INFORMATION SECURITY INSTITUTE

http://isi.jhu.edu/

The Johns Hopkins University Information Security Institute (ISI) is the University's focal point for research and education in information security, assurance, and privacy. Securing cyberspace and our national information infrastructure is more critical now than ever before, and it can be achieved only when the core technology, legal and policy issues are adequately addressed. ISI is committed to a comprehensive approach that includes input from academia, industry, and government. The University, through ISI's leadership, has thus been designated as a Center of Academic Excellence in Cyber Defense Research by the National Security Agency and the Department of Homeland Security. Through our broad range of educational opportunities including a ground-breaking graduate program and leading-edge research in foundational science and applied technologies, ISI is having a significant impact in the region and nationwide.

Our research in cryptography, networking, systems evaluation, medical privacy, electronic voting, and AI security and trustworthiness, among other areas, is widely circulated among academics and policymakers. Moreover, ISI is instrumental in homeland security efforts across Hopkins, including emergency health preparedness, bio-terrorism and national defense.

The Johns Hopkins University Information Security Institute based in the Whiting School of Engineering provides a broad and holistic perspective to the information security and assurance field relative to both research and education. In addition to a comprehensive collection of programs related to information technology, a range of management, governance, and policy issues are integrated into the Information Security Institute agenda. The breadth of focus provided represents a strength and distinction of the Johns Hopkins University Information Security Institute. Through the involvement of the faculty and resources from the Whiting School of Engineering, the Krieger School of Arts and Sciences, the Bloomberg School of Public Health, the Carey Business School, the School of Medicine, and the Applied Physics Lab, a variety of innovative as well as international research and educational initiatives in information security and assurance are supported within the Information Security Institute.

Facilities

The computing facilities include a laboratory of shared servers and PC workstations, and customizable machines and special devices for student projects. Various focused research laboratories have additional resources that provide greater specialization than the general lab. The facilities are connected to a secure high-speed network which allows access to specialized hardware in other departments and institutions. The Information Security Institute and Department of Computer Science cooperate in the use of some of these facilities.

Programs

- Security Informatics, Master of Science (https://e-catalogue.jhu.edu/engineering/full-time-residential-programs/degree-programs/information-security-institute/security-informatics-master-science/)
- Security Informatics, Master of Science/Applied Mathematics and Statistics, Master of Science in Engineering Dual Master's Program (https://e-catalogue.jhu.edu/engineering/full-time-residential-programs/degree-programs/information-security-institute/security-informatics-master-science-applied-mathematics-statistics-engineering-dual-program/)
- Security Informatics, Master of Science/Computer Science, Master of Science in Engineering Dual Master's Program (https://e-catalogue.jhu.edu/engineering/full-time-residential-programs/degree-programs/information-security-institute/security-informatics-master-science-computer-science-engineering-dual-program/)

For current course information and registration go to https://sis.jhu.edu/classes/

Courses

EN.650.601. Introduction to Information Security. 3 Credits.
This course exposes students to the cross-disciplinary and broad information security field. It surveys a range of fundamental topics of information security principles, architecture, policy and standard, risk management, cryptography, physical, operation, system and network security mechanisms, and law and ethics, among others. This course includes lectures, case studies, and homework. Students will also complete independent study class projects. Recommended Course Background: Basic knowledge of computer system and information technology.

EN.650.614. Rights In Digital Age. 3 Credits.
This course will examine various legal and policy issues presented by the tremendous growth in computer technology, especially the Internet. The rights that various parties have with respect to creating, modifying, using, distributing, storing, and copying digital data will be explored. The concurrent responsibilities, and potential liabilities, of those parties will also be addressed. The course will focus on intellectual property issues, especially copyright law, and other legal and economic considerations related to the use and management of digital data. Copyright law and its role within the framework of intellectual property law will be presented in a historical context with an emphasis on its applicability to emerging-technology issues. Specifically, the treatment of various works, such as music, film, and photography that were traditionally, analog in nature will be analyzed with respect to their treatment in the digital domain; works that are by their nature digital, such as computer software, will also be analyzed. The current state of U.S. copyright law will be presented, as will relevant international treaties and foreign laws. The goal of the course is to provide those involved or interested in digital rights management with a general awareness of the rights and obligations associated with maintaining and distributing digital data. (This course will be taught in Washington, DC and video-cast on Homewood Campus.)
Distribution Area: Social and Behavioral Sciences

EN.650.621. Critical Infrastructure Protection. 3 Credits.
This course focuses on understanding the history, the vulnerability, and the need to protect our Critical Infrastructure and Key Resources (CIKR). We will start by briefly surveying the policies which define the issues surrounding CIKR and the strategies that have been identified to protect them. Most importantly, we will take a comprehensive approach to evaluating the technical vulnerabilities of the identified sectors, and we will discuss the tactics that are necessary to mitigate the risks associated with each sector. These vulnerabilities will be discussed from the perspective of ACM, IEEE or other technical journals/articles which detail recent and relevant network-level CIKR exploits. We will cover well known vulnerable systems such the Internet, SCADA or PLC and lesser known systems such as E911 and industrial robot. Also, a class project is required. Recommended Course Background: EN.650.424 or equivalent or permission by instructor.
Distribution Area: Engineering, Natural Sciences

EN.650.624. Network Security. 3 Credits.
This course focuses on communication security in computer systems and networks. The course is intended to provide students with an introduction to the field of network security. The course covers network security services such as authentication and access control, integrity and confidentiality of data, firewalls and related technologies, Web security and privacy. Course work involves implementing various security techniques. A course project is required. Course Background: EN.601.220, EN.601.226, EN.601.418 or equivalent. No Audits.
Prerequisite(s): Students may only earn credit for one of the following courses: EN.650.624 OR EN.601.444 OR EN.601.644
Distribution Area: Engineering

EN.650.631. Ethical Hacking. 3 Credits.
Cyber security affects every facet of industry and our government, and thus is now a threat to National Security. This course is designed to introduce students to the skills needed to defend computer network infrastructure by exposing them to the hands-on identification and exploitation of vulnerabilities in servers (i.e., Windows and Linux), wireless networks, websites, and cryptologic systems. These skills will be tested by having teams of students develop and participate in instructor lead capture-the-flag competitions. Also included are advanced topics such as shell coding, IDA Pro analysis, fuzzing, and writing or exploiting network-based applications or techniques such as web servers, spoofing, and denial of service.
Distribution Area: Engineering

EN.650.640. Moral & Legal Foundations of Privacy. 3 Credits.
This course explores the ethical and legal underpinnings of the concept of privacy. It examines the nature and scope of the right to privacy by addressing fundamental questions such as: What is privacy? Why is privacy morally important? How is the right to privacy been articulated in constitutional law?

EN.650.654. Computer Intrusion Detection. 3 Credits.
Intrusion detection supports the on-line monitoring of computer system activities and the detection of attempts to compromise normal services. This course starts with an overview of intrusion detection tasks and activities. Detailed discussion introduces a traditional classification of intrusion detection models, applications in host-centered and distributed environments, and various intrusion detection techniques ranging from statistical analysis to biological computing. This course serves as a comprehensive introduction of recent research efforts in intrusion detection and the challenges facing modern intrusion detection systems. Students will also be able to pursue in-depth study of special topics of interest in course projects.
Distribution Area: Engineering, Natural Sciences

EN.650.656. 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.
Distribution Area: Engineering

EN.650.658. Introduction to Cryptography. 3 Credits.
Cryptography has a rich history as one of the foundations of information security. This course serves as the introduction to the working primitives, development and various techniques in this field. It emphasizes reasoning about the constraint and construction of cryptographic protocols that use shared secret key or public key. Students will also be exposed to some current open problems. Permission of instructor only.
Distribution Area: Engineering

EN.650.660. Software Vulnerability Analysis. 3 Credits.
Competent execution of security assessments on modern software systems requires extensive knowledge in numerous technical domains and comprehensive understanding of security risks. This course provides necessary background knowledge and examines relevant theories for software vulnerabilities and exploits in detail. Key topics include historical vulnerabilities, their corresponding exploits, and associated risk mitigations. Fundamental tools and techniques for performing security assessments (e.g., software reverse engineering, static analysis, and dynamic analysis) are covered extensively. The format of this course includes lectures and assignments where students learn how to develop exploits to well-known historical vulnerabilities in a controlled environment. Students will complete and demonstrate a project as part of the course.
Distribution Area: Engineering

EN.650.663. Cloud Computing Security. 3 Credits.
Cloud computing promises significant cost savings via economies of scale that typically are not achievable by a single organization. This course examines cloud computing in detail and introduces the security concerns associated with cloud computing. Key topics include service models for cloud computing, virtualization, storage, management, and data processing. Fundamental security principles are introduced and applied to cloud computing environments. The format of this course includes lectures and hands-on assignments. Students will complete a project and present it as part of the course.
Distribution Area: Engineering, Natural Sciences

EN.650.667. 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.
Distribution Area: Engineering

EN.650.672. Security Analytics. 3 Credits.
Security analytics refers to information technology solutions that gather and analyze security events to bring situational awareness and enable IT staff to understand and analyze events that pose the greatest risk. Increasingly, detecting and preventing cyber attacks require sophisticated use of data analytics and machine learning tools. This course will cover fundamental theories and methods in data science, modern security analytical tools, and practical use cases of security analytics. Students of this course learn concepts, tasks, and methods of data science; and how to apply data science to cyber security problems. Students also learn how to use modern software in security analytics. Recommend Course Background: Basic knowledge of statistics; Either python or R programming skill (do not require both).

EN.650.673. Mobile and Wireless Security. 3 Credits.
The past few decades have seen a rapid evolution of wireless LAN and cellular technologies. In addition to wireless access technologies, various types of network layer and application layer mobility protocols have been developed to provide seamless connectivity to mobile users. Maintaining end-to-end security for these mobile users needs to take into account authentication, authorization, integrity and confidentiality as mobile devices change their point-of-attachment. This course will provide an overview of various wireless access technologies, mobility protocol taxonomy and will describe end-to-end security including mobile end point, radio access network, network core, and application services. In addition, this will include hands-on lab experiments to examine security over wireless and mobile networks and a research group project. Overall objective of this course is to impart both theoretical and practical knowledge to the students, and at the same time make them ready for any future research to solve complex problems. Recommended Course Background: Knowledge of TCP/IP, Linux, Fundamentals of Networking
Distribution Area: Engineering, Natural Sciences

EN.650.681. Global Cybersecurity Trends and Practices. 3 Credits.
This course provides an overview of cybersecurity capabilities and practices in the global community. International organizations engaged in cybersecurity policy and governance and the national strategies of many countries are examined in detail. Students will gain insights into the political, economic, military, and technological components of cybersecurity as practiced in the U.S., UK, China, Russia, and other countries. The course is designed around four general themes: global cyber threats, strategies and policies in response to cyber threats, comparative cybersecurity capabilities of nation-states; and cybersecurity in international politics. Students will also gain an appreciation of key cybersecurity issues like critical infrastructure protection and information sharing in the international context. The course will provide students a broad perspective on the global context of cybersecurity, complementing knowledge gained in other courses in the graduate program. There will be assignments to study key literature and current events, as well as quizzes and a mid-term exam. Students will also conduct research projects that focus on the interaction of technology, policy, strategy, and governance, and present results to the class. EN.650.401/EN.650.601 recommended
Distribution Area: Engineering

EN.650.683. Cybersecurity Risk Management. 3 Credits.
Data breaches, cyber attacks, cybercrime, and information operations in social media continue to increase in frequency and severity, causing businesses and governments to focus more resources on cybersecurity risk management and compliance. Utilizing real-world data breaches and attacks as motivation, this course will provide students knowledge of risk management concepts, frameworks, compliance regimes and best industry practices used to ensure sound cybersecurity practices in government, commercial, and academic organizations. Lab exercises will provide opportunities for students to experience key aspects of the risk management process and help prepare them for post-graduation assignments as cybersecurity professionals. Recommended Course Background: EN.650.601.
Distribution Area: Engineering

EN.650.685. Cybersecurity Compliance: Regulation, Behavior, and Best Practices. 3 Credits.
This course provides a comprehensive exploration of cybersecurity compliance through the lens of regulatory frameworks and behavioral models. Students will examine key cybersecurity laws and regulations and learn how human behavior influences organizational compliance practices. By understanding both the technical and psychological aspects of compliance, students will be equipped to develop effective programs that ensure adherence to regulations while promoting a culture of compliance.
Distribution Area: Engineering, Natural Sciences

EN.650.757. Advanced Computer Forensics. 3 Credits.
This course will analyze advanced topics and state of the art issues in the field of digital forensics. The course will be run in a research seminar format and students will be given both basic and applied research projects in such areas as: intrusion analysis, network forensics, memory forensics, mobile devices, and other emerging issues.

EN.650.836. Information Security Projects. 1 Credit.
All MSSI programs must include a project involving a research and development oriented investigation focused on an approved topic addressing the field of information security and assurance from the perspective of relevant applications and/or theory. There must be project supervision and approval involving a JHUISI affiliated faculty member. A project can be conducted individually or within a team-structured environment comprised of MSSI students and an advisor. A successful project must result in an associated report suitable for on-line distribution. When appropriate, a project can also lead to the development of a so-called "deliverable" such as software or a prototype system. Projects can be sponsored by government/industry partners and affiliates of the Information Security Institute, and can also be related to faculty research programs supported by grants and Contracts. Required course for any full-time MSSI student. Open to MSSI students. Permission required for non-MSSI students.

EN.650.837. Information Security Projects. 1 Credit.
Open to MSSI students Permission Required for non-MSSI students All MSSI programs must include a project involving a research and development oriented investigation focused on an approved topic addressing the field of information security and assurance from the perspective of relevant applications and/or theory. There must be project supervision and approval involving a JHUISI affiliated faculty member. A project can be conducted individually or within a team-structured environment comprised of MSSI students and an advisor. A successful project must result in an associated report suitable for on-line distribution. When appropriate, a project can also lead to the development of a so-called "deliverable" such as software or a prototype system. Projects can be sponsored by government/industry partners and affiliates of the Information Security Institute, and can also be related to faculty research programs supported by grants and Contracts. Required for MSSI students on full-time status. No Audits.

EN.650.840. Information Security Independent Study. 3 Credits.
Individual study in an area of mutual interest to a graduate student and a faculty member in the Institute.

Cross-Listed Courses

Computer Science

EN.601.631. Theory of Computation. 3 Credits.
This course covers the theoretical foundations of computer science. Topics included will be models of computation from automata to Turing machines, computability, complexity theory, randomized algorithms, inapproximability, interactive proof systems and probabilistically checkable proofs. Students may not take both 601.231 and 601.431/601.631, unless one is for an undergrad degree and the other for grad. Required Background: discrete math or permission; discrete probability theory recommended.
Prerequisite(s): Students can receive credit for only one of EN.601.431/EN.601.631
Distribution Area: Engineering, Quantitative and Mathematical Sciences

EN.601.633. Intro Algorithms. 3 Credits.
Same material as EN.601.433, for graduate students.This course concentrates on the design of algorithms and the rigorous analysis of their efficiency. topics include the basic definitions of algorithmic complexity (worst case, average case); basic tools such as dynamic programming, sorting, searching, and selection; advanced data structures and their applications (such as union-find); graph algorithms and searching techniques such as minimum spanning trees, depth-first search, shortest paths, design of online algorithms and competitive analysis. Required Background: data structures, discrete math, proof writing.
Prerequisite(s): Students may receive credit for only one of EN.600.363, EN.600.463, EN.601.433, EN.601.633
Distribution Area: Engineering, Quantitative and Mathematical Sciences

EN.601.640. Web Security. 3 Credits.
This course begins with reviewing basic knowledge of the World Wide Web, and then exploring the central defense concepts behind Web security, such as same-origin policy, cross-origin resource sharing, and browser sandboxing. It will cover 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. Students will learn how to detect, respond, and recover from security incidents. Newly proposed research techniques will also be discussed. Required course background: data structures, computer system fundamentals and javascript/web development. Students may receive credit for only one of 601.340/440/640.
Prerequisite(s): Students may receive credit for only one of 601.340/440/640.

EN.601.641. Blockchains and Cryptocurrencies. 3 Credits.
Same as EN.601.441, for graduate students. This course will introduce students to cryptocurrencies and the main underlying technology of Blockchains. The course will start with the relevant background in cryptography and then proceed to cover the recent advances in the design and applications of blockchains. This course should primarily appeal to students who want to conduct research in this area or wish to build new applications on top of blockchains. It should also appeal to those who have a casual interest in this topic or are generally interested in cryptography. Students are expected to have mathematical maturity. Recommended Course Background: EN.601.226 AND (EN.553.310 OR EN.553.420)
Prerequisite(s): Students may receive credit for only one of EN.600.451 OR EN.601.441 OR EN.601.641
Distribution Area: Engineering

EN.601.642. Modern Cryptography. 3 Credits.
Same material as 601.442, for graduate students. Modern Cryptography includes seemingly paradoxical notions such as communicating privately without a shared secret, proving things without leaking knowledge, and computing on encrypted data. In this challenging but rewarding course we will start from the basics of private and public key cryptography and go all the way up to advanced notions such as zero-knowledge proofs, functional encryption and program obfuscation. The class will focus on rigorous proofs and require mathematical maturity. Required course background: Probability & Automata/Computation Theory
Prerequisite(s): Students may receive credit for only one of EN.601.442 OR EN.601.642.
Distribution Area: Engineering, Quantitative and Mathematical Sciences

EN.601.643. Security & Privacy in Computing. 3 Credits.
Same material as 601.443, for graduate students. Lecture topics will include computer security, network security, basic cryptography, system design methodology, and privacy. There will be a heavy work load, including written homework, programming assignments, exams and a comprehensive final. The class will also include a semester-long project that will be done in teams and will include a presentation by each group to the class. Required course background: C programming and computer system fundamentals.
Prerequisite(s): Students may receive credit for only one of EN.600.443, EN.601.443, EN.601.643.
Distribution Area: Engineering

EN.601.644. Medical Device Cybersecurity. 3 Credits.
In an increasingly connected healthcare landscape, medical devices have effectively become IT endpoints, often running general-purpose operating systems like Windows or Linux, incorporating cloud microservices, and integrating artificial intelligence to detect, prevent, and improve patient health outcomes. Protecting these devices from cyber threats is not just a technical challenge—it's a matter of patient safety. A security breach in medical devices like pacemakers or infusion pumps can have life-threatening consequences. National and international regulatory bodies, such as the FDA and EU National Competent Authorities (NCAs) and Medical Device Regulation (MDR), know the implications and have provided prescription and guidance emphasizing stringent cybersecurity measures throughout a device's lifecycle, from design and development to postmarket surveillance. The result is a heightened awareness of medical device security and its impact on healthcare delivery, requiring cybersecurity risk management. In particular, focusing on threat modeling, cybersecurity risk assessment, secure design, secure coding practices, vulnerability management and monitoring, software bill of materials, cybersecurity transparency, user labeling, penetration testing, and more. Recommended background: computing systems, operating systems, machine learning & AI. Students may receive credit for only one of 601.444/601.644.
Prerequisite(s): Students who have already taken, or are currently enrolled in EN.601.444, are not eligible to take EN.601.644.;EN.601.443 OR EN.601.643

EN.601.645. Practical Cryptographic Systems. 3 Credits.
Same material as 601.445, for graduate students. This semester-long course will teach systems and cryptographic design principles by example: by studying and identifying flaws in widely-deployed cryptographic products and protocols. Our focus will be on the techniques used in practical security systems, the mistakes that lead to failure, and the approaches that might have avoided the problem.We will place a particular emphasis on the techniques of provable security and the feasibility of reverse-engineering undocumented cryptographic systems.
Prerequisite(s): Students may receive credit for EN.600.454/EN.601.445 or EN.601.645, but not both.
Distribution Area: Engineering

EN.601.740. Language-based Security. 3 Credits.
This course will introduce Language-based Security, an emerging field in cyber security that leverages techniques from compilers and program analysis for security-related problems. Topics include but are not limited to: Control-flow and data-flow graphs, Program slicing, Code property graph (CPG), and Control-flow integrity. Students are expected to read new and classic papers in this area and discuss them in class. Recommended backgrounds are Operating Systems and preferably Compilers.

EN.601.742. Advanced Topics in Cryptography. 3 Credits.
This course will focus on advanced cryptographic topics with an emphasis on open research problems and student presentations.
Prerequisite(s): EN.601.442 OR EN.601.642 or Permission of Instructor.

EN.601.743. Advanced Topics in Computer Security. 3 Credits.
Topics will vary from year to year, but will focus mainly on network perimeter protection, host-level protection, authentication technologies, intellectual property protection, formal analysis techniques, intrusion detection and similarly advanced subjects. Emphasis in this course is on understanding how security issues impact real systems, while maintaining an appreciation for grounding the work in fundamental science. Students will study and present various advanced research papers to the class. There will be homework assignments and a course project. A college level security or crypto course at Hopkins or any other school is required.

For current faculty and contact information go to https://www.cs.jhu.edu/academic-programs/graduate-studies/ms-in-security-informatics/