Princess Sumaya University for Technology

King Hussein School for Computing Science

Course Description

11732: Information Security (3 credit hours)

This course focuses on the fundamentals of information security. Students will learn the principles of information security, security architectures and models, and aspects and methods of information security such as physical security control, operations security, access control, hacks/attacks/defense, systems and programs security, cryptography, network and web security, worms and viruses, and other Internet secure applications. The course covers the following topics: system security issues, authentication systems, IP security, web security, access control, firewalls, data integrity through encryption, virtual private networks, SSL, SSH, and IPSec.

11761: Digital Forensics and Investigation (3 credit hours)

In this cybercrime course, students will become familiar with the basics of solving cybercrimes. By learning how to identify, protect and gather evidence, retrieve data, prepare crime reports and present information in courts, students master the correct methods for investigating cybercrimes so they can be solved and prosecuted. Students read case studies to become familiar with cybercrime scene investigation techniques. Techniques and tools used to build and solve cybercrime cases are presented and analyzed. Also, the requirements for conducting a cybercrime investigation through lecture, practical exercises, scenarios and case studies are presented. Students will learn the processes, techniques, specialized documentation, and legal guidelines necessary to investigate a computer crime.

11762: Secure Software Development (3 credit hours)

This course covers the security and safety analysis in software design and development. It defines and identifies vulnerability detection and avoidance. Topics include threat modeling, defensive programming, web security and the interaction between security and usability authentication, principle of least privilege, buffer overflows, race conditions, time-of-check vs. time-of-use, trust management, access control, and other security relevant issues.

11763: Data Communication and Network Security (3 credit hours)

This course introduces key issues in data communication and network security. Topics covered include definition of security, network security, digital signatures, IP security, secure socket layer, intrusion detection, authentication, firewalls, denial of service, spam, email viruses, phishing, and an overview of many attacks that the Internet has experienced.

11764: Hacking Techniques and Intrusion Detection (3 credit hours)

This course covers the most common methods used in computer and network hacking with the intention of learning how to better protect systems from such intrusions. These methods include reconnaissance techniques, system scanning, and system access by network and application level

attacks, and denial of service attacks. Traffic analysis methods and tools will be studied in this course. Also, it covers the techniques for traffic filtering and monitoring, and intrusion detection.

11765: Biometrics (3 credit hours)

Biometrics is capturing and using physiological and behavioral characteristics for personal identification. It is set to become the successor to the PIN. This course will introduce computational methods for the implementation of various biometric technologies including face and voice recognition, fingerprint and iris identification, and DNA matching.

11766: Advanced Digital Forensics (3 credit hours)

This course cover advanced topics in computer security and forensics such as cryptography, automatic intrusion detection, pattern matching and statistical techniques, firewalls, and vulnerability scanning.

11767: Wireless Security and Forensics(3 credit hours)

This course looks at wireless network security in a defensive view. The program is designed to provide fundamental skills needed to analyze the internal and external security threats against a wireless network and to develop security policies that will protect an organization's information. Students will learn how to evaluate network and Internet security issues and design, and how to implement successful security policies and firewall strategies. In addition, they will learn how to expose system and network vulnerabilities and defend against them.

11768: OS and file systems Forensic Analysis (3 credit hours)

This course focuses on configuring a secure OS using command line and graphical utilities. Emphasis is placed on file sharing technologies such as the Network File System, NetWare's NCP file sharing, and File Transfer Protocol. Additional topics include data security, user security, file security, and network intrusion detection. Students will be required to take on the role of problem solvers and apply the concepts presented to situations that might occur in a work environment.

11769: Cryptography (3 credit hours)

This course will cover the cryptography and crypto-analysis techniques. It will introduce the symmetric and asymmetric encryption, private and public key encryption, key distribution, cryptographic hash functions stream ciphers, zero-knowledge proof systems, cryptanalytic attacks and brute-force attacks.

11781: Cyber Law and Crime Fundamentals(3 credit hours)

This course will explore the legal issues affected and created by on-line crime. The course will examine the evolution of criminal law relative to the development of new technology - primarily

as it relates to on-line crime. Students will examine 3 primary areas that include technology relevant to on-line crime, behavior criminalized in cyberspace, and privacy laws governing law enforcement investigations in cyberspace
Topics will include: the evolution, nature and scope of cyber crime; forensic analysis of digital evidence; on-line investigative techniques; including identity theft, Internet fraud, and new technologies affecting on-line crime.

12782: Forensics Expert in Courtroom (3 credit hours)

Students study the uses of technology and scientifically trained expert witnesses at trial. This course provides "hands-on" experience in developing and presenting computer evidence testimony in a courtroom setting. Topics covered are computer forensic investigations, computer evidence issues and presentation of computer evidence in court or in a deposition. Topics covered are used by members of computer incident response teams, law enforcement computer crime units, military computer specialists, lawyers and judges. However, it is recommended that students have a solid working knowledge of DOS and Microsoft Windows-based computers. Legal experience is not a prerequisite.

11783: Information System Risk Management (3 credit hours)
This course introduces and defines the main types of risks that the information system in organizations may face and need to consider to ensure their security and business continuity. This course focuses on the identification and assessment of assets, threats and vulnerability in order to plan the appropriate information system security in the organization. It will survey preventive and containment techniques available to address the potential risk areas. The contingency planning, incident response planning, business continuity planning and disaster recovery will be covered too.

11784: Information System Auditing (3 credit hours)

This course aims at introducing the foundations of auditing information systems. It covers the concepts of the audit process, governance, and compliance regulations, as well as the latest technology tools. Students will learn the role of an auditor and the types of audits performed, various information security and audit frameworks, as well as the tools and techniques of auditing technical controls, foundations of auditing operating systems, and foundations of auditing applications. In addition, this course will cover the following topics: the information systems audit process, data collection methodologies, regulations and compliance, auditing, vulnerability testing, penetration testing, auditing technical controls, auditing networks & operating systems, and auditing business application systems.

11786: Special Topics in IS Security and Digital Criminology (3 credit hours)

Topics will be assigned by the department on evolving techniques and related topics to support the study plan and to encourage further research by students.

11787: Disaster and Crises Management (3 credit hours)

This course covers topics related to disaster recovery and emergency planning and management as applied to the information-systems function in corporations. Topics include security risk evaluation and management, creation of threat profiles, continuity of operations planning, contingency planning, and incident reporting. A self-directed approach/tool for the conduct of information security risk evaluation is introduced. Projects include developing a security protection strategy and plan.

11789: IT Project Management (3 credit hours)

This course defines and covers the characteristics of IT projects and introduces the student to a variety of project management techniques that can be applied in an IT project context. Managing scope, time, cost, and quality will be explored. The course will cover project management issues associated with information systems security projects as well as other IT projects such as packaged software implementation (e.g., ERP systems), in-house developed systems, and outsourced projects.

11791: Seminar (3 credit hours)

In this course students will have the opportunity to merge their studies with their professional interests and experiences. Students will select topics for study and research according to their areas of interest in information systems security, cyber crimes, computer criminology, legal, ethical and social impacts of ICT and IS security. Ultimately, each student will produce a written paper. Successful course completion requires compliance with rigorous academic research standards, production of a final paper and an oral presentation by the student on the paper topic.

11792: Research Project (3 credit hours)

Students will conduct an individual study to demonstrate the ability to formulate, investigate, and analyze a problem and to report results. Written report and oral presentation are required. The project proposal must be approved by a major professor and/or supervisory committee. The project document should be written with direction from a major professor and/or supervisory committee and in accordance with the description to be provided to students. Upon completion, both the project and the document must be successfully defended to the department in an open forum with approval from the major professor and/or supervisory committee.

11799: Dissertation (9 credit hours)

Each student must complete, document, present and defend a thesis under the supervision of a faculty member in the fields of Information Systems Security and Digital Criminology. Every candidate must complete a thesis (equivalent to 9 credit hours) describing research work of publishable quality. The thesis must be defended before a committee consisting of the supervisor and at least three other faculty members, one from outside the university, in the relevant fields. The thesis defense is open to all interested faculty and students. Upon the completion of 15 credits, a student is eligible to register for thesis.