CYBERSECURITY

The part-time Cybersecurity program balances theory with practice, providing students with the highly technical knowledge and skills needed to protect and defend information systems from attack. Students choose from focus area that explore cyber attacks from within a system, protect information assets, and identify anomalies and unexpected patterns.

Program Committee

Lanier Watkins, Program Chair
Principal Professional Staff
JHU Applied Physics Laboratory

Robert S. Grossman, Vice Program Chair Emeritus
Principal Professional Staff (retired)
JHU Applied Physics Laboratory

Anthony N. Johnson, Program Manager
Senior Professional Staff
JHU Applied Physics Laboratory

Eleanor Boyle Chlan
Senior Professional Staff (retired)
JHU Applied Physics Laboratory

Theodore Colbert, III
Executive Vice President, The Boeing Company
President and Chief Executive Officer, Boeing Global Services

Anton Dahbura
Co-Director, Institute for Assured Autonomy
Johns Hopkins University

Mary Galvin
Alumni
JHU Engineering for Professionals

John Hurley
Professor, Cyberspace Strategies and Data Analytics
National Defense University

Tom Longstaff
CTO, Software Engineering Institute
Carnegie Mellon University

William Robinson
Interim Vice Provost for Strategic Initiatives
Vanderbilt University

Ralph Semmel
Director
JHU Applied Physics Laboratory

J. Miller Whisnant
Principal Professional Staff
JHU Applied Physics Laboratory

Programs

- Cybersecurity, Graduate Certificate (https://e-catalogue.jhu.edu/engineering/engineering-professionals/cybersecurity/cybersecurity-graduate-certificate/)
- Cybersecurity, Master of Science (https://e-catalogue.jhu.edu/engineering/engineering-professionals/cybersecurity/cybersecurity-master-science/)
- Cybersecurity, Post-Master's Certificate (https://e-catalogue.jhu.edu/engineering/engineering-professionals/cybersecurity/cybersecurity-post-masters-certificate/)

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 EN.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): EN.605.202 Data Structures; EN.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.
Have you ever wondered how hardware and software faults could affect the security and privacy of a computing environment? Modern general-purpose operating systems have become the lifeline for business and personal use.Throughout the course, students will examine and analyze the modern security mechanisms (e.g. MACs, ASLR, SMEP/SMAP, CFI, PAC, TPMs, and more) and learn the strengths and weaknesses of each approach, ensuring a solid defense against APTs and rootkits. Examining both software and hardware implementations, students will compare how effective these security components are amongst the major OS vendors. As virtualization has become ubiquitous in computing, students will also utilize KVM to build customized virtual machine solutions. Finally, students will examine how these mechanisms compare and are applied to modern mobile operating systems environments.Prerequisite(s): Familiarity with operating system concepts.

EN.695.613. Securing Industrial Control Systems. 3 Credits.
This course resides where Information Technology (IT) meets Operational Technology (OT) and introduces the practice of cybersecurity related to Industrial Control Systems (ICSs), their components, and the Purdue Model for ICS network organization. Industrial or OT environments were originally designed to be operated on and tended to with onsite (physical) configuration and support. As the industry evolves and requests for additional connectivity and remote functionality increase, these systems have become more connected and more vulnerable to both physical and remote threats. Students will be introduced to a variety of topics including process variable telemetry (sensors, actuators, controllers), control loops, DCS/SCADA/PLCs, HMIs, data historians, safety systems, and so on. ICSs are meant to provide stability during steady-state operations and respond appropriately to non-steady-state conditions - imagine if employees couldn't trust the data they see, or the autonomous control was overridden or defeated. Through lectures, real-world cyber-attack case studies, hands-on exercises, and independent research opportunities students will be given the resources to identify and understand ICS vulnerabilities, and best secure ICS environments.

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): EN.695.601 Foundations of Information Assurance.

EN.695.615. Cyber Physical Systems Security. 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 be comprised of theory, computation, and projects to better enhance student learning and engagement . The course will begin with the mathematics of continuous and digital control systems and then shift the focus to the complex world of CPS, where both a general overview for the different domains (Industrial Control, Transportation, Medical Devices, etc.) and more detailed case studies will be provided . Students will complete a number of projects, both exploiting security vulnerabilities and developing security solutions for UAVs and industrial controllers. Several advanced topics will be introduced including behavioral analysis and resilient CPS.Course Notes: There are no prerequisite courses; however, students will encounter many concepts and technologies in a short period of time. Student should have a basic understanding of python programming, networking, matrices, and Windows and Linux operating systems.

EN.695.616. Securing Industrial Control Systems. 3 Credits.
This course resides where Information Technology (IT) meets Operational Technology (OT) and introduces the practice of cybersecurity related to Industrial Control Systems (ICSs), their components, and the Purdue Model for ICS network organization. Industrial or OT environments were originally designed to be operated on and tended to with onsite (physical) configuration and support. As the industry evolves and requests for additional connectivity and remote functionality increase, these systems have become more connected and more vulnerable to both physical and remote threats. Students will be introduced to a variety of topics including process variable telemetry (sensors, actuators, controllers), control loops, DCS/SCADA/PLCs, HMIs, data historians, safety systems, and so on. ICSs are meant to provide stability during steady-state operations and respond appropriately to non-steady-state conditions - imagine if employees couldn't trust the data they see, or the autonomous control was overridden or defeated. Through lectures, real-world cyber-attack case studies, hands-on exercises, and independent research opportunities students will be given the resources to identify and understand ICS vulnerabilities, and best secure ICS environments.

EN.695.617. Zero Trust Principles and Practice. 3 Credits.
As cyber threats become increasingly advanced, traditional security measures are no longer sufficient to maintain an organization's security posture. As cyber threats continue to evolve, it is critical to adopt robust security measures. This course will explore the concept, principles, benefits, and challenges of implementing Zero Trust in today's digital environment to help protect an organization. Students will be oriented to core principals of Zero Trust, explore practical use cases and success stories demonstrating the implementation of Zero Trust principles across diverse industries. Throughout the session students will discover best practices for deploying Zero Trust security frameworks to safeguard critical assets and gain an understanding of how organizations can effectively scale and adapt Zero Trust strategies to meet their specific security needs.

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.
Information technology security is a broad field. This course focuses on the foundational technologies that build the Web-based Internet (Web) as we know it today. The goal of this course is to guide the learner to adopt a professional security mindset by applying the techniques of threat modeling, risk assessment, and apply the foundational security principles from the two "triad" models: "confidentiality, integrity, and availability" (CIA) and "authentication, authorization, and accounting" (AAA). The self-motivated learner will investigate vulnerabilities, threats, and mitigations with the objective of protecting the data, applications, frameworks, and the supporting complex technology stacks. Security at this level cannot be achieved by technology alone, the course will provide an opportunity to exercise a smart combination of methodologies and techniques that can build confidence and rapport to champion web security within their IT community. Applicable cryptology, digital certificates, and Public Key Infrastructure will be reviewed. Each module will involve hands-on labs that implement local virtual machines, containers, cloud computing environments, and an operative blockchain enabling the learner to probe more deeply into the cybersecurity challenge of each technology solution. The assignments will involve programming and system configuration thus a novice-level exposure of Python, PHP, JavaScript, Linux Commands, basic Internet architecture and common protocols is recommended. Prerequisite(s): EN.605.202 Data Structures

EN.695.623. Information Security and Privacy. 3 Credits.
As the world becomes more connected and reliant on digital communications, best security practices are required to maintain the privacy of individual and enterprise systems. This course will focus mainly on network perimeter protection, host-level protection, authentication technologies, intellectual property protection, formal analysis techniques, intrusion detection and other current advanced topics. Emphasis in this course is on understanding how security issues impact real-world systems, while maintaining an appreciation for grounding the work in fundamental science. The course will consist of group exercises and interactive discussions. There will be programming assignments and a course project. Students will also be expected to read assigned research papers and lead a presentation and discussion on at least one research paper.

EN.695.624. Introduction to Internet of Things Security and Privacy. 3 Credits.
The course covers security and privacy topics on the Internet of Things (IoT) and aims to provide the students with a comprehensive, practical approach to analyze weaknesses and learn security and privacy best practices that apply to highly heterogeneous IoT devices and networks. The course introduces widely used IoT platforms (e.g., SmartThings, AWS IoT, openHAB, Windows IoT) and compares them based on technical criteria such as network topology used, programming languages, communication protocols, and security/privacy considerations. The students will have an opportunity to understand and analyze common cybersecurity and privacy threats impacting IoT technologies, and reviews key security concepts, communication/network protocols, and cryptographic algorithms used to countermeasure those threats. Additionally, the course proposes a comprehensive security methodology to protect the IoT at different levels of the IoT architectural stack (e.g., hardware, software, application, and system). The methodology reviews novel security and privacy solutions proposed in the literature and evaluates their effectiveness and practicality.
Prerequisite(s): EN.695.644 Digital Forensics Technologies and Techniques or equivalent course with some knowledge of Network Security.

EN.695.631. AI for Cybersecurity. 3 Credits.
The Cybersecurity of the nation's critical infrastructure is the premier national security issue of our time. Artificial Intelligence (AI) is positioned to help with this problem by serving as a force multiplier for cybersecurity professionals. This course seeks to introduce successful AI approaches to securing enterprise networks through hands-on assignments. This course specifically focuses on the use of machine learning to enhance security in-depth approaches such as spam filtering, phishing detection, network/host intrusion detection, malware/botnet detection, and secure authentication.

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 cryptography. It begins with a brief survey of classical cryptographic techniques that influenced the modern development of the subject. The course then focuses on more contemporary work: symmetric block ciphers and the Advanced Encryption Standard, public key cryptosystems, digital signatures, authentication protocols, and cryptographic hash functions. The course also provides an overview of quantum resistant cryptography and, as time permits, other recent developments such as homomorphic encryption. Complexity theory and computational number theory provide the foundation for much of the contemporary work in cryptology; pertinent ideas from complexity and number theory are introduced, as needed, throughout the course.

EN.695.642. Intrusion Detection. 3 Credits.
This course explores the use of network and host-based intrusion detection and prevention systems (IDS/IPS) as part of an organization's overall cybersecurity posture and threat informed decision strategy. A variety of approaches, models, analyzes, technologies, frameworks and algorithms along with the practical concerns of deploying IDS/IPS in an enterprise/legacy IT heterogenous and homogenous environment will be discussed, along with Operational Technology (OT), as-a-service infrastructure, and Internet of Things (IoT's) enclaves. Topics include the products, architectures, configurations and components of IDS/IPS, host and network-based IDS/IPS, network analysis, technologies, Machine Learning, Linux Firewall IPTables, Uncomplicated Firewalls (UFW), Network Packet Analysis, Cyber Incident Response, IDS/IPS in context, graph theory and Tor Networking. The use of ROC (receiver operating characteristic/curves) to discuss false positives, false negatives, precision recall graphs, and missed detection trade - offs as well as discussions of current research topics will provide a comprehensive understanding of when and how IDS/IPS can complement host and network security. A variety of IDS tools will be used to collect and analyze potential attacks to include; OSSEC, Tripwire, Snort, Suricata, Neo4j, Zeek (new name Bro), Nmap, Keras, Wireshark, delayhost utility, and Rapid Miner. The course will use virtual machines in labs and assignments to provide hands-on experience with IDS including using test data to quantitatively compare different IDS/IPS's.
Prerequisite(s): EN.695.641 Cryptology

EN.695.643. Introduction to Ethical Hacking. 3 Credits.
This course exposes students to the world of ethical computer hacking by discussing foundational concepts, frameworks, and theoretical knowledge that will provide a richer understanding of how and why vulnerable hosts/systems are attacked to motivate and better apply defensive tactics, techniques, and solutions. The class looks at fundamental hacking approaches through practical exposure via hands-on assignments, discussions, and two quizzes. For lab assignments, students are expected to use a computer that will remain air-gapped/off all networks while they complete the deliverable. The course goal is to learn fundamental principles of reconnaissance, scanning, escalation, pivoting, and exploitation that can be leveraged to defend computing infrastructures, networks, and systems. Students will primarily use virtual machines in labs. Course topics include; Ideology/Motives, Penetration Testing, Cryptography and PKI, Web Exploitation, Mobile Devices, Scanning & Reconnaissance, Network Exploitation, Information Gathering & Social Engineering, Wi-Fi Exploitation, Rootkits, OS Security, Buffer Overflows, Race Conditions, and Post Exploitation (escalate/pivot).
Prerequisite(s): EN.695.601 Foundations of Information Assurance and one of EN.635.611 Principles of Network Engineering or EN.605.671 Principles of Data Communications Networks. Course Note(s): Homework assignments will include programming.

EN.695.644. Computer Forensics. 3 Credits.
This course introduces the student to the field of applied Computer Forensics as practiced by corporate security and law enforcement personnel. The emphasis is on "dead-box" (powered-off) data extraction and analysis with open-source tools. Topics covered include legal and regulatory issues, forensic imaging and data acquisition from a "dead" system, computer file systems (FAT/NTFS) and data recovery, Windows Registry and configuration records, Windows log analysis and operating system artifacts, memory dump analysis (RAM), software artifacts, computer network forensics, introductory mobile device forensics, case reporting and documentation, end-to-end computer forensic examinations, peer review, and testifying in court.

EN.695.645. Mobile Device Forensics. 3 Credits.
This course introduces the student to the field of applied Mobile Device Forensics as practiced by corporate security and law enforcement personnel. The emphasis is on "live" (powered-on) data extraction and analysis of Linux-based Android mobile devices/cell phones with open-source tools. Topics covered include data extraction from a "live" system; cell phone file systems (EXT/YAFFS) and data recovery; cell phone configuration records; Android/Linux log analysis and operating system artifacts; memory dump analysis (NAND); Android Operating System application artifacts to include SMS/MMS messaging apps, contacts list, calendar, Gmail, browser bookmarks/searches, call logs, picture/video, and GPS/maps; installed application artifacts such as Facebook, Twitter, and TikTok; cell phone network forensics; Subscriber Identity Module (SIM) card analysis; and Secure Digital (SD) card analysis.

EN.695.646. Engineering Runtime Malware Detection. 3 Credits.
This course focuses on fundamental runtime behaviors often attributed to malware executing on a system. The student will be given high level explanations of each of these behaviors and their importance to the malware lifecycle. The students will be exposed to currently support Windows kernel technologies such as minifilters and callback routines. Students will learn how to collect and analyze execution data in real time from the Windows Kernel. The course will also allow students to build their own malware analysis engine for a Windows 10 operating system. The focus of the analysis engine is to detect malware early in its execution based on identification of suspicious behaviors including those discussed in class. The students will be graded on homework and a group semester project to build and test a malware detection analysis engine using log files of malware and benign process executions provided by the instructor. Students will setup a Windows 10 virtual machine with the kernel data collectors for use in their homework. The project will be presented to the class towards the end of the semester. Programming knowledge in a language is required for the homework and semester project. Previous knowledge of Windows system internals, malware is helpful but not required. Students will not be given any malware binaries by the instructor at any time during this course.

EN.695.647. Cyber Threat Hunting and Intelligence. 3 Credits.
Cyber security has traditionally taken a reactive approach. To defend against a threat, we needed to know what the threat was and how it manifests. However, the threat landscape can shift quickly. Advanced Persistent Threats stay under the radar for a long time, so we don't learn about the threat and how to find it. Ransomware quickly moves from initial access to impact, so we can't afford to take a reactive approach. This course teaches a proactive approach to cyber security by incorporating cyber threat intelligence and threat hunting. Students will use tools and techniques to derive technical intelligence about threat actors. They will identify strategies for collection to inform operational and strategic requirements. In addition, they will develop hunting hypotheses using threat intelligence as cues, convert those hypotheses to analytics, and validate the hypotheses to determine whether a threat actor has successfully breached the network. This is a technical course where students will apply these concepts in hands-on environments. Students should be familiar with attacker methodologies, intrusion detection concepts, and network traffic analysis.

EN.695.648. Cyber Strategy and Leadership. 3 Credits.
This course is designed to help create the next generation of executive leaders in cyber security who can build and run effective information security programs. The target audience for this course is someone with 5+ years of previous Cyber Security-related work experience. This course will teach students how to rise above the Individual Contributor level by learning technical, leadership, strategic, and political skills in cyber security. To enable such activities the class focuses on teaching the various knowledge, skills, and abilities that a Chief Information Security Officer needs to demonstrate. Students will be well-prepared to step into a CISO role, allowing them to create, update and maintain successful cybersecurity programs in any organization.

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): EN.605.681 Principles of Enterprise Web Development or equivalent. Basic knowledge of XML. EN.695.601 Foundations of Information Assurance or EN.695.622 Web Security would be helpful but is not required.

EN.695.712. Authentication Technologies. 3 Credits.
Authentication plays a strong role in cybersecurity, and is a critical layer underpinning the “CIA triad.” This course will explore current technologies, issues, and policies surrounding practical authentication. Grouped by something you know, something you have, and something you are, topics will include passwords, certificates and public key infrastructures, graphical authentication, smart cards, biometrics, trusted computing, location authentication, identity federation, and a range of other topics determined by class interest. Each topic will be examined from the perspective of technical strengths, weaknesses, mitigations, and human factors, and will include discussions of authentication policies, trends, and privacy perspectives. 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 prepare and present a research project that reflects an understanding of key issues in authentication. Recommended: EN.695.621 Public Key Infrastructure and Managing E-Security.
Prerequisite(s): EN.605.202 Data Structures; EN.695.601 Foundations of Information Assurance. EN.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 online course in a seminar-style format leads the students to participate in learning activities, record summary presentation of a selection of papers, write a peer-reviewed publication-quality paper, and record a workshop presentation for virtual panel review.

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 SD-WAN (Software-Defined Wide Area Networks). 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): EN.605.202 Data Structures; EN.695.601 Foundations of Information Assurance and EN.605.671 Principles of Data Communications Networks or EN.635.611 Principles of Network Engineering.

EN.695.722. Covert Channels. 3 Credits.
This course will be a survey course for covert channels and information leakage (side channel) with hands-on investigations into building and defeating covert channels. We will begin with the long history of covert channels dating back to the 1970's up to the present and beyond by looking at current research in this area. We will explore both storage and timing covert channels and information leakage from general purpose computers, mobile devices, and modern industrial control system devices. It is necessary to be able to write code in at least 1 language (python is preferred), be familiar with computer networking and the use of network packet sniffers.
Prerequisite(s): EN.695.642 Intrusion Detection AND intermediate knowledge of Python.

EN.695.723. Advanced Web Security. 3 Credits.
This course reviews the basic knowledge of the World Wide Web, and then examines advances in the central defense concepts behind Web security, such as same-origin policy, cross-origin resource sharing, and browser sandboxing. Concurrently, we will also explore the most popular Web vulnerabilities, such as cross-site scripting (XSS) and SQL injection, as well as how to attack and penetrate software with such vulnerabilities. You will learn how to detect, respond, and recover from security incidents. Newly proposed research techniques will be investigated with students demonstrating their understanding through discussions and peer evaluated exercises.
Prerequisite(s): EN.695.622 Web Security or similar previous exposure.

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 exposes students to the world of information assurance analysis by discussing foundational concepts and frameworks that can be used to analyze various technologies, mediums, protocols and platforms. Analysis is a fundamental part of the information assurance process and effective implementation can inform policy, forensic and incident response procedures, and cyber security practices. Students will be able to perform analysis activities by using the theoretical knowledge gained on case studies, assignments, and hands-on labs resulting in a richer understanding for information assurance. 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). This data is used for a variety of analytical techniques, such as collection approach evaluation, population estimation, hypothesis testing, experiment construction and evaluation, and developing evidence chains for forensic analysis. The course will also cover Internet of Things (IoT's), Artificial Intelligence, Mobile Application Security, addressing, Border Gateway Protocols (BGP), lookups, anonymization, Industrial Control Systems (ICS), as well as analyzing DNS, HTTP, SMTP, and TCP protocols. Students will primarily use SiLK, NetFlow, Wireshark, Splunk, Node-Red IoT framework, and TCPDump tools. Students will also be introduced to various IoT and ICS protocols; WNAN, ZigBee, EMV, and SIGFOX, as well as, CIP, MODBUS, DNP3, OPC, HART, BACnet, and ICCP, respectively.
Prerequisite(s): EN.695.601 Foundations of Information Assurance. Familiarity with basic statistical analysis. EN.695.642 Intrusion Detection or EN.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): EN.605.612 Operating Systems.

EN.695.744. Reverse Engineering and Vulnerability Analysis. 3 Credits.
Have you ever wondered why software vulnerabilities lead to security issues? Or how malicious actors exploit vulnerabilities? The Reverse Engineering course will help answer these questions and more! Throughout the course, students will use industry standard tools and develop customized solutions to help further binary/code analysis. Using real-world vulnerability classes, students will examine how attackers identify flaws in modern software and exploit these flaws bypassing state-of-the-art protection mechanisms found in modern operating systems. Students will also identify how to patch these issues and develop extensions of protection mechanisms to thwart attacks, raising the bar for the attacker and improving the security posture of a system. Using a combination of static analysis, dynamic analysis, fault injection and fuzzing, this course will provide students with the modern skills needed to help stop attackers!Prerequisite(s): Familiarity with computer architecture concepts.

EN.695.745. Malware Analysis. 3 Credits.
Attackers and attacker toolchains continue to evolve and make detection and prevention very difficult. Malware analysts are continually examining modern malware to look for commonalities and new 0-day techniques that are used to exploit a system and maintain a strong foothold. Identifying the Indicators of Compromise (IOCs) is important for helping determine the extent of an intrusion as well as helping alert others to similar attacks. Students will utilize advanced analysis techniques, user mode/kernel mode debugging and dynamic analysis to uncover how modern malware operates. Being able to bypass code obfuscation techniques, examine shellcode, identify command-and-control (C2) systems and configuration are critical components for analyzing and stopping malware. In addition, as ransomware has become ubiquitous, students will examine a real-world ransomware attack and develop a customized decryption utility to help a 'customer' recover from a ransomware attack. Throughout the course, relevant operating systems internals will be discussed. By the end of the course, students will have a better understanding of how to identify attacks and reverse engineer tools to uncover the attacker's secrets!
Prerequisite(s): EN.695.744 Reverse Engineering

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.
Prerequisite(s): EN.695.641 Cryptology

EN.695.791. Information Assurance Architectures and Technologies. 3 Credits.
This course explores concepts and issues pertaining to information assurance architectures and technologies (IAA), such as a three-level enterprise and cybersecurity architecture offered as one of the security common languages from the National Institute of Standards and Technology (NIST). Key NIST Cybersecurity Center of Excellence (NCCoE) Practice guides pertaining to IAA issues are introduced and analyzed. NIST/NCCoE security guidance and metrics for Zero Trust Architecture (ZTA), continuous diagnostics and mitigation (CDM), and artificial intelligence/machine learning (AI/ML) security guidance and metrics are applied to analysis of selected enterprise and cybersecurity programs, such the Department of Defense (DoD) Zero Trust Reference Architecture, Department of Homeland Security (DHS) Cybersecurity & Infrastructure Security Agency (CISA) Trusted Internet Connections Program (CISA TIC), Federal Aviation Administration (FAA) Air Traffic Modernization (NextGen) process, and Food and Drug Administration (FDA) (for approval of medical devices). Cloud computing security architecture issues for IAA technologies including FedRAMP (Federal Resources Analysis and Management Program) authorization are analyzed. Topics include protecting control systems from non-control systems for information technology (IT) and operational technology (OT) enterprise and cybersecurity risk management. For example, these IT/OT interface issues are critical for the NIST Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements. IAA analyses include enterprise Internet of Things (IoT) mobility issues and a virtual laboratory project based on selected Amazon Web Services (AWS) security capabilities for Zero Trust Architecture (ZTA).
Prerequisite(s): EN.605.202 Data Structures; EN.695.601 Foundations of Information Assurance or equivalent, and EN.605.671 Principles of Data Communications Networks or EN.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 EN.695.795 and EN.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.695.601 AND EN.695.401 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): EN.695.801 Independent Study in Cybersecurity I and permission of a faculty mentor, the student's academic advisor, and the program chair.
Prerequisite(s): EN.695.801