MSc in Cyber Security
Thesis Track

Courses Description

430601	Advanced Cyber Security	3 Cr. Hr.

Cyber security aims to protect the computer system's resources like hardware, software and information. This course provides students with understanding of the core concepts of cyber security: concepts for confidentiality, integrity and availability; threats, vulnerabilities, threat modeling, risks and access control. This course will also cover basic concepts of application security including secure software system development and operating system security focusing on Windows and Linux. Concepts in secure software development will include security architecture and models. Business continuity planning, disaster recovery, legal aspects of security, physical security and human aspects of cyber security will also be discussed in this course.

430602	Hardware Security	3 Cr. Hr.

Computer Hardware is the most valuable and expensive property for the organizations and business. Problem in hardware components results into malfunction of system and lost or corruption of file. This course is designed to study the approaches for hardware security which enables the students for protection of computer hardware from the physical factors like fire, heat, incorrect voltage, dust or malicious activities. Upon completing the course, students will understand the vulnerabilities in current digital system design flow and the physical attacks to these systems. The students explore the secure processor architectures, and the concepts of channel attacks, Hardware Trojan and trusted integrated circuit (IC) design, Trust platform module (TPM), and physical unclonable function (PUF).

430603	Network Security Management	3 Cr. Hr

Organizations are open to vulnerabilities some of which are predictable and most of them unpredictable. Standard mechanisms may not work for unpredictable incidents. This course focuses on identifying the need for effective security management within organizations, developing knowledge and skills to assess security in organizations, and to incorporate appropriate levels of security in various stages of a system's lifecycle considering legal, cost, privacy and technology constraints. This course establishes a foundation for developing comprehensive and proactive security programs to ensure protection of an organization's information assets. Topics covering governance and security policy, threat and vulnerability management, information leakage, crisis management and business continuity, legal and compliance, security awareness and security implementation considerations are covered in the course. Standards such as the ISO/IEC 27001 which is well-known for providing requirements for an information security management system are briefly discussed.

430604	Security Risk Analysis and Management	3 Cr. Hr.

Risk management processes assesses the overall security condition of organizations, analyses the collected data and plan to select appropriate security controls to implement it. The objective of this course is to enable students to understand the details of risk management and develop a basic risk management program for security of organization's information assets. The course will discuss in detail the phases of risk management lifecycle, the details of risk management process including risks and their components, risk assessment and risk mitigation, different risk assessment frameworks like COBIT, ISO/IEC standards, NIST framework etc., risk profiling, risk treatment strategies and risk monitoring. Security policies help to define the ways to implement the planned security in the form of written documents like security procedures, guidelines and recommendations. The course will also focus on understanding different types of security policies including general security policy, issue specific policy and systems policy. At the end, the course will focus on planning and building a risk management program in detail.

430605	Security in IoT and Wireless Networks	3 Cr. Hr.

This course introduces the fundamentals and state of the art in wireless network security. The course will cover wireless vulnerabilities and attacks at various layers of the protocol stack, from the physical layer up to the application layer and include service security issues. The first part of the course addresses conventional wireless networks and begins by introducing the wireless security basics and physical layer security including wireless electronic warfare: jamming, anti-jamming, source localization and target-tracking. Subsequently, link-layer threats are discussed including wireless encryption, selfish and malicious behavior. Wireless multihop networks are explored from network security, privacy, trust, and reputation perspective along with attacks such as black hole, flooding, Sybil, and warm hole. The course briefly addresses security aspects in cellular networks. The second part of the course focuses on vulnerabilities, attacks and countermeasures for the Internet of Things (IoT) ecosystem including IoT security architecture, security classification, IoT privacy, authentication and authorization, cloud integration, attacks and mitigation strategies, and techniques for IoT communication and applications.

430606	Advanced Cryptography	3 Cr. Hr.

The objective of this course is to develop a foundational understanding of cryptography as used in the real world. The course introduces the mathematical background required to understand the basics of cryptography. Topics on number theory, modular algebra and discrete log problems are covered. The course advances with classical cipher design and analysis, modern private key block cipher design, modes of use, stream ciphers and analysis. The course provides an extensive coverage of the techniques and methods needed for the proper functioning of the public key encryption algorithms. The key exchange problem and solutions using the Diffie-Hellman algorithm are discussed. The course defines one way functions and trap-door functions and presents the construction of Message Authentication Codes (MAC) and hash algorithms and schemes. The course includes key management and distribution including PKI.

430608	Network Security and Its Applications and Monitoring	3 Cr. Hr.

Most of the serious attacks on computer systems involve exploitation of the underlying network infrastructure, either as the target of attack or as a vehicle to launch attacks on end systems. This course provides an in-depth study of network attacks and corresponding defense mechanisms. The course covers three broad areas within network security: 1) Network Attacks: eavesdropping, distributed denial of service, malware, phishing, worm and virus propagation, social engineering 2) Countermeasures: demilitarized zones, firewalls, intrusion detection systems, deep packet inspection, secure routing protocols, domain name system, secure socket layer, IP security, virtual private networks, VoIP, and 3) Future Trends: security aspects of software-defined networks, Internet of Things, smart gird, cloud based systems and next generation cellular and wireless networks. The course involves reading, lectures, discussions and a term project.

430610	Ethical Hacking and Penetration Testing	3 Cr. Hr.

Penetration testing enables ethical hackers to legally attempt to locate and exploit computer systems with the intention to make those systems secure. This course covers tools, techniques, and methodologies required for performing network penetration testing. It covers all phases of penetration testing as outlined by different standards such as the Penetration Testing Execution Standard (PTES). Students will be able to build their own penetration testing infrastructure that includes the hardware, software, network infrastructure, and tools needed to conduct penetration tests. The course discusses the tools and techniques required to retrieve sensitive information about a target environment; map the target environment's attack surface by creating a comprehensive inventory of machines, accounts, and potential vulnerabilities; understand different kinds of exploits that penetration testers use to compromise target machines, and post-exploitation activities including gathering information from compromised machines. High-level structure of a penetration test report to document findings will also be discussed in the course.

430612	Malware Analysis	3 Cr. Hr.

The increasingly networked nature of the world has also enabled the spread of various types of malicious software, from a simple adware to more sophisticated Cyber-weaponry. This course will provide the students with the knowledge and skills to detect, analyze, understand, control, and eradicate malware which is an increasingly important issue in information security. This course provides students with an understanding of the issues and techniques used in malware detection and classification. This course will introduce students to the detailed process of malware analysis, packing and unpacking of malwares, static and dynamic analysis of malware, and the malicious activities and techniques. The course also focuses on how to overcome malware tricks like obfuscation, anti-disassembly, anti-debugging, and anti-virtual machine techniques. The course will equip the students with the skills needed to use advanced tools and methodologies that perform malware analysis.

430616	Cloud Computing Security	3 Cr. Hr.

As cloud computing increases its footprint throughout the world, unresolved issues related to security and privacy, data integrity and availability are raised. The fundamental question is how to protect the critical data that is increasingly being stored in the cloud? This course explores cloud computing models, thread models and security issues pertaining to cloud-based systems and explores how to build a security strategy that keeps data safe and mitigates risk. The major topics covered include infrastructure security, attacks and attack surfaces in a cloud, data security in clouds, secure computation and outsourcing, privacy in clouds, virtual machine security, trustworthy clouds, cloud forensics, cloud network security, cloud malware and regulatory compliances. The course also discusses industry best practices for cloud security and discusses how to architect and configure security-related features in a cloud platform.

430618	Seminar	3 Cr. Hr.

Graduate Students are writing scientific research proposals. They are simulating mathematical and experimental methods as scientific research tools. They are reviewing, analyzing and. Project.

430620	Advanced Database Security	3 Cr. Hr.

The objective of this course is to develop a foundational understanding of principles and practices of implementing computer database security in modern businesses and industries, including database security principles, database auditing, security implementation and database reliability. This course will focus on: Security issues faced by enterprises, typical database product, security architecture, operating system security principles, administration of users, profiles, password policies, privileges and roles, database application security models, database auditing models, application data auditing, practices of database auditing.

430625	Research Methodology	3 Cr. Hr.

Research Methodology is a graduate-level course that provides students with basic knowledge and insights into the theory of science, qualitative and quantitative research methodology and research ethics. The course will enable students to read and critically assess technical papers, identify and use criteria for good scientific practice, conduct literature review and use existing knowledge from literature to generalize and identify open areas. Students will be introduced to tools and techniques for selecting research topics, devising research questions, identifying hypotheses, planning and conducting research. Different types of research including case studies, survey, experimental, action and qualitative research are discussed. Statistical methods for data collection, sampling, measurement, data analysis and inference will be covered. Different forms of result analysis including quantitative, qualitative and mixed data analysis will also be covered in detail. The course also introduces students to ethical issues in research and appropriate documentation of research processes and outcomes. After completion of this course, students will have an overall understanding of quality in research and utilize this ability to reason in a

critical manner, ensure quality control and further development of the knowledge present in the scientific literature.

430626	Security of Internet Applications and Distributed Systems	3 Cr. Hr.

Web applications are simultaneously one of the most widely used and widely attacked forms of deployed code. At the same time, the concepts of computer security are best taught within a relatable context so that students can immediately apply their knowledge to relevant situations. The unique challenges inherent in building secure web applications made available to billions of potential users and attackers requires understanding how to use and integrate concepts from software engineering, systems programming, and computer security. This course integrates the concepts that underlie designing, deploying, attacking, and defending web applications to provide students with a foundational understanding of how to design and deploy scalable and secure web applications. This class will teach students the concepts and techniques that enable web applications to maintain high performance in the face of numerous users and attackers. Students will learn and be able to apply software engineering concepts to manage the complexity of client-side and server-side software. Students will learn and be able to apply computer systems concepts to manage the scalability of the web application, and provide performing service to large numbers of simultaneous users. Students will learn and be able to apply computer security concepts to designing a web application which is robust to known and unknown attacks. Students will gain familiarity and facility with modern tools which enable creating applications that apply the aforementioned design, performance, and security concepts. Students will learn and be able to apply fundamental security concepts so that they can evaluate the security of future application designs in the face of potential future attacks.

430629	Graduation Project	3 Cr. Hr.

It can be described as a research experience, where the problem is defined, and a hypothesis is created, experiments are designed to test the hypothesis, and conclusions are drawn.

	Thesis	9 Cr. Hr.

A master thesis provides opportunities for MSc students to plan, complete, interpret, and report research. Thesis projects must not have been published previously.