EN.695 (CYBERSECURITY)

Courses

EN.695.601. Foundations of Information Assurance. 3 Credits.
This course surveys the broad fields of enterprise security and privacy, concentrating on the nature of enterprise security requirements by identifying threats to enterprise information technology (IT) systems, access control and open systems, and system and product evaluation criteria. Risk management and policy considerations are examined with respect to the technical nature of enterprise security as represented by government guidance and regulations to support information confidentiality, integrity and availability. The course develops the student's ability to assess enterprise security risk and to formulate technical recommendations in the areas of hardware and software. Aspects of security-related topics to be discussed include network security, cryptography, IT technology issues, and database security. The course addresses evolving Internet, Intranet, and Extranet security issues that affect enterprise security. Additional topics include access control (hardware and software), communications security, and the proper use of system software (operating system and utilities). The course addresses the social and legal problems of individual privacy in an information processing environment, as well as the computer "crime" potential of such systems. The class examines several data encryption algorithms. Course Note(s): This course can be taken before or after 605.621 Foundations of Algorithms. It must be taken before other courses in the degree.

EN.695.611. Embedded Computer Systems-Vulnerabilities, Intrusions, and Protection Mechanisms. 3 Credits.
While most of the world is preoccupied with high-profile network-based computer intrusions, this online course examines the potential for computer crime and the protection mechanisms employed in conjunction with the embedded computers that can be found within non-networked products (e.g., vending machines, automotive onboard computers, etc.). This course provides a basic understanding of embedded computer systems: differences with respect to network-based computers, programmability, exploitation methods, and current intrusion protection techniques, along with material relating to computer hacking and vulnerability assessment. The course materials consist of a set of eight study modules and five casestudy experiments (to be completed at a rate of one per week) and are augmented by online discussion forums moderated by the instructor. This course also includes online discussion forums that support greater depth of understanding of the materials presented within the study modules.
Prerequisite(s): 605.202 Data Structures; 695.601 Foundations of Information Assurance, a basic understanding and working knowledge of computer systems, and access to Intel-based PC hosting a Microsoft Windows environment.

EN.695.612. Operating Systems Security. 3 Credits.
This course covers both the fundamentals and advanced topics in operating system (OS) security. Access control mechanisms (e.g., SACL/DACL), memory protections, and interprocess communications mechanisms will be studied. Students will learn the current state-of-the-art OS-level mechanisms and policies designed to help protect systems against sophisticated attacks. In addition, advanced persistent threats, including rootkits and malware, as well as various protection mechanisms designed to thwart these types of malicious activities, will be studied. Advanced kernel debugging techniques will be applied to understand the underlying protection mechanisms and analyze the malicious software. Students will learn both hardware and software mechanisms designed to protect the OS (e.g., NX/ASLR/SMEP/SMAP). The course will use virtual machines to study traditional OS environments on modern 64-bit systems (e.g., Windows, Linux, and macOS), as well as modern mobile operating systems (e.g., iOS and Android). Prerequisite(s): Familiarity with operating system concepts.

EN.695.614. Security Engineering. 3 Credits.
This course covers cybersecurity systems engineering principles of design. Students will learn the foundational and timeless principles of cybersecurity design and engineering. They will learn why theories of security come from theories of insecurity, the important role of failure and reliability in security, the fundamentals of cybersecurity risk assessment, the building blocks of cybersecurity, intrusion detection design, and advanced topics like cybersecurity situational understanding and command and control. The course develops the student's ability to understand the nature and source of risk to a system, prioritize those risks, and then develop a security architecture that addresses those risks in a holistic manner, effectively employing the building blocks of cybersecurity systems— prevention, detection, reaction, and attack-tolerance. The student will learn to think like a cyber-attacker so that they can better design and operate cybersecurity systems. Students will attain the skill of systematically approaching cybersecurity from the top down and the bottom up and have confidence that their system designs will be effective at addressing the full spectrum of the cyber-attack space. The course also addresses how the cybersecurity attack and defense landscape will evolve so that the student is not simply ready to address today's problems, but can quickly adapt and prepare for tomorrow's. The course is relevant at any stage in a student's curriculum: whether at the beginning to enable the student to understand the big picture before diving into the details, at the end as a capstone, or in the middle to integrate the skills learned to date.
Prerequisite(s): 695.601 Foundations of Information Assurance.

EN.695.615. Cyber Physical. 3 Credits.
The age of cyber physical systems (CPS) has officially begun. Not long ago, these systems were separated into distinct domains, cyber and physical. Today, the rigid dichotomy between domains no longer exists. Cars have programmable interfaces, unmanned aerial vehicles (UAVs) roam the skies, and critical infrastructure and medical devices are now fully reliant on computer control. With the increased use of CPS and the parallel rise in cyber-attack capabilities, it is imperative that new methods for securing these systems be developed. This course will investigate key concepts behind CPS including control systems, protocol analysis, behavioral modeling, and intrusion detection system (IDS) development. The course will comprise theory, computation, and projects to better enhance student learning and engagement, beginning with the mathematics of continuous and digital control systems and then focusing on the complex world of CPS, where general overviews for the different domains (industrial control, transportation, medical devices, etc.) are complemented with detailed case studies (Siemens ICS & ArduPilot UAVs). Several advanced topics, including behavioral analysis and resilient CPS, will be introduced. Students will complete several projects, both exploiting security vulnerabilities and developing security solutions for UAVs and industrial controllers. Prerequisite(s): Knowledge of IP addresses and packets, matrix algebra, and Windows and Linux operating systems.

EN.695.621. Public Key Infrastructure and Managing E-Security. 3 Credits.
This course describes public key technology and related security management issues in the context of the Secure Cyberspace Grand Challenge of the National Academy of Engineering. Course materials explain Public Key Infrastructure (PKI) components and how the various components support e-business and strong security services. The course includes the basics of public key technology; the role of digital certificates; a case study that emphasizes the content and importance of certificate policy and certification practices; identification challenges and the current status of the National Strategy for Trusted Identities in Cyberspace; and essential aspects of the key management lifecycle processes that incorporate the most recent research papers of the National Institute of Standards and Technology. Students will examine PKI capabilities and digital signatures in the context of the business environment, including applicable laws and regulations. The course also presents the essential elements for PKI implementation, including planning, the state of standards, and interoperability challenges. The course also provides an opportunity for students to tailor the course to meet specific cybersecurity interests with regard to PKI and participate in discussions with their peers on contemporary cybersecurity topics.

EN.695.622. Web Security. 3 Credits.
This course examines issues associated with making web applications secure. The principal focus is on server-side security such as CGIsecurity, proper server configuration, and firewalls. The course also investigates the protection of connections between a client and server using current encryption protocols (e.g., SSL/TLS) as well discussing the related attacks on these protocols (e.g., Heartbleed, CRIME, etc.). The course also investigates keeping certain data private from the server system (e.g., via third-party transaction protocols like SET, or PCI DSS standard). Elementary Number Theory will be reviewed. Finally, the course explores client-side vulnerabilities associated with browsing the web, such as system penetration, information breach, identity theft, and denial-of-service attacks. Related topics such as malicious e-mails, web bugs, spyware,and software security are also discussed. Labs and various serverside demonstrations enable students to probe more deeply into security issues and to develop and test potential solutions. Basic knowledge of operating systems is recommended. Students will download and install a Virtual Machine to be used in the course. Prerequisite(s): 605.202 Data Structures

EN.695.634. Intelligent Vehicles: Cybersecurity for Connected and Autonomous Vehicles. 3 Credits.
New technologies within the automotive industry are fusing the physical, digital, and biological worlds to create intelligent vehicles that are designed to enhance occupants' experiences and improve driver safety and efficiency and improve pedestrian safety. The success of these commercial and industrial efforts rest in the principles of assured autonomy. These intelligent technologies exist in a connected ecosystem that includes the Transportation, Energy, and Communication sectors. Examples of the interconnectivity capabilities include: Autonomous Vehicle - transducer, interface, and supporting capabilities; Electric Vehicles - grid connected vehicle charging infrastructure; and Vehicle-to-Vehicle and Vehicle-to-Everything Communication Technologies. This course helps students understand the significance of assured autonomy safety and functional correctness of intelligent vehicles throughout the technology's lifecycle. This course follows a seminar format where students are expected to lead class discussions and write a final report as part of a course project. The course project will teach experimental design and the scientific method. The outcome of the project will be a proposal that, if executed, could result in a workshop-quality publication. Execution of the proposed experiment is encouraged but not required for the class. Proposals will be graded by both the instructor and by classmates. This course is oriented around helping students learn how to make a compelling research contribution to the area of intelligent vehicles and assured autonomy.Students will also learn to critique scientific papers in this research area by reading articles from the literature and analyzing at least one paper in order to lead a class discussion.Prerequisites: This course is suitable for graduate students with little prior experience in the area.

EN.695.637. Introduction to Assured AI and Autonomy. 3 Credits.
In order to drive a future where artificial intelligence (AI) enabled autonomous systems are trustworthy contributors to society, these capabilities must be designed and verified for safe and reliable operation and they must be secure and resilient to adversarial attacks. Further, these AI enabled autonomous systems must be predictable, explainable and fair while seamlessly integrated into complex ecosystems alongside humans and technology where the dynamics of human-machine teaming are considered in the design of the intelligent system to enable assured decision-making. In this course, students are first introduced to the field of AI, covering fundamental concepts, theory, and solution techniques for intelligent agents to perceive, reason, plan, learn, infer, decide and act over time within an environment often under conditions of uncertainty. Subsequently, students will be introduced to the assurance of AI enabled autonomous systems, including the areas of AI and autonomy security, resilience, robustness, fairness, bias, explainability, safety, reliability and ethics. This course concludes by introducing the concept of human-machine teaming. Students develop a contextual understanding of the fundamental concepts, theory, problem domains, applications, methods, tools, and modeling approaches for assuring AI enabled autonomous systems. Students will implement the latest state-of-the-art algorithms, as well as discuss emerging research findings in AI assurance.

EN.695.641. Cryptology. 3 Credits.
This course provides an introduction to the principles and practice of contemporary cryptology. It begins with a brief survey of classical cryptographic techniques that influenced the modern development of cryptology. The course then focuses on contemporary work: symmetric block ciphers and the Advanced Encryption Standard, public key cryptosystems, digital signatures, authentication protocols, cryptographic hash functions, and cryptographic protocols and their applications. Pertinent ideas from complexity theory and computational number theory, which provide the foundation for much of the contemporary work in cryptology, are introduced as needed throughout the course. Course Note(s): This course should be taken after the other two required foundation courses and before any other courses in the Analysis track.
Prerequisite(s): EN.695.601 AND EN.605.621OR EN.605.601[C] AND EN.605.611 AND EN.605.621

EN.695.642. Intrusion Detection. 3 Credits.
This course explores the use of intrusion detection systems (IDS) as part of an organization's overall security posture. A variety of approaches, models, and algorithms along with the practical concerns of deploying IDS in an enterprise environment will be discussed. Topics include the history of IDS, anomaly and misuse detection for both host and network environments, and policy and legal issues surrounding the use of IDS. The use of ROC (receiver operating characteristic) curves to discuss false positives and missed detection tradeoffs as well as discussion of current research topics will provide a comprehensive understanding of when and how IDS can complement host and network security. TCPDump and Snort will be used in student assignments to collect and analyze potential attacks. Prerequisite(s): 605.202 Data Structures; 605.101 Introduction to Python or knowledge of Python.

EN.695.643. Introduction to Ethical Hacking. 3 Credits.
This course exposes students to the world of computer hacking. The primary goal is to give students an understanding of how vulnerable systems can be attacked as a means to motivate how they might be better defended. The class takes a systems engineering view of hacking and emphasizes practical exposure via hands-on assignments. Students are expected to use a computer that will remain off all networks while they complete assignments.
Prerequisite(s): 695.601 Foundations of Information Assurance and one of 635.611 Principles of Network Engineering or 605.671 Principles of Data Communications Networks. Course Note(s): Homework assignments will include programming.

EN.695.711. Java Security. 3 Credits.
This course examines security topics in the context of the Java language with emphasis on security services such as confidentiality, integrity, authentication, access control, and nonrepudiation. Specific topics include mobile code, mechanisms for building "sandboxes" (e.g., class loaders, namespaces, bytecode verification, access controllers, protection domains, policy files), symmetric and asymmetric data encryption, hashing, digital certificates, signature and MAC generation/verification, code signing, key management, SSL, and object-level protection. Various supporting APIs are also considered, including the Java Cryptography Architecture (JCA) and Java Cryptography Extension (JCE). Security APIs for XML and web services, such as XML Signature and XML Encryption, Security Assertions Markup Language (SAML), and Extensible Access Control Markup Language (XACML), are also surveyed. The course includes multiple programming assignments and a project.
Prerequisite(s): 605.681 Principles of Enterprise Web Development or equivalent. Basic knowledge of XML. 695.601 Foundations of Information Assurance or 695.622 Web Security would be helpful but is not required.

EN.695.712. Authentication Technologies. 3 Credits.
Authentication technologies in cybersecurity play an important role in identification, authentication, authorization, and non-repudiation of an entity. The authentication process in cybersecurity, which is considered to be one of the weakest links in computer security today, takes many forms as new technologies such as cloud computing, mobile devices, biometrics, PKI, and wireless are implemented. Authentication is the security process that validates the claimed identity of an entity, relying on one or more characteristics bound to that entity. An entity can be, but is not limited to, software, firmware, physical devices, and humans. The course explores the underlying technology, the role of multi-factor authentication in cyber security, evaluation of authentication processes, and the practical issues of authentication. Several different categories and processes of authentication will be explored along with password cracking techniques, key logging, phishing, and man-in-the-middle attacks. Examples of authentication breaches and ethical hacking techniques will be explored to examine the current technologies and how they can be compromised. Case studies of authentication system implementation and their security breaches are presented. Federated authentication process over different network protocols, topologies, and solutions will be addressed. Related background is developed as needed, allowing students to gain a rich understanding of authentication techniques and the requirements for using them in a secure environment including systems, networks, and the Internet. Students will present a research project that reflects an understanding of key issues in authentication.
Prerequisite(s): 605.202 Data Structures; 695.601 Foundations of Information Assurance. 695.621 Public Key Infrastructure and Managing E-Security is recommended.

EN.695.715. Assured Autonomy. 3 Credits.
Autonomic systems leverage the growing advances in control, computer vision, and machine learning coupled with technological advances in sensing, computation, and communication. While this emerging highly connected, autonomous world is full of promise, it also introduces safety and security risks that are not present in legacy systems. This course focuses on the complexities inherent in autonomous systems and the multifaceted and multilayered approaches necessary to assure their secure and safe operation. As these systems become more pervasive, guaranteeing their safe operation even during unforeseen and unpredictable events becomes imperative. There are currently no real solutions to provide these runtime guarantees necessitating cutting edge research to provide state awareness, intelligence, control, safety, security, effective human-machine interaction, robust communication, and reliable computation and operation to these systems. This course follows a seminar-style format where students are expected to lead class discussions and write a publication-quality paper as part of a course project.

EN.695.721. Network Security. 3 Credits.
This course covers concepts and issues pertaining to network security and network security architecture and evolving virtualization and related cloud computing security architecture. Topics include mini-cases to develop a network security context. For example, we will assess the NIST (National Institute of Standards and Technology) unified information security framework. This framework is supported by information security standards and guidance, such as a risk management framework (RMF) and continuous monitoring (CM) process. Applied cryptography and information security—encryption algorithms, hash algorithms, message integrity checks, digital signatures, security assessment and authentication, authorization and accounting (AAA), security association, and security key management (generation, distribution, and renewal) —are discussed with consideration given to emerging cryptographic trends, such as the evolution and adoption of NSA's (National Security Agency's) Suite B cryptography. This course presents network and network security architecture viewpoints for selected security issues, including various security mechanisms, different layers of wired/wireless security protocols, different types of security attacks and threats and their countermeasures or mitigation, Next Generation Network (NGN) security architecture that supports the merging of wired and wireless communications, and Internet Protocol version 6 implementation and transition. The course concludes with more comprehensive cases that consider network security aspects of virtualization and cloud computing architecture.
Prerequisite(s): 605.202 Data Structures; 695.601 Foundations of Information Assurance and 605.671 Principles of Data Communications Networks or 635.611 Principles of Network Engineering.

EN.695.737. AI for Assured Autonomy. 3 Credits.
This is an introductory course in Artificial Intelligence It teaches the basic concepts, principles, and fundamental approaches to Artificial Intelligence. Its main topics include AI Fundamentals, Probability and Statistics, Python Essentials, Supervised Machine Learning, Unsupervised Machine Learning, Neural Networks, Reinforcement Learning, Deep Learning, Natural Language Processing, Decision Tree/Search Algorithms and Intro to Assured Autonomous Systems. Prerequisites: The student should have taken an undergraduate level course on, or be otherwise familiar with, operating systems and networks. Prior programming experience with C, Python or Java is highly recommended. Knowledge of algebra and discrete mathematics is also recommended.

EN.695.741. Information Assurance Analysis. 3 Credits.
This course provides students with an overview of analysis as it applies to information assurance. Analysis is a fundamental part of the information assurance process, and effective analysis informs policy, software development, network operations, and criminal investigations. To enable students to perform effective analysis, the focus of the course is on the analysis process and approach rather than on specific tools. Topics include the collection, use, and presentation of data from a variety of sources (e.g., raw network traffic data, traffic summary records, and log data collected from servers and firewalls). These data are used by a variety of analytical techniques, such as collection approach evaluation, population estimation, hypothesis testing, experiment construction and evaluation, and constructing evidence chains for forensic analysis. Students will construct and critique an analytical architecture, construct security experiments, and retroactively analyze events. The course will also cover selected non-technical ramifications of data collection and analysis, including anonymity, privacy, and legal constraints.
Prerequisite(s): 695.601 Foundations of Information Assurance. Familiarity with basic statistical analysis. 695.642 Intrusion Detection or 695.611 Embedded Computer SystemsVulnerabilities, Intrusions, and Protection Mechanisms is recommended.

EN.695.742. Digital Forensics Technologies and Techniques. 3 Credits.
Digital forensics focuses on the acquisition, identification, attribution, and analysis of digital evidence of an event occurring in a computer or network. This course provides a broader scientific understanding of the technologies and techniques used to perform digital forensics. In particular, various signature extraction techniques, detection, classification, and retrieval of forensically interesting patterns will be introduced. This will be complemented by studying fundamental concepts of data processing technologies like compression, watermarking, steganography, cryptography, and multiresolution analysis. Emerging standards along with issues driving the changing nature of this topic will be explored. Antiforensic techniques that are used to counter forensic analysis will also be covered. Students will be exposed to relevant theory, programming practice, case studies, and contemporary literature on the subject.
Prerequisite(s): 605.612 Operating Systems.

EN.695.744. Reverse Engineering and Vulnerability Analysis. 3 Credits.
This course covers both the art and science of discovering software vulnerabilities. Beginning with the foundational techniques used to analyze both source and binary code, the course will examine current threats and discuss the actions needed to prevent attackers from taking advantage of both known and unknown vulnerabilities. The course will cover passive and active reverse engineering techniques in order to discover and categorize software vulnerabilities, create patches and workarounds to better secure the system, and describe security solutions that provide protection from an adversary attempting to exploit the vulnerabilities. Techniques covered include the use of static analysis, dynamic reverse engineering tools, and fault injection via fuzzing to better understand and improve the security of software.

EN.695.749. Cyber Exercise. 3 Credits.
Students will learn about the nature and purpose of cyber exercises and their role in training and assessing people, teams, technology, and procedures. During the course of the semester, students will design a cyber exercise that meets the specific needs of their organization. At the conclusion of the class, students will have a model template they can use to design, build, and execute their own exercise.

EN.695.791. Information Assurance Architectures and Technologies. 3 Credits.
This course explores concepts and issues pertaining to information assurance architectures (IAA) and technologies, such as layered security architecture guidance and cases from the National Institute of Standards and Technology (NIST) and NIST Cybersecurity Center of Excellence (NCCoE); cryptographic commercial issues and evolving federal guidance; hypervisor and cloud computing security architecture; and IAA and technologies applications. Topics include critical infrastructure protection and Comprehensive National Cybersecurity Initiative (CNCI) Trusted Internet Connections (TIC) 2.0 multi-agency security information management (SIM) and selected security analytics issues. Commercial IAA examples of network security architecture and security analytics are also discussed for evolving enterprise mobility issues. The relationships of IAA and technologies with selected multi-tier architectures are discussed for applications such as enterprise risk management; security for virtualized environments; systems security engineering for services; and mobile device security. IAA multi-tier architecture issues are illustrated with cases, such as the NIST NCCoE use cases for Data Integrity: Recovering from Ransomware and Other Destructive Events; Access Rights Management for the Financial Services Sector; Situational Awareness for Electric Utilities; and Derived Personal Identity Verification (PIV) Credentials. Selected large-scale programs are discussed, such as enterprise risk management for the Federal Aviation Administration (FAA) Air Traffic Modernization process; and NIST Smart Grid Cybersecurity Strategy, Architecture, and HighLevel Requirements.
Prerequisite(s): 605.202 Data Structures; 695.601 Foundations of Information Assurance or equivalent, and 605.671 Principles of Data Communications Networks or 635.611 Principles of Network Engineering.

EN.695.795. Capstone Project in Cybersecurity. 3 Credits.
This course permits graduate students in cybersecurity to work with other students and a faculty mentor to explore a topic in depth and apply principles and skills learned in the formal cybersecurity courses to a real world problem. Students will work in self-organized groups of two to five students on a topic selected from a published list. Since students will have selected different courses to meet degree requirements, students should consider the combined strengths of the group in constituting their team. Each team will prepare a proposal, interim reports, a final report, and an oral presentation. The goal is to produce a publication quality paper and substantial software tool. This course has no formal content; each team should meet with their faculty mentor at least once a week and is responsible for developing their own timeline and working to complete it within one semester. The total time required for this course is comparable to the combined class and study time for a formal course. Course prerequisite(s): Seven cybersecurity graduate courses including two courses numbered 695.7xx, all CyS foundation courses, and meeting the track requirement; or admission to the post-master's certificate program. Students must also have permission of a faculty mentor or academic advisor, and the program chair. Course note(s): Students may not receive graduate credit for both 695.795 and 695.802 Independent Study in Cybersecurity II. This course is only offered in the spring.

EN.695.801. Independent Study in Cybersecurity I. 3 Credits.
This course permits graduate students in cybersecurity to work with a faculty mentor to explore a topic in depth or conduct research in selected areas. Requirements for completion include submission of a significant paper or project. Prerequisite(s): Seven Cybersecurity graduate courses including the foundation courses, three track-focused area courses, and two courses numbered at the 700 level or admission to the post-master's certificate program. Students must also have permission from the instructor.
Prerequisite(s): EN.695.401 Foundations of Information Assurance AND EN.605.421 Foundations of Algorithms

EN.695.802. Independent Study in Cybersecurity II. 3 Credits.
Students wishing to take a second independent study in Cybersecurity should sign up for this course. Prerequisite(s): 695.801 Independent Study in Cybersecurity I and permission of a faculty mentor, the student's academic advisor, and the program chair.