Master of Science/Postgraduate Award in Cyber Security and Management

Developed and awarded by The University of Warwick, UK

MODULE OUTLINES

Security Architectures and Network Defence

This module is designed to be the first module that is studied by students on MSc Cyber Security and Management. It defines the cyber security context and introduces a broad range of cyber security terminology in order for students to comprehend future study concerning the cyber domain.

The overall aim of the module is for students to comprehend the common security controls available to prevent, detect and recover from network security incidents and to mitigate risk.

Information Risk Management and Governance

This module develops an understanding both of the risks that digital information and network assets are exposed to, and of how to manage the risks for the benefit of the enterprise; this includes home users, e commerce, and all organisations using digital networks for infrastructure, both closed and open. Therefore, this module is relevant for the majority of organisations in existence today or likely to exist in the future.

Digital Forensics

Digital forensics seeks to overcome the substantial challenges of drawing correct inference from digital data, so that decisions about the identity of the wrongdoer, and the sanctions that follow, may be made with greater confidence from a better informed perspective.

There are a number of principles that have been established by the digital forensics community. From these a range of tools and techniques have been developed for doing standard things in typical circumstances. Analysing the capabilities and limitations of these tools and techniques is an important part of the module. Representing what has been inferred to a non specialist audience is also a critical part of any investigation and is practised in the module.

Ultimately, this module exposes the student to the entire investigative lifecycle of a case.

Crypto Systems and Data Protection

This module aims to give students critical insight into how to select the appropriate cryptographic solution to solve the information assurance problem at hand. The properties and uses of cryptographic hashes are critically analysed. Particular attention is given to their role in assuring data integrity and in password management. Different attacks (brute force, dictionary, rainbow tables, synthetic collisions) and mitigations (salting, stretching, large keyspace) are also analysed.

Industrial

Procurement and Inventory Management

This module puts emphasis on the design and management of processes and control systems of the inbound supply chain. The content that is covered in this module includes procurement processes and strategies, risk pooling and multi-stage inventory control systems, value of collaboration and streamlined information and financial flow in supply chains, supplier relationship management as well as elementary and advanced methods for analysis and planning.

Project Planning, Management and Control

This module treats the management of "projects" in the widest context of a business activity with specific limited objectives and timescale, and encompasses both product development and "change" projects. It provides an appreciation of the issues and current techniques for successful project planning and control, including the selection and motivation of project teams.

Supply Chain Management

This the appreciation