The Johns Hopkins University Information Security Institute (JHUISI) (isi.jhu.edu) 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: 79
- 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 Admission 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 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 students register for EN.650.736/EN.650.737/EN.650.738 for the capstone project. These courses are not counted toward the 10-course requirement.

In general, 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 coursework 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.

---

### JHUISI Courses

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>EN.650.401</td>
<td>Introduction to Information Security</td>
<td>3</td>
</tr>
<tr>
<td>EN.650.414</td>
<td>Rights in Digital Age</td>
<td>3.00</td>
</tr>
<tr>
<td>EN.650.424</td>
<td>Network Security</td>
<td>3.00</td>
</tr>
<tr>
<td>EN.650.431</td>
<td>Ethical Hacking</td>
<td>3.00</td>
</tr>
<tr>
<td>EN.650.432</td>
<td>Embedded Computer Systems</td>
<td>3.00</td>
</tr>
<tr>
<td>EN.650.433</td>
<td>Practical Cryptographic Systems</td>
<td>3.00</td>
</tr>
<tr>
<td>EN.650.457</td>
<td>Computer Forensics</td>
<td>3.00</td>
</tr>
<tr>
<td>EN.650.458</td>
<td>Introduction to Cryptography</td>
<td>3.00</td>
</tr>
<tr>
<td>EN.650.460</td>
<td>Software Vulnerability Analysis</td>
<td>3.00</td>
</tr>
<tr>
<td>EN.650.461</td>
<td>Cloud Computing Security</td>
<td>3.00</td>
</tr>
<tr>
<td>EN.650.471</td>
<td>Cryptography &amp; Coding</td>
<td>4.00</td>
</tr>
<tr>
<td>EN.650.621</td>
<td>Critical Infrastructure Protection</td>
<td>3.00</td>
</tr>
<tr>
<td>EN.650.633</td>
<td>Moral &amp; Legal Foundations of Privacy</td>
<td>3.00</td>
</tr>
<tr>
<td>EN.650.640</td>
<td>Computer Intrusion Detection</td>
<td>3.00</td>
</tr>
<tr>
<td>EN.650.641</td>
<td>Implementing Effective Information Security Projects</td>
<td>3.00</td>
</tr>
<tr>
<td>EN.650.657</td>
<td>Advanced Computer Forensics</td>
<td>3.00</td>
</tr>
<tr>
<td>EN.650.661</td>
<td>Human Factors in Information Security</td>
<td>3.00</td>
</tr>
<tr>
<td>EN.650.736</td>
<td>Information Security Projects</td>
<td>1.00</td>
</tr>
<tr>
<td>EN.650.737</td>
<td>Information Security Projects</td>
<td>1.00</td>
</tr>
<tr>
<td>EN.650.738</td>
<td>Information Security Projects</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4.00</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.

• Two quarter-based courses, e.g., several courses of course numbers starting with ME from the School of Medicine Division of Health Sciences Informatics (http://dhsi.med.jhmi.edu), are equivalent of one WSE course of 3 credit hours.

### Core Technology Courses

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>EN.600.442</td>
<td>Modern Cryptography</td>
<td>3.00</td>
</tr>
<tr>
<td>EN.600.443</td>
<td>Security &amp; Privacy in Computing</td>
<td>3.00</td>
</tr>
</tbody>
</table>
Elective Policy/Health/Management Courses

Foundational Management Courses
EN.663.644 Writing Articles and Technical Reports 1.50
EN.663.645 Improving Presentation Skills for Scientists and Engineers 1.50
EN.663.660 Managing People and Resolving Conflicts 1.50
EN.663.670 Project Management 1.50
EN.663.671 Leading Change 1.50
EN.663.673 Leading Teams in Virtual, International and Local Settings 1.50
EN.663.674 Fundamentals of Management 1.50

Core Policy Courses
EN.650.414 Rights in Digital Age 3.00
EN.650.640 Moral & Legal Foundations of Privacy 3.00
EN.660.311 Law and the Internet 3.00

Core Health Courses
AS.280.340 Fundamentals of Health Policy & Management 3.00

Core Management Courses
EN.650.653 Financial Issues in Managing a Secure Operation 3.00
EN.650.655 Implementing Effective Information Security Projects 3.00

Foundational Technology Courses
EN.600.642 Advanced Topics in Cryptography 3.00
EN.600.643 Advanced Topics in Computer Security 3.00
EN.650.401 Introduction to Information Security 3
EN.650.424 Network Security 3.00
EN.650.431 Ethical Hacking 3.00
EN.650.445 Practical Cryptographic Systems 3.00
EN.650.457 Computer Forensics 3.00
EN.650.458 Introduction to Cryptography 3.00
EN.650.460 Software Vulnerability Analysis 3.00
EN.650.461 Cloud Computing Security 3
EN.650.471 Cryptography & Coding 4.00
EN.650.654 Computer Intrusion Detection 3.00
EN.650.657 Advanced Computer Forensics 3.00
EN.650.661 Human Factors in Information Security 3.00

Elective Policy/Health/Management Courses
The following are sample courses offered by the Bloomberg School of Public Health, the Carey Business School, and the Krieger School of Arts and Sciences.*
PH.300.651 Introduction to U.S. Healthcare System Policy

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

Concurrent Bachelor’s/Master’s Degree Program in Conjunction with the M.S.S.I.
A concurrent 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 concurrent 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.

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.

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.

Joint Program with the Certificate in National Security Studies of the School of Arts and Sciences
A joint M.S.S.I. Degree and the Certificate in National Security Studies (CNSS) (http://advanced.jhu.edu/academics/certificate-programs/national-security-studies/degree-requirements) in the Krieger School of Arts and Science is now being offered. The CNSS requires completion of...
five core courses. Two designated courses can be double counted for the MSSi and the CNSS. Each program should be contacted if a student is interested in completing this course of study.

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.

Professor Emeritus
Gerald Masson
Computer Science: reliable computing, computer networking, real-time monitoring of software operations, computer architecture, computer networking, security informatics relative to networks and software operations.

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
William Agresti, Ph.D.
Professor, Carey Business School: system design and development, information systems architecture, and IT integration for business, software engineering, IT measurement and knowledge management.

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

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

George E. Kalb
Embedded computer systems-vulnerabilities, intrusions and protection mechanisms, embedded systems security, software engineering.

Michael Kociemba
Information security, management, and infrastructure protection.

Timothy R. Leschke, Ph.D.
Computer forensics

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.

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. 3.00 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.

Area: Social and Behavioral Sciences.
EN.650.424. Network Security. 3.00 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. [Systems] Co-listed with EN.600.424.
Prerequisites: 600.226 and (600.344 or 600.444) or permission; 600.120 (or equivalent) recommended.
Instructor(s): A. Mishra
Area: Engineering, Quantitative and Mathematical Sciences.

EN.650.431. Ethical Hacking. 3.00 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.650.433. Embedded Computer Systems. 3.00 Credits.
This course provides an understanding of differences in network-based computers, program mobility, current intrusion protection technologies and exploitation methods along with material relating to computer hacking and vulnerability assessment. Department Majors Only. Course taught On-line.
Instructor(s): G. Kalb
Area: Engineering.

EN.650.445. Practical Cryptographic Systems. 3.00 Credits.
This semester long course will teach skill of how cryptographic systems work and fail - as part of a complete hardware and software system. The skills will be taught by examples i.e., by studying and identifying flows in widely deployed crypto systems. We will place a particular emphasis on the failure of security by obscurity and the feasibility of reverse-engineering undocumented crypto systems. Co-listed with EN.600.454.
Instructor(s): M. Green.

EN.650.457. Computer Forensics. 3.00 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.650.458. Introduction to Cryptography. 3.00 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.650.460. Software Vulnerability Analysis. 3.00 Credits.
Competent execution of security assessments on modern software systems requires extensive knowledge in the reverse engineering and vulnerability analysis technical domains. This course examines software vulnerability analysis relevant theory and its application within security assessments in detail. Key topics include historical vulnerabilities, their corresponding exploits, and any associated preventative measures. Fundamental tools and techniques for performing software reverse engineering and vulnerability analysis are covered extensively. The format of this course includes lectures and hands-on assignments. Students will complete and demonstrate a project as part of the course.
Instructor(s): R. Johnston
Area: Engineering.

EN.650.461. Cloud Computing Security. 3.00 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.650.471. Cryptography & Coding. 4.00 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): D. Fishkind
Area: Engineering, Quantitative and Mathematical Sciences.
EN.650.472. Security Analytics. 3.00 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
Area: Engineering, Natural Sciences.

EN.650.621. Critical Infrastructure Protection. 3.00 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 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. 3.00 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.650.424 or permission of the instructor.
Instructor(s): S. Nielson
Area: Engineering.

EN.650.640. Moral & Legal Foundations of Privacy. 3.00 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.650.652. Healthcare Security Management. 3.00 Credits.
The course will address information security in the public health and medical fields, with special emphasis on clinical care, research and the role of the academic medical center. In many respects, the course builds on EN.650.651 Health Information, Privacy, Law and Policy’s treatment of privacy and how such privacy is protected in the health and medical arena, including but not limited to HIPAA. Open to MSSI students or Permission required.
Instructor(s): D. Lacey.

EN.650.653. Financial Issues in Managing a Secure Operation. 3.00 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. 3.00 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. 3.00 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.650.657. Advanced Computer Forensics. 3.00 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.650.661. Human Factors in Information Security. 3.00 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.650.666. Advanced Topics in Software Security. 3.00 Credits.
Topics vary but mainly focus on recent advances in exploitation techniques and defenses for software including software running on embedded systems software, software running on nontraditional devices such as microcontrollers in PCs. Recommended Course Background: EN.600.460 or EN.650.442 or permission of instructor
Instructor(s): S. Checkoway

EN.650.736. Information Security Projects. 1.00 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.
Instructor(s): A. Dahbura; X. Li

EN.650.737. Information Security Projects. 1.00 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.
Instructor(s): A. Dahbura; X. Li

EN.650.738. Information Security Projects. 1.00 - 4.00 Credits.
Instructor(s): G. Masson.

EN.650.739. Special Network Security Projects. 1.00 - 4.00 Credits.
Instructor(s): Staff.

EN.650.840. Information Security Independent Study. 3.00 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. 1.00 - 4.00 Credits.
Instructor(s): G. Masson.

Cross Listed Courses

Computer Science

EN.600.424. Network Security. 3.00 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. [Systems] Recommended.
Course Background: EN.600.120 (or equivalent)
Prerequisites: EN.600.226 AND ( EN.600.344 OR EN.600.444 ) or permission
Instructor(s): S. Nielson
Area: Engineering.

EN.600.433. Computer Systems. 3.00 Credits.
Graduate version of 600.333. Students may receive credit for 600.333 or 600.433, but not both. [Systems] Recommended.
Instructor(s): P. Froehlich
Area: Engineering.

EN.600.442. Modern Cryptography. 3.00 Credits.
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] Recommended Course Background: EN.600.363/463, EN.600.271/471 and EN.550.171 or equiv.
Instructor(s): A. Jain
Area: Engineering, Quantitative and Mathematical Sciences.

EN.600.443. Security & Privacy in Computing. 3.00 Credits.
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.
Instructor(s): A. Rubin
Area: Engineering.

Information Security Institute
EN.600.450. Network Embedded Systems & Sensor Networks. 3.00 Credits.
This course is an introduction to fundamental concepts of networked embedded systems and wireless sensor networks. It is intended for juniors, seniors and first year graduate students in Computer Science and other engineering majors with the prerequisite background. Covered topics include: embedded systems programming concepts, low power and power aware design, radio technologies, communication protocols for ubiquitous computing systems, and some of the mathematical foundation of sensor behavior. Laboratory work consists of a set of programming assignments that consider a set of the issues described in class. Recommended Course Background: EN.600.226, EN.600.120, and EN.600.344/EN.600.444
Instructor(s): M. Chang
Area: Engineering.

EN.600.451. Introduction to Bitcoin and Other Crypto-currencies. 3.00 Credits.
This course covers the basics of Bitcoin and the underlying technologies driving it. The course is intended for students interested in the cryptographic techniques devised to make digital currencies and payment systems secure. Topics include Bitcoin transactions, the blockchain, mining, and decentralized consensus. The course will include a brief introduction to public-key cryptography, digital signatures, hash functions, proof of work/space, multisignatures, and elliptic curve cryptography. The course concludes with an overview of the Bitcoin scripting language and Bitcoin 2.0 platforms. [Systems] Recommended Course Background: EN.600.344/444 (Computer Networks) and EN.550.171 (Discrete Math)
Prerequisites: EN.600.226
Instructor(s): G. Ateniese
Area: Engineering.

EN.600.460. Software Vulnerability Analysis. 3.00 Credits.
This course will examine vulnerabilities in C source, stack overflows, writing shell code, etc. Also, vulnerabilities in web applications: SQL Injection, cookies, as well as vulnerabilities in C binary fuzzing, and exploit development without source among other topics. Co-listed with EN.650.460
Instructor(s): S. Checkoway
Area: Engineering.

EN.600.463. Algorithms I. 3.00 Credits.
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] Students may receive credit for EN.600.363 or EN.600.463, but not both.
Instructor(s): V. Braverman
Area: Engineering, Quantitative and Mathematical Sciences.

EN.600.471. Theory of Computation. 3.00 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.600.271 and EN.600.471, unless one is for an undergrad degree and the other for grad. [Analysis] Recommended Course Background: EN.550.171 or instructor permission.
Instructor(s): X. Li
Area: Engineering, Quantitative and Mathematical Sciences.

EN.600.642. Advanced Topics in Cryptography. 3.00 Credits.
This course will focus on advanced cryptographic topics with an emphasis on open research problems and student presentations.
Instructor(s): A. Jain.

EN.600.643. Advanced Topics in Computer Security. 3.00 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.