M.S. in Secure Computing

For Masters of Secure Computing Students Entering
Academic Year 2017 – 2018

Program Director: S. Myers

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

An Introduction to Secure Computing

Secure Computing is a curriculum of instruction that is centered on the protocols and practices of security; both the technological and the social contexts. Thus, Secure Computing includes the core subjects that define computer security, such as access control, networking, cryptography, formal verification, auditing, forensics, and secure system administration. However, Secure Computing also includes the span of material covered by informatics. Thus, Secure Computing includes the technical aspects of computer security integrated with an understanding of fields such as human computer interaction and design, social engineering, economic incentives, and organizational and societal policy and law. Modern day information security problems are solved neither by technical or social contexts independently, but typically require comprehensive approaches.

This document defines the program of study for the Masters of Secure Computing. The program’s goal is to makes our students highly competent in the multidisciplinary world of computer security. This document presents the requirements necessary for completion of the Secure Computing degree, the resources that are available to students, our expectations of student conduct and ethics, discussions of how we evaluate student progress, and descriptions and course registration information for security courses.
Vision

Secure Computing builds upon strong theoretical foundations to construct practical solutions for the intertwined challenges of security and privacy. Secure Computing addresses the immediate problems of today, such as phishing and e-commerce fraud, mobile device security, cloud computing, embedded systems security, corporate espionage and advanced persistent threats. It also addresses emerging research problems, including privacy in ubiquitous computing environments (e.g., the Internet of Things), cyberwar, and the security and privacy of digital currencies, such as bitcoin.

The vision of the Secure Computing program is to ensure students leave with core competencies that allow them to not only understand today’s problems and challenges, and deploy and use modern technologies, but to have the foundational and broad view necessary to understand emerging problems, and technologies, so they can evolve and grow in this fast paced field. Thus, we expect students to be exposed to both the theory and practice of a large number of fields. This is accomplished through combinations of classroom activities, laboratories, internships, research through independent study and extra-curricular activities.

Examples of the foundational skills our students will be exposed to include:
- Cryptography
- Networking
- Protocol Analysis
- Engineering Ethics
- Social Engineering
- Formal Methods
- Secure and Reliable Coding
- Secure Network Operation and Management
- Privacy Preserving and Enhancing Technologies
- Economics of Security
- Human Computer Interaction and Design

The Program

This program is built upon four core components:
1. Computing and Networking Foundations;
2. Secure Computing Core;
3. Applied Security & Professional Practice; and
4. Electives.

The first component ensures that students have a fundamental and deep understanding of the computing systems and networks upon which modern information technology is built. Without understanding these systems, it is hard, if not impossible, to comprehend the security problems and solutions.

The second component introduces students to a variety of theories and skills of modern security and privacy in different domains of information technology. These courses cover both technical and social approaches.

The third element ensures students gain hands-on practical knowledge in applying security skills. This is typically done through student internships, but may also be accomplished by faculty mentored independent study, or courses that are deemed to have a sufficient applied component.
Finally, the students have a certain number of electives. Students with weak technical backgrounds may need to use electives to take courses mastering basic programming and mathematical skills. However, students with strong backgrounds will often use their electives to pursue a collection of electives that concentrate in a specific area to which they can apply their Secure Computing skills.

Program Goals

Some of the core goals for the Secure Computing master's degree program include:

- Develop the mathematical foundation required for Secure Computing.
- 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, in systems, and in network administration.
- Develop an interdisciplinary understanding that enables design and implementation that can address social engineering and economics of security.

A Comparison to Computer Science

Secure Computing is simultaneously more tightly focused and more interdisciplinary than comparable computer science programs. The program focuses on security. For example, it requires the study of cryptography and protocol analysis, as opposed to a larger focus that includes other areas of computer science. As is appropriate, the programs are strongly woven together: Secure Computing students need to take at least three courses in computing and networking foundations from Computer Science, and conversely Informatics security courses are often heavily populated with students majoring in computer science. The Secure Computing is more interdisciplinary in that includes social and organizational contexts for security problem, and considers information security problems in the social domain, as well as technical.
The Secure Computing Master's Program

The Masters of Science Degree in Secure Computing is structured as follows. A student must complete 36 credit hours of courses with the requirement that the following number of credit hours be achieved in each of the four areas as described below:

<table>
<thead>
<tr>
<th>Area</th>
<th>Credit Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computing and Networking Foundations</td>
<td>9</td>
</tr>
<tr>
<td>Security Informatics Core</td>
<td>12</td>
</tr>
<tr>
<td>Applied Security &amp; Professional Practice</td>
<td>6</td>
</tr>
<tr>
<td>Electives</td>
<td>9</td>
</tr>
</tbody>
</table>

The following subsections describe exactly which courses can be used to attain credit for each of the areas mentioned. Course name and credit hours are listed in the appropriate section. Course descriptions can be found later in this document, and on the School of Informatics and Computing’s web page. Courses may not be double-counted across categories; that is, a course that appears in multiple categories may only be used to fulfill credit requirements for one of those categories.

Computing and Network Foundations

These courses ensure that students have a firm grasp of information systems. Students need to take 9 credit hours from the following list of courses. Note that not all courses are offered every semester, or even every year. Students must satisfy a networking and operating system requirement, either by taking one of (CSCI P436/CSCI P536) for operating systems and one of (CSCI P438/CSCI P538) for networking. Students who have previously taken such courses in prior studies can ask to be exempted from taking these specific courses, but must still take 9 credit hours in the area.

<table>
<thead>
<tr>
<th>Course Name</th>
<th>Credit Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCI P436 Introduction to Operating Systems</td>
<td>4</td>
</tr>
<tr>
<td>CSCI P438 Introduction to Computer Networks</td>
<td>4</td>
</tr>
<tr>
<td>CSCI B534 Distributed Systems</td>
<td>3</td>
</tr>
<tr>
<td>CSCI P538 Computer Networks</td>
<td>4</td>
</tr>
<tr>
<td>CSCI P535 Pervasive Computing</td>
<td>3</td>
</tr>
<tr>
<td>CSCI P536 Advanced Operating Systems</td>
<td>3</td>
</tr>
<tr>
<td>CSCI B541 Hardware System Design I</td>
<td>3</td>
</tr>
<tr>
<td>CSCI P542 Hardware System Design II</td>
<td>3</td>
</tr>
<tr>
<td>CSCI B543 Computer Architecture</td>
<td>3</td>
</tr>
<tr>
<td>CSCI P535 Embedded and Real-Time Systems</td>
<td>3</td>
</tr>
<tr>
<td>CSCI B561 Advanced Database Concepts</td>
<td>3</td>
</tr>
<tr>
<td>CSCI B649 Internet Services and Protocols</td>
<td>3</td>
</tr>
</tbody>
</table>
Secure Computing Core

These courses ensure that students have a firm grasp of the fundamental ideas, skills, models and tools of information security. Students need to take 12 credit hours from the following list of courses. *Students must take 1520 and 1533 for 6 of these core credits.* This ensures that students get a well-rounded background in Secure Computing. Note that not all courses are offered every semester, or even every year (with the exception of 1520 and 1533, which are offered every year).

<table>
<thead>
<tr>
<th>Course Name</th>
<th>Credit Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>INFO 1520 Security and Software Assurance</td>
<td>3</td>
</tr>
<tr>
<td>INFO 1521 Malware: Threat &amp; Defense</td>
<td>3</td>
</tr>
<tr>
<td>INFO 1525 Organizational Informatics and Econ. Of Security</td>
<td>3</td>
</tr>
<tr>
<td>INFO 1533 Systems and Protocol Security and Info. Assurance</td>
<td>3</td>
</tr>
<tr>
<td>INFO 1536 Mathematical Foundations (Cryptography)</td>
<td>3</td>
</tr>
<tr>
<td>INFO 1537 Legal and Social Informatics of Security</td>
<td>3</td>
</tr>
<tr>
<td>INFO 1538 Introduction to Cryptography</td>
<td>3</td>
</tr>
<tr>
<td>INFO 1539 Cryptographic Protocols</td>
<td>3</td>
</tr>
<tr>
<td>INFO 1590 Topics in Informatics (See important note below)...</td>
<td>3</td>
</tr>
<tr>
<td>CSCI B649 Trusted Computing</td>
<td>3</td>
</tr>
</tbody>
</table>

Note that 1590 is a “Topics” course, which means many different courses are offered under this course listing. This course may be taken multiple times to satisfy credit hours in this area so long as the courses are taught by core program faculty, as listed at the top of this document, or 2) You have the approval of the Secure Computing program director. If you have any concerns, please check with the graduate office.

Applied Security & Professional Practice

The goal of these credits is to ensure that you have the opportunity to practice skills in an applied and preferably professional setting. Our goal is for most students to be able to have internships in organizations where they will be exposed to some practical aspect of information security in a day-to-day manner. The School’s Career Services group is an excellent resource that is useful in helping students find internships. We recommend that you start early. You need to start thinking about this in your first weeks! Please see the section on Career Services later in this document for contact and other useful information. Each 10-hour per week internship over a semester/summer provides 1 credit hour. Secure Computing students are highly sought as paid interns; and it is not unusual for summer internship courses to provide both income and 4 hours of degree credit. A student may take a maximum of two internships, for a maximum of 6 credit hours. Further, a student may work no more than 40 hours per week for credit.
Beyond an internship, students may also satisfy their Applied Security & Professional Practice credit requirements through specific course (listed below). Finally, if a student is working with a particular faculty on a research project, then an independent study may also be possible. Please note that faculty are not obligated to supervise independent studies.

<table>
<thead>
<tr>
<th>Course Name</th>
<th>Credit Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>INFO 1591 Graduate Internship</td>
<td>3</td>
</tr>
<tr>
<td>CSCI-Y790 Independent Study</td>
<td>3</td>
</tr>
<tr>
<td>CSCI-A538 Network Tech &amp; Administration</td>
<td>3</td>
</tr>
<tr>
<td>CSCI-A548 Mastering The World Wide Web</td>
<td>3</td>
</tr>
</tbody>
</table>

**Electives**

The remaining credits are electives. There are three ways these credits are typically used to take courses that: 1) buttress weaknesses in your incoming education, 2) are in an area related to information security that are (frequently) outside of the school which we think of as concentrations, and 3) are traditional electives; courses which are simply of general interest to the student. It is important to note that unless you have the program director’s permission for a specific course beforehand, all electives credit must be at the 500 level or higher.
Example Courses of Study

Students entering the Secure Computing may be joining the program from a technical or social science background. The following courses of study present examples of two different paths for people entering with different strengths and interests.

Example 1: An Arriving Computer Science Student

Imagine a student arriving with a BSc in computer science. That student has previously taken a course in networking, but never in operating systems. The student’s mathematics background is weak, so she decides to take a probability course in math to help prepare for her course in cryptography. She also has an interest in Data Mining, which she has found intersects nicely with Information Security, and so she uses her last two electives on those. She found summer employment penetration testing in the security field, working full time, so she is able to finish her professional practice over the summer.

<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 Core</strong></td>
<td>INFO 537 Economics of Security</td>
<td>INFO 538 Crypto</td>
<td></td>
<td>INFO 520 Network Security</td>
<td>INFO 533 Information Assurance</td>
</tr>
<tr>
<td><strong>Application and Professional Practice</strong></td>
<td>Network Admin (3)</td>
<td>Professional Internship I591</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Computing Foundations</strong></td>
<td></td>
<td></td>
<td></td>
<td>B534 P436</td>
<td>P438</td>
</tr>
<tr>
<td><strong>Electives</strong></td>
<td>Intro Programming</td>
<td>Business Risk</td>
<td></td>
<td></td>
<td>Business Modeling</td>
</tr>
</tbody>
</table>
Example 2: An arriving Economics Student

The student arrives. The student has never programmed, but has a casual understanding of computers. Having taken economics, the student has a strong mathematics background. Thus, the student takes an introductory course on programming and data structures, and an applied course on systems administration in his first year to improve his computing skills, while concurrently taking mathematical and organizational security courses.

In the second year, he takes the more technical and required security core courses, as well as foundational courses on computing. He uses his remaining electives to pursue some security related courses from the business school.

<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 Core</strong></td>
<td>INFO 525</td>
<td>INFO 533</td>
<td>INFO 538</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>INFO 520</td>
<td>(Systems Assm)</td>
<td>(Crypto)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Application and Professional Practice</strong></td>
<td></td>
<td>Professional Internship 1591 (x2)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Computing Foundations</strong></td>
<td></td>
<td>P534 (Pervasive)</td>
<td>P538 (Networks)</td>
<td>P436 (Operating Sys)</td>
<td></td>
</tr>
<tr>
<td><strong>Electives</strong></td>
<td>Probability</td>
<td>Data Mining I</td>
<td></td>
<td>Data Mining II</td>
<td></td>
</tr>
</tbody>
</table>

**Security Core Courses**

The following are brief descriptions of the security core courses.

**INFO 1520 Security for Networked Systems**

This course is an extensive survey of system and network security. Course materials will cover threats to information confidentiality, integrity and availability in a computing system and network, and defense mechanisms that control these threats. The course will also provide necessary foundation on information security, such as cryptographic primitives/protocols, authentication, authorization and access control technologies, and hands-on experiences through programming assignments and course projects.

**INFO 1521 Malware Epidemic: Threat and Defense**

The objective of this course is to offer a technical review of mobile and cloud security, particularly security weaknesses in those new computing paradigms that can be exploited by mobile or web-based malware, and also explore new technical directions to address these security challenges. Students will be trained to understand the new security threats through literature review and gain hands-on experiences through course projects.
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.

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.

INFO 536 Foundational Mathematics of Cybersecurity
Students will learn mathematical tools necessary to understand modern cyber security. The course will cover introductory mathematical material from a number of disparate fields including probability theory, computational theory, complexity theory, group theory, and information theory.

INFO 1537 Legal and Social Informatics of Security
Security technologies make explicit organizational choices that allocate power. Security implementations allocate risk, determine authority, reify or alter relationships, and determine trust extended to organizational participants. The course begins with an introduction to relevant definitions (security, privacy, trust) and then moves to a series of timely case studies of security technologies. This course may be taken as an alternative 1525. The course also requires a project, including a work plan, a timeline, peer evaluations, and professional presentations.

INFO 1538 Introduction to Cryptography
This class considers issues of network security, treating in depth the topics covered in INFO 1536. In particular, the class involves adversarial modeling, a detailed treatment of security primitives, and methods for analysis of security. It spans the ethics and technology of security, with examples drawn both from deployed and proposed protocols. Topics to be covered include studies of rational and malicious cheating, symmetric and asymmetric cryptography, security reductions and heuristics.

INFO 1539 Cryptographic Protocols
This class will cover current and timely topics in the field of Secure Computing. Topics will vary from year to year. Examples of topics that could have been covered in recent years include phishing and cyberfraud, trusted computing basis, electronic voting, and digital rights management systems.
INFO I590 Topics in Informatics—Today's Privacy Challenges: Technology and Policy
In this class, students will learn about how privacy-infringing technologies work and how to design solutions that empower people to manage their privacy. In our interconnected world, people are continuously leaking data to anyone who knows how to listen for it. Malls now track the movement of patrons through the Wi-Fi signals on their phones. Online advertisers track people’s movements across the web to provide more meaningful advertisements.

Students will spend part of the course doing hands-on experimentation with privacy-infringing technologies to better understand how they work. We will then shift to discussing how to design solutions that address these types of issues through technological, policy, and educational means.

INFO I590 Topics in Informatics—Advanced Topics in Privacy
This seminar is driven by student-led roundtable discussions of seminal and influential research papers, and short lectures on improving research skills. Building on knowledge gained in class, students will work on research projects in groups targeting either a potential academic publication or a prototype for a potential industrial startup. This seminar most recently focused on wearable and sensor-based computing and social networks.

CSCI B649 Trusted Computing
We will explore current methods for characterizing, establishing and attesting trust of a system. We will cover a variety of topics including hardware-based trusted components, trusted identities and identity management, reputation systems, trust negotiation, etc.

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 Center for Applied Cybersecurity’s (CACR) Security Seminar. It is assumed that students will regularly attend most of these seminars. It is a crucial part of learning the current and future trends in Secure Computing. These speakers are typically world experts in their respective fields.

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, security or privacy protocol, and corresponding security definitions and models.
• Appreciation of types and categories of bugs, attacks, and patches.
• Understanding basic computer science concepts and how engineers solve problems.
• Mathematics and research methods.
Foundational Security Literature

• Familiarity with the foundational literature of cryptography, security and privacy systems.
• Understanding of the core concepts of frequently deployed 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.

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 popular operating systems and servers (e.g., Linux, OS X, Windows)
• 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.

Resources

Travel Funding

Secure Computing students can apply for one-time travel funds to cover some of the costs of attending a conference related to Secure Computing. Funding is awarded to students upon admission. Applications for travel funds are reviewed and approved by the graduate directors. These funds must be used for travel, hotel, food, and/or registration fees. Each Secure Computing student will be provided up to $800 during his/her entire program. Items such as alcohol, entertainment, etc. are not allowed. All expenses must be approved prior to the event. All receipts are required for reimbursement. Receipts must be submitted within 60 days of the end of travel.

Application forms for travel funds may be found at http://www.soic.indiana.edu/graduate/forms1/other-forms.shtml

Career Services
The School of Informatics and Computing has a dedicated Career Services staff to provide opportunities and resources that will empower students to define their career goals, develop professional life skills, obtain related experience, and realize their career potential. The SoIC hosts two major career fairs each year where students can meet with more than 90 companies in the fall semester and more than 70 during the spring semester. In 2014-2015, 145 companies recruited on-campus and conducted more than 1500 interviews in the School. Career Services staff are there to help students with every step in the process including figuring out what they want to do, getting their application materials prepared, connecting with employers, practicing interviewing skills, and negotiating job and internship offers.

The Fall 2015 Career Fair is scheduled for Thursday, September 10 and employers will be participating in other recruiting activities beginning even earlier in the week, so students should not wait to get the help they need. Students can log in to SoIC Careers using their CAS credentials to schedule career advising appointments, search employers, apply for job/internship opportunities, see who will be attending the Fair, find the Job Search Guide and list of upcoming workshops, and more!

All students must fully read and agree to the Recruiting Guidelines for the School and have an approved resume in SoIC Careers before they will be able to apply for on-campus interviews and other opportunities, so students should upload their resumes in SoIC Careers as soon as possible so they can be approved before those deadlines begin in early September.

For more information on how Career Services can help, see the Career Services website (www.soic.indiana.edu/career/)
Classroom performance:

The minimal standard is that you must maintain an average of 3.0 or above. You are expected to never receive a grade of C or below. If you do achieve such a score, the course will not be counted for credit, towards your degree, nor towards your credit areas.

Practice performance:

The standard 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 with which you take courses, perform independent study, and the Program Director.

Professional performance:

The standard requires that the student interact with the broader security community as a whole as the student progresses in the program. Initial professional evaluations may be a result of teaching assistantships, seminar attendance, or presentations in the classroom. Later 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, presentation and writing skills.

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 Secure Computing program in two years is unlikely (given past performance) and the student will not complete the program 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 the Program Director, and possibly with the Associate Dean of Graduate Studies. Should the student feel that he or she is struggling, that student should alert the Program Director immediately. 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.

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 Center for Applied Cybersecurity’s (CACR) Security Seminar. It is assumed that students will regularly attend most of these seminars. (Thursday at 12p) It is a crucial part of learning the current and future trends in Secure Computing. These speakers are typically world experts in their respective fields.
Academic Misconduct

Academic misconduct represents a broad range of academic offenses, examples of which include cheating, fabrications, interference, violation of course rules, facilitating academic dishonest, and plagiarism. It is essential that you properly cite a source, and only include others' works when that work is properly delineated and credited. As an IU student you are expected to uphold Student Code of Conduct, as described here: [http://www.iu.edu/~code/code/index.shtml](http://www.iu.edu/~code/code/index.shtml)

Given that Secure Computing students are often dealing in areas where trust is paramount, there will be no warnings given for academic misconduct! Rather, the faculty and program director will push for the strongest penalties possible.

Academic Probation

An Secure Computing student may be placed on academic probation for the following reasons:

- The GPA falls below 3.0.
- Satisfactory progress is not being made towards the degree as determined by Secure Computing faculty or Program Director in the evaluation of the student’s work.
- Failure to fulfill requirements which were stipulated at the time of admission, including English exams or required language training for international students.

When a student is put on academic probation, recommendation will be given to the student to improve his/her academic standing with deadlines set. The student's performance is evaluated again at those deadlines to determine if improvements have been made and goals have been met. If performance does not improve, the student will not ordinarily be allowed to continue in the graduate program.

Course Registration & Transfer

Course Registration Guidelines

Full-time Status
To be considered a full-time student, the student must register for 8 credit hours, according to IU policy. The student should choose three courses (typically 3 credit hours each) that count towards the intended degree. Students must enroll in three courses even if they are making up incompletes from a previous semester. Students are expected to maintain a normal load as they make up incompletes.

*Tip:* "Add and drop" instead of "drop and add": When replacing courses, be sure to add the new course first and then drop the old, in order to always be above the minimum number of credits for status.

Waitlist
If a course which you desire is shown as full, be sure to add yourself to the waitlist, which serves as a place holder for you in line. When students who enrolled in the course drop, or when the enrollment cap is expanded, students on the waitlist will be admitted into the course in order.
Drop and refunds
Be sure to finalize your schedule promptly. For course drops in the first week, IU refunds the full tuition for the course. In the second, third, and fourth weeks, refunds are 75%, 50%, and 25%. Later drops receive no refunds. We strongly encourage you to become familiar with the Office of the Bursar’s policies and fee payment information.

Withdrawals from courses
During the automatic withdrawal period, students who withdraw will be assigned an automatic grade of W (see the Registrar's official calendar for exact dates). After that period, withdrawals are only possible with approval from the Dean, which is normally given only for urgent reasons such as illness. Note that CS students must successfully complete at least 9 credits of courses towards their degrees each semester to be considered making satisfactory progress. The amount of tuition refund (if any) for a dropped course depends on when the course is dropped.

Applicability of fee remissions
Fee remissions normally are not applicable to outside courses not counting towards Secure Computing degree.

*AI and RA
Students offered a student academic appointment (SAA), as a Research Assistant (RA) or Associate Instructor (AI), have a workload that is a 50% FTE appointment (20 hours per week). Students with a SAA, are required to register for at least 6 credit hours to maintain full-time status.

Students with research assistantships must secure their RA supervisors' advance written permission to take any outside courses in addition to the required 9 credits of Secure Computing courses contributing towards their degrees. This approval must be provided to the Graduate Student Services Specialist prior to registration.

* Non-native speakers of English are required to pass an English exam. For more information, see link: TEPAIC.

Independent Study
The Secure Computing Program offers one independent study course

1. CSCI Y790

How to sign up: For independent study or research courses you can locate the faculty member through the Indiana University Course Browser and register up to the allowed amount of credits per the outlined program requirements. If you require assistance with enrollment, please contact the CSGSO at soicsiu@indiana.edu.

Y790's with supervision outside SEC: If the Independent Study supervisor is outside of the Secure Computing Faculty, you will need to find a Secure Computing faculty member to co-supervise the project. The Secure Computing faculty member must assess the student's work at the end of the semester and submit the grade for the course. Please be sure that all
needed information is provided to him or her at the end of the semester, in time for the grade submission deadline.

**Transfer Credits**

Some graduate coursework completed at other universities may be transferred into degree and licensure programs. All coursework transferred must be from an accredited college or university and no transfer credit will be given for courses with a grade lower than a B. Transferred courses must be relevant to the student's program of studies and must be approved by the Secure Computing Director.

To transfer credits, the student should identify the course at IU that may be considered equivalent to the course to be transferred, contact the instructor who teaches the course, provides documents, such as course description, course syllabus, sample homework assignments, projects and/or exams, as required by the instructor. In the case the instructor approves of the transfer, the student should prepare the [Course Transfer form](#) for the instructor to sign and submit the completed form to the CS Graduate Studies Office.

**Leave of Absence**

To request a leave of absence from the graduate program, a student should discuss the nature and length of the leave with the Secure Computing Program Director. The Leave of Absence form needs to be completed, and signed by the Director of the SECURE COMPUTING. Submit the completed form to the CSGSO.

**During Program of Studies:** Students who do not enroll in classes for a period of one year must apply for re-admission to the program. They must meet current admission criteria, and if re-admitted, must fulfill current program requirements.

**Internship and Curricular Practical Training (CPT)**

A student may take at most two internships for a maximum of 6 credits. These will be assigned credit hours based on the hours worked so that they roughly correspond to 1 credit per 10 hours worked over a "semester or summer" 3-3.5 months of work. One cannot exceed 40 hours of work per week for credit.

International Students planning summer employment under the CPT program must enroll in INFO-I591 and complete the arrangements with International Services and the Computer Science Department to obtain CPT approval. I591 is not allowed with a RAship or AIship, due to the policy that AIs and RAs are not allowed to take additional employment.

CPT is Work authorization that allows F-1 international students to participate in paid off-campus academic internships during a student’s degree program.

- The work must be integral to the degree program.
- Approval must be granted prior to completion of your academic program.
- CPT is approved or denied by the Office of International Services (OIS) and the Computer Science Graduate Studies Office (CSGSO)
- Employment must not begin until the date authorized in the I-20 issued by OIS
- You must be a full-time, F-1 status student for at least one full academic year
Accepting an Employers Offer

• Accept only ONE offer from ONE employer.
• You must have a letter from your prospective employer for work in your major field of study.
• Withdraw all pending applications
• Cancel all scheduled interviews
• Cease seeking employment/internships elsewhere.

Offer Letter Requirements

• Name of Company
• Physical Address – No P.O. Box
• Contact Phone Number
• Email of Employer/Supervisor
• Your Job Title
• A Full Job Description - With Job Duties Listed
• Start Date and End Date of Employment
• Total Hours you will be working

BEFORE starting internship, the student must complete the following:

Notifying the CS GSO

You will need to notify the Computer Science Graduate Studies Office (CSGSO) when your employer provides you with an offer letter.

Please submit the following information to the soiccsiu@indiana.edu email address:

• Your Full Name
• Your Program
• Student ID Number
• A PDF version of the Offer Letter from your Employer
• A Description of the nature of the employment and how this employment directly relates to your course work and program.

The CS GSO Office will review your email, offer letter and required information. We will ask you to enroll in the appropriate course. We will then ask you to complete the following OIS process:

Upload the offer letter in iStart

• Follow the instructions carefully and upload your offer letter into iStart for OIS Approval

• When OIS approves the offer letter they will notify you via email with instructions for completing the Academic Advisor Form
Complete the Academic Advisor Form in iStart

- Indicate Regina Helton as the Academic Advisor (Regina is the point of contact for this process)
- Use the soicesiu@indiana.edu email address on the Academic Advisor form (and on any OIS related communication)

Points to Remember:

- The approval process cannot be rushed or completed out of order
- It is important that you use the soicesiu@indiana.edu email address on all OIS related communication
- Employment must not begin until the date authorized in the I-20 issued by OIS

We encourage you to view the additional employment guideline information: http://www.soic.indiana.edu/career/students/recruiting-guidelines.html

After the Internship

AFTER the Internship is completed, the student must provide the Secure Computing program with an “Exit” letter - a formal letter from the employer stating that the term of employment or internship was satisfactorily completed. A grade will then be assigned. Failure to submit the exit letter will result in a grade of “I” (incomplete). This will turn to an "F" on the transcript one year after registration in the course unless the Exit letter is provided.

Graduation

Graduation instructions are sent out prior to the end of the students last term. Students will need to follow the directions provided via email by the CSGSO. Students will be asked to submit their Program of Study listing all courses that have been completed, including grades for each course, and the overall GPA. This information should be submitted to the CSGSO via email at: soicesiu@indiana.edu for review.
**Student Name:** SANTA CLAUS

**Master Degree in Secure Computing**
Program of Studies Form
36 Credit Hours / GPA = 3.0+

<table>
<thead>
<tr>
<th>Applied Requirement (6 credits)</th>
<th>Course</th>
<th>Term</th>
<th>Course</th>
<th>Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCI A538</td>
<td>Network Tech. &amp; Administration</td>
<td>Spring 2014</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>CSCI A548</td>
<td>Mastering the World Wide Web</td>
<td>Fall 2014</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td><strong>OR</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Graduate Internship</strong> (6 credits)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>INFO I591</td>
<td>Graduate Internship</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>INFO I591</td>
<td>Graduate Internship</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Cybersecurity (6-9 credits)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>INFO I533</td>
<td>Systems &amp; Protocol Security</td>
<td>Fall 2013</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>INFO I520</td>
<td>Security for Networked Systems</td>
<td>Spring 2014</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>INFO I525</td>
<td>Economics of Security</td>
<td>Spring 2014</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>INFO I536</td>
<td>Foundational Math.of Cybersec.</td>
<td>Fall 2014</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td><strong>CS Networking Electives (9 credits)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CSCI P436</td>
<td>Intro. to Operating Systems</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CSCI P438</td>
<td>Intro. to Computer Networks</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CSCI B534</td>
<td>Distributed Systems</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ILS Z573</td>
<td>Educa. of Information</td>
<td>Summer</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>CSCI B649</td>
<td>Topics Course</td>
<td>Summer</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td><strong>INFO-1521</strong></td>
<td>Malware: Threat &amp; Defense</td>
<td>Fall 2013</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td><strong>Concentration Electives (6-9 credits)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>list online</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CSCI-A 591</td>
<td>Intro to Computer Science</td>
<td>Spring 2013</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>INFO-I590</td>
<td>Topics in Info: Big Data</td>
<td>Spring 2013</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>INFO-I590</td>
<td>Topic in Info: CX</td>
<td>Spring 2013</td>
<td>3</td>
<td></td>
</tr>
</tbody>
</table>

**Graduate Studies Notes:**

---

Security Student Handbook
Informatics School of Informatics & Computing
Master Degree in Secure Computing
Program of Studies Form
36 Credit Hours / GPA = 3.0+

<table>
<thead>
<tr>
<th>Applied Requirement (6 credits)</th>
<th>Course</th>
<th>Term</th>
<th>Course Credit</th>
<th>Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>OR</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Graduate Internship (6 credits)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>INFO I591</td>
<td>Graduate Internship</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>INFO I591</td>
<td>Graduate Internship</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cybersecurity (6-9 credits)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CS Networking Electives (9 credits)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Concentration Electives (6-9 credits) list online |        |      |               |       |

<table>
<thead>
<tr>
<th>Total Credits</th>
<th>GPA</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Graduate Studies Notes: