Programme Content

Course Code	Core Courses
SE6001	Computer Security
SE6002	Application Security
SE6003	Cryptography
SE6011	Network Security
Elective Courses	
SE6004	Security & Risks Management
SE6013	Software Security
SE6014	Security Monitoring & Threat Detection
SE6015	Malware
SE6016	Forensics
SE6020	Mobile, Cloud, Zero Trust
SE6021	Introduction to AI & Cyberthreat Intelligence - *TBC*
SE6022	Cybersecurity & AI
SE6005	Capstone Project

***Note: Not all courses listed in the curriculum will be offered in a semester. Courses offered are subject to availability of instructors and resources.**

SE6001: 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.

SE6002: 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

SE6003: 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, and intro to HTTPs. Module includes study of security of cryptosystems such as RSA, AES, Elliptic Curve

SE6011: 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.

SE6004: 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.

SE6013: 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 defenses (architectural approaches and run-time enforcement). We will also apply software analysis and vulnerability detection tools in different scenarios.

SE6014: 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.

SE6015: 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

SE6016: 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.

SE6020: Mobile, Cloud, Zero Trust
This course explores contemporary security domains that are critical in today's digital ecosystem: Mobile Security, Cloud Security, Application Security, and Zero Trust Architecture. You will learn threat models, mitigation techniques, and tools to design secure systems across mobile platforms, cloud environments, and hybrid infrastructures. This course is designed for students interested in pursuing a career pathway focused on systems and application security, with an emphasis on relevant job roles and industry expectations.

SE6022: Cybersecurity & AI
This course aims to provide students with a comprehensive understanding of the intersection between artificial intelligence (AI) and cybersecurity, from both application and security perspectives. It is designed to equip students with the knowledge and skills to leverage AI techniques for solving complex cybersecurity problems, as well as to identify, analyse, and mitigate security risks inherent in AI-driven systems.

The course will develop students' ability to apply AI and machine learning methods to domains such as threat detection, malware analysis, security monitoring, and threat intelligence. In parallel, it will introduce the emerging security challenges associated with AI systems, including adversarial machine learning, data poisoning, model exploitation, and AI supply chain risks.

Through a combination of conceptual foundations and applied learning, the course aims to foster critical thinking, system-level understanding, and practical problem-solving skills. Students will gain the ability to evaluate the effectiveness, limitations, and risks of AI-driven cybersecurity solutions, and to design robust and secure AI-enabled systems suitable for real-world deployment.

SE6005: Capstone Project

This course is a very important component, accounting for 6AU.

Students can complete this component by going on internship or doing a cybersecurity project.

The course requires 2 semesters to complete. Internship 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.

The internship duration must be at least 3 months (exact length is set by company, not students). Student will have to write a report on what they have done during the internship. The cybersecurity project gives students unique hands-on opportunities to realize cyber security workflow taught in the program for domain-specific applications. It gives an opportunity to students to work with faculty in CCDS and other schools to solve inter- disciplinary cyber security problems. Our office will provide a list of projects proposed by faculty. Students will have to submit a master project report.