Course Content

MC6001: Computer Security

This course aims to equip you with foundational knowledge on issues and techniques required for cyber security. You will learn different security policies and security models and have the ability to recognize security features and discover pitfalls in computing systems, including the operating system and basic software vulnerabilities. Includes: Access controls, passwords and biometrics, user tokens, identity management, unix security, introduction to software security like buffer overflows etc. Case studies included.

MC6002: Application Security

Application security architectures and framework; You will learn these applications & its vulnerabilities: Security of payment card system, email security, web security: various attacks such as cross scripts, SQL injection.; key issues in penetration testing, introduction to mobile and cloud security

MC6003: Cryptography

This course focuses on both mathematical and practical foundations of cryptography. The course discusses random numbers, asymmetric and symmetric cryptography, digital signatures and hash functions, intro to HTTPs. Module includes study of security of cryptosystems such as RSA, AES, Elliptic Curve

MC6004: Security & Risks Management

The course aims to identify the problems associated with info-security management through understanding case studies.

To effectively address them, one needs to design solutions that encompass multiple dimensions, including technology, people, processes and (internal as well as external) regulations. This course provides an introductory but broad perspective of cyber and info-security.

MC6005: Industrial Attachment

Industrial attachment (IA) is a very important component, accounting for 6AU. It gives students a platform to practise what they have learnt, and a chance to expose them to real working environment. This will be helpful in their career search in cybersecurity. All students will have to complete and pass a 3-4.5 month (exact length is set by company, not students) Industrial attachment once they complete all their coursework requirement of 8 modules (4 compulsory & 4 electives). Our office will supply them a list of interested companies. Students are also free to source for their own company subject to program chair agreement. Student will have to write a short report on what they have done during the industrial attachment.

MC6011: Network Security

Introduction to networking and security as applied to networks. Exercises cover network programming in a language of the students' choice. Understanding and analyze packet traces using tools like Wireshark. After this course, the student will have a fundamental understanding of networking, TLS and security as it applies to networked systems.

MC6012: Cyber Physical Systems Security

In this course, you will learn about the basics of cyber physical systems, including the design principles and methodologies. There is also a detailed treatment of the security challenges for cyber physical systems, which vary in practice due to the diverse nature of the application environment of cyber physical systems. These different forms of security breaches, observed across diverse cyber physical systems, will be put in a well-characterised taxonomy. The techniques to handle these attacks will be described in a generic manner, including key management and wireless/RFID communication. The attack surfaces and protection/mitigation principles will then be elaborated with practical case studies, such as automotive & smart card systems and smart grid.

MC6013: Software Security

The course presents the challenges, principles, mechanisms and tools to make software secure. We will discuss the main causes of vulnerabilities and the means to avoid and defend against them.

The focus is on secure programming practice, including specifics for various languages, but also covering system-level defences (architectural approaches and run-time enforcement). We will also apply software analysis and vulnerability detection tools in different scenarios.

MC6014: Security Monitoring & Threat Detection

Module focuses on technical aspects of operational security: system management, situational awareness, security monitoring and incident management.

System security functions such as managing the lifecycle of system components via configuration and change management, malware protection, and the provision of backup and recovery services. Security policies and their implementation and management, ranging from network segmentation to user access control, will also be covered.

Module will also cover security situational awareness, that is, strategic input to audits and assessments by gathering information about potential threats and vulnerabilities.

External sources such as threat intelligence services and security alerts and advisories will also be discussed along with how to supplement these by proactive organisational information gathering via honeypots and penetration tests.

Security monitoring to identify immediate threats, as well as providing a capability to analyse long term trends in incidents and user behaviour, will be discussed. Technical monitoring to consolidate and analyse inputs from system events and intrusion alerts will also be covered along with a discussion of how user behaviours, such as accesses or transactions, may be monitored to identify suspicious or fraudulent activity.

Module will also cover Incident Management, including topics such as analysis and containment of the security incident, recovering operational capability and reporting of any lessons learned.

MC6015: Malware

Taxonomy of Malware; Malicious malware activities; Malware analysis: static analysis, dynamic analysis, fuzzing, symbolic execution, concolic execution; analysis environments, anti-analysis and evasion techniques; Malware detection; Malware Response

MC6016: Forensics

This course is concerned with the acquisition, analysis and reporting of digital evidence concerned with a security event or crime. The course includes evidential requirements, gathering evidence, the forensic process and associated tools, core digital artefacts, and domain-specific issues. Evidence gathering includes the established seizure and imaging process and also extends to situations where the baseline processes are not feasible, such as smartphones, volatile data, and selective recovery from network storage. Related process issues such as triage and search and discovery techniques will also be explored, as will approaches to assurance of the tools used in the forensic process. Presentation and reporting aspects specific to forensic evidence will be described. Core digital artifacts include disk and file systems, date and time records, operating system components, and evidence resulting from network activity.

MC6017: Topics in Crypto and Cybersecurity

Crypto Topics: Secure cryptosystem, crypto acceptance tests, dealing with vendors, managing project. Latest algorithms breakthrough, latest major cybersecurity security incidents.

Hardware Topics: Security Evaluation/Certification, Applications/ Reasons for Security, hardware security analysis via chip analysis, Design for Trust, Hardware trojans, Side-Channel attacks.

MC6018: Blockchains and Cryptocurrency

Following Bitcoin's mainstream adoption, the attention has shifted to the broader use of blockchains and distributed ledger technologies for enhancing the integrity and non-repudiation properties of processes, such as via smart contracts. This course will cover the evolution of blockchains, from the theory underpinning Bitcoins, to the generalisation of these to blockchains, and subsequent smart contracts and distributed ledge technologies. Practical sessions will be conducted to teach participants to write smart contracts in purpose-built languages such as Ethereum. We will also discuss the utility of these technologies to better understand the hype and their potential, particularly for cyber security applications.

MC6019: Privacy Preserving Technologies & Security in AI

This course covers the recent progresses in the field of fully homomorphic encryption, secure multi-computation, searchable encryption, allowing larger degree of freedom of data sharing without undermining the confidence in protecting the confidential information. The same is allowed in machine learning.