**Curriculum Proposal**

Please type or select the requested information. Print completed forms, add appropriate paper attachments, and route through MSU's curricular process for recommendations and decisions.

<table>
<thead>
<tr>
<th>College: Science, Engineering and Technology</th>
<th>Undergraduate</th>
<th>Proposal # 123</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department: Computer and Information Sciences</td>
<td>Graduate</td>
<td>Effective Date of Change: 04-07</td>
</tr>
<tr>
<td>Program: Information Systems</td>
<td>CIP # 11.040100</td>
<td>(For Office Use Only)</td>
</tr>
</tbody>
</table>

**Course Designator and Number**

<table>
<thead>
<tr>
<th>Title</th>
<th>Proposed: Information Warfare</th>
</tr>
</thead>
<tbody>
<tr>
<td>24-Char. Abbrev: Information Warfare</td>
<td></td>
</tr>
<tr>
<td>ISYS 450/550</td>
<td>4</td>
</tr>
</tbody>
</table>

**Type of Change**

- COURSE PROPOSALS
- Proposed: New Course

**Rationale or Justification for change:**

This new course is an integral part of our new Information Systems program and is critical to ABET accreditation for Information Systems.

***For General Education or Cultural Diversity Courses Only***

<table>
<thead>
<tr>
<th>GE Category #</th>
<th>GE Category Name (Maximum of 3 Categories)</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>

- For Writing Intensive Courses, attach a description of the kind and quantity of writing.
- For Upper Division Courses, include a description of the respects in which it is broad and general rather than narrow and specific, and so suitable as GE.

Attach paper copies of the following:

a. Syllabus or course outline.

b. Course's student learning outcomes associated with each GE competency or CD designation.

c. List of strategies to be used to assess students' achievement of each GE competency or CD designation.

***For New Courses***

<table>
<thead>
<tr>
<th>Instructional Type:</th>
<th>Lecture</th>
</tr>
</thead>
<tbody>
<tr>
<td>Course is an elective.</td>
<td></td>
</tr>
<tr>
<td>Grading Format:</td>
<td>Grade</td>
</tr>
<tr>
<td>X Course is required for program</td>
<td>Information Systems (ISYS)</td>
</tr>
<tr>
<td>X Pre- or Co-requisites:</td>
<td>ISYS 350 or IT 350</td>
</tr>
</tbody>
</table>

Course will be offered:

- Fall Semester
- Spring Semester
- Summer Session

- Course content or title is similar to courses in other departments. (Attach copy of letter of agreement with other program(s) contacted. Indicate the nature of the discussions and/or resolution of differences or potential conflicts.)

Attach paper copies of the following:

a. Syllabus or course outline.

b. Course's student learning outcomes.

c. A list of resources required to offer and support this course.

d. A description of how teaching this course will affect department staffing.

e. If 400/500 level course, an explanation of added expectations of graduate students.

**Revised September 2002**
### Signature Page

**Department**

- **Recommended** (Category/ies: )
- **Not Recommended** (Category/ies: )

- **Comments:**

**College Curriculum Committee**

- **Recommended** (Category/ies: )
- **Not Recommended** (Category/ies: )

- **Comments:**

**College Dean**

- **Recommended** (Category/ies: )
- **Not Recommended** (Category/ies: )

- **Comments:**

**General Education Subcommittee**

- **Recommended** (Category/ies: )
- **Not Recommended** (Category/ies: )

- **Comments:**

**Undergraduate Curriculum and Academic Policy Committee**

- **Recommended** (Category/ies: )
- **Not Recommended** (Category/ies: )

- **Comments:**

**Faculty Association Graduate Committee**

- **Recommended**
- **Not Recommended**

- **Comments:**

**Graduate Dean**

- **Recommended**
- **Not Recommended**

- **Comments:**

**Academic Affairs Council**

- **Recommended** (Category/ies: )
- **Not Recommended** (Category/ies: )

- **Comments:**

**Senior Vice President and Vice President for Academic Affairs**

- **Approved** (Category/ies: )
- **Not Approved** (Category/ies: )

- **Comments:**

---

*Revised September 2002*

Catalog Description

Information warfare principles and technologies, including information warfare concepts; protocols, authentication, and encryption; network attack techniques, methodologies, and tools; network defense; malware: trojans, worms, viruses, and malicious code; electronic crimes and digital evidence.

Prerequisites

- ISYS 350(4) Information Security (or IT 350)

Topics

Knowledge Unit 1. Information Warfare Concepts

- Goal: to be able to demonstrate comprehension-level mastery of the concepts of information warfare and the roles of entities seeking to protect national intelligence and corporate intelligence
- Approximate classroom hours: 15
- Mastery level 2: Comprehension
- Objectives:
  - 1.1 defend the role of offensive information warfare
  - 1.2 explain the advantages of intelligence in industrial espionage
  - 1.3 explain the civilian role in information warfare
  - 1.4 explain the law enforcement role in information warfare
  - 1.5 explain the military role in information warfare
  - 1.6 explain the role of defensive information warfare
  - 1.7 explain US Government concerns about the information infrastructure

Knowledge Unit 2. Protocols, Authentication, and Encryption

- Goal: to be able to demonstrate application-level mastery of the nature of the protocols which allow network communication and their weaknesses; tools for capturing network data and computer passwords; evidence gathered using the tools
- Approximate classroom hours: 15
- Mastery level 3: Application
- Objectives:
  - 2.1 apply network sniffer on a network to capture data
  - 2.2 demonstrate how to use an encrypted email system
2.3 utilize one-time passwords, Kerberos, and other authentication systems
2.4 utilize password cracking and password resetting tools
2.5 utilize screening routers and software filters
2.6 utilize security probing software to determine the weaknesses of a computer system

Knowledge Unit 3. Network attack techniques, methodologies and tools

- Goal: to be able to demonstrate analysis-level mastery of various tools and techniques for gaining access to networks and computers to find their vulnerabilities
- Approximate classroom hours: 10
- Mastery level 4: Analysis
- Objectives:
  - 3.1 discuss hacker motivations
  - 3.2 examine the professional hacker's methodology for attacking a network
  - 3.3 infer hacker techniques, tools and methodologies
  - 3.4 infer ways to maintain access to a network

Knowledge Unit 4. Network defense

- Goal: to be able to demonstrate analysis-level mastery of the threats faced by a given network configuration and means to counter those threats including both prevention and detection
- Approximate classroom hours: 10
- Mastery level 4: Analysis
- Objectives:
  - 4.1 analyze insider attack threats
  - 4.2 analyze perimeter attack threats
  - 4.3 analyze the output of network scans to find attacks
  - 4.4 infer hacker techniques, tools and methodologies

Knowledge Unit 5. Malware: Trojans, Viruses, Worms, and Malicious Code

- Goal: to be able to demonstrate analysis-level mastery of the various forms and means of infection and propagation of malware; tools and techniques to prevent and detect malware; impact of various forms of malware
- Approximate classroom hours: 5
- Mastery level 4: Analysis
- Objectives:
  - 5.1 analyze the impact of various forms of malware
  - 5.2 analyze the threat posed by spyware
  - 5.3 differentiate between various forms of malware

Knowledge Unit 6. Electronic Crimes and Digital Evidence
• Goal: to be able to demonstrate comprehension-level mastery of planning for a computer incident; levels of jurisdiction; preserving digital evidence; incident assessment, responses and reports
• Approximate classroom hours: 5
• Mastery level 2: Comprehension
• Objectives:
  o 6.1 classify the levels of jurisdiction over a computer crime
  o 6.2 classify the steps for an initial response to an incident
  o 6.3 comprehend the legal issues with regard to preserving digital evidence
  o 6.4 explain how a network security specialist can help the collection of digital evidence
  o 6.5 explain how to handle a computer incident
  o 6.6 explain the difficulties in prosecuting a computer crime incident
  o 6.7 explain the factors involved in identifying a computer incident
  o 6.8 explain the steps in planning for a computer incident
  o 6.9 identify and explain the incident response goals and priorities

Additional topics may also be covered based on time and student interest.

Graduate Students

Students taking the 500-level version of this course are required to perform beyond expectations of undergraduate students by completing one or more of the following, at the discretion of the instructor:

• A term paper that summarizes and critiques an article from a scholarly journal in the area of information warfare.
• A project that implements advanced ideas in information warfare.
• A presentation about an advanced area in information warfare, or that presents the student’s term paper or project.
• Some other activity that demonstrates grasp of the material beyond what is expected of undergraduates.

Instructional and Library

Resources currently in place within the department and the University Library will support this new course. No new resources are required.

Staffing

This course will be able to be staffed by the faculty that have been designated in the proposed Department of Information Systems and Technology by the Dean of the College of Science, Engineering, and Technology, Dr. John Frey. This course will be cross-listed between the "Information Systems" and "Information Technology" programs
in the new department. This course will not need assistance from faculty of the new Computer Science Department.

Possible Textbook(s)


Syllabus for ISYS 4/550: Information Warfare

Instructor

Name: Prof. Sample Faculty
Office: 200 Wissink Hall
Department: Information Systems and Technology, Minnesota State University, Mankato
Office hours: Monday through Friday from 1:00 to 4:00 pm
Phone: 507-389-1212
Email: sample.faculty@mnsu.edu
Course page: https://d2l.mnsu.edu/

Meeting
MTRF 10-11

Catalog Description
Information warfare principles and technologies, including information warfare concepts; protocols, authentication, and encryption; network attack techniques, methodologies, and tools; network defense; malware: trojans, worms, viruses, and malicious code; electronic crimes and digital evidence.

Prerequisites
- ISYS 350(4) Information Security (or IT 350)

Topics

The following content areas will be covered.

1. Information Warfare Concepts (about 15 hours)
2. Protocols, Authentication, and Encryption (about 15 hours)
3. Network attack techniques, methodologies and tools (about 10 hours)
4. Network defense (about 10 hours)
5. Malware: Trojans, Viruses, Worms, and Malicious Code (about 5 hours)
6. Electronic Crimes and Digital Evidence (about 5 hours)

Additional topics may also be covered based on time and student interest.

Objectives

By the end of this course, you should be able to

- defend the role of offensive information warfare
- explain the advantages of intelligence in industrial espionage
- explain the civilian role in information warfare
- explain the law enforcement role in information warfare
- explain the military role in information warfare
- explain the role of defensive information warfare
- explain US Government concerns about the information infrastructure
- apply network sniffer on a network to capture data
- demonstrate how to use an encrypted email system
- utilize one-time passwords, Kerberos, and other authentication systems
- utilize password cracking and password resetting tools
- utilize screening routers and software filters
- utilize security probing software to determine the weaknesses of a computer system
- discuss hacker motivations
- examine the professional hacker's methodology for attacking a network
- infer hacker techniques, tools and methodologies
- infer ways to maintain access to a network
- analyze insider attack threats
- analyze perimeter attack threats
- analyze the output of network scans to find attacks
- infer hacker techniques, tools and methodologies
- analyze the impact of various forms of malware
- analyze the threat posed by spyware
- differentiate between various forms of malware
- classify the levels of jurisdiction over a computer crime
- classify the steps for an initial response to an incident
- comprehend the legal issues with regard to preserving digital evidence
- explain how a network security specialist can help the collection of digital evidence
- explain how to handle a computer incident
- explain the difficulties in prosecuting a computer crime incident
- explain the factors involved in identifying a computer incident
- explain the steps in planning for a computer incident
- identify and explain the incident response goals and priorities

Students with Disabilities
Every attempt will be made to accommodate qualified students with disabilities. If you are a student with a documented disability, please see me as early in the semester as possible to discuss the necessary accommodations, and/or contact the Disability Services Office at (507) 389-2825 (V) or 1-800-627-3529 (MRS/TTY).

**Textbook**

This course will use one more more of the following textbooks:


Additional readings may be assigned by the instructor.

**Grading**

Your course grade will be based on:

[Varies by faculty]

If you receive 90% or more of the possible points, you are guaranteed an A, 80% a B, et cetera. However, a score just below the grade cutoff will not necessarily earn the higher grade. Therefore, you should try to attain a score well above the cutoff to achieve the grade you want.

**Exams**

The exams will cover reading assignments, lectures, and class discussion. It is your responsibility to remember the exam schedule. If you forget to attend an exam or are more than ten minutes late for the exam, you must forfeit the grade for that exam.

You may take the exam at an alternate testing time if you participate in a university-sponsored activity that requires your attendance. You must arrange with the instructor at least a week ahead of the exam date.

If you miss an exam because of illness or family emergency, you may arrange with the instructor for a makeup exam. You must produce written proof of the reason you cannot take a test at the normally scheduled time.
Graduate Students

If you are taking the 500-level version of this course, you must complete one or more of the following additional requirements, at the discretion of the instructor:

- A term paper that summarizes and critiques an article from a scholarly journal in the area of information warfare.
- A project that implements advanced ideas in information warfare.
- A presentation about an advanced area in information warfare, or that presents the student's term paper or project.
- Some other activity that demonstrates grasp of the material beyond what is expected of undergraduates.

Programming Assignments

[Varies by faculty]

Homework

[Varies by faculty]

Class Policies

Attendance

[Varies by faculty]

Late Policy

[Varies by faculty]

Academic Honesty

Please be aware that the University's policy for Academic Honesty appears in the Student Handbook. Each student is expected to have read this material. If you do not understand what is meant by this policy, or if you are confused by terms such as plagiarism, cheating, or collusion, please discuss this policy with me, your advisor, or another faculty member as soon as possible. I absolutely require that each student in this class will fulfill his or her academic obligations in a fair and honest manner.

Anything that you observe in other students that is of questionable integrity should be brought to my attention. You may do so anonymously if you desire (e-mail works fine for this).
For the writing of papers and program design documents, it is quite easy to define cheating in terms of traditional definitions of plagiarism; however, for the writing of computer programs, the distinction is not as obvious to many students. It is easy to use the English paper comparison when thinking about what is appropriate and what constitutes dishonest academic work when writing computer programs. Like writing a paper, you may discuss general ideas with fellow students.

You must write each programming assignment yourself. It is acceptable to discuss logic and other strategies such as the number of variables or methods, but it is NOT acceptable to show another student even a single line of your program until after the due date.

Protect your programming assignments. If another student obtains a copy of your program even though you are unaware of the infraction, you are still guilty of collusion. Do not leave an ACC workstation unattended, even for a little while. Other students monitor your patterns and, while you are out for even a few seconds, walk up to your workstation and email a copy of your program to themselves! You should also be careful where you leave paper copies of your program. Do not leave files on ACC computers. A trash receptacle anywhere near the ACC is likely to be rummaged. Make sure you log out of the course website when you are done using it, close all browser windows, and log out of the system.

I strongly suggest you consult your student handbook or talk with me if you are unsure as to what is acceptable academic behavior. The consequences are quite severe. Academic misconduct will automatically result in my informing Judicial Affairs, a division of Student Affairs, of the misconduct. This misconduct usually results in a failing grade for the course. (And it can be worse.)

Specific items that will be considered cheating on programming assignments are:

- Turning in work done by somebody else as your own (with or without that person's consent). This includes turning in a copy of something that can be mechanically transformed into a copy of someone else's work. Do not try to disguise cheating by simply modifying someone else's work and calling it your own. I use software that detects this type of cheating.
- Allowing someone else to turn in your work as his or her own work. This includes allowing fellow students access to your copy, even without your knowledge or consent.
- Using a solution developed by a student in a previous semester or another section.

**Errors in Grading**

If something has been graded incorrectly, or if a grade has been recorded incorrectly, you must request a correction no later than one week after the grade has been posted. Course grades are final, and cannot be changed unless there has been a substantial error.
Grades are based on the quality of your work and on how well you are prepared for class. While working hard is admirable, your grade will not be based on how much time you spent working on an assignment or preparing for an examination.

**Weather and Other Problems**

In the event inclement weather conditions or other problems cause class not be held on a given day, any work due for that day will be due at the next class meeting. It will not cause any other changes in the schedule. Weather-related closings will be made by the university and announced on the Twin Cities and local media. You can call the MSU WeatherLine at 2463 for weather-related closing or cancellation information.

**Classroom Etiquette**

Please turn off or silence your cell phone or pager while in class. If you are expecting an urgent call (such as from your sick child):

- Use the "silent" mode of your cell phone or pager.
- Sit right next to the door.
- Leave the room as quietly as possible when you receive the call, so you do not disturb other students.