Information and Cybersecurity (CYBER)

Please note: CYBER courses are only available for Information and Cybersecurity (MICS) students.

Expand all course descriptions [+]Collapse all course descriptions [-]

CYBER W200 Beyond the Code: Cybersecurity in Context 3 Units

Terms offered: Spring 2020, Fall 2019, Summer 2019
This course explores the most important elements beyond technology that shape the playing field on which cybersecurity problems emerge and are managed. The course emphasizes how ethical, legal, and economic frameworks enable and constrain security technologies and policies. It introduces some of the most important macro-elements (such as national security considerations and interests of nation-states) and micro-elements (such as behavioral economic insights into how people understand and interact with security features). Specific topics include policymaking, business models, legal frameworks, national security considerations, ethical issues, standards making, and the roles of users, government, and industry.
Beyond the Code: Cybersecurity in Context: Read More [+]
Rules & Requirements

Prerequisites: MICS students only

Hours & Format

Fall and/or spring: 14 weeks - 3 hours of web-based lecture per week

Summer: 14 weeks - 3 hours of web-based lecture per week

Online: This is an online course.

Additional Details

Subject/Course Level: Information and Cybersecurity/Graduate

Grading: Letter grade.

Instructor: Hoofnagle

Beyond the Code: Cybersecurity in Context: Read Less [-]

CYBER W202 Cryptography for Cyber and Network Security 3 Units

Terms offered: Spring 2020, Fall 2019, Summer 2019
This course focuses on both mathematical and practical foundations of cryptography. The course discusses asymmetric and symmetric cryptography, Kerchkoff's Principle, chosen and known plaintext attacks, public key infrastructure, X.509, SSL/TLS (https), and authentication protocols. The course will include an in-depth discussion of many different cryptosystems including the RSA, Rabin, DES, AES, Elliptic Curve, and SHA family cryptosystems. This course also introduces advanced topics of applied cryptography, including a brief introduction to homomorphic encrypted computation and secure multi-party computation to protect sensitive data during arbitrary computation, cryptocurrency and its cryptographic building blocks, and quantum computing.
Cryptography for Cyber and Network Security: Read More [+]
Rules & Requirements

Prerequisites: MICS students only

Hours & Format

Fall and/or spring: 14 weeks - 3 hours of web-based lecture per week

Summer: 14 weeks - 3 hours of web-based lecture per week

Online: This is an online course.

Additional Details

Subject/Course Level: Information and Cybersecurity/Graduate

Grading: Letter grade.

Instructor: Tygar

Cryptography for Cyber and Network Security: Read Less [-]

CYBER W204 Software Security 3 Units

Terms offered: Spring 2020, Fall 2019, Summer 2019
The course presents the challenges, principles, mechanisms and tools to make software secure. We will discuss the main causes of vulnerabilities and the means to avoid and defend against them. The focus is on secure programming practice, including specifics for various languages, but also covering system-level defenses (architectural approaches and run-time enforcement). We will also apply software analysis and vulnerability detection tools in different scenarios.
Software Security: Read More [+]

Objectives Outcomes

Course Objectives: *Apply and manage secure coding practices throughout software project development

*Gain a good comprehension of the landscape of software security vulnerabilities, with specifics for various programming languages and types of software applications

*Gain the ability to analyze the security of a software system and convincingly advocate about the significance of vulnerabilities

*Know representative tools for software security analysis and testing, use them in practice and understand their capabilities and limitations

*Recognize insecure programming patterns and know how to replace them with secure alternatives

Student Learning Outcomes: Students will be able to apply and manage secure coding practices throughout software project development
Students will be able to recognize insecure programming patterns and know how to replace them with secure alternatives
Students will gain a good comprehension of the landscape of software security vulnerabilities, with specifics for various programming languages and types of software applications
Students will gain the ability to analyze the security of a software system and convincingly advocate about the significance of vulnerabilities
Students will know representative tools for software security analysis and testing, use them in practice and understand their capabilities and limitations

Rules & Requirements

Prerequisites: CYBER W202 must be taken prior to or concurrently with CYBER W204. Knowledge of at least one non-scripting programming language (e.g. C, C++, or Java); fundamental knowledge of information systems (review of operating systems notions). MICS students only

Hours & Format

Fall and/or spring: 14 weeks - 3 hours of web-based lecture per week

Summer: 14 weeks - 3 hours of web-based lecture per week

Online: This is an online course.

Additional Details

Subject/Course Level: Information and Cybersecurity/Graduate

Grading: Letter grade.

Software Security: Read Less [-]

CYBER W207 Applied Machine Learning for Cybersecurity 3 Units

Terms offered: Spring 2020, Fall 2019, Summer 2019
Machine learning is a rapidly growing field at the intersection of computer science and statistics concerned with finding patterns in data. It is responsible for tremendous advances in technology, from personalized product recommendations to speech recognition in cell phones. This course provides a broad introduction to the key ideas in machine learning, with a focus on applications and concepts relevant to cybersecurity. The emphasis will be on intuition and practical examples rather than theoretical results, though some experience with probability, statistics, and linear algebra will be important.
Applied Machine Learning for Cybersecurity: Read More [+]

Rules & Requirements

Prerequisites: Master of Information and Cybersecurity students only. Experience with probability and statistics. Intermediate competency in Python, C, or Java, and competency in Linux, GitHub, and relevant Python libraries; or permission of instructor. Linear algebra is recommended

Hours & Format

Fall and/or spring: 14 weeks - 3 hours of web-based lecture per week

Summer: 14 weeks - 3 hours of web-based lecture per week

Online: This is an online course.

Additional Details

Subject/Course Level: Information and Cybersecurity/Graduate

Grading: Letter grade.

Instructor: Gillick

Applied Machine Learning for Cybersecurity: Read Less [-]

CYBER W210 Network Security 3 Units

Terms offered: Spring 2020, Fall 2019, Summer 2019
Introduction to networking and security as applied to networks. Exercises cover network programming in a language of the student's choice, understanding and analyzing packet traces using tools like wireshark and mitmproxy, as well as applying security principles to analyze and determine network security. After this course, the student will have a fundamental understanding of networking, TLS and security as it applies to networked systems.
Network Security: Read More [+]

Rules & Requirements

Prerequisites: MICS students only. Basic understanding of internet network protocols

Hours & Format

Fall and/or spring: 14 weeks - 3 hours of web-based lecture per week

Summer: 14 weeks - 3 hours of web-based lecture per week

Online: This is an online course.

Additional Details

Subject/Course Level: Information and Cybersecurity/Graduate

Grading: Letter grade.

Network Security: Read Less [-]

CYBER W211 Operating System Security 3 Units

Terms offered: Spring 2020, Fall 2019
This survey of operating system security compares approaches to security taken among several modern operating systems. The course will teach how to conceptualize design issues, principles, and good practices in securing systems in today’s increasingly diverse and complex computing ecosystem, which extends from things and personal devices to enterprises, with processing increasingly in the cloud. We will approach operating systems individually and then build on them so that students learn techniques for establishing trust across a set of interoperating systems.
Operating System Security: Read More [+]

Rules & Requirements

Prerequisites: CYBER W200, CYBER W202, CYBER W204, and CYBER W210. Working knowledge of at least one object-oriented programming language and computer architecture (e.g. Intel x86-64bit). MICS students only

Hours & Format

Fall and/or spring: 14 weeks - 3 hours of web-based lecture per week

Summer: 14 weeks - 3 hours of web-based lecture per week

Online: This is an online course.

Additional Details

Subject/Course Level: Information and Cybersecurity/Graduate

Grading: Letter grade.

Operating System Security: Read Less [-]

CYBER W215 Usable Privacy and Security 3 Units

Terms offered: Spring 2020, Fall 2019
Security and privacy systems can be made more usable by designing them with the user in mind, from the ground up. In this course, you will learn many of the common pitfalls of designing usable privacy and security systems, techniques for designing more usable systems, and how to evaluate privacy and security systems for usability. Through this course, you will learn methods for designing software systems that are more secure because they minimize the potential for human error.
Usable Privacy and Security: Read More [+]
Rules & Requirements

Prerequisites: MICS students only. CYBER W200, CYBER W202

Hours & Format

Fall and/or spring: 14 weeks - 3 hours of web-based lecture per week

Summer: 14 weeks - 3 hours of web-based lecture per week

Online: This is an online course.

Additional Details

Subject/Course Level: Information and Cybersecurity/Graduate

Grading: Letter grade.

Usable Privacy and Security: Read Less [-]

CYBER W220 Managing Cyber Risk 3 Units

Terms offered: Summer 2019, Spring 2019
This course offers valuable perspective for both the non-technical business manager and the technical cybersecurity or IT manager. It is the vital connector between the technical world of threats, vulnerabilities, and exploits, and the business world of board-level objectives, enterprise risk management, and organizational leadership. Now more than ever, managers have a need and responsibility to understand cyber risk.
Just as financial risks and other operational risks have to be effectively managed within an organization, cyber risk has to be managed. It spans far beyond information technology, with broad implications in the areas of organizational behavior, financial risk modeling, legal issues, and executive leadership.
Managing Cyber Risk: Read More [+]
Objectives Outcomes

Student Learning Outcomes: Compare and employ approaches to cyber risk management and measurement.
Develop a basic cybersecurity strategic plan and understand how it aligns with the core business value of the company.
Navigate corporate structures to create a strong cyber security program and obtain senior leadership buy-in.
Understand security product verticals, identify common use cases for those products, and define requirements for acquiring solutions relevant to a business use case.
Understand the basic principles and best practices of responding to a cybersecurity incident

Rules & Requirements

Prerequisites: MICS students only

Hours & Format

Fall and/or spring: 14 weeks - 3 hours of web-based lecture per week

Summer: 14 weeks - 3 hours of web-based lecture per week

Online: This is an online course.

Additional Details

Subject/Course Level: Information and Cybersecurity/Graduate

Grading: Letter grade.

Managing Cyber Risk: Read Less [-]

CYBER W233 Privacy Engineering 3 Units

Terms offered: Spring 2020, Summer 2019, Spring 2019
This course surveys privacy mechanisms applicable to systems engineering, with a particular focus on the inference threat arising due to advancements in artificial intelligence and machine learning. We will briefly discuss the history of privacy and compare two major examples of general legal frameworks for privacy from the United States and the European Union. We then survey three design frameworks of privacy that may be used to guide the design of privacy-aware information systems. Finally, we survey threat-specific technical privacy frameworks and discuss their applicability in different settings, including statistical privacy with randomized responses, anonymization techniques, semantic privacy models, and technical privacy mechanisms.
Privacy Engineering: Read More [+]
Objectives Outcomes

Student Learning Outcomes: Students should be able to implement such privacy paradigms, and embed them in information systems during the design process and the implementation phase.
Students should be familiar with the different technical paradigms of privacy that are applicable for systems engineering.
Students should develop critical thinking about the strengths and weaknesses of the different privacy paradigms.
Students should possess the ability to read literature in the field to stay updated about the state of the art.

Rules & Requirements

Prerequisites: MICS students only; or, permission of instructor

Hours & Format

Fall and/or spring: 14 weeks - 3 hours of web-based lecture per week

Summer: 14 weeks - 3 hours of web-based lecture per week

Online: This is an online course.

Additional Details

Subject/Course Level: Information and Cybersecurity/Graduate

Grading: Letter grade.

Privacy Engineering: Read Less [-]

CYBER W242 Government, National Security, and the Fifth Domain 3 Units

Terms offered: Summer 2019
A variety of actors exploit government and private networks, systems, and data. Perpetrators target these systems to engage in cybercrime, espionage, disinformation campaigns, disruption of essential services, destruction of critical infrastructure, and the deletion, theft, or alteration of data. The government, military, and private sector have various roles and responsibilities with regard to the protection of the cyber domain. In this course, students critically evaluate these roles and responsibilities, the manner in which government networks, systems, and data are secured, and the ability of national and international cybersecurity strategies and partnerships to provide effective and efficient protection of the fifth domain.
Government, National Security, and the Fifth Domain: Read More [+]
Objectives Outcomes

Student Learning Outcomes: Critically assess national and international cybersecurity strategies
Describe and evaluate national and international public-private partnerships.
Discuss the fifth domain and its protection within the context of national security.
Identify lessons learned and recommend ways to improve national and international approaches to cybersecurity.
Identify the roles and responsibilities of the military, government, and the private sector in cybersecurity.
Utilize an evidence-based approach to analyze the security of government networks and systems and privacy of retained data.

Rules & Requirements

Prerequisites: MICS students only. CYBER W200, CYBER W202

Hours & Format

Fall and/or spring: 14 weeks - 3 hours of web-based lecture per week

Summer: 14 weeks - 3 hours of web-based lecture per week

Online: This is an online course.

Additional Details

Subject/Course Level: Information and Cybersecurity/Graduate

Grading: Letter grade.

Government, National Security, and the Fifth Domain: Read Less [-]

CYBER W289 Public Interest Cybersecurity: The Citizen Clinic Practicum 3 Units

Terms offered: Summer 2019

This course provides students with real-world experience assisting politically vulnerable organizations and persons around the world to develop and implement sound cybersecurity practices. In the classroom, students study basic theories and practices of digital security, intricacies of protecting largely under-resourced organizations, and tools needed to manage risk in complex political, sociological, legal, and ethical contexts. In the clinic, students work in teams supervised by Clinic staff to provide direct cybersecurity assistance to civil society organizations. We emphasize pragmatic, workable solutions that take into account the unique needs of each partner organization.

Public Interest Cybersecurity: The Citizen Clinic Practicum: Read More [+]

Rules & Requirements

Prerequisites: Master of Information and Cybersecurity students only

Hours & Format

Summer: 14 weeks - 6 hours of clinic and 3 hours of web-based lecture per week

Online: This is an online course.

Additional Details

Subject/Course Level: Information and Cybersecurity/Graduate

Grading: Letter grade.

Instructor: Weber

Public Interest Cybersecurity: The Citizen Clinic Practicum: Read Less [-]

CYBER W295 Capstone 3 Units

Terms offered: Spring 2020, Fall 2019

This capstone course will cement skills and knowledge learned throughout the Master of Information and Cybersecurity program: core cybersecurity technical skills, understanding of the societal factors that impact the cybersecurity domain and how cybersecurity issues impact humans, and professional skills such as problem-solving, communication, influencing, collaboration, and group management – to prepare students for success in the field. The centerpiece is a semester-long group project in which teams of students propose and select a complex cybersecurity issue and apply multi-faceted analysis and problem-solving to identify, assess, and manage risk and deliver impact.

Capstone: Read More [+]

Objectives Outcomes

Student Learning Outcomes: Engage in a highly collaborative process of idea generation, information sharing, and feedback that replicates key aspects of managing cybersecurity in an organizational setting.
Learn or reinforce communication, influencing, and management skills.
Practice using multi-faceted problem-solving skills to address complex cybersecurity issues.

Rules & Requirements

Prerequisites: CYBER W200, CYBER W202, and CYBER W204. MICS students only. Must be taken in final term of the MICS program

Hours & Format

Fall and/or spring: 14 weeks - 1.5 hours of web-based lecture and 1.5 hours of web-based discussion per week

Summer: 14 weeks - 1.5 hours of web-based lecture and 1.5 hours of web-based discussion per week

Online: This is an online course.

Additional Details

Subject/Course Level: Information and Cybersecurity/Graduate

Grading: Letter grade.

Capstone: Read Less [-]

CYBER 298 Directed Group Study in Cybersecurity 1 - 4 Units

Terms offered: Prior to 2007

This course provides an opportunity for graduate students to work on group projects in special topics in cybersecurity under the direction of an instructor. Students meet regularly with the instructor to scope the project, define final deliverables, identify relevant readings, identify content areas necessary to master in order to complete the project, and discuss progress.

Directed Group Study in Cybersecurity: Read More [+]

Rules & Requirements

Prerequisites: Master of Information and Cybersecurity students only; consent of instructor

Repeat rules: Course may be repeated for credit when topic changes. Students may enroll in multiple sections of this course within the same semester.

Hours & Format

Fall and/or spring: 14 weeks - 2-5 hours of directed group study per week

Summer: 14 weeks - 2-5 hours of directed group study per week

Additional Details

Subject/Course Level: Information and Cybersecurity/Graduate

Grading: Letter grade.

Directed Group Study in Cybersecurity: Read Less [-]

CYBER 299 Individual Study in Cybersecurity 1 - 12 Units

Terms offered: Prior to 2007

This course provides an opportunity for graduate students to work individually on special topics in cybersecurity under the direction of an instructor. Students meet regularly with the instructor to scope the project, define final deliverables, identify relevant readings, identify content areas necessary to master in order to complete the project, and discuss progress.

Individual Study in Cybersecurity: Read More [+]

Rules & Requirements

Prerequisites: Master of Information and Cybersecurity students only; consent of instructor

Repeat rules: Course may be repeated for credit when topic changes. Students may enroll in multiple sections of this course within the same semester.

Hours & Format

Fall and/or spring: 14 weeks - 2-13 hours of independent study per week

Summer: 14 weeks - 2-13 hours of independent study per week

Additional Details

Subject/Course Level: Information and Cybersecurity/Graduate

Grading: Letter grade.

Individual Study in Cybersecurity: Read Less [-]