CYBERSECURITY (CYS)

CYS 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. This course is a cross-listing that, covers the same material as CSC 535.

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.