MASTER OF SCIENCE IN INFORMATION ASSURANCE PROGRAM

DEPARTMENT OF COMPUTER SCIENCE

HAMPTON UNIVERSITY

HTTP://SCIENCE.HAMPTONU.EDU/COMPSCI/

The Master of Science in Information Assurance focuses on providing a broad interdisciplinary information assurance education that prepares graduates to successfully defend, protect, design, implement and maintain secure information and information systems.

Graduates of the M.S. degree program in Information Assurance have the requisite expertise to:

- Function in the world-at-large as productive and ethical professionals and as responsible citizens. They will have a very good understanding of ethical issues and their applications.
- Understand and employ current trends and adapt to advances in the technology of the Information Assurance profession.
- Develop and implement security strategies to improve the security posture of organizations.
- Work in teams, to apply theoretical and analytical methods and principles of software development to address security issues in software development.
- Apply techniques, methodologies, tools and skills to build high-quality security systems that function effectively and reliably in the emerging information infrastructure.
- Communicate effectively, both orally and in writing, with other security and computing professionals.

The MS IA program is designed for prospects with an undergraduate degree in Computer Science or a degree in engineering, science or mathematics with a strong background in computer science. For prospects without the appropriate qualifications, a set of bridge courses provide the necessary background for regular admission to the MS program.

Graduates of the program who complete the appropriate courses will also receive Senior Systems Managers, CNSSI 4012. With System Administrators (SA), CNSSI 4013 pending. [1]

BRIDGE PROGRAM IN INFORMATION ASSURANCE (NON-DEGREE PROGRAM)

The Bridge Program in Information Assurance prepares students for graduate work in the Master of Science program. The main goal of this program is to provide students from other disciplines with the necessary background to pursue a Master's degree in Information Assurance. A secondary goal is to provide formal training for people in various technical disciplines who need significant background in computing. The Bridge Program consists of comprehensive courses at the 500-level that provide the equivalent of the core undergraduate computer science curriculum. This core set of courses is listed in the curriculum for the Association of Computing Machinery (ACM) which sets the standards for undergraduate curricula. The following minimum requirements must be met before a student can be admitted to the program:

- A bachelor's degree of higher
- Two semesters of calculus and one semester of discrete mathematics
- Formal training or experience in programming to the level of Computer Science 501

[1] http://www.cnss.gov/instructions.html

Degree Plan of Study: Information Assurance

Bridge Program Requirement (if applicable)

Department	Course	Title	Credit
CSC	501	Programming	4
CSC	506	Advanced Programming and Data Structures	3
CSC	507	Architecture and Operating Systems	3

Core Courses (24 Hours + Comprehensive Examination 1 Hour)

Department	Course	Title	Credit	Certification
CSC	510	Mathematical Foundations	3	4013[2]
CIA	523	Ethics, Law and Policy in Cyberspace	3	4013
CIA	582	Introduction to Information Assurance	3	4012[3], 4013
CIA	583	Secure Software Engineering	3	
CIA	610	Cryptography	3	4013
CIA	670	Computer Forensics and Incident Handling	3	
CIA	675	Computer Viruses and Malicious Software	3	4013
CIA	683	Advanced Computer and Network Security	3	4012, 4013
CIA	702	Comprehensive Examination	1	

Elective Courses (12 Hours)

Department	Course	Title	Credit	Certification
CIA	684	Systems Security Administration, Management, and Certification	3	4012
CIA	685	Risk Management	3	4012
CIA	686	Systems Security for Senior Management	3	4012
CIA	690	Network Security and Intrusion Detection	3	
CIA	691	Wireless Networks	3	
CIA	692	Secure Distributed Computing	3	
CIA	695	Special Topics	3	

[2] CNSSI 4013 System Administrator is pending

[3] Pending clarification.

COURSE DESCRIPTIONS

CSC 510 Mathematical Foundations Lecture 3/Credit 3.

Propositional and Predicate Calculus. Proof techniques. Queuing theory. Mathematical formulations of data structures. Basic models of computation expressions and grammars. Prerequisite: Discrete Mathematics and Data Structures.

CIA 523: Ethics, Law and Policy in Cyberspace Lecture 3/Credit 3

Study of ethical issues, legal resources and recourses, and policy implications inherent in our evolving online society. Provides an overview of the ethical challenges faced by individuals and organizations in the information age. Introduces the complex and dynamic state of the law as it applies to behavior in cyberspace. Prerequisite: Graduate standing.

CIA 582 Introduction to Information Assurance Lecture 3/Credit 3

An introduction to the various technical and administrative aspects of Information Security and Assurance. This course provides the foundation for understanding the key issues associated with protecting information assets, determining the levels of protection and response to security incidents, and designing a consistent, reasonable information security system, with appropriate intrusion detection and reporting features. The purpose of the course is to provide the student with an overview of the field of Information Security and Assurance. Students will be exposed to the spectrum of Security activities, methods, methodologies, and procedures. Coverage will include inspection and protection of information assets, detection of and reaction to threats to information assets, and examination of pre- and post-incident procedures, technical and managerial responses and an overview of the Information Security Planning and Staffing functions. Prerequisite: Graduate standing.

CIA 583: Secure Software Engineering Lecture 3/Credit 3

An overview of methodologies, tools and techniques for producing secure software systems. Students will cooperatively develop a secure software product. The course will also provide an introduction to professional resources and ethical issues for software developers. Prerequisites: CIA 582.

CIA 610 Cryptography Lecture 3/Credit 3

Cryptographic techniques to achieve confidentiality, integrity, authentication and non-repudiation are examined. The underlying mathematical concepts are introduced. Topics to be covered include symmetric and public key encryption, hashing, digital signatures, cryptographic protocols and other recent developments in the field. Prerequisite: CSC 510

CIA 670 Computer Forensics and Incident Handling Lecture 3/Credit 3

Identifying, acquiring, preserving, and analyzing electronic evidence from single machines, networks, and Internet. It will explore both technical and legal issues of computer forensics investigations. Topics include forensics law and regulation issues, incidence response, open and commercial tools, evidence recovery theory and practice of computer file systems, memory, registry, network logs and communications. Special focus will be given to windows systems and networks.

CIA 675 Computer Viruses and Malicious Software Lecture 3/Credit 3

This course involves the study of malicious software (malware) including computer viruses, worms, and Trojan horses. Topics include the various mechanisms used in the construction of malicious software; existing commercial anti-virus software; preventative and reactive means for dealing with malicious software on workstations, servers, and in networks; training and education of users; and reliable sources to monitor for alerts as well as the prevention of hoaxes.

CIA 683 Advanced Computer and Network Security Lecture 3/Credit 3.

Introduction to security problems in computing and networking. Information Security Models. Encryption and decryption techniques. Cryptographic protocols and practices. Operations Security. Program Security. Security in networks and distributed systems. Database Security. Electronic commerce security. Legal and ethical issues in computer and network security. Prerequisite: CIA 582.

CIA 684 Systems Security Administration, Management, and Certification Lecture 3/Credit 3.

Outlines the principles of systems security administration, management, and certification. Provisioning, procurement and installation of network, hardware and software systems for mission critical enterprises. System configuration and maintenance. Incident handling and response. Facilities Management. Contingency Plans. Law, standards of contract. Operations Management. System certification, testing and validation. Prerequisite: CIA 582.

CIA 685 Risk Management Lecture 3/Credit 3

Outlines the aspects of computer security and risk management. Accreditation, implementation, extension, and operation principles for secure information systems. Security policy and plan development. Contingency, continuity and disaster recovery planning. Incident handling and response. Prerequisite: Prerequisite: CIA 582.

CIA 686 Systems Security for Senior Management Lecture 3/Credit 3

Develops the knowledge necessary for senior security management to analyze and judge the reported systems for validity and reliability to ensure such systems will operate at a proposed trust level. Topical review and discussion on current trends in CNSS 4012 standard. Includes grant final approval to operate, grant review accreditation, verify compliance, ensure establishment of security controls, ensure program managers define security in acquisitions, assign responsibilities, define criticality and sensitivity, allocate resources, multiple and joint accreditation, assess network security. Prerequisite: CIA 582.

CIA 690 Network Security and Intrusion Detection Lecture 3/Credit 3

Provides a comprehensive overview of network security and intrusion detection. Topics include security overview, authentication, attacks and malicious code, communication security, Web security, network security topologies, intrusion detection, firewalls and VPNs, security baselines, security algorithms, physical security, disaster recovery, forensics overview, and other state-of-the-art developments.

CIA 691 Wireless Networks — Lecture 3/Credit 3

Examines security of wireless networks which have become ubiquitous such as cellular networks, wireless LANs, mobile ad hoc networks, wireless mesh networks, and sensor networks. Unprotected wireless networks are vulnerable to several security attacks including eavesdropping and jamming that have no counterpart in wired networks. Topics will include: authentication, secure hand-offs, key management in wireless networks, attacks on MAC protocols, selfish and malicious behavior in wireless routing protocols, secure multicast.

CIA 692 Secure Distribute Computing — Lecture 3/Credit 3

Covers theoretical and applied aspects of security and privacy needed for the middleware and service-ware architectures to offer reasonable assurance for modern distributed systems. Topics include cloud computing, distributed storage systems, virtualization, distributed systems architectures, technologies and management; distributed system design, security and privacy issues; and applications such as Web services and mobile commerce.

CIA 695 Special Topics in Information Assurance — Lecture 3/Credit 3

A treatment of advanced topics of interest in Information Assurance not routinely covered by existing courses. May be repeated when topics vary. Prerequisite