Module Synopses

Infocomm Security

Provides students with an understanding of infocomm security concepts and issues. Students will be able to identify the risks, threats and the vulnerabilities of the Internet and learn how to defend against security breaches by identifying effective countermeasures to be taken against identified vulnerabilities. Students will also learn about ethical and responsibility issues through case studies of security breaches.

Network Fundamentals

Equips students with the fundamental concepts and skills in data networking, both wired and wireless. Students will learn basic network devices, functions, standards, and protocols and will acquire basic networking skills like designing and setting up a local area network.

Fundamentals of Programming

Aims to help students pick up a programming language and learn how to solve and automate tasks through programming. Students will be taught programming fundamentals such as variables, data types, operators, control structures, methods and data structures such as arrays. At the end of the module, students will be competent in using programming for problem solving.

Digital Forensics and Investigation

Equips students with the fundamental concepts and techniques of computer and mobile forensics. Students will learn to acquire, analyse and present both computer and mobile data as evidence. This module will cover tools and techniques of computer and mobile forensics, data recovery, imaging and storage of electronic evidence.

Programming in Security

Introduces students to a common programming language and the libraries to code simple security applications. The basic programming techniques and constructs in this programming language will be explained, including regular expressions, functions, data structures (eg lists, tuples and dictionaries), classes and use of security modules like nmap. This module strives to build up the foundation in programming for cyber security and develop students towards problem solving and coding practical IT security applications..

Applied Cryptography

Teaches students the principles and application of cryptography to secure data and network. Different encryption algorithms and techniques will be introduced, including conventional and public-key cryptography, authentication and digital signatures. Students will learn to apply these concepts to secure and authenticate electronic mails and messages. Key management, digital certificates and public-key infrastructure will be discussed to understand the deployment of public-key cryptography.

Ethical Hacking

Aims to introduce students to the methodologies used in vulnerability assessment and penetration testing. Students are taught offensive skills for the organisation's wired and wireless networks in order to understand vulnerabilities in computer and information systems.

Cyber Defences

Provides students with a foundation on network and systems security to protect computer resources. Students are taught defensive skills for the organisation's wired and wireless networks in order to protect important assets against hackers.

Computer Law and Investigation

Examines the criminal trial process and cases involving computer hacking, denial of service, modification of data, distortion and fabrication of information. Students will examine the Computer Misuse and Cybersecurity Act, Evidence Act and the Criminal Procedure Code when dealing with the various cyber threats issues.

Secure Coding

Covers the concepts and fundamentals of secure coding principles, and techniques to prevent security vulnerabilities in web applications. Through a series of hacking and coding practical exercises, students will learn the implications of insecure code in applications and subsequently how to defend their web applications against potential hackers by coding securely.

Securing Microsoft Windows

Aims at equipping the students with hands-on knowledge in securing and hardening a Windows operating system. The course will cover the security mechanism used in the operating system, configuring different levels of security measures, best practices and security related tools and utilities.

Linux Administration and Security

Teaches students on the use of various Linux commands / system tools for user management, security administration, software installation, network administration and configuration of services. Students will also learn how to secure the Linux operating system.

Malware Reverse Engineering

Equips students with the basic knowledge of malware analysis to reverse-engineer the malware using practical tools and techniques. The three phases of behavioral, code and memory analysis of malware will be taught. Students will learn how to explore and understand the key characteristics of malware and the techniques of reverse-engineering compiled Windows executables and browser-based malware.

Security Policy and Incident Management

Equips students with the fundamental concepts and techniques of security policy and incident management. Students will learn the essentials of security policy development, risk assessments and security models. Students will also learn to monitor security events, perform network forensics analysis and proactive detection of attacks, and be introduced to security incident response.

Infocomm Professional Seminar

Provides students an opportunity to monitor and integrate emerging technology trends and developments, structured data gathering for the identification of new and emerging technological products, services and techniques. Students are to conduct research and identify opportunities for new and emerging technology to support businesses with consideration of the ethical principles and implications with IT law.