Information Security Institute

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 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 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 PC workstations running Windows, 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. Its full-time, part-time, or adjunct faculty deliver these courses at multiple sites spanning the Homewood campus in northern Baltimore, the medical and health facilities in eastern Baltimore, the part-time graduate program operations at APL and the Montgomery County Campus, and the SAIS and KSAS facilities in Washington, D.C.

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 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 U.S. citizens and U.S. permanent residents 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:

<table>
<thead>
<tr>
<th>GRE General Test</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verbal</td>
</tr>
<tr>
<td>Quantitative</td>
</tr>
<tr>
<td>Analytical</td>
</tr>
<tr>
<td>TOEFL Internet based</td>
</tr>
<tr>
<td>IELTS</td>
</tr>
<tr>
<td>153 (62%)</td>
</tr>
<tr>
<td>160 (84%)</td>
</tr>
<tr>
<td>3.5</td>
</tr>
<tr>
<td>79</td>
</tr>
<tr>
<td>7.0</td>
</tr>
</tbody>
</table>

• 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 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.

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.

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.

All courses supporting the M.S.S.I. are categorized as one of four types:

1. Technology;
2. Policy;
3. Health;

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.
Each course is further classified into core, elective or foundational category. All M.S.S.I. course programs must satisfy the following distribution requirements:

- A minimum of four courses in the Technology category: at least three Core Technology courses and at least one core technology course in Cryptography.
- A minimum of four core courses in the Policy/Health/Management categories: at least one course from each category of Policy, Health and Management.
- Two additional courses from core or elective technology courses; or when deemed appropriate relative to a student's background, interests, and goals and with the prior approval by the faculty advisor, from elective Policy/Health/Management courses or (at most one) from foundational technology courses.

Project Requirement

The students register for EN.650.736/EN.650.737/EN.650.738 for the capstone project. The /EN.650.737/ are not counted toward the ten-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.

Course Requirement Details

- All courses toward the degree requirement must be 400-level or above.
- The overall grade point average of the courses counted toward the coursework requirements must be 3.00 or higher.
- 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 EN.650.736/ and independent study courses.
- At most two courses with grade less than B- may be counted toward the course work requirements. No courses with grade less than C- may be counted.
- 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.
- Courses not found on the area-specific lists can be used to meet area requirements with written approval from the student’s advisor and one additional faculty member.
- A grade of D or F results in probation. A second D or F is cause for being dropped from the program.

JHUISI Courses

Core Technology Courses

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Name</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>EN.600.442</td>
<td>Modern Cryptography</td>
<td>3</td>
</tr>
<tr>
<td>EN.600.443</td>
<td>Security &amp; Privacy in Computing</td>
<td>3</td>
</tr>
<tr>
<td>EN.600.643</td>
<td>Advanced Topics in Computer Security</td>
<td></td>
</tr>
<tr>
<td>EN.650.424</td>
<td>Network Security</td>
<td>3</td>
</tr>
<tr>
<td>EN.650.445</td>
<td>Practical Cryptographic Systems</td>
<td>3</td>
</tr>
<tr>
<td>EN.650.457</td>
<td>Computer Forensics</td>
<td>3</td>
</tr>
<tr>
<td>EN.650.458</td>
<td>Introduction to Cryptography</td>
<td>3</td>
</tr>
<tr>
<td>EN.650.460</td>
<td>Software Vulnerability Analysis</td>
<td>3</td>
</tr>
<tr>
<td>EN.650.471</td>
<td>Cryptography &amp; Coding</td>
<td>4</td>
</tr>
<tr>
<td>EN.650.633</td>
<td>Computer Security Architectures</td>
<td></td>
</tr>
<tr>
<td>EN.650.654</td>
<td>Computer Intrusion Detection</td>
<td></td>
</tr>
<tr>
<td>EN.650.657</td>
<td>Advanced Computer Forensics</td>
<td></td>
</tr>
<tr>
<td>EN.650.668</td>
<td>Advanced Topics in Software Security</td>
<td></td>
</tr>
</tbody>
</table>

Elective Technology Courses

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Name</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>EN.600.444</td>
<td>Computer Networks</td>
<td>3</td>
</tr>
<tr>
<td>EN.600.471</td>
<td>Theory of Computation</td>
<td>3</td>
</tr>
<tr>
<td>EN.650.433</td>
<td>Embedded Computer Systems</td>
<td>3</td>
</tr>
<tr>
<td>EN.650.621</td>
<td>Critical Infrastructure Protection</td>
<td></td>
</tr>
<tr>
<td>EN.650.736</td>
<td>Information Security Projects</td>
<td>0</td>
</tr>
<tr>
<td>&amp; EN.650.737</td>
<td>Information Security Projects</td>
<td></td>
</tr>
<tr>
<td>&amp; EN.650.738</td>
<td>Information Security Projects</td>
<td></td>
</tr>
<tr>
<td>EN.650.840</td>
<td>Information Security Independent Study</td>
<td></td>
</tr>
</tbody>
</table>

Core Policy Courses

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Name</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>EN.650.414</td>
<td>Rights in Digital Age</td>
<td>3</td>
</tr>
<tr>
<td>EN.650.640</td>
<td>Moral &amp; Legal Foundations of Privacy</td>
<td></td>
</tr>
</tbody>
</table>

Core Health Courses

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Name</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>EN.650.652</td>
<td>Healthcare Security Management</td>
<td></td>
</tr>
<tr>
<td>AS.280.340</td>
<td>Fundamentals of Health Policy &amp; Management</td>
<td>3</td>
</tr>
<tr>
<td>School of Medicine courses ME.600.701, ME.600.702, and ME.600.705 may be taken to fulfill core health course requirements. Bloomberg School of Public Health PH.306.655 may be used to fulfill the core health course requirement.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Core Management Courses

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Name</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>EN.650.653</td>
<td>Financial Issues in Managing a Secure Operation</td>
<td></td>
</tr>
<tr>
<td>EN.650.655</td>
<td>Implementing Effective Information Security Projects</td>
<td></td>
</tr>
</tbody>
</table>
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.*

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>PH.300.651</td>
<td>Introduction to U.S. Healthcare System Policy</td>
</tr>
<tr>
<td>BE.320.435</td>
<td>E-Commerce Security</td>
</tr>
<tr>
<td>AS.406.661</td>
<td>Technology of Mass Destruction</td>
</tr>
<tr>
<td>AS.406.665</td>
<td>Art and Practice of Intelligence</td>
</tr>
<tr>
<td>AS.406.666</td>
<td>Contemporary Terrorism and the American Response</td>
</tr>
<tr>
<td>AS.406.668</td>
<td>Intelligence and Counter-Terrorism</td>
</tr>
</tbody>
</table>

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

Foundational Courses

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>EN.600.120</td>
<td>Intermediate Programming</td>
<td>4</td>
</tr>
<tr>
<td>EN.600.226</td>
<td>Data Structures</td>
<td>4</td>
</tr>
<tr>
<td>EN.600.415</td>
<td>Databases</td>
<td>3</td>
</tr>
<tr>
<td>EN.600.418</td>
<td>Operating Systems</td>
<td>3</td>
</tr>
<tr>
<td>EN.600.421</td>
<td>Object Oriented Software Engineering</td>
<td>3</td>
</tr>
<tr>
<td>EN.600.433</td>
<td>Computer Systems</td>
<td>3</td>
</tr>
<tr>
<td>EN.600.463</td>
<td>Algorithms I</td>
<td>3</td>
</tr>
</tbody>
</table>

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 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 (C.N.S.S.) in the Krieger School of Arts and Sciences is now being offered. The C.N.S.S. requires completion of five core courses. Two designated courses can be double counted for the M.S.S.I. and the C.N.S.S. 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/ people

Faculty

Interm Executive Director
Anton Dahbura
Information Security Institute.

Program Director
Xiangyang Li
Master of Science in Security Informatics.

Professors

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

Aviel Rubin
Professor (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 Professor
Giuseppe Ateniese
Computer Science: applied cryptology, cryptology and network security, security and privacy in computing, applied cryptography and network security, DNSSEC and medical information privacy protection.

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

**Assistant Research Professor**

Stephen Checkoway  
Computer Science: systems security, voting security, post-election auditing.

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

**Lecturers**

William Agresti  
Professor and Associate Dean for Professional Programs (Carey Business School): system design and development, information systems architecture, and IT integration for business, software engineering, IT measurement and knowledge management.

Kevin Fairbanks  
Assistant Professor (U.S. Naval Academy): digital forensics.

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

George Kalb  
Information Security Institute; Adjunct Professor, Lecturer, Part-time Programs in Engineering and Applied Science: embedded computer systems—vulnerabilities, intrusions and protection mechanisms, embedded systems security, software engineering.

Michael Kociemba  
Instructor (Carey Business School): information security, management, and infrastructure protection.

Darren Lacey, J.D.  
Chief Information Security Officer for Johns Hopkins University.

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

Lanier Watkins  

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

### Courses

**EN.650.412. Java Security. 3 Credits.**  
This course provides a comprehensive coverage of the security aspects of the Java platform. Java’s security model and the VM and language features that support security are covered. Java APIs relevant to development of secure software are discussed. The course concentrates on the practical aspects of using these APIs. Use of the Java Cryptography APIs is addressed and material on security in J2EE (Java 2 Enterprise Edition) is presented. Topics covered include the java.security.* packages, the Java Cryptography Architecture and Java Cryptography Extension (JCA and JCE), Java Secure Sockets Extension (JSSE), Java Authentication and Authorization Service (JAAS), Java Generic Security Services (Java GSS-API), and the Java Certification Path API.  
Instructor(s): E. Ceesay  
Area: Engineering.

**EN.650.414. 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 into Hodson Hall Room 213.)  
Instructor(s): M. Jacobs  
Area: Social and Behavioral Sciences.

**EN.650.424. 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. [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.650.432. Law & Policy Informations Assurance. 3 Credits.**  
Instructor(s): G. Masson; M. Lavine  
Area: Engineering.
EN.650.433. Embedded Computer Systems. 3 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 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 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): K. Fairbanks
Area: Engineering.

EN.650.458. 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.
Instructor(s): X. Li
Area: Engineering.

EN.650.460. Software Vulnerability Analysis. 3 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. Students should have experience in C++ Programming.
Instructor(s): S. Checkoway
Area: Engineering.

EN.650.470. Basics of Applied Cryptography and Network Security. 3 Credits.
This course will cover some key aspects of applied cryptography. Topics include algorithms for encryption and decryption using symmetric key and public key techniques, design and analysis of block and stream ciphers, pseudo-random number generation, hash functions and their uses, message authentication codes, authentication protocols, key establishment, key management, digital signatures and secret sharing.

EN.650.471. Cryptography & Coding. 4 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.650.480. Intrusion Detection Systems. 3 Credits.
This course will relate to laboratory assignments and research exercises. Department Majors Only. Course taught On-line.

EN.650.490. Network Security. 3 Credits.
This course will study information security and assurance methodologies 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.650.500. Fundamentals of Cybersecurity. 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 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): A. Siegel.

EN.650.621. Critical Infrastructure Protection.
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): M. Green.

EN.650.630. Moral and Legal Foundations of Privacy.
This course explores the ethical and legal underpinnings of privacy. Inquiries into the values that underline the right; constitutional and common law foundations; balancing privacy against other rights and interests. Core Policy course for MSSI degree
Instructor(s): A. Siegel.

EN.650.632. Law & Policy of Info Assurance.
This course introduces information assurance as a response to changes in technology, asymmetric threats and computer crime. It traces the concepts through civilian applications as OMB and NIST standards as well as private sector issues related to privacy, contingency response, and reliable infrastructures. It examines these concepts from a risk assessment and standards based approach central to government planning and the private sector.

This course will study information security and assurance methodologies from the perspective of implementation and performance on reduced instruction set architectures. All 1st year MSSI students entering after Fall '08 will be required to take this course.
Instructor(s): G. Masson.

EN.650.640. Moral & Legal Foundations of Privacy.
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): M. Jacobs; W. Sauers.
EN.650.650. Special Topics in Security and Privacy of Medical Information.
This course will cover topics in security and privacy of medical information. Topics will include security and access control with respect to medical records (EPR, PHR), securing communication standards (HL7, DICOM), recent attacks on patient monitoring systems, security architectures for portable patient records, break the glass systems, privacy, anonymity and medical identity theft. Students are expected to enter this class with basic knowledge in computers and networking and should be comfortable programming.
Instructor(s): S. Garera
Area: Quantitative and Mathematical Sciences.

EN.650.651. Health Info Privacy Law.
Core health course for MSSI Course meets Oct. 23-December 22 This course pertains to issues relating to protecting health information privacy in the modern era. Theoretical and ethical discussions underlying health information privacy are covered. The primary focus of the course is to provide a modern context through which privacy protections are debated, constructed, implemented, and enforced. The course attempts to instruct students on the legal, policy, and practical issues surrounding the protection of health information privacy. The major federal and state privacy laws and policies and how these laws and policies are implemented in the public and private sectors is considered.

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.

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): W. Agresti.

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.

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.

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.

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.

Topics vary but mainly focus on recent advances in exploitation techniques and defenses for software including software running on embedded systems software, browsers, and nontraditional devices such as microcontrollers in PCs. Recommended Course Background: EN.600.460 or EN.650.442 or permission of instructor.
EN.650.668. Advanced Topics in Software Security. 3 Credits.
Topics vary but mainly focus on recent advances in exploitation techniques and defenses for software including software running on embedded systems software, browsers, and 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. 6 Credits.
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 MSSI student that begins enrollment in Fall 2013 or later. Open to MSSI students. Perm Req’d for non-MSSI students.
Instructor(s): A. Dahbura; X. Li.

EN.650.737. Information Security Projects. 6 Credits.
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 course for any MSSI student that begins enrollment in Fall 2013 or later. Open to MSSI students. Perm Req’d for non-MSSI students.
Instructor(s): A. Dahbura; X. Li.

EN.650.738. Information Security Projects. 3 Credits.
Instructor(s): G. Masson.

EN.650.739. Special Network Security Projects. 3 Credits.
Instructor(s): Staff.

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.
Instructor(s): G. Masson.

EN.650.890. Information Security Research. 3 Credits.
Instructor(s): G. Masson.

Cross Listed Courses

Computer Science

EN.600.412. Security and Privacy in Cloud Computing. 1 Credit.
This course focuses on the security and privacy issues in Cloud Computing systems. While the cloud computing paradigm gains more popularity, there are many issues related to confidentiality, integrity, and availability of data and computations involving a cloud. In this course, we examine cloud computing models, look into the threat model and security issues related to data and computation outsourcing, and explore practical applications of secure cloud computing. Students should have some background in network and/or data security.
Instructor(s): R. Hasan
Area: Engineering.

EN.600.415. Databases. 3 Credits.
Graduate level version of EN.600.315. Students may receive credit for EN.600.315 or EN.600.415, but not both. Recommended Course Background: EN.600.226
Instructor(s): D. Yarowsky
Area: Engineering.

EN.600.421. Object Oriented Software Engineering. 3 Credits.
Graduate level version of EN.600.321. Students may receive credit for EN.600.321 or EN.600.421, but not both. Recommended Course Background: EN.600.226 and EN.600.120
Instructor(s): S. Smith
Area: Engineering.

EN.600.424. 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. [Systems] EN.600.120 (or equivalent) recommended.
Prerequisites: 600.226 and (600.344 or 600.444) or permission; 600.120 (or equivalent) recommended.
Instructor(s): Staff
Area: Engineering.

EN.600.433. Computer Systems. 3 Credits.
Graduate version of 600.333. Students may receive credit for 600.333 or 600.433, but not both. [Systems]
Instructor(s): P. Froehlich
Area: Engineering.

EN.600.442. Modern Cryptography. 3 Credits.
This course focuses on cryptographic algorithms, formal definitions, hardness assumptions, and proofs of security. Topics include number-theoretic problems, pseudo-randomness, block and stream ciphers, public-key cryptography, message authentication codes, and digital signatures. Recommended Course Background: EN.600.226 and a 300-level or above systems course; EN.600.271/EN.600.471 and EN.550.171 or equivalent.
Instructor(s): C. Pappacena
Area: Engineering, Quantitative and Mathematical Sciences.
EN.600.443. Security & Privacy in Computing. 3 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]
Prerequisite: A basic course in operating systems and networking, or permission of instructor.
Instructor(s): A. Rubin
Area: Engineering.

EN.600.444. Computer Networks. 3 Credits.
This course considers intersystem communications issues. Topics covered include layered network architectures; the OSI model; bandwidth, data rates, modems, multiplexing, error detection/ correction; switching; queuing models, circuit switching, packet switching; performance analysis of protocols, local area networks; and congestion control. Recommended Course Background: EN.600.333 or EN.600.433 or permission. Students can only receive credit for EN.600.344 or EN.600.444, not both.
Instructor(s): A. Terzis
Area: Engineering.

EN.600.450. Network Embedded Systems & Sensor Networks. 3 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.600.463. Algorithms I. 3 Credits.
Graduate version of EN.600.363. Students may receive credit for EN.600.363 or EN.600.463, but not both. Recommended Course Background: EN.600.226 and EN.550.171 or instructor permission required.
Instructor(s): V. Braverman
Area: Engineering, Quantitative and Mathematical Sciences.

EN.600.471. Theory of Computation. 3 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. Recommended Course Background: EN.550.171 or instructor permission.
Prerequisites: Students may not take both 600.271 and 600.471, unless one is for an undergrad degree and the other for grad. Prerequisite: 550.171 or permission.
Instructor(s): V. Variyam
Area: Engineering, Quantitative and Mathematical Sciences.