COMPUTER SCIENCE

Dr. Felicia Doswell, Department Head (I)
(757) 823-9454

Formed in 1990, the Norfolk State University Department of Computer Science was designed to provide students with fundamental training in the theoretical and practical aspects of computer science and information technology. The department offers a general computer science degree and options in Information Assurance, Information Systems and Computer Engineering. This wide range of options gives students the opportunity to pursue studies in Cybersecurity, Robotics, Software Engineering, Computer Networking, Web Design and Development.

The Bachelor of Science degree in Computer Science at Norfolk State University is accredited by the Computing Accreditation Commission of ABET, https://www.abet.org (https://www.abet.org/), under the General Criteria and the Computer Science Program Criteria.

The Department of Computer Science offers the B.S. Degree in Computer Science, which includes the following specialty areas:

- Computer Science (General Program)
- Computer Engineering
- Information Systems
- Information Assurance

The program addresses a number of career opportunities within the curriculum. The Computer Engineering option is suitable for students who are interested in the design and implementation of hardware. The Information Systems option qualifies students for employment in business environments. The Information Assurance option is suitable for students who have an interest in securing the nation's critical infrastructure from terrorists, hackers, criminals and other individuals intending harm against the nation and its people.

The Department of Computer Science also offers the B.S. degree in Information Technology. The BS.ITE program aims to provide graduates with the skills and knowledge to take on appropriate professional positions in information technology upon graduation and grow into leadership positions or pursue research or graduate studies in the field. This option is suitable for students who are interested in information technology applications especially networking, web design and management.

The Department of Computer Science offers two graduate programs: a Master of Science Degree in Computer Science and a Master of Science Degree in Cybersecurity. The Master of Science degree in Computer Science was initiated in August 2003.

This degree program has a general computer science concentration as well as concentrations in information assurance and communication networks. The Master of Science degree in Cybersecurity was started in 2015. The purpose this program is to produce professionals who will manage, maintain, and integrate cybersecurity in organization settings. The M.S. in Cybersecurity is designed to focus on computer security and to increase the pool of well-educated security professionals. Theory and practical training will be combined with critical thinking and communication skills that are required by professionals in the cybersecurity field. Students will be prepared to apply their knowledge to defend against cyber threats directed toward the USA. In addition, students will be prepared to provide needed cybersecurity services to US agencies and organizations. Students will not only be trained to defend against cybersecurity attacks but also to use digital forensics to identify attackers.

Computer Science Programs

- Computer Science, M.S. (https://catalog.nsu.edu/graduate/science-engineering-technology/computer-science/ms-computer-science/)
- Cybersecurity, M.S. (https://catalog.nsu.edu/graduate/science-engineering-technology/computer-science/ms-cybersecurity/)

Computer Science Courses

Computer Science

CSC 521 Database Principles and Design (3 Credits)
An introductory course emphasizing the basic concepts and principles of database systems. Topics include relational, hierarchical, and network approaches to data organization.

CSC 530 Data Communication (3 Credits)
This course focuses on the basic principles of computer communication, hardware, and software design. Topics include transmission media, data encoding, transmission techniques, protocols, switching networks, broadcast networks, and local area networks.

CSC 535 Computer Security I (3 Credits)
This course is designed for IT professionals to learn computer and network security theories and practices that can be used to significantly reduce the security vulnerability of computers on internal networks or the Internet. Topics include cryptography, program security, operating systems security, database security, network security, security administration, computer ethics, and legal issues.

CSC 555 Management of Information Security (3 Credits)
This course is designed for Security System Administrators and Managers responsible for designing, planning, and managing security installations in Business and Government Institutions. Topics include management of information security, security planning, security protection (technical and procedural), best practices, risk management, operations security, legal issues, and certification and accreditation.

CSC 564 Operating Systems (3 Credits)
Topics include the history and evolution of operating systems, the concepts behind and structure of various operating systems, process scheduling, inter-process communication, input and output, multiprogramming, memory management, and file systems. Concepts of distributed operating systems are also introduced.

CSC 566 Advanced Computer Topics I (3 Credits)
This course covers advanced computer topics not covered in the curriculum. Designed as a Computer Science elective, not as a replacement for any specific required course.

CSC 567 Advanced Computer Topics II (3 Credits)
This course covers advanced computer topics not covered in the curriculum. Designed as a computer science elective, not as a replacement for any specific required course.

CSC 570 Artificial Intelligence (3 Credits)
This course offers an in-depth study of concepts and problem-solving techniques of artificial intelligence. Topics include knowledge representation, functional and logic programming, machine learning, natural language understanding, computer vision, robotics, and societal impact.

CSC 571 Game Design and Development (3 Credits)
This course introduces students to game design and development concepts. Topics include the history of games, genres, play elements, story and character development, game play and storyboard design, level and user interface design, and the game design document.

CSC 572 3D Game Programming (3 Credits)
This is a project-oriented course on 3D game programming. Students will work in teams to design, implement and test a three-dimensional game with interactivity, game state diagram, animation, sound, and constraints. Students will also learn the basics of graphic design and animation.

CSC 573 Modeling and Simulation (3 Credits)
This course introduces students to the major areas of simulation and the languages and systems used in these areas. Areas of simulation covered include gaming, military, health, network, business processes, and transportation. The types of simulation software discussed include process oriented, discrete event oriented, general purpose, and simulation environments.

CSC 576 Advanced Computer Topics III (3 Credits)
This course covers advanced computer topics not covered in the curriculum. Designed as a computer science elective, not as a replacement for any specific required course.

CSC 577 Advanced Computer Topics IV (3 Credits)
This course covers advanced computer topics not covered in the curriculum. Designed as a Computer Science elective, not as a replacement for any specific required course.

CSC 580 Computer Graphics (3 Credits)
This course focuses on interactive computer graphics hardware and software: display devices, 2D and 3D geometric transformations, raster algorithms, representation of curves and surfaces, hidden line removal and surfaces, shading algorithms, and color graphics.

CSC 593 Systems Programming (3 Credits)
Fundamentalsa ofa systema anda networka programming methodology, techniques, system calls, and library calls.

CSC 596 Compiler Construction (3 Credits)
An introduction to the fundamentals of compiler construction and language translation. Topics include lexical analysis, specifications of syntax, algorithms for syntactic analysis, code generation, and optimization techniques.

CSC 611 Machine Learning (3 Credits)
Machine learning is a subfield of artificial intelligence concerned with the design, analysis, implementation, and applications of programs that learn from experience. This course is about learning to extract statistical structure from data for making decisions, predictions, and visualizations. It gives in-depth coverage of advanced methods in machine learning, emphasizes approaches with practical relevance, and discusses a number of recent applications of machine learning.

CSC 612 Computational Science (3 Credits)
This course provides students with an overview of applications of computational skills needed to solve scientific research problems. The computational skills in review include programming languages, algorithms, database implementation, internet technologies, data visualization, statistics, modeling and simulation, and operations research.

CSC 625 Analysis of Algorithms (3 Credits)
This course covers the design and analysis of algorithms. Topics include Turing machines; NP-complete theory; best, average, and worst-case analysis; divide-and-conquer; greedy method; dynamic programming; graph traversal; backtracking and branch-and bound techniques. The course also covers sorting, searching, graph algorithms, and optimization.

CSC 630 Computer Networks (3 Credits)
This is an advanced graduate-level course focusing on the concept of internetworking in general and the TCP/IP Internet technology in particular. The course reviews both the architecture of network interconnections and the principles underlying protocols that make interconnected networks function as a single, unified communication system. It also covers how an internet communication system can be used for distributed computation and communication.

CSC 635 Computer Security II (3 Credits)
This course is an advanced course in Computer Security. It covers topics of current interest in Information Assurance. Topics to be covered include Digital Forensics, Intrusion Detection, Steganography, Security Usability, Cloud Computing, and Wireless Security.

CSC 650 Cryptography (3 Credits)
Study of historical and modern cryptographic techniques and algorithms. Topics include symmetric and asymmetric key cryptography, one-way functions, secure hash functions, digital signatures, key exchange, authentication, key management, PKI, DES, AES (Rijndael), and current topics.

CSC 660 Parallel Computing (3 Credits)
Study of high-performance computing techniques. Includes the study of parallel computer architecture, memory, and I/O. Also, parallel computer algorithms to include shared and distributed memory, parallel computation models, graph algorithms, numerical algorithms, and divide-and-conquer will be covered.

CSC 668 Advanced Computer Architecture (3 Credits)
Principles and advanced topics of the instruction set architecture for uni-processors, embedded system processor, and multi-processor.

CSC 672 Digital Forensics (3 Credits)
This course focusses on cutting-edge topics in Digital and Network Forensics. It introduces students to the applicable laws and ethical responsibilities of a digital forensics professional, the technical skills required, and open research problems in digital forensics. The course includes lectures, discussions, and demonstrations. It is designed around a virtual lab environment that provides robust and realistic hands-on experiences in dealing with a range of digital forensics topics.

CSC 678 Scientific Visualization (3 Credits)
Fundamental concepts of the algorithms and design principles underlying modern 3D computer graphics and data and scientific visualization.

CSC 691 Graduate Independent Study I (3 Credits)
Supervised independent project designed to give computer science graduate students an opportunity to explore a single topic in a one-to-one learning relationship with a faculty member.

CSC 697 Ethical Hacking and Penetration Testing (3 Credits)
An in-depth study of the practical aspects of computer security including the study of common security vulnerabilities in a laboratory setting.

CSC 701 Continuing Registration (1-9 Credits)
A one-credit-hour course that allows students to maintain continuous registration status. Does not count towards the MS.CSC degree credits.

CSC 702 Practicum (1 Credits)
A one-credit-hour course that allows students to apply their skills in a work setting. The credit earned through this course will not be counted towards MS.CSC degree credit. A student can take this course and repeat it up to three times when s/he is away from campus on outside employment for internship or practical training in a related technical field. This is a Pass/Fail course.

CSC 703 Graduate Research (3-9 Credits)
This course provides an opportunity to learn how to conduct research through practical experience with a research advisor. It exposes students to a subset of the following tasks based on the student's knowledge of research activities: development and implementation of a research topic, reviewing technical literature for relevancy to research topics, writing status reports, writing technical reports or papers of conference submission quality, attending and making technical presentations.

CSC 720 Wireless Sensor Networks (3 Credits)
An advanced, graduate-level course focusing on the study of wireless sensor networks from communications, security, and computing platform viewpoints.

CSC 730 Advanced Topics in Networking (3 Credits)
Optical networks, dynamic spectrum access in wireless networks, cognitive radio networks, network coding, and other newly emerged networking technologies are covered. Optical Network topics include WDM network elements, routing and wavelength assignment algorithms, blocking probability analysis, virtual/physical topology design, survivability, and IP over WDM. Other topics include enabling technologies for cognitive radio, channel assignment/selection, routing, security, and spectrum management.

CSC 745 Network Defense (3 Credits)
Focuses on network defense and countermeasures, including firewalls, intrusion detection and prevention systems, virtual private networks.

CSC 750 Evolutionary Computing (3 Credits)
The course covers the fundamentals of applying biological evolutionary characteristics to optimization of very complex problems.

CSC 755 Cloud Computing (3 Credits)
A one-semester graduate-level course focusing on cloud computing technologies and solutions. It is designed to give students a solid foundation in cloud computing fundamentals. The course covers both the conceptual and practical aspects of cloud computing.

CSC 760 Secure Software Development (3 Credits)
Introduction to core concepts and the latest research trends and results in developing secure software. Topics include the best practices in developing secure software within Software Development Lifecycle (SDLC), vulnerability assessment, and code analysis techniques.

CSC 765 Advanced Topics in Information Assurance (3 Credits)
This course covers state-of-the art advances, emerging trends, and threats in cybersecurity. Topics to be covered include current topics in Information Assurance, advanced digital forensics, new approaches to management of cybersecurity and new threats, vulnerabilities and controls.

CSC 781 Advanced Graduate Computer Topics I (3 Credits)
Advanced computer topics that are not generally covered in the graduatea600/700 levela curriculum.aDesignedaas a Computer Science graduate elective, not as a replacement for any core course.

CSC 782 Advanced Graduate Computer Topics II (3 Credits)
Advanced computer topics that are not generally covered in the graduatea600/700 levela curriculum.aDesignedaas a Computer Science graduate elective, not as a replacement for any core course.

CSC 791 Graduate Independent Study II (3 Credits)
Supervised independent project designed to give computer science graduate students an opportunity to explore a single topic in a one-to-one learning relationship with a faculty member.

CSC 795 Master's Project (3 Credits)
Guided master's research project under the supervision of a research project advisor and the course instructor; requires extensive expository work and other tasks and a formal project report with a public presentation of the project's work.

CSC 798 Master's Thesis I (3 Credits)
First semester of the master's thesis sequence. Under the supervision of the thesis advisor, students prepare a thesis proposal and work toward the goal of completing all background material needed for their research. A satisfactory thesis draft and presentation to the committee will be used to satisfy completion of the course.

CSC 799 Master's Thesis II (3 Credits)
The culmination of the two-semester master's thesis sequence. Students must complete a thesis document and defend the work in a public presentation to their committee.

Cybersecurity

CYS 564 Secure Operating Systems (3 Credits)
This course introduces students to Operating Systems with emphasis on security. Students will be introduced to the foundations of Operating Systems, the vulnerabilities of Operating Systems, threats from attackers, potential harm that can be caused by attacks, defense, and risk mitigation. The notion of a trusted Operating System will be introduced as a standard useful for comparing various Operating Systems.

CYS 573 Network Fundamentals (3 Credits)
This course introduces students to the basics of networks and their functionality, including the Open Systems Interconnection model, network components, local and wide area networks, routers, switches, wireless communication, network security, Internet protocols, and network applications such as web and email. It also covers the fundamentals of configuring and troubleshooting network features on popular computing platforms.

CYS 672 Computer and Network Forensics (3 Credits)
This course introduces students to the fundamentals of digital forensics, including forensic duplication and analysis, network surveillance, intrusion detection and response, incident response, anti-forensics techniques, anonymity and pseudonymity, cyber law, computer security policies and guidelines, court report writing and presentation, and case studies. Students will apply information security practices and technologies in virtual lab environments to gain hands-on experience solving realistic cybersecurity problems.

CYS 688 Human Aspects of Cybersecurity (3 Credits)
This course focuses on the theory and practice of implementing secure database systems. Emphasis will be placed on database security principles, database application security models, database auditing models, security implementation and database reliability.

CYS 697 Ethical Hacking and Penetration Testing (3 Credits)
This course is designed for students pursuing a graduate degree in cyber security with particular interest in working as a white hat hacker. The students will be trained theoretically and practically in understanding vulnerabilities in network architectures, operating systems, database management systems and web servers. They will learn how exploits are designed by an adversary attacker to penetrate into vulnerable systems. The students will also learn how the hacker can move into a hacked system and remove her/his footprints. The course will expose students to a host of tools used for network scanning, finger printing and password cracking. These tools include Nmap, Nessus and Backtrack among others. There will be a thorough discussion on the emerging hack technology for wireless LANs and defenses against them.

CYS 721 Database Security (3 Credits)
This course focuses on the theory and practice of implementing secure database systems. Emphasis will be placed on database security principles, database application security models, database auditing models, security implementation and database reliability.

CYS 755 Healthcare Information Security (3 Credits)
This course is designed for students seeking to learn more about the field of health care information security. It covers the fundamentals of computer and network security theories and practices that can be used to significantly reduce the security vulnerability of health care information on internal networks or the Internet. An in-depth view of health care information is provided by examining health care regulatory requirements and the functions of a health care organization, including its medical business operations, hardware, software, networking, and security. Topics include electronic health records, security policy, web security, database security, security administration, and health care ethics, privacy, and law.

CYS 765 Advanced Topics in Cybersecurity (3 Credits)
This course covers state-of-the art advances, emerging trends, and threats in cybersecurity. Topics to be covered include current topics in Information Assurance, advanced digital forensics, new approaches to management of cybersecurity and new threats, vulnerabilities, and controls.

CYS 795 Cybersecurity Capstone (6 Credits)
This project course is the capstone experience for graduate students in the Master's degree in Cybersecurity. This course provides students with the opportunity to carry out in-depth research on a specified topic in cybersecurity. The student's project will reflect the integration and application of the cybersecurity knowledge gained over the course of the program.

CYS 798 Cybersecurity Capstone I (3 Credits)
This course prepares students for their capstone experience in the Cybersecurity MS degree program. Capstone I provides the opportunity hone the skills needed to accomplish in-depth research and career growth; to choose a specific topic in, cybersecurity as the focus for their research; to identify a CYS faculty advisor who agrees to oversee their capstone project; and to develop a viable research proposal.

CYS 799 Cybersecurity Capstone II (3 Credits)
This course is the capstone experience for graduate students in the Master's degree in Cybersecurity. Capstone provides students the opportunity to carry out in-depth research on a specific topic in cybersecurity under the guidance of a faculty research advisor. The student's project will reflect the integration and application of cybersecurity knowledge and skills gained over the course of the program.

Faculty

Dr. Felicia Doswell, Associate Professor
Networks, security, privacy, internet technology, web performance evaluation, and game design.

Dr. Jonathan Graham Jr., Professor
Computational intelligence, digital forensics, smart intrusion detection systems, cybersecurity research, education and development.

Dr. Cheryl Hinds, Assistant Professor
Wireless Sensor Network Security,Usability Security.

Dr. Mary Ann Hoppa, Assistant Professor
Information visualization, metrics, microlearning, knowledge management, “hard problems” in cybersecurity, and wearable technology.

Dr. George Hsieh, Professor
Networking, network security, information assurance, communication systems and applications.

Dr. Yen-Hung Hu, Associate Professor
Network Security, Secure Programming, IT Compliance and Trustworthy Computing

Dr. Thorna Humphries, Associate Professor and Graduate Program Director
Software engineering, data management, computer science education, and security.

Dr. Samuel Olatunbosum, Associate Professor
Cybercrime and internet security, cloud computing efficiency, and societal impact of social networks.

Dr. Claude Turner, Associate Professor
Security and privacy in wireless and data networks, Digital Forensics, Resource impact of security, Computer Science and Cyber Security Education.

Dr. Luay Wahsheh, Associate Professor
Computer security, information assurance, wireless network security, software security, and database security.

Dr. Aurelia T. Williams, Professor
Information assurance, computer forensics, network security, data communications, and computer science education.

For more information contact the Graduate Program Coordinator:

Dr. Rasha Morsi
Computer Science Department Norfolk State University
(757) 823-0047
csgrad@nsu.edu | http://www.cs.nsu.edu