M.S. in Secure Computing

For Masters of Secure Computing Students
Entering Academic Year 2021 – 2022

** DRAFT **

Program Director: XiaoFeng Wang
Associate Director: Apu Kapadia
Program Faculty: L. J. Camp, Y. Huang, A. Kapadia, X. Liao, S. Patil, and X. Wang, L. Xing

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

This document defines the program of study for the Masters of Secure Computing. The program's goal is to make our students technically competent in the multidisciplinary world of cybersecurity across a range of topics such as access control, networking, cryptography, formal verification, auditing, forensics, secure system administration, human computer interaction and design, social engineering, economic incentives, and organizational and societal policy and law.

Students will be exposed to both the theory and practice of cybersecurity through combinations of classroom activities, laboratories, internships, research through independent study and extra-curricular activities. 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.

The Program

This program is built upon four core components:

1. **Computing Foundations**: this 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 cybersecurity problems and solutions. Depending on chosen concentration of study, students will take the appropriate Computing Foundations Track.

2. **Secure Computing Core**: this component introduces students to a variety of theories and skills of modern cybersecurity and privacy in different domains of information technology. These courses cover both technical and social approaches.

3. **Applied Security & Professional Practice**: this component ensures that 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.

4. **Electives**: this component allows students to enhance their basic programming and mathematical skills, or to pursue electives in other areas that complement their cybersecurity skill

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:

Area	Credit Hours
Computing Foundations	9
Security Informatics Core	12
Applied Security & Professional Practice	6
Electives	9

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 Luddy School of Informatics, Computing, and Engineering'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 Foundations - Data Centered Track

These courses ensure that students have a firm grasp of information systems. Students need to take the 9 credit hours from the following list of courses. *Students must satisfy information systems requirement by taking two courses (CSCI A541* ***and*** *INFO 500) for computing foundations and one course (CSCI A542) for security foundations.* 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.

Required courses unless exempted:
INFO I500 Fundamental Computer Concepts for Informatics (3 cr.)
CSCI A541 - CS Boot Camp (3 cr.)

CSCI A542 - Technical foundations in cybersecurity (3 cr.)

Substitutions from the following list are allowed if exemptions are granted for the required courses:
INFO I519 Introduction to Bioinformatics (3 cr.)
INFO I523 Big Data Applications and Analytics (3 cr.)
INFO I524 Big Data Software and Projects (3 cr.)
INFO I526 Applied Machine Learning (3 cr.)
INFO I535 Management, Access, and Use of Big Complex Data (3 cr.)
INFO I571 Introducing Cheminformatics (3 cr.)
INFO I572 Computational Chemistry and Molecular Modeling (3 cr.)
INFO I573 Programming for Science Informatics (3 cr.)
INFO I585 Bioinspired Computing (3 cr.)
INFO I619 Structural Bioinformatics (3 cr.)
INFO I621 Computational Techniques in Comparative Genomics (3 cr.)

Computing Foundations - Human-Centered Track

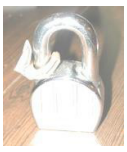
These courses ensure that students have a firm grasp of information systems. Students need to take the 9 credit hours from the following list of courses. *Students must satisfy information systems requirement by taking two courses (CSCI A541* ***and*** *INFO 500) for computing foundations and one course (CSCI A542) for security foundations.* 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.

Required courses unless exempted:
INFO I500 Fundamental Computer Concepts for Informatics (3 cr.)
CSCI A541 - CS Boot Camp (3 cr.)
CSCI A542 - Technical foundations in cybersecurity (3 cr.)

Substitutions from the following list are allowed if exemptions are granted for the required courses:
INFO I504 Social Dimensions of Science Informatics (3 cr.)
INFO I506 Globalization and Information (3 cr.)
INFO I651 Ethnography of Information (3 cr.)
INFO I502 Human-Centered Research Methods in Informatics (3 cr.)
INFO I504 Social Dimensions of Science Informatics (3 cr.)
INFO I506 Globalization and Information (3 cr.)
INFO I507 Introduction to Health Informatics (3 cr.)
INFO I527 Mobile and Pervasive Design (3 cr.)
INFO I528 Participatory Design (3 cr.)
INFO I530 Field Deployments (3 cr.)
INFO I549 Advanced Prototyping (3 cr.)
INFO I561 Meaning and Form in HCI (3 cr.)
INFO I605 Social Foundations of Informatics (3 cr.)
INFO I651 Ethnography of Information (3 cr.)

Computing Foundations - Secure Programming Track

These courses ensure that students have a firm grasp of computing systems. Students need to take 9 credit hours from the following list of courses.
Students must satisfy a networking and operating system requirement by taking CSCI P536 for operating systems and 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.

Required courses unless exempted:
CSCI P538 Computer Networks (3 cr)
CSCI P536 Advanced Operating Systems (3 cr)

Substitutions from the following list are allowed if exemptions are granted for the required courses:
CSCI B534 Distributed Systems(3 cr)
CSCI P535 Pervasive Computing
CSCI B541 Hardware System Design I (3 cr)
CSCI P542 Hardware System Design II (3 cr)
CSCI B543 Computer Architecture (3 cr)
CSCI P535 Embedded and Real-Time Systems (3 cr)
CSCI B561 Advanced Database Concepts (3 cr)

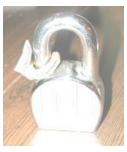
Secure Computing Core

These courses ensure that students have a firm grasp of the fundamental ideas, skills, models and tools of cybersecurity. Students need to take 12 credit hours from the following list of courses. ***All MSSC Students must take I520 /B544. Additionally, students in the Secure Programming track must take CSCI B547 as part of these core credits.*** This ensures that students get a well-rounded background in Secure Computing.

Secure Programming Track
CSCI B544 Security for Networked Systems (required) (3 cr)
CSCI B547 Systems and Protocol Security and Info. Assurance (required) (3 cr)
CSCI B546 Malware: Threat & Defense (3 cr)
INFO I525 Organizational Informatics and Econ. of Security (3 cr)
INFO I536 Mathematical Foundations (Cryptography) (3 cr)
INFO I537 Legal and Social Informatics of Security (3 cr)
CSCI B504 Introduction to Cryptography (3 cr)
INFO I539 Cryptographic Protocols (3 cr)

Data Science Track
INFO I520/ CSCI B544 Security for Networked Systems (required) (3 cr)
INFO I521/ CSCI B546 Malware: Threat & Defense (3 cr)
INFO I525 Organizational Informatics and Econ. of Security (3 cr)
INFO I536 Mathematical Foundations (Cryptography) (3 cr)
INFO I537 Legal and Social Informatics of Security (3 cr)
INFO I538/ CSCI B504 Introduction to Cryptography (3 cr)
INFO I590/CSCI B649 Usable Privacy and Security (3 cr)
INFO I590/CSCI B548 Privacy in Pervasive Computing (3 cr)
INFO I590/CSCI B649 Data-Driven Security and Privacy (3 cr)
INFO I539 Cryptographic Protocols (3 cr)

Human Centered Track
INFO I520/ CSCI B544 Security for Networked Systems (required) (3 cr)
INFO I521/ CSCI B546 Malware: Threat & Defense (3 cr)
INFO I525 Organizational Informatics and Econ. of Security(3 cr)
INFO I536 Mathematical Foundations (Cryptography) (3 cr)
INFO I537 Legal and Social Informatics of Security (3 cr)
INFO I538/ CSCI B504 Introduction to Cryptography (3 cr)



INFO I539 Cryptographic Protocols (3 cr)
INFO I590/CSCI B649 Usable Privacy and Security (3 cr)
INFO I590/CSCI B548 Privacy in Pervasive Computing (3 cr)
INFO I590/CSCI B649 Data-Driven Security and Privacy (3 cr)
INFO I590/CSCI B649 Topics in Informatics/Systems (3 cr)
(See important note below)

Note that I590/B649 are "Topics" courses, 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 students have the opportunity to practice skills in an applied or professional setting. Students are required to obtain 6 credits through courses or internship credits.

Internship credit must be obtained from organizations where students are exposed to some practical aspect of cybersecurity. Each 10-hour per week internship over a semester/summer provides 1 credit hour. **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.** The School's Career Services group is an excellent resource that is useful in helping students find internships, and students are recommended to start this process early. Please see the section on Career Services later in this document for contact and other useful information.

Students may also satisfy their Applied Security & Professional Practice credit requirements through specific courses (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.

Courses:
CSCI Y798 Graduate Internship (3 cr)
CSCI-Y790 Independent Study (3 cr)
CSCI-A538 Network Tech & Administration (3 cr)
CSCI-A548 Mastering The World Wide Web (3 cr)

Electives

The remaining 9 credits are electives. Unless you have the program director's permission for a specific course beforehand, *all electives credit must be at the 500 level or higher.* Students may use these credits to enhance their mathematical or computing skills, or to concentrate on areas that complement their cybersecurity skills.
Customized minors are common. Previous graduates have had minors in a wide range of scholarly areas, combining courses from multiple departments. The exceptional strength of cultural departments

Past minors include standard disciplines including psychology, sociology, public health, public policy, and criminology. Individualized minors have included crypto finance, risk communication, and statistical methods.

Example Course of Study

The following course of study presents an example of a student with a specific computer science background with interests in datamining.

Example : An Arriving Computer Science Student

Imagine a student arriving with a BSc in computer science. The student does not have a prior background in networking or operating systems. 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.

	1st semester	2nd semester	Summer	3rd semester	4th semester
Security Core	I520/B544 Network Security I525 Economics of Security	I533/B547 Sys and Protocols		I521/B546 Malware	
Application and Professional Practice		Network Admin (3)	CSCI Y798 Professional Internship		
Computing Foundations	P438 or P538 Computer Networks	P436 or P536 Operating Systems		B561 Advanced Database	
Electives				Datamining	P556 Applied Machine learning Business Risk

Security Core Courses The following are brief descriptions of the security core courses.

INFO I520 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 I521 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 I525 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 I533 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 I537 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 I525. The course also requires a project, including a work plan, a timeline, peer evaluations, and professional presentations.

INFO I538 Introduction to Cryptography
This class considers issues of network security, treating in depth the topics covered in INFO I536. 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 I539 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 cyber-fraud, 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.

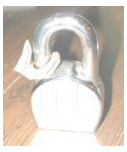
Seminar Series

Master's degree students have the opportunity to attend seminars by distinguished faculty and industry practitioners with the purpose to broaden and stimulate your intellectual development. The School organizes regular *Colloquia* with invited speakers and the Center for Applied Cybersecurity's (CACR) organizes a *Security Seminar* series. *Students are encouraged to regularly attend these seminars* to engage in discussion with current and future trends in cybersecurity.

Career Service

The School of Informatics, Computing, and Engineering 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. SICE 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, for example, 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 getting their application materials prepared, connecting with employers, practicing interviewing skills, and negotiating job and internship offers.

The Fall Career Fair is scheduled for each September 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 SICE Careers using their CAS credentials to schedule career advising appointments, search employers, apply for job/internship opportunities, and more.

All students must fully read and agree to the Recruiting Guidelines for the School and have an approved resume in SICE Careers before they will be able to apply for on-campus interviews and other opportunities, so students should upload their resumes in SICE 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.sice.indiana.edu/career/)

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 that you desire is shown as full, be sure to add yourself to the waitlist, which serves as a placeholder 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 (http://bursar.indiana.edu/home/) policies and fee payment information.

Withdrawals

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 Secure Computing 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.

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.

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 CSCI Y790.

How to sign up: For independent study or research courses you can locate the faculty member through the Indiana University Course Browser.

Y790's with supervision outside SC

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

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.

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 per week over a "semester or summer" (I.e., 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 CSCI Y798 and complete the arrangements with International Services and the Computer Science Department to obtain CPT approval. Y798 is not allowed with an 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.

Student Name: _____

Master Degree in Secure Computing (To be updated)
Program of Studies Form
36 Credit Hours / GPA = 3.0+

Applied Requirement (6 credits)	**Course**	**Term**	**Course**	**Grade**
CSCI A538	Network Tech. & Administration	Spring	3	
CSCI A548	Mastering the World Wide Web	Fall	3	
OR				
Graduate Internship (6 credits)				
INFO I591	Graduate Internship			
INFO I591	Graduate Internship			
Cybersecurity (6-9 credits)				
INFO I533	Systems & Protocol Security	Fall	3	
INFO I520	Security for Networked Systems	Spring	3	
INFO I525	Economics of Security	Spring	3	
INFO I536	Foundational Math.of Cybersec.	Fall	3	
CS Networking Electives (9 credits)				
CSCI P436	Intro. to Operating Systems	Fall		
CSCI P438	Intro. to Computer Networks	Fall		
CSCI B534	Distributed Systems	Fall		
Concentration Electives (6-9 credits) list online				
CSCI-A 591	Intro to Computer Science	Spring	3	
INFO-I590	Topics in Info: Big Data	Spring	3	
INFO-I590	Topic in Info: CX	Spring	3	

Student Name:_____ **ID:**_____

Master Degree in Secure Computing

Program of Studies Form

(To be updated)

36 Credit Hours / GPA = 3.0+

Applied Requirement (6 credits)	Course	Term	Course Credit	Grade
OR				
Graduate Internship (6 credits)				
INFO I591	Graduate Internship			
INFO I591	Graduate Internship			
Cybersecurity (6-9 credits)				
	.			
CS Networking Electives (9 credits)				
Concentration Electives (6-9 credits) list online				
			Total Credits	**GPA**

Graduate Studies Notes: