Computer Crime & Forensics

Professor Mich Kabay; Associate Professors David Blythe, Jeremy Hansen, and Huw Read; Assistant Professor Susan Helser; Lecturers Matthew Bovee and Kris Rowley.

Cybercrime is a pervasive threat and the organizational demand for individuals capable of providing collaboration and support in dealing with this threat continues to grow. To prepare students from a variety of disciplines with the foundational study for this demand, the Computer Crime and Forensics minor provides a background in criminal justice and digital forensics, as well as computer science, computer programming, and information assurance. Students wishing to pursue the minor must obtain the approval of the School Director and complete each of the required courses with a grade of C or higher.

Goals:

To develop in students:

- An understanding and appreciation of the fundamentals of computer science, cybersecurity, and information assurance;
- Knowledge and basic facility with a high-level programming language;
- A foundation of understanding and skills in digital forensics and cyber-investigation;
- The foundation for practical work and further study in information assurance, cyberlaw, and digital forensics;
- Understanding of the constraints, legal procedures, and multi-jurisdictional nature and scope, of digital incidents and the responses to them; and,
- The ability to identify, think critically, analyze, and solve, cybercrime and cyberlaw problems.

Outcomes:

Upon graduation successful students will competently demonstrate:

- Use of the fundamental concepts and terminology regarding computers, computer security, and information assurance;
- Application of the essential cybercrime and digital forensic concepts, techniques and procedures;
- Ability to recognize, define, and use, the technical terminology of information assurance (IA);
- Application of the fundamentals of information assurance in both personal and organizational contexts;
- A breadth of knowledge, and the ability to apply it, regarding cyberlaw and cybercrime, including: identifying and classifying cybercrimes; the motivations of cybercriminals; seizure and handling of digital evidence; admissibility of digital incident evidence; preparing and delivering professional testimony; and, the key regulations and laws regarding cyber crimes of varying types and jurisdictions; and,
- High ethical, personal and professional standards, especially in regards to information assurance and its impact on individuals, organizations, and society.

Careers for this Minor:

Computers and mobile phones are now common tools used in the commission of ordinary crime, and the frequency, magnitude, and scope, of cybercrimes have increased dramatically. The Computer Crime & Forensics minor prepares students with the following career paths to better deal with them:

- Attorneys
- Crime Analysts
- Federal, state and local law enforcement
- Federal intelligence agents
- Private security personnel
- Probation and parole officers

Computer Crime and Forensics Minor Curriculum Map 2017-2018 Catalog

Students must complete all of the six courses listed below, each with a grade of C or higher.

CJ 301	Criminal Procedure	3
CJ 341	Cyber Law and Cyber Crime [1]	3
CS 140	Programming and Computing [2]	4
IA 340	Introduction to Information Assurance [3]	3
DF 395	Cyber Criminalistics [4]	3
CJ 423	Evidence [5]	3
Total Cr.		19

1 Cross-listed as IA 241; Prerequisite: CJ 101 or instructor permission
2 Prerequisite: C or higher in IS 100 or CS 100, or instructor permission
3 Prerequisite: C or higher in IS 131 or CS 140, or instructor permission
4 Open to CJ 2nd semester sophomores or higher, or by instructor permission
5 Offered every other year. Open only to juniors and seniors. Prerequisites: CJ 101 and CJ 102

Computer Science Courses

CS 100 Foundations of Computer Science and Information Assurance 3 Cr.
This survey of computing and information assurance fundamentals is required for computer science and information assurance majors. The course focuses on learning to use key concepts and terminology in information technology, computer science, networking, and information security. Discussions regarding computing ethics, safety, and professionalism are included throughout. Prerequisites: By permission only for non-computer science and non-CSIA majors.

CS 120 Business Applications & Problem Solving Techniques 3 Cr.
An introductory course in management information processing. The course explores the most important aspects of information systems with specific emphasis on business applications, practical usage, and current information. The student will obtain skills in word processing, spreadsheet analysis, and presentation tools using professional software packages. Structured problem-solving techniques will be emphasized throughout the course. Practical implementation projects and case studies will be used to reinforce topics such as computer, academic, and professional ethics for an information-based society. Not open to CS or CSIA majors.

CS 140 Programming and Computing 4 Cr.
An introduction to fundamental computing concepts and programming, designed for students with little programming background. The course uses a high-level language and emphasizes object-oriented design and implementation techniques. Good software engineering practice and language-specific concepts are introduced by means of programming projects that illustrate the importance of software quality attributes. This course serves as the basis for more advanced programming classes. Classroom 3 hours, laboratory 2 hours. Prerequisite: C or higher in IS 100 or CS 100, or by instructor permission.

CS 212 Assembly Language & Reverse Engineering 3 Cr.
An introduction to assembly lanuage and reverse engineering, including relationship among machine language, assemblers, disassemblers, compilers, and interpreters. This courses provides requisite skills for computer forensics, malware analysis, and cryptology. Prerequisites: 'C' or higher in IS 131 or CS 140.

CS 221 GUI Programming 3 Cr.
A study of the design and implementation of the graphical user interface. The course will present fundamentals of usability and human factors in GUI design. One or more of the following will be studied and implemented in a student project: Visual Basic programming, Web programming, GUI code generators. Prerequisite: IS 131.

CS 228 Introduction to Data Structures 3 Cr.
An introduction to the basic concepts of algorithm analysis, data representation, and the techniques used to operate on the data. Topics include searching, sorting, linked lists, stacks, queues, trees, hash tables, graphs, Prerequisite: C or higher in IS 131 or CS 140.

CS 240 Database Management 3 Cr.
A study of the concepts and structures necessary to design and implement a database management system. Various data models will be examined and related to specific examples of database management systems including Structured Query Language (SQL). Techniques of system design, system implementation, data security, performance, and usability will be examined. Prerequisite: C or higher in IS 131 or CS 140.

CS 250 Virtual Systems Administration 3 Cr.
This course includes a combination of classroom lecture on network and virtualization theory as well as a variety of hands on exercises to provide students with an understanding of how to configure and manage a VMware ESX environment. Students will also learn how to carry out administration tasks specific to the day-to-day operations of the NUCAC-DF. Some of these tasks will include how to build and maintain classroom environments, understanding requirements given by professors and instructors for classrooms, and overall maintenance of the systems in the Center for Advanced Computing and Digital Forensics. Pre-Requisite: by instructor permission.

CS 260 Data Communications and Networks 3 Cr.
An introductory study in fundamental concepts of computer networks and data communication including a survey of major protocols, standards, and architectures. Students use concepts and terminology of data communications effectively in describing how software applications and network services communicate with one another. Students read and analyze network traces to monitor communications, diagnose issues, and evaluate protocols. Prerequisite: C or higher in IS 131 or CS 140.

CS 270 Operating Systems & Parallelism 3 Cr.
An introduction to the theory and structure of modern operating systems, including hardware abstraction, process management, memory management, system performance, and security. Specific attention to multi-threaded processing, semaphores, locking and interprocess communication. Prerequisites: C or higher in IS 131 or CS 140.

CS 300 Management Information Systems 3 Cr.
This course provides an overview of information systems, their role in organizations, and the relationship of information systems to the objectives and structure of an organization. Management of software projects, decision making with regard to systems development, and organizational roles with regard to information systems is also discussed. Not open to CS or CSIA students.

CS 301 Software Engineering 3 Cr.
An in-depth introduction to the software development life cycle, the techniques of information analysis, testing, and the logical specification of software. Particular attention to project management, documentation, and interpersonal communication. Utilizing industry-standard methods, the student progresses through the phases of specification, design, implementation, and testing of information systems. Object-oriented design techniques are used to design new logical and new physical systems for business-related problems. Prerequisite C” or higher in IS 131 or CS 140.

CS 330 Ethics in Computing and Technology 3 Cr.
The course examines ethical dilemmas resulting from current technological trends, as well as the ethical standards and creeds of a variety of organizations (e.g., Association for Computing Machinery). Students learn to evaluate case studies from an ethical perspective. Students are expected to conduct literature surveys, produce bibliographies, write literature reviews, and present oral summaries of research as well as offer critical evaluation of writings related to ethics and technology. This course meets the General Education Ethics requirement.

CS 406 Special Topics in Computer Science 3 Cr.
A study of topics chosen from areas of current interest that are not offered as part of the permanent curriculum. Topics are chosen by instructors on a semester-by semester basis. Students may take the course more than once, provided each semester taken covers a substantively different topic. Prerequisite: By permission of instructor.

CS 407 Politics of Cyberspace 3 Cr.
This course explores the interrelations of modern computing and communications technology with politics, power, news, privacy, crime, and creativity. The course assumes only a rudimentary familiarity with the basic concepts and terminology of modern Internet usage and computing and is not a technology-focused course. Prerequisite: Open to 2nd-semester sophomores or higher, or by instructor permission.

CS 410 Computing Internship 3 Cr.
Internships in computing and information technology provide computing majors with the opportunity to apply and expand their knowledge within the computing discipline. Students must be Junior standing, or higher and have good academic standing. The student must have the internship approved beforehand by a computing faculty member and have the written consent of the Chair or Director of Computing. In addition, a supervisor within the sponsoring organization must agree to provide a written description of the internship beforehand, and provide progress reports during and after the internship experience. Prerequisites: Good Academic Standing, Junior or higher status.

CS 420 Computer Science capstone I 3 Cr.
A two-semester course sequence normally taken in the Senior year. Based on the subject matter mastered during their previous coursework, students (individually or in a group) identify a current topic to study in depth. As part of their studies, they develop either a working software project or produce a substantial data or hardware artifact. This course represents the first semester of a students work towards such a project. Prerequisites: Junior standing or higher, Computer Science majors only.

CS 421 Computer Science capstone II 3 Cr.
As the second semester of the two-course capstone sequence, this course serves as a continuation of CS 420. Prerequisites: CS 420.

CS 430 Computer Science Undergraduate Thesis I 3 Cr.
The computer science undergraduate thesis is a two-semester course sequence normally taken in the Senior year. The course introduces students to the breadth of tasks involved in independent research, including library work, problem formulation, experimentation, and writing and speaking. Based on the subject matter mastered during previous coursework, students (individually or in a group) identify a current topic to study in depth. Students produce an original research paper. This course represents the first semester of a student's work towards such a project. Prerequisites: Junior standing or higher, Computer Science majors only.

CS 431 Computer Science Undergraduate Thesis II 3 Cr.
As the second semester of the two-course thesis sequence, this course serves as a continuation of CS 430. Prerequisite: CS 430.

Digital Forensics Courses

DF 242 Computer Forensics I 4 Cr.
This course provides the student with an ability to perform basic forensic techniques and use appropriate media analysis software. Knowledge of the security, structure and protocols of network operating systems and devices are covered as students learn to gather evidence in a networked environment and to image and restore evidence properly without destroying its value. Students learn and practice gaining evidence from a computer system while maintaining its integrity and a solid chain of custody. Within the laboratory, students gain hands-on experience in the use of current investigative tools. Classroom 3 hours, laboratory 2 hours. Cross-listed as CJ 442. Prerequisites: CJ 341 or IA 241 and a C or higher in IS 130 or CS 140.

DF 311 Network Forensics 3 Cr.
Introduces digital forensic concepts and practices on local area networks, wide area networks and large scale networks such as the Internet. Lectures include topics based on table of contents in (Davidoff and Ham 2012) such as investigative techniques, and how to conduct an investigation, manage evidence and follow a cyber-trail. A large part of the course involves demonstrations and hands-on labs, including: use of network forensic tools such as packet monitors, security information and event managers (SIEMs), tracers, and other tools useful for analyzing events. Many of the labs involve analysis of packet captures of both actual attacks and theoretical malfeasance by offenders. Students have a final lab exercise instead of a final exam and are expected to research and present a final project. Prerequisite: IS 460 or CS 260.

DF 312 Malware Forensics 3 Cr.
This predominantly laboratory-based course is an introduction to malware forensics including both static and dynamic analysis. Students study profiling, malware behavior, behavior of malware on computer networks, anti-reversing and anti-debugging techniques, and packers. Prerequisite: CS 212.

DF 395 Cyber Criminalistics 3 Cr.
This survey course uses lecture, case studies and hands-on lab exercises in digital investigation and cyber forensics to introduce students to the investigation and analysis of cybercrime and cyber criminals. Topics include: cybercrime typology, cyber-criminal profiling, network tracking, introduction to the tools of the cyber- criminalist, techniques of cybercrime scene assessment, digital evidence management and analyzing the forensic remnants of a cyber event. During the course of the laboratory exercises, students create a personal lab notebook recording their lab exercises and manage evidence including maintaining a proper chain of custody. Prerequisites: Open to CJ 2nd semester sophomores or higher, or by instructor permission.

DF 411 Cyber Investigation 3 Cr.
An introduction to cyber investigation, including elements of cybercrime, cyberwarfare and cyberterrorism. The course examines investigative techniques for cyber-investigators, case studies of representative cybercrimes and cyber warfare incidents, some cyber investigation tools and expert witnessing. The course builds up to a mock trial where students act as a cyber-investigation task force on an actual case of cybercrime. This is a course that incorporates extensive reading as well as hands-on lab exercises. Prerequisites: Open to CS or CSIA 2nd-semester sophomores or higher, or by instructor permission.

DF 423 Advanced Digital Forensics 3 Cr.
This course Expands upon concepts learned throughout the digital forensics concentration in the BSCSIA major. It is based upon the Certified Cyber Forensic Professional (CCFP) certification review class and covers the six domains (Ethics and Law, Forensic Science, Investigation, Digital Forensics, Application forensics and Hybrid and Emerging Technologies). Students completing this class successfully are prepared to take the CCFP certification exam and, if they pass, are qualified to become certified either as CCFPs or (ISC) Associates until they achieve three years of field experience. Prerequisite: DF 242, DF 311, DF 411 or permission of instructor.

Information Assurance Courses

IA 241 Cyberlaw and Cybercrime 3 Cr.
This course includes extensive discussion of the legal constraints, both civil and criminal, that underlie acceptable behavior using computers and networks today. Cross-listed as CJ341. Prerequisite: CJ 101 or instructor permission.

IA 340 Introduction to Information Assurance 3 Cr.
This course introduces the foundations of information assurance, with focus on concepts and terminology used in describing, analyzing, and implementing information security. Topics include the history and mission of information assurance, history of computer crime, modern and historical cryptology, information warfare, penetrating computer systems and networks, malware, social engineering, spam, phishing, physical and facilities security, network security, identification and authentication, securing stored data, data backups and archives, patch management, and protecting digital rights. 3 hours; laboratory 2 hours. Prerequisite: C or higher in IS 131 or CS 140 or permission of instructor.

IA 342 Management of Information Assurance 3 Cr.
This course focuses on management of the information assurance process. Topics include human factors in reducing security breaches, security incident detection and response, remediation, management's role in information assurance, and other considerations in framing and implementing information assurance policies. The final section reviews current topics of particular interest and activity in the field of information assurance. Prerequisite: IS 340 or IA 340 or permission of instructor.

IA 360 Network Security 3 Cr.
This course focuses on the concepts, terminology and practice of network security. Topics include the fundamental goals of network security and practical applications of wired and wireless network security techniques such as applications of cryptology in network protocols, authentication, access control, network security devices such as firewalls and intrusion detection and prevention systems, incident response, log analysis, honeypots and honeynets. Classroom 3 hours, laboratory 2 hours. Prerequisite: IS 460 or CS 260.

IA 455 Contemporary Issues in Information Assurance 3 Cr.
A capstone seminar for Computer Security and Information Assurance majors which will vary every term in accordance with the current issues of the time. Students work with the instructor as they explore today's issues and trends in preparation of a thesis or project. Emphasis is placed on critical thinking, research and evaluation of current issues. A comprehensive computer security exam is included in this course. Prerequisites: IA 340, IA 342. Open to CSIA Junior 2 or higher, or by instructor permission.

IA 456 Cyber Defense Practicum 3 Cr.
This course provides practical application of the concepts learned over the course of the CSIA program. This is the technical capstone for the program and is a required course. The class is divided into three teams. Each team rotates through red (attack), blue (defend) and white (monitor/analyze) cells over the semester. Network attack analysis, intrusion detection systems and the use of network forensics in attaché analysis and defense are covered. Several open source and commercial tools during the class are used. Scenarios on a variation of the virtual network are ran. Blue teams harden the devices on the network to resist attack and are scored on how successful they are. Red teams develop a suite of attacks that allow completion of the scenario and are scored on the completeness of attack preparations. White teams analyze the read attacks and the blue responses and present analysis to the class at the close of the exercise. The scenario changes slightly for the iterations presented. This is a100% lab class. Prerequisites: IS 340 or IA 340 and IS 460 or CS 260.