KING FAHD UNIVERSITY OF PETROLEUM & MINERALS
COLLEGE OF COMPUTER SCIENCES AND ENGINEERING
DEPARTMENT OF INFORMATION & COMPUTER SCIENCE

Master of Science in Information Assurance and Security

Student Guide

Version 1.1
August 2019

Revision History

Date	Version	Description	Author
2016-03-23	1.0	Guide created	S. Zhioua
2019-08-25	1.1	Unify all ICS graduate guides	M. Alshayeb

Table of Content

1. Introduction 4
2. ICS Department Vision and Mission 4
3. Program Educational Objectives and Outcomes 4
3.1 Program Educational Objectives 4
3.2 Program Learning Outcomes 4
4. Program Requirements 4
4.1 Course Requirements 5
4.1.1 Core Courses 5
4.1.2 SEC Elective Courses 5
4.1.3 Recommended Free Elective Courses 5
4.2 Degree Plan 6
5. Admission Requirements 7
5.1 General University Admission Requirements for MS degree 7
5.2 Admission Requirements 7
6. Courses Description 8

1. Introduction

The Department of Information and Computer Science offers a Master of Science in "Information Assurance and Security", a research-oriented program targeting those who may ultimately pursue a doctoral degree in this field. The program is in compliance with the international standards and recommendations.

2. ICS Department Vision and Mission

The vision of the ICS department is to be a **regional leader that is recognized worldwide in education, research and professional development in the areas of Computer Science and Software Engineering.** The mission of the Department of Information and Computer Science is to:

1. Provide high quality undergraduate and graduate educational programs in the fields of Computer Science and Software Engineering.
2. Contribute significantly to the research and the discovery of new knowledge and methods in computing.
3. Offer expertise, resources, and services to the community.
4. Keep its faculty members current by providing opportunities for professional development

3. Program Educational Objectives and Outcomes

3.1 Program Educational Objectives

The objective of the Master of Science in Information Assurance program is that: the graduates will:

1. Meet the local needs for researchers and professionals who would uphold high knowledge, skills, and ethics in the field of Information Assurance and Security.
2. Adapt and adjust to rapid advancement and continuous evolvement of the rapidly changing field of Information Assurance and Security.
3. Have strong foundation and knowledge to conduct research and discovery to pursue a Ph.D. degree related to security or other related field.

3.2 Program Learning Outcomes

Graduates of the Master of Science in Information Assurance program will be able to:

1. Research and investigate advanced problems related to the field of Information Assurance and Security.
2. Analyze, implement, and select the most appropriate solutions to advanced problems related to the field of Information Assurance and Security.
3. Write security policies and put in place an effective security architecture that comprises modern hardware and software technologies and protocols.
4. Use effective, proper and state-of-the-art security tools and technologies.

4. Program Requirements

The Master of Science in Information Assurance and Security requirement is thirty (30) credit hours that include twenty-four (24) credit hours of coursework (i.e., 8 courses) and six (6) credit hours of thesis work. Nine (9) credit hours are designated as major core courses. Nine (9) credit hours of the other fifteen (15) credit hours must be taken from Information Assurance and Security elective courses. The remaining six (6) credit hours are free electives to be taken from related graduate courses (e.g., Mathematics (MATH), Computer Science (ICS), Software Engineering (SWE), Computer Engineering (COE), Systems Engineering (SE), and Electrical Engineering (EE)) subject to the approved degree plan.

Two senior-level undergraduate courses may be taken for credit as elective courses subject to the approval of the student's advisor, graduate committee, and the Department Chairman.

In short, the formula for the program requirements is:

3 SEC Core + 3 SEC Elective + 2 Free Elective + Thesis

4.1 Course Requirements

4.1.1 Core Courses

SEC 511	Principles of Information Assurance & Security
ICS 555	Cryptography and Data Security
SEC 521	Network Security

4.1.2 SEC Elective Courses

SEC 524	Computer and Network Forensics
SEC 528	Security in Wireless Networks
SWE 531	Secure Software
SEC 534	Database Security
SEC 536	Web Application Security
SEC 538	Trusted Computing
SEC 544	Biometric Systems
SEC 546	Embedded Systems Security
SEC 548	Watermarking and Steganography
ICS 531	Advanced Operating Systems
SEC 595	Special Topics in Information Assurance & Security
SEC 611	Cryptographic Computations
SEC 621	Advanced Network Security
SEC 631	Security in Operating Systems and Cloud Computing

4.1.3 Recommended Free Elective Courses[1]

ICS 5XX and ICS 6XX

SWE 5XX and SWE 6XX

EE 562	Digital Signal Processing I
EE 563	Speech and Audio Processing
EE 575	Information Theory
EE 576	Error Control Coding
EE 577	Wireless and Personal Communications
EE 578	Simulation of Communication Systems
EE 663	Image Processing
EE 664	Wavelet Signal Processing
EE 665	Signal and Image Compression
COE 502	Parallel Processing Architectures
COE 503	Message Passing Multiprocessing Systems
COE 504	Heterogeneous Computing
COE 541	Local and Metropolitan Area Networks
COE 543	Mobile Computing and Wireless Networks

[1] Elective courses are to be taken according to the approved degree plan.

MATH 421 Introduction to Topology
MATH 450 Modern Algebra I
MATH 455 Number Theory
MATH 521 General Topology I
MATH 523 Algebraic Topology
MATH 552 Fields and Galois Theory
MATH 586 Design and Analysis of Experiment
ISE 502 Probabilistic Modeling ISE
ISE 509 Reliability Engineering
ISE 522 Advanced Stochastic Simulation
ISE 531 System Reliability/Maintainability
ISE 536 Human Factor Engineering

Other graduate courses can be taken subject to the approved degree plan.

4.2 Degree Plan

The degree plan for the Master of Science in Information Assurance and Security is shown in Table 1.

Table 1: Degree Plan

Course No.	Title	LT	LB	CR	
First Semester					
SEC 511	Principles of Information Assurance & Security	3	0	3	
ICS 555	Cryptography and Data Security	3	0	3	
SEC 5XX or SEC 6XX	SEC Elective I	3	0	3	
		9	0	9	**9**
Second Semester					
SEC 521	Network Security	3	0	3	
SEC 5XX Or SEC 6XX	SEC Elective II	3	0	3	
SEC 5XX Or SEC 6XX	SEC Elective III	3	0	3	
SEC 599	Graduate Seminar	1	0	0	
		10	0	9	**9**
Third Semester					
XXX 5XX Or XXX 6XX	Free Elective I[2]	3	0	3	
XXX 5XX Or XXX 6XX	Free Elective II[2]	3	0	3	
		6	0	6	**6**
Fourth Semester					
SEC 610	MS Thesis	0	0	6	**6**
		Total			**30**

[2] Elective courses are to be taken according to the approved degree plan

5. Admission Requirements

The applicant should have the equivalent degree of an undergraduate computer science major of King Fahd University of Petroleum and Minerals. In general, applicants with a four-year degree in related fields in science and engineering (e.g., computer science, software engineering, computer engineering, systems engineering, electrical engineering, information technology) may be considered for admission. However, an applicant lacking an adequate undergraduate training may be admitted if recommended by the department's graduate committee and the Chairman, with the understanding that additional coursework must be taken to remove the deficiency in the undergraduate training, which is not credited towards the degree.

In addition to the general university admission requirements set by the KFUPM Deanship of Graduate Studies stated in section 5.1, the department also sets other admission requirements relevant to the program stated in section 5.2.

5.1 General University Admission Requirements for MS degree

The minimum requirements for possible admission as a regular graduate student to pursue a Master program in engineering or science are as follows:

1. A four-year Bachelor's (B.S.) Degree in engineering or science from a recognized institution with a major in the proposed field or evidence of suitable background for entering the proposed field.
2. A Grade-Point Average (GPA) of 3.00 or higher on a scale of 4.00 or equivalent, and a GPA of 3.00 in the subject of the major field. Official transcripts and degree certificates are required for final admission.
3. Completion of TOEFL with a minimum score of 520 (PBT), 190 (CBT) or 68 (IBT). The TOEFL score must be sent directly to the Deanship of Graduate Studies. The KFUPM code is 0868. IELTS is also acceptable [min 5.5]
4. Acceptable General Graduate Record Examination (GRE) which should also be reported directly.
5. At least three letters of recommendation from the faculty who taught the applicant undergraduate courses. [Sealed and signed]
6. Satisfactorily meeting any additional departmental or university admission requirements.

5.2 Admission Requirements

The priority for the enrollment in the proposed program is for applicants who hold a BS degree in Computer Science or a related discipline such as Software Engineering or Computer Engineering. Applicants who hold BS in other related disciplines should have a satisfactory background in core areas of computer science which may include computer networks, operating systems, algorithms, and programming.

Unsatisfactory background in any of these areas is considered a deficiency. Provisional admission may be granted to qualified students. Such students must take the appropriate deficiency course(s) at KFUPM with a grade of B or better before a change of status to regular graduate student.

6. Courses Description

SEC 511 Principles of Information Assurance & Security (3-0-3)
Introduction to information Assurance & Security. Information confidentiality, availability, protection, and integrity. Security systems lifecycle. Risks, attacks, and the need for security. Legal, ethical, and professional issues in information security. Risk management including identification and assessment. Security technologies and tools. Security laws, audit and control. Cryptography foundations, algorithms and applications. Physical security, security and personnel, security implementation and management. Securing critical infrastructure. Trust and security in collaborative environments.
Prerequisite: Graduate Standing

ICS 555 Cryptography and Data Security (3-0-3)
Introduction to data security and cryptography, Mathematical principles of cryptography, Conventional and modern block and stream symmetric-key cryptosystems, Public-key cryptosystems, Message integrity and cryptographic hash functions, Digital signatures, Authentication, and Key exchange protocols. Several exercises and assignments on using cryptosystem and cryptanalysis tools.
Prerequisite: Consent of Instructor

SEC 521 Network Security (3-0-3)
Network infrastructure security issues, including perimeter security defences, firewalls, virtual private networks, intrusion detection systems, wireless security, and network security auditing tools. Secure network applications. Network security protocols such as SSL, SSL/TLS, SSH, Kerberos, IPSec, IKE. Network threats and countermeasures. Network auditing and scanning. VoIP Security. Remote exploitation and penetration techniques. Network support for securing critical infrastructure. Design and development of software-based network security modules and tools based on hands-on experiences and state-of-the-art technologies.
***Note**: SEC 521 cannot be taken for credit with CSE 551*
Prerequisite: ICS 555

SEC 524 Computer and Network Forensics (3-0-3)
Methodical approaches for collecting and preserving evidence of computer crimes, laws/regulation, and industry standards. Hands-on experience on identifying, analyzing, recreating, and addressing cyber based crimes. Ethical issues associated with information systems security. Foundational concepts such as file system structures, MAC times, and network protocols. Use of tools for evidence recovery. Use of established forensic methods in the handling of electronic evidence. Rigorous audit/logging and date archival practices. Prevention, detection, apprehension, and prosecution of security violators and cyber criminals, and general legal issues.
Prerequisite: SEC 521

SEC 528 Security in Wireless Networks (3-0-3)
Security of wireless networks such as cellular networks, wireless LANs, mobile ad hoc networks, wireless mesh networks, and sensor networks. Overview of wireless networks. Study of threats and types of attacks, including attacks on MAC protocols. Selfish and malicious behavior in wireless routing protocols. Countermeasures/solutions and their limitations. Encryption and authentication. Secure hand-off techniques. Energy-aware security mechanisms. Secure multicasting. Key pre-distribution and management in wireless networks.
Prerequisite: SEC 521

SEC 534 Database Security (3-0-3)

Study of database security and auditing issues, challenges and protection methods. A review of relational and object database concepts. Database security and auditing issues. Authentication methods. Authorization based on privileges, roles, profiles, and resource limitations, and rolebased authorization constraints. A study of access control mechanisms for current DBMSs, content-based and fine-grained access control, access control systems for object-based design and XML. Data confidentiality and privacy for databases. Secure statistical databases. Integrating databases and applications security. Database security protection via inference detection. Security implementation and administration, with applications to ecommerce, and emerging research in database security.

Prerequisite: SEC 511

SEC 536 Web Application Security (3-0-3)

Web applications security requirements, threats and countermeasures. Contemporary web application vulnerabilities and exploitation techniques, based on the Open Web Application Security Project (OWASP). Web defacement and server penetration techniques. Content-based attacks and effective countermeasures. Intellectual property protection and watermarking. Auditing and scanning Web applications and infrastructure for security weaknesses. Analysis of Web applications for key vulnerabilities and attacks. Security mechanisms and protocols and their roles in securing Web applications. Secure Web programming mechanisms in ASP.NET, Java, PHP, XML and SQL. Secure Web applications for e-commerce, e-banking and e-government transactions. Numerous hands-on exercises and projects on using tools and writing secure Web applications.

Prerequisite: SEC 511

SEC 538 Trusted Computing (3-0-3)

A comprehensive overview of trusted computing technology and its applications, TPM chips, secure boot, attestation, DRM, sealed storage, nature of trust, methods for characterizing, establishing, and attesting trust of a system. Trusted Virtualization. Operating system and hardware support for TC. Key management. Code signing. Identity management. Implications of certification. Trusted Mobile Platforms. Trust negotiation, transitive trust, trust evaluation and reputation systems. Trust computing architectures and modeling. Trust computing in P2P and cloud computing paradigms. Design and development of software applications and components to utilize trust computing for protecting information providers and end users.

Prerequisite: SEC 511 and ICS 555

SEC 544 Biometric Systems (3-0-3)

Theory of signal processing, especially image and sound processing, for purposes of biometric system design. An introduction to basic methods and techniques for the study of authentication based on static biometric features such as fingerprints, hand geometry, facial features, thermograms, iris and retina, voice, and handwriting. Study of recognition based on dynamic features including lip movements, typing, and gait, study of standards and applications of biometry.

Prerequisite: Graduate Standing

SEC 546 Embedded Systems Security (3-0-3)

Study of various security models and techniques for embedded systems both from a hardware as well as a software perspective. Smart card security. RFID attack models (including power analysis, side channel, and timing attacks), and security techniques. Security in wireless sensor networks (key management techniques, attack models, detection and prevention techniques).

eHealth (embedded medical systems) security. Cryptographic hardware. Industrial control systems (SCADA). Physical hardware. Security for System-on-chip, and Internet-devices such as Internet thermostats and automated doors.
Prerequisite: Graduate Standing

SEC 548 Watermarking and Steganography (3-0-3)
Study of enabling technologies for digital watermarking and steganography including the history of information hiding, basic principles and techniques such as still images, video, and 3-D video objects, and their applicability to owner authentication, content authentication, information embedding and communication with side information. Evaluation and benchmarking of watermarking and steganography mechanisms. Study of malicious attacks inclusive of bit rate limitation, counterfeiting marks and removal attacks. Overview of attempts to formalize watermarking. Steganography vs. watermarking. Applications of steganography. software for steganography, and steganalysis techniques.
Prerequisite: Graduate Standing

SEC 595 Special Topics in Information Assurance & Security (3-0-3)
Advanced topics selected from current journals of Information Assurance and Security and that deal with theoretical development or applications in the field.
Prerequisite: Graduate Standing

SEC 599 Graduate Seminar (1-0-0)
Graduate students are required to attend seminars given by faculty members, visiting scholars, and fellow graduate students. Additionally, each student must deliver at least one presentation on a contemporary research topic. Among other things, this course is designed to give the student an overview of how to conduct research, research methodology, journal specifications and submission requirements, and on professional societies. The course grade is a Pass or Fail.
Prerequisite: Graduate Standing

SEC 606 Independent Research (Pass/Fail) (3-0-3)
This course is intended to allow the student to conduct research on advanced topics in his area of research for his Master degree. The faculty offering the course should submit a research plan to be approved by the *graduate program committee* of the ICS Department. The student is expected to deliver a public seminar and a report on his research outcomes at the end of the course.
Prerequisite: Graduate Standing

SEC 610 Master Thesis (0-0-6)
The student has to undertake research at an in-depth level under the supervision of a faculty member for a specific problem in the area of Information Assurance and Security.
Prerequisite: SEC 599

SEC 611 Cryptographic Computations (3-0-3)
Review of number theory, set algebra and finite fields. Computations in finite fields using standard and non-standard bases. High performance algorithms and architectures for cryptographic applications. Side channel analysis attack resistant computations.
Prerequisite: ICS 555

SEC 621 Advanced Network Security (3-0-3)

Intrusion detection and prevention systems. Security engineering processes. Advanced firewall considerations. Honeynets. Network forensics. Distributed denial of service attacks (Botnet, Rootkits, Zero-Day Exploits). Cyber crime and cyber war. Enterprise security policy development. Complex enterprise security infrastructure design and integration. Web and email security. P2P network security, and trust management.

Prerequisite: SEC 521

SEC 631 Security in Operating Systems and Cloud Computing (3-0-3)

Advanced security research topics in operating systems and emerging computing paradigm such as grid and cloud computing. Secure operating system requirements, fundamentals and definitions. Security in traditional and popular operating systems such as Unix, Linux, OpenBS,D and Windows. Security kernels. Verifiable security goals, trusted processes, and information flow integrity. Secure capability systems. Security in virtualization and secure virtual machine systems. Security issues and countermeasures in cloud computing.

Data security and storage in the Cloud. Security management in the cloud services: PaaS, SaaS, and IaaS. Case Studies of secure systems, design, and evaluation: SELinux and Solaris.

Prerequisite: SEC 521