Cybersecurity

School of Interdisciplinary Informatics, College of Information, Science, and Technology

Vision Statement
The School of Interdisciplinary Informatics (SII) is the academic home of the Master of Science (MS) in Cybersecurity (previously Information Assurance). Cybersecurity is a rapidly expanding, multi-faceted science that integrates a diverse set of disciplines to address fundamental problems in the design, development, implementation and support of secure information systems. The Master of Science is a full graduate degree program balancing theory with practice in order to provide students with the knowledge and skills necessary to protect information systems. Because of the wide variety of subject areas to which Cybersecurity can be applied, this degree program has two paths; Cyber Operations, a concentration with highly technical content, and Interdisciplinary, with the opportunity for the students to tailor the degree to specific management goals. Students may also choose between a thesis or capstone exit option based on their individual interests.

Program Contact Information
Dr. William Mahoney, Graduate Program Chair (GPC)
Peter Kiewit Institute (PKI) 282F
402-554-3975
wmahoney@unomaha.edu

Ms. Leslie Planos, Advisor
Peter Kiewit Institute (PKI) 176C
402-554-3819
lplanos@unomaha.edu


Admissions
Application Deadlines
• Fall: July 1
• Spring: December 1
• Summer: April 1

Program-Specific Requirements
1. All applicants must have the equivalent of a 4-year undergraduate degree.
2. International applicants without a baccalaureate or equivalent degree from an English-speaking institution of higher education in the US, the United Kingdom, Canada, English-speaking Africa, Australia, Ireland or New Zealand are required to submit TOEFL scores.
   a. Paper-based TOEFL: 550
   b. Computer-based TOEFL: 213
   c. Internet-based TOEFL: 80
   d. IELTS: 6.5
   e. PTE: 53
3. International applicants without a baccalaureate or equivalent degree from an English-speaking institution of higher education in the US, the United Kingdom, Canada, English-speaking Africa, Australia, Ireland or New Zealand are required to submit GRE scores. There is no minimum GRE requirement, but for international applicants the score will be one factor used in evaluating the student’s portfolio.
4. Three (3) letters of recommendation from references who can evaluate your work and/or academic achievements
5. Writing Sample from work or previous academic experiences.
   Alternatively, if you do not have a writing sample, please submit a two-page double-spaced word-processed essay that addresses the following two topics:
   a. Discussion of two accomplishments that demonstrate your potential for success in the graduate program
   b. Discussion of your unique personal qualities and life experiences that distinguish you from other applicants to this graduate program
6. Resume
   • Include your work experience and background
7. OPTIONAL: Interview
   • Although not required, the Graduate Program Committee may ask to conduct a telephone interview to further assess the experiences of the applicant.

Requirements
Foundation Courses
Foundation courses ensure that all students in the degree have a solid groundwork upon which to build the rest of the program. These courses not only provide essential prerequisite knowledge and skills for other courses in the program, but they also contain a distinct body of knowledge that is an important part of the cybersecurity professional’s education. All foundation courses are required for all students, however, students who have obtained an undergraduate degree in a related field may already have this foundation. In such a case, most, if not all, foundation courses are waived. Students with undergraduate degrees in other disciplines, including Computer Science, Management Information Systems, or Engineering, will usually require one or more foundation courses. Occasionally, a student’s work experience may be sufficient to waive one or more of the foundation courses.

Waivers for foundation courses are potentially granted by the Graduate Program Committee upon the recommendation of the faculty member who is responsible for an individual course. Students requesting a waiver for a particular course should be prepared to meet with a faculty member and answer questions in the area of the course. They should bring to the meeting any relevant transcripts, course syllabi, course material, or evidence of practical experience. Some foundation courses may have an option for testing out.

Foundation courses cannot be used to satisfy the 33 semester hours required for the MS in CYBR degree. Students who have not completed all the foundation course requirements may be admitted on a provisional status until those requirements have been completed. All foundation courses must be completed prior to or concurrent with the first six (6) hours of MS in CYBR graduate coursework.

Foundation Requirements
(9 hours if not waived)

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCI 2240</td>
<td>INTRODUCTION TO C PROGRAMMING</td>
<td>3</td>
</tr>
<tr>
<td>or CYBR 2250</td>
<td>LOW-LEVEL PROGRAMMING</td>
<td></td>
</tr>
<tr>
<td>CSCI 3550</td>
<td>COMMUNICATION NETWORKS</td>
<td>3</td>
</tr>
</tbody>
</table>
### Degree Requirements

#### Capstone Option

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>CYBR 8366</td>
<td>FOUNDATIONS OF INFORMATION ASSURANCE</td>
<td>3</td>
</tr>
<tr>
<td>CYBR 8410</td>
<td>DISTRIBUTED SYSTEMS AND NETWORK SECURITY</td>
<td>3</td>
</tr>
<tr>
<td>CYBR 8420</td>
<td>SOFTWARE ASSURANCE</td>
<td>3</td>
</tr>
<tr>
<td>CYBR 8386</td>
<td>COMPUTER AND NETWORK FORENSICS</td>
<td>3</td>
</tr>
</tbody>
</table>

Total Credits: 9

#### Concentration

Select a concentration 18

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>CYBR 8950</td>
<td>GRADUATE CAPSTONE IN INFORMATION ASSURANCE</td>
<td>3</td>
</tr>
</tbody>
</table>

Total Credits: 33

### Thesis Option

#### Core Courses

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>CYBR 8366</td>
<td>FOUNDATIONS OF INFORMATION ASSURANCE</td>
<td>3</td>
</tr>
<tr>
<td>CYBR 8410</td>
<td>DISTRIBUTED SYSTEMS AND NETWORK SECURITY</td>
<td>3</td>
</tr>
<tr>
<td>CYBR 8420</td>
<td>SOFTWARE ASSURANCE</td>
<td>3</td>
</tr>
<tr>
<td>CYBR 8386</td>
<td>COMPUTER AND NETWORK FORENSICS</td>
<td>3</td>
</tr>
</tbody>
</table>

Concentration Select a concentration 15

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>CYBR 8990</td>
<td>THESIS IN INFORMATION ASSURANCE</td>
<td>6</td>
</tr>
</tbody>
</table>

Total Credits: 33

Exit Requirements:

- Capstone 3 Credits CYBR 8950
- Thesis 6 Credits CYBR 8990
  - All candidates should carefully review the Graduate College requirements for forming the Supervisory Committee, Thesis/Thesis Equivalent Proposal Approval Forms, and final approval and submission of the thesis.

### Interdisciplinary Concentration

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISQA 8060</td>
<td>RESEARCH IN MIS</td>
<td></td>
</tr>
<tr>
<td>ISQA 8080</td>
<td>SEMINAR IN MANAGEMENT INFORMATION SYSTEMS</td>
<td></td>
</tr>
<tr>
<td>ISQA 8530</td>
<td>E-COMMERCE SECURITY</td>
<td></td>
</tr>
<tr>
<td>ISQA 8546</td>
<td>COMPUTER SECURITY MANAGEMENT</td>
<td></td>
</tr>
<tr>
<td>ISQA 8560</td>
<td>INFORMATION WARFARE AND SECURITY</td>
<td></td>
</tr>
<tr>
<td>ISQA/CYBR 8570</td>
<td>INFORMATION SECURITY POLICY AND ETHICS</td>
<td></td>
</tr>
<tr>
<td>ISQA 8580</td>
<td>SECURITY RISK MANAGEMENT AND ASSESSMENT</td>
<td></td>
</tr>
<tr>
<td>ISQA 8596</td>
<td>IT AUDIT AND CONTROL</td>
<td></td>
</tr>
<tr>
<td>CSCI 8340</td>
<td>DATABASE MANAGEMENT SYSTEMS II</td>
<td></td>
</tr>
<tr>
<td>CSCI 8430</td>
<td>TRUSTED SYSTEM DESIGN, ANALYSIS AND DEVELOPMENT</td>
<td></td>
</tr>
<tr>
<td>CSCI 8530</td>
<td>ADVANCED OPERATING SYSTEMS</td>
<td></td>
</tr>
<tr>
<td>CSCI/MATH 8566</td>
<td>NUMBER THEORY &amp; CRYPTOGRAPHY</td>
<td></td>
</tr>
<tr>
<td>CSCI 8610</td>
<td>FAULT TOLERANT DISTRIBUTED SYSTEMS</td>
<td></td>
</tr>
<tr>
<td>CYBR 8080</td>
<td>SPECIAL TOPICS IN INFORMATION ASSURANCE</td>
<td></td>
</tr>
<tr>
<td>CYBR 8900</td>
<td>INDEPENDENT STUDY IN INFORMATION ASSURANCE</td>
<td></td>
</tr>
</tbody>
</table>

Total Credits: 18

#### Electives

Select 18 hours from the following:

- ISQA 8060: RESEARCH IN MIS
- ISQA 8080: SEMINAR IN MANAGEMENT INFORMATION SYSTEMS
- ISQA 8530: E-COMMERCE SECURITY
- ISQA 8546: COMPUTER SECURITY MANAGEMENT
- ISQA 8560: INFORMATION WARFARE AND SECURITY
- ISQA/CYBR 8570: INFORMATION SECURITY POLICY AND ETHICS
- ISQA 8580: SECURITY RISK MANAGEMENT AND ASSESSMENT
- ISQA 8596: IT AUDIT AND CONTROL
- CSCI 8340: DATABASE MANAGEMENT SYSTEMS II
- CSCI 8430: TRUSTED SYSTEM DESIGN, ANALYSIS AND DEVELOPMENT
- CSCI 8530: ADVANCED OPERATING SYSTEMS
- CSCI/MATH 8566: NUMBER THEORY & CRYPTOGRAPHY
- CSCI 8610: FAULT TOLERANT DISTRIBUTED SYSTEMS
- CYBR 8080: SPECIAL TOPICS IN INFORMATION ASSURANCE
- CYBR 8900: INDEPENDENT STUDY IN INFORMATION ASSURANCE
- CYBR 8910: INTERNSHIP

Total Credits: 33

### Thesis Option

#### Cyber Operations Concentration

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>CYBR 8446</td>
<td>INDUSTRIAL CONTROL SYSTEM SECURITY</td>
<td>3</td>
</tr>
<tr>
<td>CYBR 8456</td>
<td>HOST-BASED VULNERABILITY DISCOVERY</td>
<td>3</td>
</tr>
<tr>
<td>CYBR 8466</td>
<td>NETWORK-BASED VULNERABILITY DISCOVERY</td>
<td>3</td>
</tr>
</tbody>
</table>

Electives

Select 15 hours from the following:

- CYBR 8446: INDUSTRIAL CONTROL SYSTEM SECURITY
- CYBR 8456: HOST-BASED VULNERABILITY DISCOVERY
- CYBR 8466: NETWORK-BASED VULNERABILITY DISCOVERY
- CYBR 8450: APPLIED CRYPTOGRAPHY
- CYBR 8460: SECURITY OF EMBEDDED SYSTEMS
- CYBR 8470: SECURE WEB APPLICATION DEVELOPMENT
- CSCI 8430: TRUSTED SYSTEM DESIGN, ANALYSIS AND DEVELOPMENT
- CYBR 8080: SPECIAL TOPICS IN INFORMATION ASSURANCE

Total Credits: 33

Exit Requirements:

- Capstone 3 Credits CYBR 8950
- Thesis 6 Credits CYBR 8990
  - All candidates should carefully review the Graduate College requirements for forming the Supervisory Committee, Thesis/Thesis Equivalent Proposal Approval Forms, and final approval and submission of the thesis.
In particular, the GPC will recommend to the Graduate College that any foundation courses as well as courses taken as part of the degree program. The Graduate College’s Quality of Work Standards shall be applied to courses completed in this program.

### Interdisciplinary Concentration

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Electives</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Select 15 hours from the following:</td>
<td>15</td>
</tr>
<tr>
<td>ISQA 8060</td>
<td>RESEARCH IN MIS</td>
<td>1-3</td>
</tr>
<tr>
<td>ISQA 8080</td>
<td>SEMINAR IN MANAGEMENT INFORMATION SYSTEMS</td>
<td>1-3</td>
</tr>
<tr>
<td>ISQA 8530</td>
<td>E-COMMERCE SECURITY</td>
<td></td>
</tr>
<tr>
<td>ISQA 8546</td>
<td>COMPUTER SECURITY MANAGEMENT</td>
<td></td>
</tr>
<tr>
<td>ISQA 8560</td>
<td>INFORMATION WARFARE AND SECURITY</td>
<td></td>
</tr>
<tr>
<td>ISQA/CYBR 8570</td>
<td>INFORMATION SECURITY POLICY AND ETHICS</td>
<td></td>
</tr>
<tr>
<td>ISQA 8580</td>
<td>SECURITY RISK MANAGEMENT AND ASSESSMENT</td>
<td></td>
</tr>
<tr>
<td>CSCI 8340</td>
<td>DATABASE MANAGEMENT SYSTEMS II</td>
<td></td>
</tr>
<tr>
<td>CSCI 8430</td>
<td>TRUSTED SYSTEM DESIGN, ANALYSIS AND DEVELOPMENT</td>
<td></td>
</tr>
<tr>
<td>CSCI 8530</td>
<td>ADVANCED OPERATING SYSTEMS</td>
<td></td>
</tr>
<tr>
<td>CSCI/MATH 8566</td>
<td>NUMBER THEORY &amp; CRYPTOGRAPHY</td>
<td></td>
</tr>
<tr>
<td>CSCI 8610</td>
<td>FAULT TOLERANT DISTRIBUTED SYSTEMS</td>
<td></td>
</tr>
<tr>
<td>CYBR 8080</td>
<td>SPECIAL TOPICS IN INFORMATION ASSURANCE</td>
<td></td>
</tr>
<tr>
<td>CYBR 8900</td>
<td>INDEPENDENT STUDY IN INFORMATION ASSURANCE</td>
<td></td>
</tr>
<tr>
<td>CYBR 8910</td>
<td>INTERNSHIP</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Total Credits</strong></td>
<td>15</td>
</tr>
</tbody>
</table>

1. **ISQA 8060** is strongly recommended as an elective for students considering the thesis option.

### Quality of Work Standards

The Graduate College’s Quality of Work Standards shall be applied to foundation courses as well as courses taken as part of the degree program. In particular, the GPC will recommend to the Graduate College that any foundation courses will be followed by the Graduate College’s Quality of Work Standards.

1. A student receiving a grade of “C” or below on any foundation course will be placed on probation or dismissed from the program.
2. A student receiving a grade of “C-” or “C” in any foundation course will be placed on probation or dismissed from the program.
3. A student not maintaining a “B” (3.0 on a 4.0 scale) average in foundation courses will be placed on probation or dismissed from the program.

### Cybersecurity

#### CYBR 8000 CENTER OF ACADEMIC EXCELLENCE-CYBER OPERATIONS COMPLETION CERTIFICATE (0 credits)
This course is utilized to provide a specific designation for students that have completed the Center of Academic Excellence - Cyber Operations coursework. It is a zero credit hour class used to designate the completion of this focus area in the cybersecurity curriculum.

**Prerequisite(s)/Corequisite(s):** Instructor Permission. The program committee will work with the UG advisors to ascertain that the student has fulfilled all requirements for this designation - if he/she has or will within the last semester, they will be allowed to register for this class.

#### CYBR 8080 SPECIAL TOPICS IN INFORMATION ASSURANCE (1-6 credits)
The course provides a format for exploring advanced research areas for graduate students in Information Assurance and related fields. Specific topics vary, in keeping with research interests of faculty and students. Examples include applied data mining, mobile security, web services and applications, vulnerability assessments, cloud computing security, and other issues in Information Assurance research.

**Prerequisite(s)/Corequisite(s):** Instructor Permission.

#### CYBR 8366 FOUNDATIONS OF INFORMATION ASSURANCE (3 credits)
Contemporary issues in computer security, including sources for computer security threats and appropriate reactions; basic encryption and decryption; secure encryption systems; program security, trusted operating systems; database security, network and distributed systems security, administering security; legal and ethical issues. (Cross-listed with CYBR 4360, CSCI 8366)

**Prerequisite(s)/Corequisite(s):** CSCI 3320 or CSCI 8325 or ISQA 3300 or OR By instructor permission

#### CYBR 8386 COMPUTER AND NETWORK FORENSICS (3 credits)
Computer forensics involves the preservation, identification, extraction and documentation of computer evidence stored on a computer. This course takes a technical, legal, and practical approach to the study and practice of incident response, computer forensics, and network forensics. Topics include legal and ethical implications, duplication and data recovery, steganography, network forensics, and tools and techniques for investigating computer intrusions. This course is intended as a second course in information assurance for undergraduate students as well as other qualified students. It is also intended as a foundation course for graduate digital forensics studies. (Cross-listed with CYBR 4380, CSCI 4380)

**Prerequisite(s)/Corequisite(s):** CYBR 1100, CIST 3600, CSCI 3500 or ISQA 3400, CYBR 3350 or CYBR 3370; or instructor permission.

#### CYBR 8410 DISTRIBUTED SYSTEMS AND NETWORK SECURITY (3 credits)
The course aims at understanding the issues surrounding data security, integrity, confidentiality and availability in distributed systems. Further, we will discuss various network security issues, threats that exist and strategies to mitigate them. This course will cover topics in cryptography, public key infrastructure, authentication, hashing, digital signatures, ARP protection, IP and IPSEC, IP Tables, SSL/TLS, firewalls, etc. (Cross-listed with CSCI 8410)

**Prerequisite(s)/Corequisite(s):** IASC 8366 or equivalent(s); or instructor permission. Not open to non-degree graduate students.
CYBR 8420  SOFTWARE ASSURANCE (3 credits)
Software assurance is a reasoned, auditable argument created to support the belief that the software will operate as expected. This course is an intersection of knowledge areas necessary to perform engineering activities or aspects of activities relevant for promoting software assurance. This course takes on a software development lifecycle perspective for the prevention of flaws. (Cross-listed with CSCI 8420)
Prerequisite(s)/Corequisite(s): CSCI 4830 or CSCI 8836 OR by permission of the Instructor. Not open to non-degree graduate students.

CYBR 8436  QUANTUM COMPUTING AND CRYPTOGRAPHY (3 credits)
The course aims at understanding the exciting concepts behind quantum computing and quantum cryptography. The course will introduce the principles of qubits, superposition, entanglement, teleportation, measurement, quantum error correction, quantum algorithms such as quantum Fourier transformation, Shor’s algorithm and Grover’s algorithm, quantum key exchange, quantum encryption, and secure quantum channels that built using these principles. We will discuss the security definitions and protocols within the quantum realm. We will discuss what advantages. (Cross-listed with CYBR 4430).
Prerequisite(s)/Corequisite(s): Co-requisites: CYBR 3570 or CSCI 4560; or Instructor permission.

CYBR 8440  SECURE SYSTEMS ENGINEERING (3 credits)
This course takes a global risk-based view of the process of defining, verifying, validating and continuously monitoring secure information systems. The course will investigate a number of secure system solutions, starting with the definition of the system security needs, and tracing through methods of verification and validation of security controls, as well as ways to continuously monitor the corresponding assurances. (Cross-listed with CYBR 4440)
Prerequisite(s)/Corequisite(s): CSCI 8366 or IASC 8366.

CYBR 8446  INDUSTRIAL CONTROL SYSTEM SECURITY (3 credits)
The objective of this course is to research vulnerabilities into, and provide guidance for securing, industrial control systems (ICS). ICS is a general term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system items such as Programmable Logic Controllers (PLC). The student will learn to identify network and device vulnerabilities and potential countermeasures to these weaknesses. (Cross-listed with CYBR 4440)
Prerequisite(s)/Corequisite(s): CSCI 3550.

CYBR 8450  APPLIED CRYPTOGRAPHY (3 credits)
In this course we will implement stream and block ciphers in different modes, public key algorithms, hash functions, message authentication codes, random number generators, etc. Along the way we will also explore weaknesses of these algorithms and implement well-known attacks on them. We will also solve crypto challenges and puzzles. This is a hand-on course and will require programming proficiency. The preferred language will be Python; you can, however, use other object oriented languages.
Prerequisite(s)/Corequisite(s): CSCI 2030, CSCI 3320, CYBR 3570 or equivalent or Instructor Permission.

CYBR 8456  HOST-BASED VULNERABILITY DISCOVERY (3 credits)
The class will cover security issues at an implementation and hardware level. The students will learn assembly language and the use of a reverse assembler and debugger. This will allow the student to analyze various “packing” algorithms for computer viruses, the viruses themselves, operating system “hooking”, “fuzzing”, and other machine code, host-based exploits. The class will be using both Windows and Linux as operating systems. (Cross-listed with CYBR 4450.)
Prerequisite(s)/Corequisite(s): Permission of the instructor and CSCI 3710.

CYBR 8460  SECURITY OF EMBEDDED SYSTEMS (3 credits)
An embedded system is some combination of computer hardware and software, either fixed in capability or programmable, which is specifically designed for a particular function. Industrial machines, automobile electronic systems, medical equipment, cameras, household appliances, airplanes, vending machines, cellular phones and PDAs are among the myriad possible hosts of an embedded system. This class concerns itself with the security aspects of these often computationally restricted computing platforms
Prerequisite(s)/Corequisite(s): IASC 8366, CYBR 4450 or CYBR 8456.

CYBR 8466  NETWORK-BASED VULNERABILITY DISCOVERY (3 credits)
The course is an advanced class in which the students learn various techniques for testing for and identifying security flaws in network software and web applications. Internet technologies such as HTTP, DNS, DHCP, and others are examined in the context of cyber security. Students are expected to participate in numerous hands-on experiments related to Information Assurance with respect to web technologies. (Cross-listed with CYBR 4460)
Prerequisite(s)/Corequisite(s): Instructor Permission

CYBR 8470  SECURE WEB APPLICATION DEVELOPMENT (3 credits)
Web applications are pervasive fixtures of 21st century culture. Web application security is an inclusive, amorphous, term that spans application level security, i.e. ensuring high level code cannot be exploited, server level security, i.e. ensuring server resources such as databases and file systems cannot be exploited, and network security, i.e. ensuring unauthorized parties cannot access a server or tamper with user sessions. This course cross-cuts the web application security concepts across the different categories above and takes a heavily hands-on approach to introduce students to the world of secure web app. design and development.
Prerequisite(s)/Corequisite(s): Instructor Permission

CYBR 8546  COMPUTER SECURITY MANAGEMENT (3 credits)
The purpose of this course is to integrate concepts and techniques from security assessment, risk mitigation, disaster planning, and auditing to identify, understand, and propose solutions to problems of computer security and security administration. (Cross-listed with CIST 4540, CYBR 4540, ISQA 8546)
Prerequisite(s)/Corequisite(s): IASC 4360 or permission of the instructor.

CYBR 8570  INFORMATION SECURITY POLICY AND ETHICS (3 credits)
The course will cover the development and need for information security policies, issues regarding privacy, and the application of computer ethics. (Cross-listed with ISQA 8570)
Prerequisite(s)/Corequisite(s): CIST 2100 or BSAD 8030, or permission of instructor.
CYBR 8900 INDEPENDENT STUDY IN INFORMATION ASSURANCE (1-3 credits)
The course provides a format for exploring advanced research areas for graduate students in Information Assurance and related fields. The class is designed for students that would like to explore specific Information Assurance topics at a greater depth, or topics that are not currently a part of the IA curriculum. The class is proposed and organized by the student, with participating faculty mentoring.

Prerequisite(s)/Corequisite(s): Instructor Permission

CYBR 8910 INTERNSHIP (1-3 credits)
The purpose of this course is to provide the students with an opportunity for practical application and further development of knowledge and skills acquired in the MS in CyberSecurity (CYBR) program. The internship gives students professional work experience and exposure to the challenges and opportunities faced by IT professionals in the workplace.

Prerequisite(s)/Corequisite(s): Students must have completed a minimum of 12 credit hours towards the MS in CYBR program. Instructor permission is required to register. Not open to non-degree graduate students.

CYBR 8950 GRADUATE CAPSTONE IN INFORMATION ASSURANCE (3 credits)
This is the graduate capstone course where students extend and apply their knowledge in defining, implementing, and assessing secure information systems. Students will demonstrate their ability to specify, apply, and assess different types of countermeasures at different points in the enterprise with a special focus on system boundaries. Students will complete and defend a Certification and Accreditation package. This course is intended for graduate students in the MS in IA degree program, coursework option, that are close to graduation (see prerequisites). This course replaces the MS in IA comprehensive examination requirement.

Prerequisite(s)/Corequisite(s): CYBR 8366, CYBR 8410, and CYBR 8456 and concentration area (systems or management and policy). Students must have 6 credit hours or less left in the program.

CYBR 8986 SPECIAL TOPICS IN INFORMATION ASSURANCE (1-3 credits)
The course provides a format for exploring advanced research areas for undergraduate students in Information Assurance and related fields. Specific topics vary, in keeping with research interests of faculty and students. Examples include applied data mining, mobile security, web services and applications, vulnerability assessments, cloud computing security, and other issues in Information Assurance research. (Cross-listed with CYBR 4980)

Prerequisite(s)/Corequisite(s): Instructor Permission.

CYBR 8990 THESIS IN INFORMATION ASSURANCE (1-6 credits)
A research project, designed and executed under the supervision of the chair and approval by members of the graduate student’s thesis advisory committee. In this project the student will develop and perfect a number of skills including the ability to design, conduct, analyze and report the results in writing (i.e., thesis) of an original, independent scientific investigation.

Prerequisite(s)/Corequisite(s): Instructor Permission.