisite **متطلب سابق**		**(8) units** **(8) وحدة**	**Level 1** **المستوى الاول**		
		Units الوحدات	Course Name اسم المقرر	Course code رمز المقرر	م
None لايوجد	Core اجباري	4	Information Security Management إدارة أمن المعلومات	SEC6641 امم 6641	1
None لايوجد	Core اجباري	4	Introduction to Cryptography مقدمة في التشفير	SEC6651 امم 6651	2
متطلب سابق		**(8) units** **(8) وحدة**	**Level 2** **المستوى الثاني**		
		Units الوحدات	Course Name اسم المقرر	Course code رمز المقرر	م
None لايوجد	Core اجباري	4	Network Security 1 أمن شبكات 1	SEC6611 امم 6611	1
SEC6651 امم 6651	Core اجباري	4	Access Control التحكم في الوصول للأنظمة	SEC6642 امم 6642	2

متطلب سابق		**(8) units** **وحدة (8)**	**Level 3** **المستوى الثالث**		
		Units الوحدات	Course Name اسم المقرر	Course code رمز المقرر	م
SEC6641 أما 6641	Core اجباري	4	Operating Systems Security أمن نظم التشغيل	SEC6643 أما 6643	1
SEC6611 أما 6611	Core اجباري	4	Network Security 2 أمن شبكات 2	SEC6612 أما 6612	2
متطلب سابق		**(7) units** **وحدة (7)**	**Level 4** **المستوى الرابع**		
		Units الوحدات	Course Name اسم المقرر	Course code رمز المقرر	م
SEC6643 أما 6643	Core اجباري	2	Information Security Law and Regulation قوانين ولوائح أمن المعلومات	SEC6609 أما 6609	1
None لايوجد	Elective اختياري	4	Elective course مادة اختيارية	SEC**** أما ****	2
SEC6612 أما 6612	Core اجباري	1	Industrial Seminar ندوة	SEC6601 أما 6601	3
متطلب سابق		**(6) units** **وحدة (6)**	**Level 5** **المستوى الخامس**		
		الوحدات	Course Name اسم المقرر	Course code رمز المقرر	م
None لايوجد	Elective اختياري	4	Elective course مادة اختيارية	SEC*** أما ****	1
None لايوجد	Core اجباري	2	دراسة بحثية Research Study	SEC6602 أما 6602	2
متطلب سابق		**(12) units** **وحدة (12)**	**Level 6** **المستوى السادس**		
		Units الوحدات	Course Name اسم المقرر	Course code رمز المقرر	م
SEC6602 أما 6602	Core اجباري	12	رسالة Thesis	SEC6690 أما 6690	1

مجموع عدد وحدات المقررات (**37**) وحدة
مجموع عدد وحدات المقررات مع وحدات الرسالة (**49**)
وحدة مجموع عدد المقررات مع الرسالة (**12**) مقرر

Elective Course List

Prerequisite متطلب سابق	Units الوحدات	Course Name اسم المقرر	Course code رمز المقرر	
SEC6643 أما 6643	4	Database Security أمن قواعد البيانات	SEC6644 أما 6644	1
SEC6642 أما 6642	4	Privacy and Identity Management الخصوصية وإدارة الهوية	SEC6648 أما 6648	2
SEC6651 أما 6651	4	Advanced Cryptography التشفير المتقدم	SEC6652 أما 6652	3
SEC6612 أما 6612	4	Cloud Security أمن السحابة	SEC6616 أما 6616	4

SEC6612 امم 6612	4	Cyber Crime and Digital Forensics الجرائم الالكترونية والأدلة الرقمية	SEC6605 امم 6605	5
SEC6643 امم 6643	4	Embedded Systems Security امن النظم المضمنة	SEC6645 امم 6645	6
SEC6643 امم 6643	4	Software Security أمن البرمجيات	SEC6646 امم 6646	7
SEC6612 امم 6612	4	Penetration Testing اختبار الاختراق	SEC6618 امم 6618	8

Important websites for students

Department	Website
College Website	Link
Program Page	Link
Alia System Portal	Link
Deanship of Admission, Registration, and Graduate Studies	Link
E-Services	Link
Guidance Manuals	Link
Graduate Studies Regulations and Publications	Link
Files and Forms Library	Link
Care and Guidance Department	Link
Special Needs Center	Link
X Platform	@ccis_imamu

Contact Information

Email	Phone and Extension	Department
infosec.graduate@imamu.edu.sa	011 259 7991	Program Management
Academic.med@imamu.edu.sa	0112586699	College Vice-Deanship for Academic Affairs
ccis.vicedean@imamu.edu.sa	011 2586977	College Vice-Deanship
ccis.dean@imamu.edu.sa	011 2581818	College Deanship
ccis.spg.z.n@imamu.edu.sa	011 2597816	Social and Psychological Guidance Unit

Course Description

Credit Hours	Course Name	Course Code
4	**Information Security Management**	**SEC6641**

This course is intended to present information security from a system and management perspective, including its definition, process, requirements, frameworks, how to integrate information security into the systems design process, and the security management of the information systems lifecycle. This course will cover foundational technical concepts as well as managerial and policy topics such as security policies, standards, and practices; risk analysis; risk assessments; law and compliance related to information security management; governance and strategic planning for security; developing the security program; and security management models and practices.

Credit Hours	Course Name	Course Code
4	**Introduction to Cryptography**	**SEC6651**

This course covers the basic topics in the field of cryptographic algorithms and their applications. This includes the basic Cryptography terminologies, secure/unsecure channel, attackers and their capabilities, encryption, decryption, keys and their characteristics, signatures, Cipher types together with typical attack methods such as frequency Analysis. Furthermore, the course covers Public Key Infrastructure support for digital signature and encryption and its challenges.

Credit Hours	Course Name	Course Code
4	**Network Security I**	**SEC6611**

The course details the different network security mechanisms used at the different layers of the communication stack. After a review of security properties, it presents cryptographic protocols. Then it details network security protocols including SSL/TLS, IPSec, PGP – S/MIME, SSH and DNSSEC. The security mechanisms to protect access to the radio network are presented through the study of wireless local area networks and mobile cellular networks.

Credit Hours	Course Name	Course Code
4	**Access Control**	**SEC6642**

The Access control foundation course presents the students with the basic fundamental principles of access control models and techniques in addition to secure flow of information. Also, to understand the effectiveness and limitations of these models and techniques. Expose the students to research work and literature review conducted in access control and connect the students to topics related to access control in operating systems, networks, and databases. Finally, Present the students with modern day problems in access control (e.g., Facebook and social media).

Credit Hours	Course Name	Course Code
4	**Network Security 2**	**SEC6612**

This course addresses some of the advanced network security concepts. The topics include the following:

- Attacker goals, capabilities, and motivations (such as underground economy, digital espionage, cyberwarfare, insider threats, hacktivism, advanced persistent threats)
- Network specific threats and attack types (e.g., denial of service, spoofing, sniffing and traffic redirection, Social engineering (e.g., phishing)
- Examples of malware (e.g., viruses, worms, spyware, botnets, Trojan horses or rootkits)
- Man-in-the-Middle, message integrity attacks, routing attacks, and traffic analysis
- Defense mechanisms and countermeasures (e.g., network monitoring, intrusion detection, firewalls, spoofing and DoS protection, honeypots, tracebacks, and Vulnerability analysis)
- Web security model and web application attacks.

Credit Hours	Course Name	Course Code
4	**Operating System Security**	**SEC6643**

This course covers both fundamentals and advanced topics in operating system (OS) security both theoretical and practical. It will study OS level mechanisms and policies in investigating and defending against real-world threats at operating system level. It presents students to techniques used for memory and file system protection, the types of malware and threats, and techniques used to defend against such threats including intrusion detection, virtualization, and disaster recovery. During this course, students will have the opportunity to investigate recent research papers as well as existing industrial technologies developed on the course topics.

Credit Hours	Course Name	Course Code
2	**Industrial Seminar**	**SEC6601**

This course intended to keep the students connected with the professional and academic information security experts. The topics will vary based on the latest trends in the field from industry and research problems. Students will be exposed to real environment and practices as well as open problems in information security.

Credit Hours	Course Name	Course Code

2	**Information Security Regulations and Laws**	**SEC6609**

The information Security regulations and laws connect Information security experts to laws and regulations in the kingdom of Saudi Arabia. The students are presented to laws covering a range of topics in both criminal law and laws concerned with commerce.

Credit Hours	Course Name	Course Code
2	**Research Study**	**SEC6602**

The main goal of this course is to write a complete thesis proposal satisfying the theses' requirements and regulations. This research study course is a pre-requisite for registering the master thesis. Initially, students are associated with potential supervisors based on research interests. Then, students are guided by those supervisors towards writing a complete master thesis proposal. This course is conducted as weekly lectures and meetings in which students and supervisors discuss research topics with the aim to write a complete thesis proposal.

Credit Hours	Course Name	Course Code
12	**Thesis**	**SEC6690**

The thesis aims to introduce students to scientific research in the Information Security discipline. The students will explore in depth an area of research and information security by applying the knowledge acquired through the core and elective courses of the program. The main research topics in the Information Security program include problem solving, knowledge representation and reasoning, machine learning, natural language processing, computer vision, constraint-based reasoning, deep learning, data mining and so on. The students are expected to understand the topics of the these, formulate the problematic of the thesis, arise some research questions, study the literature review, analyze the existent solutions, propose strategies, recommendations, and answers to the raised research questions.

Credit Hours	Course Name	Course Code
4	**Cyber Crime & Digital Forensics**	**SEC6605**

This course is designed to introduce students to Cyber Crimes and Digital Forensics on the national and international levels. The course will cover cybercrimes, prevention, understanding the digital forensics profession and investigations, data acquisition, processing crime and incident scenes, recovering graphics files, and digital forensics analysis and validation. Finally, policies, procedures, and cybercrime governance activities will be covered.

Credit Hours	Course Name	Course Code
4	**Cloud Security**	**SEC6616**

The course presents cloud security principles and mechanisms to protect data, applications, and infrastructure. It also explores different threats and vulnerabilities to cloud computing and how to fix and mitigate them. The course covers the fundamentals of the concepts of cloud security, architectural principles, techniques, design patterns and real-world best practices applied to Cloud service.

Credit Hours	Course Name	Course Code
4	**Penetration Testing**	**SEC6618**

This course prepares students to assess and examine security measures of an origination. Students will learn necessary skills to expose vulnerabilities and weaknesses and then suggest proper recommendations. The course covers in-depth methodologies, techniques, and tools to identify vulnerabilities, exploit, and assess security risks to networks, operating systems, and applications. The course goal is to provide knowledge of the successful ethical penetration testing.

Credit Hours	Course Name	Course Code
4	**Database Security**	**SEC6644**

This course covers the different aspects of database security. It provides an overview of the techniques and practices in access control, auditing and failure recovery. It mainly focuses on relational and object-oriented models. The course also focuses on the security issues in database systems and shows how current and future systems shall design to ensure confidentiality, integrity, and availability.

Credit Hours	Course Name	Course Code
4	**Embedded Systems Security**	**SEC6645**

Embedded systems are growing rapidly across various industries. They play vital role in automating and controlling processes, harvesting and analyzing massive data, and taking numerous actions. Securing systems that rely on embedded hardware and application become persistent needs in today’s modern interconnected cyber infrastructure. This course provides an overview of security and privacy challenges related to the deployment of IoT solutions using embedded systems that range from microprocessor/microcontroller-based systems, cards/RFIDs/Near Field Communications (NFC), System-On-Chip (SoC) . The students are presented to applications that exploit various embedded system in the era of Internet of Things (IoT). They are also going to examine benefits, threats and attacks when used as assets for Cyber Security. Also, review related standards and security evaluation methodologies for embedded security and consider/compare related technology e.g. TEE, TPM & Android Host Card Emulation (HCE).

Credit Hours	Course Name	Course Code
4	**Software Security**	**SEC6646**

The course details secure design & programming techniques to defend against software vulnerabilities such as buffer overflow and code injection. The course also explores secure software development through the use of secure design, secure coding, program analysis, and advanced testing

Credit Hours	Course Name	Course Code
4	**Privacy and Identity Management**	**SEC6648**

This course aims to provide an overview to identity management and privacy by presenting working definitions of Personal Identifiable Information (PII); identity management and privacy challenges and best practices; and the combined people, processes, policies, and technology required to manage and secure PII

Credit Hours	Course Name	Course Code
4	**Advanced Cryptography**	**SEC6652**

The course introduces advanced topics related to cryptographic algorithms and applications. It starts by briefly scanning historical, stream, and Block ciphers, in addition to number theory concepts and public key cryptography based on integer factorization problem. Then, it presents necessary mathematical background for modern cryptosystems based on the discrete logarithm problem. The course also presents in greater details one of the most advanced cryptosystems, which is Elliptic Curve Cryptography (ECC). Advanced digital signature algorithms such as ECC digital signature and DSA are covered by the course. Moreover, the course presents recent techniques related to the topic of key establishment. Finally, the course introduces recent research directions and the state of the art cryptography-based technologies such as Blockchain and cryptocurrencies, and illustrates the concept of Quantum computing and its impact on cryptography

ماجستير العلوم في أمن المعلومات

M.Sc. in Information Security

2023 – 1445 H

𝕏 **@ccis_imamu**

✉ **infosec.graduate@imamu.edu.sa**

🌐 **units.imamu.edu.sa/colleges/ComputerAndInformation**