CAPITOL COLLEGE

1927

Master of Science in Information Assurance

For every advance in information technology, there seems to be a corresponding increase in the potential for a disastrous network breach. Experience how to tackle a breach from every angle – before, during, and after. The National Security Agency and Department of Homeland Security have designated Capitol College a National Center of Academic Excellence in Information Assurance Education. The Master of Science in Information Assurance (MSIA) curriculum is mapped to all current federal domains at the most advanced level specified in the standards, and also covers the 10 domains of the CISSP (Certified Information Systems Security Professional).

This online program is designed for information system professionals who desire to professionalize their skills and boost their credentials. The curriculum is geared toward government and corporate IT security professionals by providing in-depth instruction on new security ideas, concepts, and techniques to prevent, protect, and react to malicious intrusion and to secure information assets.

- Online course delivery with audio – using VoIP
- Real-time lectures in the evening (EST) – recorded for later playback
- No resident requirement – earn your degree from home or on the road
- Transfer up to 9-credits of equivalent graduate coursework

MSIA CURRICULUM (36 credits)

Required Core Courses (24 credits)

IAE-670 Network Systems Security Concepts
IAE-671 Legal Aspects of Computer Security and Information Privacy
IAE-673 Secure Information Transfer and Storage
IAE-674 Security Risk Management
IAE-675 Computer Forensics and Incident Handling
IAE-677 Malicious Software
IAE-680 Perimeter Protection
IAE-682 Internal Protection

Electives (12 credits)

Choose any combination of four courses from the elective options posted in the right-hand column.

For more information, contact:
Office of Admissions
800-950-1992
gradadmit@capitol-college.edu

Capitol College
11301 Springfield Road, Laurel MD 20708
www.capitol-college.edu

Information Assurance Electives

IAE-611 Wireless Security
IAE-621 Applied Wireless Network Security
IAE-679 Vulnerability Mitigation
IAE-684 Complementary Security

Internet Engineering Electives

IE-701 Principles of Designing and Engineering Computer Networks
IE-707 Network Architecture Convergence Using Wireless Technology (prerequisite = experience using OPNET)
IE-712 Design and Practice of Secure Information Networks

Law & Policy Electives

IE-717 Invention, Innovation and the Use of Intellectual Property
MBA-658 Legal, Political, and Ethical Implications for Leadership
SM-587 Law and Regulation of E-Commerce

I.T. General Management Electives

SM-563 Managing Information Systems
SM-567 Telecommunications and Computer Networks
SM-569 Decision Support and Expert Systems

IAE-611 Wireless Security (3 credits)
This 8-week course provides students with an in-depth understanding of the security vulnerabilities in the various methods of wireless communications and their corresponding countermeasures. This course also provides training on practical methods for designing, configuring, testing, and maintaining wireless networks appropriate to their organizations' operating requirements. Students will be introduced to wireless network protocols, access modes, portable communications and computing devices, management tools, security solutions, and current industry best practices for managing wireless communications in a secure environment. Case studies will be used throughout the course. Offered every 8-week term.

IAE-621 Applied Wireless Network Security (3 credits)
This 16-week course provides students with practical, real-world experience with wireless network security with an understanding of wireless fundamentals, wireless network threats, tools to test wireless security, and safeguards. Specifically, this course provides a CD-ROM of the most popular hacking, cracking and wireless security network analysis tools and trains students to use them to test and secure wireless networks. This course will train students on current industry best practices for managing wireless networks in a secure environment. Students will be required to purchase and install wireless network equipment to create a home wireless network for the purpose of conducting experiments on various wireless security vulnerabilities and countermeasures. Case studies will be used throughout the course. Offered every 16-week semester.

IAE-670 Network Systems Security Concepts (3 credits)
This 8-week course explores security terms, definitions, concepts, and issues that face industries today. This course also will examine how the concept of security, and being secure, integrates into the overall enterprise mission. The importance of user involvement, security training, ethics, trust, and informed management will be explored. Offered every 8-week term.

IAE-671 Legal Aspects of Computer Security and Information Privacy (3 credits)
This 8-week course provides an overview of the legal rights and liabilities associated with operation and use of computers and information. It discusses the key statutes, regulations, treaties, and court cases (in the United States and abroad) that establish legal rights and responsibilities as to computer security and information privacy. The course also helps students to learn how to reduce their risk of potential legal liability for computer security or information privacy failures, and how to enforce their security and privacy rights against other parties. Case studies and lessons learned from information security failures are used throughout the course. Offered every 8-week term.

IAE-673 Secure Information Transfer and Storage (3 credits)
This 8-week course will provide the student a history of cryptography from Caesar's cipher to elliptic-curve cryptography of today. Students will study public and private key algorithms and understand their functionality, and how they work with network protocols. One-way hashes and Digital signatures will be discussed, and used by the students in submissions to the instructor. Public-key infrastructure with certificate authorities and web-of-trust infrastructure methods will be learned. Offered every 8-week term.

IAE-674 Security Risk Management (3 credits)
This 8-week course will begin with an understanding of why risk management evaluations are useful. This class will discuss the general methodologies for security risk assessment and security test and evaluation, including the interviews and documentation research necessary. The student will be provided practical lab exercises to provide a hands-on analysis of a fictitious site. Detection, recovery, and damage control methods in contingency/disaster recovery planning research, documentation and training; methods of and procedures for contingency planning and security policy formulation and enforcement. Offered every 8-week term.

IAE-675 Computer Forensics and Incident Handling (3 credits)
This 16-week course begins with lectures discussing the laws and rights to privacy by individuals and what organizations may or may not do. Online ethics are considered. It then moves on to understanding incident handling and how incident response teams work, managing trouble tickets, and basic analysis of events to determine if an incident has occurred. It concludes with computer forensics issues and practices, and rules of evidence. Offered every 16-week semester.

IAE-677 Malicious Software (3 credits)
This 16-week course examines malicious software detection and malicious software defenses including tripwire and signature software techniques. Viruses, worms and Trojan horses, logic bombs, malicious CGI scripts will be discussed. Students will review the anatomy of well-known viruses and worms to understand how they work. Mobile code issues as they apply to web and application technologies and resulting insecurities will be discussed in detail. Students will then review the underlying methodologies used by the anti-virus vendors and freeware offerings to protect electronic assets from harm or other compromise. Offered every 16-week semester.

IAE-679 Vulnerability Mitigation (3 credits)
This 8-week Defense-in-Depth course provides the student detailed understanding of the need for internal and external vulnerability assessment. An integral technical part of any risk management program, this course goes hand-in-hand with the more analytical practices in IAE-674. Offered every 8-week term.

IAE-680 Perimeter Protection (3 credits)
In this 16-week Defense-in-Depth course, firewalls and network IDS issues will be discussed. A detailed understanding of firewall configuration and rule sets, load balancing, web farms, wireless access, web security issues and network intrusion detection will be explored to prepare the student with the basic tools to coordinate the design and implementation of perimeter network defenses for a high-volume, high-access site. Offered every 16-week semester.

IAE-682 Internal Protection (3 credits)
This 8-week course explores the protections available to the practitioner through host operating systems and third party equipment and software, to protect the inner network from the attacker who has successfully circumvented the perimeter or from the disgruntled insider. Use of methodologies including host-based intrusion detection methods, audit settings and review PC Firewalls, host operating hardening for Linux and Windows 2000, and Virtual LANs will be reviewed. Offered every 8-week term.

IAE-684 Complementary Security (3 credits)
This 16-week class discusses security disciplines that are important to the rounded InfoSec or information warfare professional, such as personnel security, physical security, and operational security. Additionally authentication standards in practice will be discussed as an advent of operational security, including RADIUS, TACACS+, Kerberos, NTLM2 and biological methods. Offered every 16-week semester.