The Johns Hopkins University Information Security Institute (JHUISI) 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. JHUISI is committed to a comprehensive approach that includes input from academia, industry and government. The University, through JHUISI's leadership, has thus been designated as a Center of Academic Excellence in Information Assurance Education and Research by the National Security Agency and the Department of Homeland Security, and leading experts in the field. Through our broad range of educational opportunities including a ground-breaking graduate program and leading edge research in foundational science and applied technologies, JHUISI is having a significant impact in the region and nationwide.

Our research in cryptography, networking, wireless, systems evaluation, medical privacy and electronic voting, among other areas is widely circulated among academics and policymakers. Moreover, JHUISI 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, 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, several customizable machines for student projects, and multiple high-speed laser printers. 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.

M.S.S.I. Graduate Program
The flagship educational experience offered by Johns Hopkins University in the area of information security and assurance is represented by the Master of Science in Security Informatics (M.S.S.I.) degree. A wide range of courses is available in support of this unique and innovative graduate program.

The M.S.S.I. is a full-time day program offered on the Homewood Campus in North Baltimore. Most students complete the program in three full-time semesters though some graduate students may finish their degree part-time after completing the required two consecutive semesters of residency as a full-time student.

Application Requirements for the M.S.S.I. Degree
- Application to the M.S.S.I. degree is open to outstanding candidates who hold a bachelor's degree with sufficient technical exposure to computer science that serves as preparation for the core technology courses, including intermediate programming, data structure, discrete mathematics, and computer system fundamentals.
- All applicants are obligated to take and submit the results of the Aptitude Test of the Graduate Record Examination as one of the requirements for admission.
- International students are obligated to take either the TOEFL test or the IELTS test.

The preferred scores are as follows:

**GRE General Test**
- Verbal: 153 (62%)
- Quantitative: 160 (84%)
- Analytical: 3.5

**TOEFL Internet based**
- 100

**IELTS**
- 7.0

- The institution code for both the GRE and TOEFL is 5332.
- The department code for the GRE is 0404. The department code for TOEFL is 78.
- These scores in the above serve as general guidelines for admission. The Admissions Committee in making its final decisions will consider the combination of professional knowledge, academic excellence, letters of recommendation, and the statement of purpose, as well as GRE, TOEFL, and IELTS scores of the applicants.
- A student is required to apply online at [https://app.applyyourself.com/?id=jhu-grad](https://app.applyyourself.com/?id=jhu-grad).

Course Requirements for the M.S.S.I.
Upon admission to the Master of Science in Security Informatics, a student is assigned a graduate advisor from the Information Security Institute who must approve the courses to be applied to the M.S.S.I. degree.

The Master of Science in Security Informatics program has a course requirement of a minimum of 10 courses, plus a team-based capstone project including a report and presentation. Students must choose one of two tracks – Technology & Research Track or Policy & Management Track.

All courses supporting the M.S.S.I. are categorized as one of four areas of Technology, Policy, Health, and Management. Each course is further classified into Core, Elective or Foundational category.

The Technology & Research Track program of study must satisfy the following course distribution requirements:
- Five Technology courses: at least four Core Technology courses including at least one Core Technology course in Cryptography.
- Three Core Policy/Management/Health courses: at least one Core Policy course and one Core Management course.
- Two additional courses from Core or Elective Technology categories; or when deemed appropriate relative to a student's background,
interests, and goals AND with the prior approval of the faculty advisor and the institute, from other course areas.

The Policy & Management Track program of study must satisfy the following course distribution requirements:

• Three Technology courses: at least two Core Technology courses including at least one Core Technology course in Cryptography.
• Five Core/Foundational Policy/Health/Management courses: at least one course from each of Core Policy/Management/Health categories and at least one Foundational Management course.
• Two additional courses from Core/Elective Technology or Core/Foundational Policy/Management/Health categories; or when deemed appropriate relative to a student's background, interests, and goals AND with the prior approval of the faculty advisor and the institute, from other course areas.

Project Requirement
The M.S.S.I. Capstone Project will include both technology and non-technology components, and will be conducted within a team-structured environment comprised of students and faculty mentors (plus external mentors if appropriate). These projects will generally 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. They should relate to real-world problems and exhibit both theoretical and practical significance. The project must be documented by a report and presentation, as well as other applicable deliverables including but not limited to system prototypes, utility libraries, experimental demonstrations, conference or journal submissions, and so on. It should follow the best practice of software engineering.

Students should actively initiate the project while communicating with the potential faculty mentor for technical issues and the faculty advisor for project management. They are expected to develop a project plan at the end of the second semester. The project is expected to have a proposal approved at the start of the third semester and be finished by the end of the third semester. A presentation will be scheduled when the project concludes. The faculty mentor should approve each milestone of the project with the faculty advisor being informed. When the project is completed with all the deliverables, the faculty advisor assigns a score upon the recommendation of the faculty mentor.

Additional Course Requirements
• All courses toward the degree requirement must be 400-level or above. Other courses can be used with the approval of the Institute.
• Courses not found on the area-specific lists (http://engineering.jhu.edu/jhuisi/mssi-course-distribution) can be used to meet area requirements with prior approval from the student’s advisor and the Institute.
• At most two independent study courses can be counted toward the course requirements.
• No courses with grades of P may be counted with the exception of independent study courses.
• At most two courses may be transferred from other institutions. The student’s faculty advisor and the Director of Information Security Institute must approve such transfer courses.
• The overall grade point average of the courses counted towards the coursework requirements must be 3.00 or higher.

• At most two courses with grade less than B- may be counted towards the course work requirements. No courses with grade less than C- may be counted.
• A grade of D or F results in probation. A second D or F is cause for being dropped from the program.
• Completion of Academic Ethics (EN.500.603) and Responsible Conduct of Research training.

JHUISI Courses

<table>
<thead>
<tr>
<th>Course</th>
<th>Title</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>EN.601.641</td>
<td>Blockchains and Cryptocurrencies</td>
<td>3</td>
</tr>
<tr>
<td>EN.601.642</td>
<td>Modern Cryptography</td>
<td>3</td>
</tr>
<tr>
<td>EN.601.643</td>
<td>Security &amp; Privacy in Computing</td>
<td>3</td>
</tr>
<tr>
<td>EN.601.644</td>
<td>Network Security</td>
<td>3</td>
</tr>
<tr>
<td>EN.601.645</td>
<td>Practical Cryptographic Systems</td>
<td>3</td>
</tr>
<tr>
<td>EN.601.743</td>
<td>Advanced Topics in Computer Security</td>
<td>3</td>
</tr>
<tr>
<td>EN.601.745</td>
<td>Advanced Topics in Applied Cryptography</td>
<td>3</td>
</tr>
<tr>
<td>EN.650.601</td>
<td>Introduction to Information Security</td>
<td>3</td>
</tr>
<tr>
<td>EN.650.614</td>
<td>Rights In Digital Age</td>
<td>3</td>
</tr>
<tr>
<td>EN.650.621</td>
<td>Critical Infrastructure Protection</td>
<td>3</td>
</tr>
<tr>
<td>EN.650.631</td>
<td>Ethical Hacking</td>
<td>3</td>
</tr>
<tr>
<td>EN.650.640</td>
<td>Moral &amp; Legal Foundations of Privacy</td>
<td>3</td>
</tr>
<tr>
<td>EN.650.653</td>
<td>Financial Issues in Managing a Secure Operation</td>
<td>3</td>
</tr>
<tr>
<td>EN.650.654</td>
<td>Computer Intrusion Detection</td>
<td>3</td>
</tr>
<tr>
<td>EN.650.655</td>
<td>Implementing Effective Information Security Projects</td>
<td>3</td>
</tr>
<tr>
<td>EN.650.656</td>
<td>Computer Forensics</td>
<td>3</td>
</tr>
<tr>
<td>EN.650.658</td>
<td>Introduction to Cryptography</td>
<td>3</td>
</tr>
<tr>
<td>EN.650.660</td>
<td>Software Vulnerability Analysis</td>
<td>3</td>
</tr>
<tr>
<td>EN.650.661</td>
<td>Human Factors in Information Security</td>
<td>3</td>
</tr>
<tr>
<td>EN.650.663</td>
<td>Cloud Computing Security</td>
<td>3</td>
</tr>
<tr>
<td>EN.650.671</td>
<td>Cryptography &amp; Coding</td>
<td>4</td>
</tr>
<tr>
<td>EN.650.672</td>
<td>Security Analytics</td>
<td>3</td>
</tr>
<tr>
<td>EN.650.681</td>
<td>Global Cybersecurity Trends and Practices</td>
<td>3</td>
</tr>
<tr>
<td>EN.650.724</td>
<td>Advanced Network Security</td>
<td>3</td>
</tr>
<tr>
<td>EN.650.757</td>
<td>Advanced Computer Forensics</td>
<td>3</td>
</tr>
<tr>
<td>EN.650.840</td>
<td>Information Security Independent Study</td>
<td>3</td>
</tr>
</tbody>
</table>

All courses supporting the M.S.S.I. are categorized as one of four areas of Technology, Policy, Health, and Management. Each course is further classified into Core, Elective or Foundational category.

• For seven-week course modules, e.g., several courses offered through the Whiting School of Engineering Center for Leadership Education (CLE) (http://eng.jhu.edu/wse/cle), two of them count as one course of 3 credit hours.
• For quarter-based courses, e.g., several courses of course numbers starting with ME from the School of Medicine Division of Health Sciences Informatics (http://dhsci.med.jhmi.edu), two of them are equivalent of one WSE course of 3 credit hours.

Core Technology Courses

<table>
<thead>
<tr>
<th>Course</th>
<th>Title</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>EN.601.642</td>
<td>Modern Cryptography</td>
<td>3</td>
</tr>
<tr>
<td>EN.601.643</td>
<td>Security &amp; Privacy in Computing</td>
<td>3</td>
</tr>
<tr>
<td>EN.601.644</td>
<td>Network Security</td>
<td>3</td>
</tr>
<tr>
<td>EN.601.645</td>
<td>Practical Cryptographic Systems</td>
<td>3</td>
</tr>
<tr>
<td>EN.601.743</td>
<td>Advanced Topics in Computer Security</td>
<td>3</td>
</tr>
</tbody>
</table>
Elective Policy/Health/Management Courses

- EN.650.601 Introduction to Information Security
- EN.650.631 Theory of Computation

Core Policy Courses

- EN.650.653 Intro Algorithms
- EN.650.654 Cloud Computing Security
- EN.650.655 Implementing Effective Information Security Projects

Foundational Management Courses

- EN.663.644 Improving Presentation Skills for Scientists and Engineers
- EN.663.650 Global Cybersecurity Trends and Practices
- EN.663.651 Law and the Internet

Core Health Courses

- EN.650.640 Rights In Digital Age
- EN.650.641 Blockchains and Cryptocurrencies
- EN.650.681 Information Security Independent Study

Core Management Courses

- EN.663.670 Project Management
- EN.663.671 Leading Change
- EN.663.672 Security Analytics

Elective Technology Courses

- EN.663.644 Writing Articles and Technical Reports
- EN.663.645 Computer Intrusion Detection
- EN.663.646 Software Vulnerability Analysis

Elective Policy/Health/Management Courses

- PH.300.651 Introduction to U.S. Healthcare System Policy
- AS.406.665 Art and Practice of Intelligence

* For other elective options that fulfill this requirement refer to http://isi.jhu.edu/mssi/course_distribution

Combined Bachelor’s/Master’s Degree Program in Conjunction with the M.S.S.I.

A combined bachelor’s/master’s degree program including the M.S.S.I. is also available to Johns Hopkins University students. In this program, by the conclusion of the undergraduate sophomore/junior academic year, a student can apply for combined admission into the M.S.S.I. program. If accepted, the student during each subsequent semester partitions her/his course load into courses that will count for the undergraduate degree and courses that will count for the M.S.S.I. degree. Usually with one additional year of study, the student can simultaneously satisfy both sets of degree requirements. For more information on the combined bachelor’s/master’s status, please visit https://engineering.jhu.edu/academics/combined-bachelors-masters/.

Dual Master’s Program with the Department of Computer Science

Students interested in pursuing the above Dual Master’s Program (DMP) will have initially entered either the M.S.S.I. program or the M.S.E. program in Computer Science, and then apply for the DMP at a later point. A maximum of two courses (approved by the advisors) can be double counted toward each set of course requirements, thereby facilitating the feasibility of completing the DMP in two academic years plus the in-between summer. In such cases, the designation of the double counted courses would be done in conjunction with one advisor from each department and the Academic Program Administrator.

Dual Master’s Program with the Department of Applied Math and Statistics in the WSE

A similar DMP has been initiated regarding the JHUISI M.S.S.I. and the master’s program in the Department of Applied Math and Statistics in the WSE. The details of this DMP are similar in principle to those for the M.S.S.I./M.S.E. in Computer Science, but there are some significant requirement/curricular differences. Each program should be contacted if a student is interested, and students will need to comply with any application processes for consideration.

Dual Master’s Program with the School of Public Health

A similar DMP has been initiated regarding the JHUISI M.S.S.I. and the Master of Health Sciences (M.H.S.) program in the Bloomberg School of Public Health (BSPH). The details of this M.S.S.I./M.H.S. DMP are similar in principle to those for the M.S.S.I./M.S.E. in Computer Science, but there are some significant differences. Each program should be contacted if a student is interested.

For current faculty and contact information go to http://isi.jhu.edu/institute/people

Faculty

Executive Director
Anton Dahbura
Information Security Institute

Program Director
Xiangyang Li
Master of Science in Security Informatics

Professor
Aviel Rubin
Computer Science: Technical Director of Information Security Institute: network and systems security, applied cryptography, cryptographic key distribution, anonymity and computer privacy, electronic commerce, fire-walls and network perimeter defenses, security issues in e-voting, applying security to applications such as medical information systems, intellectual property protection.

**Associate Research Professor**
Susan Hohenberger
Computer Science: theory, cryptography, computer security, algorithms, complexity theory, balancing privacy and accountability in information systems.

**Assistant Professors**
Matthew Green
Computer Science: applied cryptography, cryptographic protocol design, analysis of practical security systems, privacy-preserving storage and identification technologies.

Abhishek Jain
Computer Science: cryptography & security, theoretical computer science.

**Lecturers**
Joel Coffman, Ph.D.
Senior Cyber Engineer, Applied Physics Laboratory: cloud computing, databases, software engineering, computer architecture.

Vincent Galluzzo, J.D.
Intellectual Property Protection, Privacy.

Michael Jacobs, J.D.
Computer ethics, digital rights management, intellectual property protection.

Reuben A. Johnston
Senior Cyber Security Research Engineer, Applied Physics Laboratory: Systems engineering, operations research, software security and reverse engineering.

Michael Kociemba
Information security, management, and infrastructure protection.

Timothy R. Leschke, Ph.D.
Computer forensics, Information Visualization.

Song Luo, Ph.D
Computer security and security analytics.

Seth Nielson, Ph.D.
Network security.

Williams Sauers, J.D.
Digital rights management, intellectual property protection.

Terry L. Thompson, Ph.D
Global cyber trends, cyber policy and governance.

Lanier Watkins, Ph.D.

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

---

**Courses**

**EN.650.401. Introduction to Information Security. 3.0 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. Instructor(s): X. Li.

**EN.650.457. Computer Forensics. 3.0 Credits.**
This course introduces students to the field of computer forensics and it will focus on the various contemporary policy issues and applied technologies. Topics to be covered include: legal and regulatory issues, investigation techniques, data analysis approaches, and incident response procedures for Windows and UNIX systems. Homework in this course will relate to laboratory assignments and research exercises. Students should also expect that a group project will be integrated into this course.
Instructor(s): T. Leschke

**EN.650.458. Introduction to Cryptography. 3.0 Credits.**
A first course in the mathematical theory of secure and reliable electronic communication. Cryptology is the study of secure communication: How can we ensure the privacy of messages? Coding theory studies how to make communication reliable: How can messages be sent over noisy lines? Topics include finite field arithmetic, error-detecting and error-correcting codes, data compressions, ciphers, one-time pads, the Enigma machine, one-way functions, discrete logarithm, primality testing, secret key exchange, public key cryptosystems, digital signatures, and key escrow. Students should have computing experience. Recommended Course Background: AS.110.201
Prerequisites: EN.550.171 or permission
Instructor(s): T. Leschke
Area: Engineering, Quantitative and Mathematical Sciences.

**EN.650.459. Cryptography & Coding. 4.0 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. Instructor(s): X. Li.
EN.650.614. Rights In Digital Age. 3.0 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.)
Instructor(s): M. Jacobs
Area: Social and Behavioral Sciences.

EN.650.621. Critical Infrastructure Protection. 3.0 Credits.
This course focuses on understanding the history, the vulnerability, and the need to protect our Critical Infrastructure 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 18 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.
Instructor(s): L. Watkins
Area: Engineering, Natural Sciences.

EN.650.624. Advanced Network Security. 3.0 Credits.
This course focuses on advanced security topics and research in computer networks. It builds on the basic overview of network security covered in previous security courses. Beyond the basics of developing security network communications and applications, this advanced course dives deeper into the theory and practice behind network attack, the growing reality of weaponized zero-day vulnerabilities, and the current state-of-the-art responses. Course work includes reviewing contemporary security research papers, hands-on experiments in defending/attacking networks, and writing analyses.
Prerequisites: EN.650.424 OR EN.600.424 or permission of the instructor.
Instructor(s): S. Nielson
Area: Engineering.

EN.650.631. Ethical Hacking. 3.0 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.
Instructor(s): L. Watkins
Area: Engineering.

EN.650.640. Moral & Legal Foundations of Privacy. 3.0 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?
Instructor(s): V. Galluzzo; W. Sauers.

EN.650.653. Financial Issues in Managing a Secure Operation. 3.0 Credits.
This course addresses the risks (financial, reputation, business, and third party), costs, ROI, and other business issues concerned in planning and managing a secure operation. Topics include disaster recovery, outsourcing issues; service level agreements; evaluating external security service providers; assessing security total cost of ownership; audit procedures; financial integrity; cost/benefit analyses; back-up and recovery provisions; insurance protection; contingency and business continuity plans; qualitative and quantitative risk analysis; monitoring the security of the enterprise; information economics; performance reporting; automated metrics reporting; responses to threats; effects of security policies and practices on business and customers; preparing a business case for information security investments; and developing cost-effective solutions given constraints in money, assets, and personnel. Case studies and exercises will be used to illustrate financial planning and evaluation of security operations.
Instructor(s): M. Kociemba.

EN.650.654. Computer Intrusion Detection. 3.0 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.
Instructor(s): X. Li
Area: Engineering, Natural Sciences.
EN.650.655. Implementing Effective Information Security Projects. 3.0 Credits.
This course focuses on the personnel, legal, regulatory and privacy issues that comprise the basic security management areas that must be considered when developing and implementing an effective information security program. Specific topics include security-related legislation, government and industry security frameworks, the identification and management of risk, security controls, defense in depth, critical infrastructure protection, development and implementation of an enterprise wide security strategy, and organizational roles and responsibilities.
Instructor(s): M. Kociemba.

EN.650.656. Computer Forensics. 3.0 Credits.
This course introduces students to the field of computer forensics and it will focus on the various contemporary policy issues and applied technologies. Topics to be covered include: legal and regulatory issues, investigation techniques, data analysis approaches, and incident response procedures for Windows and UNIX systems. Homework in this course will relate to laboratory assignments and research exercises. Students should also expect that a group project will be integrated into this course.
Instructor(s): T. Leschke
Area: Engineering.

EN.650.658. Introduction to Cryptography. 3.0 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.
Instructor(s): X. Li
Area: Engineering.

EN.650.660. Software Vulnerability Analysis. 3.0 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.
Instructor(s): R. Johnston
Area: Engineering.

EN.650.661. Human Factors in Information Security. 3.0 Credits.
The human factor is critical to any successful computer security solution since users are very often the weakest link in such systems. This course will examine a variety of human behaviors ranging from micro to macro cybernetic levels that are relevant to making the best case for information security. It is delivered through lectures on relevant findings in different disciplines of human computer interaction, human factors engineering, cognitive science, and product design; studies of useful user and security modeling frameworks and tools; and term research projects to explore security oriented topics in human machine systems. Its goal is to improve security informatics through informed decisions by the knowledge of the good and bad human characters in computer and cyber security.
Instructor(s): X. Li
Area: Engineering.

EN.650.663. Cloud Computing Security. 3.0 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.
Instructor(s): J. Coffman
Area: Engineering, Natural Sciences.

EN.650.671. Cryptography & Coding. 4.0 Credits.
A first course in the mathematical theory of secure and reliable electronic communication. Cryptology is the study of secure communication: How can we ensure the privacy of messages? Coding theory studies how to make communication reliable: How can messages be sent over noisy lines? Topics include finite field arithmetic, error-detecting and error-correcting codes, data compressions, ciphers, one-time pads, the Enigma machine, one-way functions, discrete logarithm, primality testing, secret key exchange, public key cryptosystems, digital signatures, and key escrow. Students should have computing experience. Recommended Course Background: AS.110.201
Prerequisites: EN.550.171 or permission of the instructor.
Instructor(s): D. Fishkind
Area: Engineering, Quantitative and Mathematical Sciences.

EN.650.672. Security Analytics. 3.0 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).
Instructor(s): S. Luo.
EN.650.681. Global Cybersecurity Trends and Practices. 3.0 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
Instructor(s): T. Thompson
Area: Engineering.

EN.650.724. Advanced Network Security. 3.0 Credits.
This course focuses on advanced security topics and research in computer networks. It builds on the basic overview of network security covered in previous security courses. Beyond the basics of developing security network communications and applications, this advanced course dives deeper into the theory and practice behind network attack, the growing reality of weaponized zero-day vulnerabilities, and the current state-of-the-art responses. Course work includes reviewing contemporary security research papers, hands-on experiments in defending/attacking networks, and writing analyses.
Prerequisites: EN.601.644 or permission of the instructor.
Instructor(s): S. Nielson
Area: Engineering.

EN.650.739. Special Network Security Projects. 1.0 - 4.0 Credits.
Instructor(s): Staff.

EN.650.757. Advanced Computer Forensics. 3.0 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.
Instructor(s): T. Leschke.

EN.650.836. Information Security Projects. 1.0 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 JHUASI 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.
Instructor(s): A. Dahbura; X. Li.

EN.650.837. Information Security Projects. 1.0 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 JHUASI 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.
Instructor(s): A. Dahbura; X. Li.

EN.650.840. Information Security Independent Study. 3.0 Credits.
Individual study in an area of mutual interest to a graduate student and a faculty member in the Institute.
Instructor(s): X. Li.

EN.650.890. Information Security Research. 1.0 - 4.0 Credits.
Instructor(s): G. Masson.

Cross Listed Courses
Computer Science
EN.601.631. Theory of Computation. 3.0 Credits.
This is a graduate-level course studying the theoretical foundations of computer science. Topics covered 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 EN.601.231 and EN.601.631, unless one is for an undergrad degree and the other for grad. [Analysis]Recommended Course Background: EN.553.171 or instructor permission.
Instructor(s): X. Li
Area: Engineering, Quantitative and Mathematical Sciences.
EN.601.633. Intro Algorithms. 3.0 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. [Analysis]
Prerequisites: Students may receive credit for only one of EN.600.363, EN.600.463, EN.601.433, EN.601.633.
Instructor(s): M. Dinitz
Area: Engineering, Quantitative and Mathematical Sciences.

EN.601.641. Blockchains and Cryptocurrencies. 3.0 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. [Analysis]
Prerequisites: Students may receive credit for only one of EN.600.451 OR EN.601.441 OR EN.601.641; EN.601.226 AND (EN.553.310 OR EN.553.420)
Instructor(s): A. Jain
Area: Engineering.

EN.601.642. Modern Cryptography. 3.0 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. [Analysis] Required course background: EN.601.231 or EN.601.631.
Prerequisites: Students may receive credit for only one of EN.600.442, EN.601.442, EN.601.642.
Instructor(s): A. Jain
Area: Engineering, Quantitative and Mathematical Sciences.

EN.601.643. Security & Privacy in Computing. 3.0 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. [Applications] Recommended Course Background: A basic course in operating systems and networking, or permission of instructor.
Prerequisites: Students may receive credit for only one of EN.600.443, EN.601.443, EN.601.643.
Instructor(s): A. Rubin
Area: Engineering.

EN.601.644. Network Security. 3.0 Credits.
Same material as 601.444, for graduate students. 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. [Systems] Recommended. Course Background: EN.601.220, EN.601.226 or equivalent
Prerequisites: Students may receive credit for only one of EN.600.424, EN.650.424, EN.601.444, EN.601.644.
Instructor(s): S. Nielson
Area: Engineering.

EN.601.645. Practical Cryptographic Systems. 3.0 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. [Systems]
Prerequisites: Students may receive credit for only one of EN.600.454, EN.650.454, EN.601.445, EN.601.645.
Instructor(s): M. Green
Area: Engineering.

EN.601.743. Advanced Topics in Computer Security. 3.0 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.
Instructor(s): A. Rubin.

EN.601.745. Advanced Topics in Applied Cryptography. 3.0 Credits.
This reading and project based course will explore the latest research in the area of applied cryptography and cryptographic engineering. Topics covered will include zero knowledge, efficient multiparty computation, cryptocurrencies, and trusted computing hardware. Readings will be drawn from the latest applied cryptography and security conferences. The course will include both reading, critical analysis, presentations and a course programming project. [Analysis or Applications]
Prerequisites: EN.600.454 OR EN.601.445 OR EN.601.645 OR EN.600.442 OR EN.601.442 OR EN.601.642
Instructor(s): M. Green.