Department of Applied Information Technology
Volgenau School of Engineering
IT 462 Applied Cyber Threat Analysis
Fall 2018

Common Syllabus  revised 08.18.2018

This syllabus contains information common to all sections of IT 462 for the Fall 2018 semester. For each section, a customized syllabus with information specific to that section will be made available to registered students via the Blackboard Learning System.

University Policies

The University Catalog is the central resource for university policies affecting student, faculty, and staff conduct in university affairs. Unless explicitly noted, any conflict between the policies in the University Catalog and the content of this document are unintentional. Please notify the author to resolve any such conflicts.

Scheduled Sections

<table>
<thead>
<tr>
<th>Section</th>
<th>Instructor</th>
<th>Campus</th>
<th>Day</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>001</td>
<td>John Doyle</td>
<td>Prince William</td>
<td>Thursdays</td>
<td>7:20 – 10:00 PW BRH 257</td>
</tr>
<tr>
<td>DL</td>
<td>John Doyle</td>
<td>Online</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Course Description

IT 462 - Information Security Principles

Studies security policies, models, and mechanisms for secrecy, integrity, availability, and usage controls. Topics include:

Models and mechanisms for mandatory, discretionary, and role-based access controls; authentication technologies; control and prevention of viruses and other rogue programs; common system vulnerabilities and countermeasures; privacy and security policies and risk analysis; intellectual property protection; and legal and social issues.

Equivalent to INFS 462.

Prerequisites
Prerequisites

The prerequisites for this course are IT 212 and IT 223, or permission from the Department of Applied Information Technology. Unless a waiver is granted, a grade of "C" or better must be achieved in each prerequisite course before a student is qualified to take this course. The prerequisite courses must be completed prior to, not concurrently with, this course.

These requirements will be strictly enforced. Any student who does not meet the prerequisite requirements will be dropped from the course by the Instructor at the start of the semester and the student will be responsible for any consequences of being dropped.

Rationale

Computer security has evolved into a comprehensive discipline called “information security” and recently embraced the name “cyber security”. The increased reliance on automated systems and the lack of adequate security plans place privacy and organizational information at risk. “Information security” has become a greater concern and effective security is critical to an organization’s success. This course will build upon the student’s knowledge of technology-based controls and focus on the identification, detection, and remediation of threats to information stored on enterprise networks.

This course has been updated over the past two semesters, steering away from its originally intended focus of preparing students to assume a leadership or managerial role in an organization and, instead, focusing on practical skills relevant to all cyber security disciplines, especially those working in incident response and security operation centers (SOCs).

This course is an option in the Information Security (INFS) concentration of the IT major, and an elective in the IT minor.

Objectives

This course is broken out into two parts: “drilling down” on fundamental cyber security concepts and applying best practices to identify, characterize, and correct threats to information systems. This course teaches current industry best practices, standards, conceptual models, and tools to identify threats, system vulnerabilities, and cyber threat intelligence and security incident and event management systems (SIEMs), as well as the utility and process for reverse engineering malicious software.

Upon successful completion of this course, students will be able to:

– Identify information assets and prioritize threats to these information assets via risk management.
– Understand information security strategies, policies and plans.
– Identify core computer networking protocols and understanding cryptographic protections
– Control access based on multiple criteria in both Windows and Linux
– Describe host-based security measures on physical and virtual systems
– Use Security Incident and Event Management (SIEM) Systems and Cyber Threat Intelligence for “Threat Hunting”
– Identify and distinguish the role played by incident response, digital forensics, and reverse engineering malicious software
– Understand the security assessment and vulnerability testing process and associated industry best practices and tools
References

Textbooks

There is one required textbook for this course and multiple online reading assignments that include industry authored “White Papers”:

Authors: Stewart, James Michael; Chapple, Mike; Gibson, Darril
Format: Softcover

Note: Students are in no way expected to be prepared by the conclusion of this course for the CISSP certification exam.

Faculty and Staff

Instructor:

Prof. John Doyle (001 and DL Section)
Email: jdoyle14@gmu.edu (subject: IT-462 DL...)
Office hours: By appointment only

Dr. Tom Winston (Course Coordinator)
Email: twinsto5@gmu.edu (subject: IT-462 [1/DL]...)

Teaching Assistant:
TBD
Grading

Grades will be awarded in accordance with the Mason Grading System for undergraduate students. See [http://www.gmu.edu/catalog/apolicies/](http://www.gmu.edu/catalog/apolicies/) under Grading System for more information.

The grading scale for this course is:

<table>
<thead>
<tr>
<th>Score</th>
<th>Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>97 - 100%</td>
<td>A+  Passing</td>
</tr>
<tr>
<td>93 - 96%</td>
<td>A    Passing</td>
</tr>
<tr>
<td>90 - 92%</td>
<td>A-   Passing</td>
</tr>
<tr>
<td>87 - 89%</td>
<td>B+   Passing</td>
</tr>
<tr>
<td>83 - 86%</td>
<td>B    Passing</td>
</tr>
<tr>
<td>80 - 82%</td>
<td>B-   Passing</td>
</tr>
<tr>
<td>77 - 79%</td>
<td>C+   Passing</td>
</tr>
<tr>
<td>70 - 76%</td>
<td>C    Passing</td>
</tr>
<tr>
<td>60 - 69%</td>
<td>D    Passing</td>
</tr>
<tr>
<td>0 - 59%</td>
<td>F    Failing</td>
</tr>
</tbody>
</table>

Raw scores may be adjusted by the Instructor to calculate final grades.

Final grades will be determined based on the following components:

- Current Event: 20%
- Quizzes: 10%
- Assignments: 30%
- Mid-term exam: 20%
- Final exam: 20%

These components are outlined in the following sections.

**DL Section**

In general, lectures will be recorded and posted on either Saturday or Sunday evening. Some previously recorded lectures may be used if they are relevant. An optional in-person review for the midterm and final exams will take place approximately one week prior to the exams.

Each week we will have a Blackboard discussion posting and quiz due on Sunday by 11:59pm.

**Blackboard Discussions**

Each student is required to research and prepare a response to questions related to course content (“Current Events”). Each posting must be at least a paragraph long and use clear, concise English prose that is grammatically correct. Points will be deducted for posts that do not directly address the questions posed or do not use clear English sentence structure.

In response to student feedback over the past two semesters, we are changing the posting requirement. Each student will still be responsible for responding to the question posed weekly (50% of the “Current Events” grade). We, however, are changing the participation portion to requiring a substantive reply to your peers. What is required is 4 substantive responses to other students’ postings every 3 weeks (weeks...
1-3, 4-6, 7-9, 10-12, and 13-15), representing the remaining 50% of the “Current Events” grade. In previous semesters, we were requiring students to reply to 2 postings each week. The reasoning behind this is 1) to help students learn from each other given the diverse set of backgrounds we have in class and 2) to help your professor calibrate understanding on certain topics, allowing him to review any content that he believes was unclear based on responses.
Quizzes. Quizzes will be given at the beginning of each class covering the material discussed in the previous week (in-person section only). These quizzes may also cover information from the required reading, which may not be explicitly discussed in class. Quizzes for the online section will be due on Sunday evening by 11:59pm each week. The quizzes carry a weight of 10% of your final grade and cannot be made up if missed unless accommodations have been discussed ahead of time.

Assignments – all sections

Students will be given 3 hands-on assignments throughout the semester. Specific expectations for the assignment will be provide in advance. In most cases, students will have a 3-4 weeks to complete the assignments from when they are posted.

Mid-term exam

The mid-term exam for the 01 Section will be conducted during the scheduled class session as announced in class and will be based on topics addressed in the previous weeks. The mid-term exam will be “closed book” – no reference materials other than those provided with the exam paper will be permitted. Mid-term exams will be returned to students once all mid-term exams for all sections have been graded.

The DL sections will receive instructions for the mid-term date approximately three weeks prior to the exam. The exam will be taken in-person, usually on a Sunday, at the Fairfax campus. Students are encouraged to check early for schedule conflicts; accommodations, though rare, can be made if there is a valid reason for the request. This requires at least 2 weeks notice. Students who are not able to make the mid-term must have documented evidence and the Dean’s approval to schedule an alternate make-up exam.

Final exam

The final exam will be held during the scheduled final exam session (see http://registrar.gmu.edu/topics/final-exam-locator/) and will be based on topics addressed throughout the entire course. The final exam will be “closed book” – no reference materials other than those provided with the exam paper will be permitted. Final exams will be retained by the Department of Applied Information Technology and will not be returned to students. DL Sections will receive instructions for the Final Exam date when that has been provided. Students who are not able to make the exam must have documented evidence and the Dean’s approval to schedule an alternate make-up exam.

Students are expected to submit work as scheduled by the Instructor. Late work may not be accepted – if accepted, a penalty may be applied. Acceptance of late work and/or application of penalties will be at the sole discretion of the Instructor. In general it is better to submit an incomplete assignment on time for partial credit than to submit a complete assignment late and risk receiving no credit.

Final grades will be posted to PatriotWeb, which is the only vehicle for students to obtain those
grades. A student with a "hold" on his/her PatriotWeb account will be unable to access grades until the hold has been removed by the Registrar.
Schedule

The reading assignment shown for each lecture is to be completed prior to that lecture.

This schedule is subject to revision throughout the course. Registered students should see Blackboard for the latest class schedule.

<table>
<thead>
<tr>
<th>Weeks 1 and 2</th>
<th>Introductions in Blackboard; Logistics; Course Overview Lecture 1: “Introduction to Security and Management” Assignment #1 Assigned</th>
</tr>
</thead>
<tbody>
<tr>
<td>Weeks 3 and 4</td>
<td>Lecture 2: “Communications and Network Security”</td>
</tr>
<tr>
<td>Week 5 and 6</td>
<td>Lecture 3: “Cryptography”</td>
</tr>
<tr>
<td>Week 7</td>
<td>Lecture 4: “Access Control” Assignment #2 Assigned</td>
</tr>
<tr>
<td>Week 8</td>
<td>Midterm Exam</td>
</tr>
<tr>
<td>Week 9</td>
<td>Lecture 5: “Security Engineering”</td>
</tr>
<tr>
<td>Week 10</td>
<td>Lecture 6: “Cyber Threat Intelligence”</td>
</tr>
<tr>
<td>Week 11</td>
<td>Lecture 7: “Security Incident and Event Management (SIEM) Systems and Threat Hunting” Assignment #3 Assigned</td>
</tr>
<tr>
<td>Week 12</td>
<td>Lectures 8: “Incident Response and Digital Forensics”</td>
</tr>
<tr>
<td>Week 13</td>
<td>Lecture 9: “Reverse Engineering and Malware Analysis”</td>
</tr>
<tr>
<td>Week 14</td>
<td>Lecture 10: “Security Assessment and Testing”</td>
</tr>
<tr>
<td>Week 15</td>
<td>Lecture 11: TBD and Final Exam Review</td>
</tr>
<tr>
<td>Week 16</td>
<td>Final Exam</td>
</tr>
</tbody>
</table>
Important Dates

Please see the https://registrar.gmu.edu/calendars/spring-2016/ for important dates, including the last days to add and drop courses.

Religious Holidays

A list of religious holidays is published by University Life. Any student whose religious observance conflicts with a scheduled course activity must contact the Instructor at least 1 week in advance of the conflict date in order to make alternative arrangements.

Attendance Policy

Students are expected to attend every class, to complete any required preparatory work (including assigned reading – see above) and to participate actively in lectures, discussions and exercises. As members of the academic community, all students are expected to contribute regardless of their proficiency with the subject matter.

Students are expected to make prior arrangements with Instructor if they know in advance that they will miss any class and to consult with the Instructor as soon as possible if they miss any class without prior notice. Any student who expects to miss more than one class session is strongly advised to drop the course and take it in a later semester when he/she can attend every class.

Departmental policy requires students to take exams at the scheduled time and place, unless there are truly compelling circumstances supported by appropriate documentation. Except in such circumstances, failure to attend a scheduled exam will result in a score of zero (0) for that exam, in accordance with Mason policy on final exams. Students should not make travel plans or other discretionary arrangements that conflict with scheduled classes and/or exams. If the University is closed due to weather or other unforeseen conditions, final exams may be rescheduled – students are strongly advised not to make plans that would prevent them from attending exams that may be rescheduled during the entire exam period, including the scheduled make-up dates.

Classroom conduct

Students are expected to conduct themselves in a manner that is conducive to learning, as directed by the Instructor. Any student who negatively impacts the opportunity for other students to learn may be asked to leave the classroom.

Electronic devices are potential distractions in the classroom environment. Cell phones, pagers and other handheld devices must be turned off or set to "silent" mode and not used while class is in session. Laptop computers and similar devices may be used only if such use is directly related to the classroom activity in progress – for some activities the Instructor may require that such devices not
Communications

Registered students will be given access to a Blackboard section for this course. Blackboard will be used as the primary mechanism (outside of lectures) to disseminate course information, including announcements, lecture slides, homework and other assignments, and scores for homework and exams.

Communication with the Instructor on issues relating to the individual student should be conducted using Blackboard Mail, Mason email, via telephone, or in person - not in the public forums on Blackboard. For this course, Blackboard Mail is the preferred method. Federal privacy law and Mason policy require that any communication with a student related in any way to a student's status be conducted using secure Mason systems – if you use email to communicate with the Instructor you MUST send messages from your Mason email account. Students must activate and monitor their Mason email accounts to receive important information from the University, including messages related to this class.

Lecture slides are complements to the lecture process, not substitutes for it - access to lecture slides will be provided in Blackboard as a courtesy to students provided acceptable attendance is maintained.

All course materials (lecture slides, assignment specifications, etc) are published on Blackboard in Adobe® Portable Document Format (PDF). This allows users of most computing platforms to view and print these files. Microsoft® Word (or a compatible word processing application) is required for preparing assignments – it is available on computers in the Mason open labs.
Privacy

Instructors respect and protect the privacy of information related to individual students.

As described above, issues relating to an individual student will be discussed via email, telephone or in person. Instructors will not discuss issues relating to an individual student with other students (or anyone without a need to know) without prior permission of the student.

Homework, quizzes, mid-term exams and other assessable work will be returned to individual students directly by the Instructor (or by a faculty or staff member or a Teaching Assistant designated by the Instructor, or via another secure method). Final exams are not returned. Under no circumstances will a student's graded work be returned to another student.

Instructors, staff, and Teaching Assistants will take care to protect the privacy of each student's scores and grades.

Disability Accommodations

The Office of Disability Services (ODS) works with disabled students to arrange for appropriate accommodations to ensure equal access to university services. Any student with a disability of any kind is strongly encouraged to register with ODS as soon as possible and take advantage of the services offered.

Accommodations for disabled students must be made in advance – ODS cannot assist students retroactively, and at least one week's notice is required for special accommodations related to exams. Any student who needs accommodation should contact the Instructor during the first week of the semester so the sufficient time is allowed to make arrangements.

Campus Notifications

Students are encouraged to subscribe to the Mason Alert system to receive notifications of campus emergencies, closings, and other situations that could affect class activities.

Each classroom has a poster explaining actions to be taken in different types of crisis. Further information on emergency procedures is available at http://www.gmu.edu/service/cert. In the event of an emergency, students are encouraged to dial 911.
Other Resources

Mason provides many useful resources for students. The following resources may be particularly useful:

- The Writing Center
- The Academic Advising Center
- The University Libraries
- Counseling and Psychological Services
- University Career Services

See http://www2.gmu.edu/resources/students/ for a complete listing of Mason resources for students.

Academic Integrity

All members of the Mason community are expected to uphold the principles of scholarly ethics.

The IT program is designed to achieve several specific outcomes. One of those outcomes is: “An understanding of professional, ethical, legal, security, and social issues and responsibilities.”

Graduating students are bound by the ethical requirements of the professional communities they join. The ethics requirements for some of the communities relevant to IT graduates are available via the following links:

- ACM Code of Ethics and Professional Conduct
- IEEE Code of Ethics
- EC-Council Code of Ethics

On admission to Mason, students agree to comply with the requirements of the Mason Honor System and Code¹. The Honor Code will be strictly enforced in this course. Honor Code cases are heard by a panel of students – students who meet the requirements are encouraged to nominate themselves to serve on the Honor Committee.

Any use of the words or ideas of another person(s), without explicit attribution that clearly identifies the material used and its source in an appropriate manner, is plagiarism and will not be tolerated. Dean Griffiths has mandated a "zero tolerance" policy for plagiarism within The Volgenau School of Information Technology and Engineering. The Instructor reserves the right to use manual and/or automated means (including such services as SafeAssign) to detect plagiarism in any work submitted by students for this course, and to direct Teaching Assistants and/or other faculty and/or staff members to do likewise in support of this course.
Instances of cheating whether perceived or real will result in actions to be determined by the instructor in accordance with University policies. This can include –

1. An Honor Code Violation  
2. A failure for the assignment in question  
3. A failure for the course.

For this course, the following requirements are specified:

- All assessable work is to be prepared by the individual student, unless the Instructor explicitly directs otherwise.
- No use of social media to post, discuss or share questions, answers or topics covered on exams, in any way, shape or form. Evidence of this will be considered an HCV. Some professors and course coordinators have special tools at their disposal to mine multiple social media outlets simultaneously; you have been warned. (Some examples include: Study Room, YikYak, and Reddit)
- No digital reproduction of any part of an exam or quiz. No posting quiz questions to online test outlets or social media sites. Electronic reproduction of any assessable work in this course is PROHIBITED, unless authorized by the course coordinator (not the section instructor).
- Usage of electronic devices is STRICTLY PROHIBITED during any period when there is assessable work in the students’ possession – this includes exams, quizzes, and any other type of assessable work.
- During exams, and quizzes, students MUST put their cellphones away, with volume or ringers turned off. Laptops must be stowed safely under desks to keep paths between rows clear. Instructors have the option to collect cellphones at the front of the room during exam or quiz periods.
- Individual students must create all new work individually for this semester. Any usage of work developed for another course, or for this course in a prior semester, is strictly prohibited without prior approval from the Instructor.

George Mason requires instructors to report all instances of perceived cheating to the Office of Academic Integrity.

For this course, the following requirements are specified:

- All assessable work is to be prepared by the individual student, unless the Instructor explicitly directs otherwise.
- All work must be newly created by the individual student for this course for this semester. Any usage of work developed for another course, or for this course in a prior semester, is strictly prohibited without prior approval from the Instructor.
Students may seek assistance with assigned work (and are encouraged to do so if they feel the need), provided:

- The directions for the assigned work do not prohibit such assistance.
- Such assistance is explicitly acknowledged in the submitted work, clearly identifying the person(s) giving assistance and the nature of the assistance given.
- Any work to be submitted is prepared entirely and exclusively by the student submitting it. Students are expressly prohibited from sharing any assessable work for this course in any manner with other students (except students assigned as Teaching Assistants or Undergraduate Peer Mentors to this course and the student's section), unless all students involved have had their work graded and returned by the Instructor, or the Instructor has explicitly approved such sharing.

Another aspect of academic integrity is the free exchange of ideas. Vigorous discussion and debate are encouraged in this course, with the firm expectation that all aspects of the class will be conducted with civility and respect for differing ideas, perspectives, and traditions.

Students are encouraged to ask for clarification of any issues related to academic integrity and to seek guidance from the Instructor, other faculty members or advisors, University staff, or the Office for Academic Integrity.

---

1 Available at [http://catalog.gmu.edu/content.php?catoid=15&navoid=1039#Honor](http://catalog.gmu.edu/content.php?catoid=15&navoid=1039#Honor)