Knowledge of key lengths, factoring methods, and cryptanalytic techniques make it possible to estimate (in the absence of a real theory of cipher design) the "work factor" required to break a particular cipher...

High quality ciphers and protocols are important tools, but by themselves make poor substitutes for realistic, critical thinking about what is actually being protected and how various defenses might fail (attackers, after all, rarely restrict themselves to the clean, well-defined threat models of the academic world).

— Matt Blaze

Security is technology. Without understanding mathematics and computer science, security will appear more magic than science. Security is technology - it is also a matter of suitable user interfaces, organizational priorities, economic factors, and legal compliance. The strengths of the targeted but personalized approach in Security Informatics include numerous connections to and collaborative efforts with research groups representing a wide range of security applications areas and complementary sciences. This document defines a program of study that makes our students highly competent in the multidisciplinary world of computer security.

Security Informatics is a curriculum of instruction that is centered on the protocols and practices of security; both the technology and the context. Security Informatics includes the core subjects that define computer security: mathematics, protocol analysis and secure system administration. Security Informatics also includes the span of material covered by informatics. Security Informatics is security integrated with human interaction, social engineering, and information technology rather than security is isolated from the large economic and social milieu.
Goals and Vision

Security Informatics builds upon strong theoretical foundations to construct practical solutions for the intertwined challenges of security and privacy. Security Informatics addresses both immediate problems of today, such as phishing, and emerging research problems, including privacy in ubiquitous computing environments.

Informatics is the evaluation and design of information technology in social, organizational, and economic contexts. Security Informatics is the study and design of security technologies within these contexts. Security Informatics integrates frameworks and heuristics from the social sciences, design principles from HCI, and incentive-aware protocols from secure systems design.

Security Informatics includes a cross-disciplinary networks of researchers, practitioners, and educators.

Some of the aspects of our vision at the School of Informatics are:
- Cryptography
- Protocol Analysis
- Engineering Ethics
- Social Engineering
- Formal Methods
- Secure Reliable Code
- Secure Network Operation and Management
- Economics of Security

SI

Security Informatics is the branch of informatics that studies and supports the design, evaluation, and implementation of technologies that enable control over information.

This program is built upon four core components. First there is the understanding of networks and systems. Security is taught with a unique focus on social and organizational informatics of security. Second is the networking core, comprising basic required networking information. Third is the concentration on an academic topic or applied question. Finally, there is a professional element that builds on the three previous areas of knowledge in a comprehensive applied manner.

In courses and laboratories, challenges to the students will be of a practical nature built upon the theoretical foundation. Meeting these challenges requires an understanding of the network to identify the problem, an understanding of security to evaluate possible solutions, and an understanding of the context to effectively implement the response. Challenges will include responses to cyber-attacks, user interactions (including social engineering), and malware distribution or defense.
We strongly encourage students to seek internships as soon as possible, to obtain that professional development element. We encourage internships, either for research or professional development, over the summer. Career Services will assist you in matching your skills with internship options. We also encourage internships during the second academic year as explicitly for professional development. The School of Informatics and Computing has an excellent relationship with UITS, and there are many local organizations that could use your help. Failure to obtain an internship will not result in failure to obtain a degree, as there are applied course options as well. Internships will be approved for any student in good standing in the program.

Program Goals

Some of the core goals for the Security Informatics master’s degree program include:

- Develop the mathematical foundation required for security informatics.
- Become well-versed in the recognition and understanding of seminal work – research, innovation and literature – that constitutes the core of security engineering.
- Acquire the technical skills to make effective use of current and emerging design applications.
- Understand the socioeconomic ramifications of security and privacy-enhancing technologies.
- Become proficient with practical skills that will be necessary in the daily business of security engineering.
- Cultivate an understanding of security in practice and how it is functions in organizations, as well as in systems and network administration.
- Develop an interdisciplinary understanding that enables design and implementation that can address social engineering and economics of security.

The Security Informatics Master’s Program

Structure

MSSI is simultaneously more tightly focused and more interdisciplinary than comparable computer science programs. The program is more focused on security, for example it requires the study cryptography and protocol analysis, as opposed to a larger focus that includes other areas of computer science. Computer science is more focused on the laboratory programming experience, while the MSSI has a strong internship element. As is appropriate the programs are strongly woven together at Indiana, with MSSI students expected to take three courses in networking and systems in Computer Science, and Informatics security courses often heavily populated.
with students majoring in computer and cognitive science. The MSSI is more interdisciplinary in that include concentrations.

The Masters of Science Degree in Security Informatics is structured as follows, with a requirement for 36 course hours. Individual program choices will vary.

The Masters of Science Degree in Security Informatics is structured as follows, with a requirement for 36 course hours. Individual program choices will vary. The program can be understood as consisting of four elements:
1. Security foundations,
2. Professional practice,
3. Computing networks,
4. Concentrations in an area of interest.

<table>
<thead>
<tr>
<th>Courses</th>
<th>Usual Session</th>
<th>Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internship, professional, preparatory</td>
<td>All</td>
<td>6</td>
</tr>
<tr>
<td>INFO I533 System &amp; Protocol Security</td>
<td>Fall</td>
<td>3</td>
</tr>
<tr>
<td>INFO I520 Security &amp; Software Assurance</td>
<td>Spring</td>
<td>3</td>
</tr>
<tr>
<td>INFO I525 Economics of Security</td>
<td>Fall</td>
<td>3</td>
</tr>
<tr>
<td>INFO I536 Mathematics of Cybersecurity</td>
<td>Fall</td>
<td>3</td>
</tr>
<tr>
<td>Computer Networking electives</td>
<td>All</td>
<td>9-12</td>
</tr>
<tr>
<td>Electives or Concentration</td>
<td>All</td>
<td>6-9</td>
</tr>
</tbody>
</table>

**Total Course Hours 36**

The program can be understood as consisting of four parallel tracks:
1. security foundations track,
2. professional practice track,
3. networking track, and
4. informatics and beyond track.

The security foundation track is focused on the core technologies of security and includes a minimum of two courses, and a normal expectation of four courses. For many students one elective will be used to ensure the mathematical foundation for these courses or the programming foundation. (Applied mathematics or practical programming courses can be counted for degree credit as professional practice.) Together these courses give you a solid understanding of the field of security.

The professional practice track normally consists of up to six hours of internship credit. Twenty hours a week for a semester of internship can provide up to the three course credit hours for the degree. MSSI students
are highly sought as paid interns; and it is not unusual for a summer internship courses to provide both income and six hours of degree credit. Foundational programming or mathematics courses or CS courses with an A work study assignment (where you can practice network administration skills in as part of your employment) can also be taken for professional credit. Professional practice may be augmented by work for credit in the multiple security centers at Indiana University, including University Information Technology Services (UITS), Research and Educational Networking Information Analysis and Sharing Center (RENSAC), Pervasive Technologies Laboratory (PTL), or the Global NOC.

With approval of appropriate professional staff (i.e., the SOIC Graduate Office) and faculty (i.e., the supervising faculty), an independent study can be substituted for the two professional courses. An independent study is a semester spent under the close supervision of a faculty member engaged in research of common interest. An independent study allows a student to focus on a specific area. Independent studies may either be oriented towards professional practice or focused on research. This option is particularly appropriate for those who have previous network administration experience and who are considering a doctoral career.

Any student may have as many internship or independent study hours as is feasible for that students’ schedule, and take as many practice or preparatory classes as is appropriate. In any case, no more than six total professional practice hours from any and all sources can be counted for degree credit.

The networking track is tightly integrated with computer science instruction, also within the School of Informatics and Computing. There is a menu of courses, from basic to specialized, that can be used to develop an understanding of networks or concentrate in a specific arena. Networking courses may also include offerings in Informatics; for example, pervasive systems, robotics, or special topics as appropriate.

The fourth track, informatics and beyond, refers to the broader field of informatics. It consists of courses that form an intellectually coherent concentration, that compliments the interdisciplinarity of security informatics.

The concentration model allows students the freedom to customize their education to meet their personal interests and needs. At least two electives must explore a view of a single method, question, point of view, discipline, or domain. Choosing an appropriate concentration early in the program will enable a better experience.
Example Courses of Study

Students entering the MSSI may be joining the program from a computer science or social science background. Students coming from computer science often require a semester of probability before completing the core courses. Students from the liberal arts often require exposure to computer science. The two following courses of study present two different paths for people entering with different strengths and interest. The first assumes an undergraduate an undergraduate statistics and probability course as well as programming and network administration experience. This is unusual.

The basic introduction to probability can be completed online. Recommended, free courses may be identified in admissions letters, or will be recommended by the faculty. The foundational mathematics of cybersecurity assumes this grounding, you will not be able to understand the material without having this grounding coming into the course.

The second assumes model is for students who enter the program without a previous knowledge of and understanding of programming. By focusing a year on the basic programming and system administrative skills, and obtaining the summer internship, it is common to complete the program in two years. The skills from your undergraduate work strongly enhance the desirability of our students for employers. While traditional technologists see a distance between security and the social sciences, security technologies are used by people, in organizations, under economic constraints. The understanding of the context with the technology makes our graduates unique, and the insights you will learn bot highly applicable and valuable.

<table>
<thead>
<tr>
<th></th>
<th>1st semester</th>
<th>2nd semester</th>
<th>Summer</th>
<th>3rd semester</th>
<th>4th semester</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Security Foundations</strong></td>
<td>INFO 525 Economics of Security</td>
<td>Programming (3)</td>
<td>Networking (3)</td>
<td>INFO 520 Network Security</td>
<td>INFO 533 Information Assurance</td>
</tr>
<tr>
<td><strong>Professional Practice</strong></td>
<td>Programming or Network Admin (3)</td>
<td>Professional Internship Online Probability Course</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Networking and Electives</strong></td>
<td></td>
<td>Networking (3)</td>
<td>Networking (6)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Concentration</strong></td>
<td>Concentration Course (6)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Example 1: Computer Science Background
Notice that this schedule assumes that you either have had a course in probability or study the material before arriving. There are free online probability courses available. Completing this material before arriving will enable you to take INFO 536 in the first semester; however, it is not possible to complete probability concurrently with probability as all the requisite knowledge of probability must be mastered by the second course lecture.

<table>
<thead>
<tr>
<th>1st semester</th>
<th>2nd semester</th>
<th>Summer</th>
<th>3rd semester</th>
<th>4th semester</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Foundations</td>
<td>INFO 525 Economics of Security&lt;br&gt;INFO 536 Foundational Mathematics of Cybersecurity</td>
<td></td>
<td>INFO 520 Network Security</td>
<td>INFO 533 Information Assurance</td>
</tr>
<tr>
<td>Professional Practice</td>
<td>Programming (3)&lt;br&gt;Programming or Network Admin (3)</td>
<td>Professional Internship</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Networking and Electives</td>
<td></td>
<td>Networking (6)</td>
<td>Networking (3)</td>
<td></td>
</tr>
<tr>
<td>Concentration</td>
<td>Concentration Course (6)</td>
<td></td>
<td>Networking (3)</td>
<td></td>
</tr>
</tbody>
</table>

**Example 2: Social Science Background**

If you are arriving with a background in social science, you are more likely to have had formal training in probability than in the computing sciences. As it is not possible to complete probability concurrently with INFO 536, we still recommend that you review the material before arriving to ensure a match of your knowledge base and the requirements.

**Courses**

The following describes the nature of each required course:

1. **INFO 1525 Organizational Informatics and Economics of Security**
   Organizational processes embed implicit and explicit decisions and information control. Security technologies and implementations make explicit organizational choices that determine individual autonomy within an organization. Security implementations allocate risk, determine authority over processes, make explicit relationships in overlapping hierarchies, and determine trust extended to organizational participants. This is a graduate case-based course that will examine implementations of security in organizations.

2. **INFO 1520 Security for Networked Systems**
   Elementary cryptography, beginning of a review and quickly moving into depth. Authentication includes password, challenge & response, Needham
Schoeder protocol and other identification protocols. Access control (ACL) and RBAC. Multilevel security (BLP model). Software security, buffer overflows, Java security model. Usually do not have time to discuss denial of service and anonymity channels (e.g., mix networks). Memory layout. Stack injection, Buffer growth.

3. INFO 1533 System & Protocol Security & Information Assurance
Basic concepts of security reviewed. Threat and adversary modeling; attacked objective and currently using MS threat modeling may use Gary McGraw’s threat modeling. Do the theory in class and then the lab in practice. ACL theory and implementation, firewalls and port blocking, applied crypto, principle of least privilege, auditing, logs, data retention.

4. INFO 536 Foundational Mathematics of Cybersecurity
Cryptography is the art of hiding information. Practicing that art requires a specific if eclectic mathematical palette. This course is designed to provide an introduction to that set of mathematics that is required for INFO 538 and INFO 539. This is not a general topical

Seminar Series
Master’s degree students have the opportunity to attend seminars by distinguished faculty and insightful practitioners with the purpose to broaden and stimulate your intellectual development. The School organizes regular Colloquia with invited speakers. There is an Honors Seminar Series that will be open for all students, and there is also the Security Seminars. Attendance is required for a number of the seminars. Failure to attend seminars can result in failure to obtain a degree.

Need to Know
As you tailor your electives for your program, consider what a highly effective security practitioner needs to know:

Technical Skills
• Ability to read and understand a cryptographic protocol.
• Appreciation of types and categories of bugs, attacks, and patches.
• Understanding computer science concepts and how engineers solve problems.
• Mathematics and research methods (particularly if you plan to obtain

Foundational Security Literature
• Familiarity with the foundational literature of cryptography and secure systems
• Understanding of the core concepts of security protocols.

Current Security Literature
• Ability to read articles and protocols critically.
• Ability to read research papers, including statistical analyses.
• Reading journals on a regular basis, tracking developments.
• Ability to track and research attacks and defenses.

Security Handbook: ’14 Class
Informatics School of Informatics & Computing
System Administration
• Ability to install, upgrade, manage and secure web servers and other applications.
• Ability to examine a log and explain its implications.
• Minimum level of expertise in configuration of Linux and Windows servers.
• Familiarity with fundamental concepts of networks, interactions, etc.

Team Collaboration
• Functioning effectively as a team member and a team leader.
• Consulting skills.
• Professional skills.

Presentation Skills
• Preparation of supporting documentation.
• Speaking.
• Functioning effectively in a professional environment.

Standards & Reviews
Each first year students may receive a review from the faculty in spring of the first year. The purpose of this review letter is to provide guidance and feedback. For example, every admitted student receives some funding to travel to an event. If you have not taken advantage of this opportunity will be reminded of the purpose of the funds and the need to network while enrolled in studies. These also serve to identify any difficulties (should these exist).

The standards of these reviews and your expectation of students follow. The graduate student evaluation has three components: classroom performance, practice, and professional advancement. There is a minimal performance standard in the classroom, which is common to all students. There is a professional practice performance standard, which is based on the area of practice. There is a professional component, which has a small variance, based on the area of concentration.

After the first year, you will be expected to complete a summary report. Ideally, summary report will be completed by January 31 of each year. After the first year, the report will inform the evaluation of your performance.

The minimal performance standard in the classroom is that you must maintain an average of 3.0 or above. You are expected to never receive a grade of C+ or below. Such a grade will result in a rating of unsatisfactory. This standard must be met by every student, and is applied in a mechanical fashion.
The practice component requires that the student illustrate progress towards independent applied security skills through projects, laboratory experience and internships. As there is great variance between practice areas, this component is evaluated and documented by the faculty advisor. Usually this is the Program Director; however, if you are engaged in independent research, your advisor will be the supervising faculty.

The professional component requires interaction with the broader security community as a whole as a student progresses in the program. Initial professional evaluations may be a result of teaching assistantships, seminar attendance, or presentations in the classroom. Professional evaluation will be a function of workshop attendance, internship performance, publication of event notes, presentation at events including rump sessions, and overall integration into the community of security professionals. This component of the evaluation is determined by the security faculty as a whole. Note that this element includes speaking and writing skills.

Plagiarism and other violations of academic integrity are basis for immediate termination from the program. While Security Informatics does not practice zero tolerance, a single violation of academic integrity is more than adequate for dismissal from the MSSI program. This dismissal does not require a previous rating of unsatisfactory, nor must it occur during evaluation.

Possible ratings in each category are excellent, exceeds expectations, satisfactory, or unsatisfactory. Receiving satisfactory on all three is acceptable, by definition. A single mark of unsatisfactory identifies a need for significant immediate improvement. Two ratings of unsatisfactory indicate that completion of the MSSI program in two years is unlike (given past performance) and can not complete it at the current level of achievement. Three unsatisfactory ratings indicate a failure to make satisfactory progress in any dimension. A student who receives three ratings of unsatisfactory requires major, immediate change if there is hope of completing the program.

If students are making unsatisfactory progress, the faculty will usually engage with the student to identify goals and avenues of improvement. This may include proposing goals for the next semester. The faculty may also set specific near-term or long-term requirements.

The faculty may also make recommendations to the School to terminate support or to terminate the student from the program. Before this time it is likely that the student will have been in discussions with their advisor or acting advisor, and possible with the Associate Dean of Graduate Studies. Should the student feel that he or she is struggling, that student should alert their advisor immediately, and initiate a discussion with the Associate Dean of Studies. Therefore, if a student is making unsatisfactory progress,
unsatisfactory ratings should not be unexpected. The student should not wait for a formal indication that the problem may have become insurmountable to seek support from the administration.

Lack of satisfactory progress from this review only applies to the security faculty and the students under their advisement. A recommendation by the group to discontinue funding is not binding on the School. For example, a student may find that they have excelled in a concentration course and move to a different program should that faculty accept the student. At the School and group level, termination of support does not mean termination from the program or group. These are distinct decisions.

SOIC Concentrations

These are examples of possible concentrations not an exhaustive list. You are welcome to propose your own. These are examples of sets of courses where two or three are clearly well-matched. While every course has been offered, not every course will be offered in the forthcoming academic year.

There are others not listed here including bioinformatics, cognitive science, cyberinfrastructure, artificial intelligence, cognitive science, programming languages, databases, and logic.

Complex Systems
SLIS-S 604 INFORMATION NETWORKS
INFO-I 601 INTRODUCTION TO COMPLEX SYSTEMS
INFO-I 586 ARTIFICIAL LIFE
INFO-I 590 TOPICS) VT: THE SIMPLICITY OF COMPLEXITY

Privacy
CSCI-B 649/INFO-I 590: ADVANCED TOPICS IN PRIVACY
INFO-I 609 ADVANCED SEMINAR: SOCIAL INFORMATICS
TEL-T 340 ELECTRONIC MEDIA ADVERTISING
TEL-T 535 ECONOMICS OF INFORMATION
TEL-T 321 TELECOMMUNICATES POLICYMAKIN
SLIS-S 643 THE INFORMATION INDUSTRY
TEL-T 650 TELECOMM & THE CONSTITUTION

Social Informatics
INFO-I 504 SOCIAL DIMENSIONS OF SCIENCE INFORMATICS
INFO-I 506 GLOBALIZATION AND INFORMATION
INFO-I 651 ETHNOGRAPHY OF INFORMATION

Embedded Systems
CSCI-B441 DIGITAL DESIGN.
CSCI-B442 DIGITAL SYSTEMS.
CSCI-P545 EMBEDDED & REAL-TIME SYSTEMS.
Technology & Society
SLIS-S 514 COMPUTERIZATION IN SOCIETY
SLIS-S 680 THE BOOK TO 1450
SLIS-S 671 SCHOOL MEDIA

Content & Semantics
SLIS-S 636 SEMANTIC WEB
SLIS-S 532 INFO ARCHITECTURE FOR THE WEB
SLIS-S 642 CONTENT ANALYSIS FOR THE WEB

Music Informatics
INFO-I 545 MUSIC INFORMATION REPRESENTATION, SEARCH, AND RETRIEVAL
INFO-I 547 MUSIC INFORMATION PROCESSING: AUDIO
K503 ELECTRONIC STUDIO RESOURCES

Concentrations Beyond SOIC
These are examples of possible concentrations not an exhaustive list. Any University minor of at least nine hours may be selected as a concentration with the approval of the Program Director. For students entering the program in 2011, the Program Director is Prof. Camp. An exhaustive list of IU minors can be found here: http://www.indiana.edu/~grdschl/graduate-degree-programs.php.

Psychology Concentration
PSY-P 647 DECISION MAKING UNDER UNCERTAINTY
PSY-P 533 INTRODUCTION TO BAYESIAN DATA ANALYSIS I
PSY-P 651 PERCEPTION/ACTION
PSY-P 654 MULTIVARIATE ANALYSIS
PSY-P 820 SOCIAL PERCEPTION

Telecom Concentration
TEL-T 504 INTRODUCTION TO TELECOMMUNICATION POLICY STANDARDS
TEL-T 610 THE NETWORKED SOCIETY
TEL-T 532 ECONOMICS OF MEDIA INDUSTRIES
TEL-T 512 COMMUNICATION AND POLITICS
TEL-T 650 TELECOMMUNICATION & THE CONSTITUTION
TEL-T 575 DIRECTED GROUP NEW MEDIA DESIGN PROJECT

Business Concentration
Please note that many of these courses require instructor permission. It is commonly the case that the instructor gives permission after a recommendation from a security faculty. Any faculty would be happy to recommend you after excellence course performance, but none of us will have the information necessary to strongly recommend you before learning more about you.
BUS-F 421 DERIV SECURITS/CORP RISK MGMT
BUS-F 525 CORPORATE FINANCIAL RISK MGMT (1.5 CR)
BUS-K 490 IND STUDY IN DECISION SCIENCES (1-3 CR)
SPEA-V 541 BENEFIT COST ANALYSIS

**SPEA Concentration**
SPEA-E 560 ENVIRONMENTAL RISK ANALYSIS
SPEA-V 673 PUB POL ANAL/MGMT SCI/OPR RSCH
SPEA-V 507 DATA ANALYS & MODELING-PUB AFF

**Criminal Justice Concentration**
CJUS-P 430 LAW AND THE LEGAL SYSTEM
FORENSICS
CJUS-P 595 DATA ANALYS IN CRIM JUSTICE I
CJUS-P 596 DATA ANALYS IN CRIM JUSTICE II
Area Studies Centers and Programs

Notice none of these have been chosen for a concentration. Yet Indiana University is uniquely strong in language and cultural studies. Many of the minors found at http://www.indiana.edu/~grdschl/graduate-degree-programs.php are for regional or area students. What follows is a truncated list of area studies where there a strong center, and thus intellectual support is likely.

No student may choose to study his or her own region of origin.

African Studies Program
Center for Languages of the Central Asian Region
Center for Latin American and Caribbean Studies
Center for the Study of Global Change
East Asian Studies Center
European Union Center
India Studies Program
Inner Asian and Uralic National Resource Center
Jewish Studies Program
Middle Eastern and Islamic Studies Program
Russian and East European Institute
West European Studies