CSC 333 / BHI 554 / HCI 530  
Summer 2023 Syllabus  
Privacy / Security / Cryptography & Special Topics

Instructors:

James Early

439 Shineman Center

[james.early@oswego.edu](mailto:james.early@oswego.edu)

Bastian Tenbergen

427 Shineman Center

[bastian.tenbergen@oswego.edu](mailto:bastian.tenbergen@oswego.edu)

**Class Times: online Place: online**

Office Hours: **Email us for an appointment**

Course Overview

Information assurance (IA) is the process of getting the right information to the right people at the right time. CSC333 course studies tools and techniques to restrict unauthorized use of protected information in a computer or information system. Students will become familiar with information security policies, standards, and procedures. This course particularly focuses on the formulation of an effective and implementable security policy. It also acquaints students with many issues involved with privacy and security policies as outlined by various national and international governmental and industrial bodies. Topics include Fundamentals of Security and Privacy, Malware and Social Engineering Attacks, Application and Networking-Based Attacks, Host, Application, Data Security, Basic Cryptography, Network Security Fundamentals, Administering a Secure Network, Mobile Device Security, Access Control Fundamentals, and Vulnerability Assessment.

Learning Objectives

CSC333 introduces students to information assurance concepts and skills. Students would study the fundamentals of information assurance principles, particularly in the context of privacy, security and cryptography. The course would integrate case studies related to ubiquitous, pervasive, virtual, and distributed health information systems. Successful students in this course will be able to:

* Provide students with a solid background in basic concepts in information assurance;
* Allow students to apply these concepts to design an effective and implementable security policy;
* Allow students to audit a security policy; and
* Allow students to discuss research articles and case studies in information assurance.

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

* Articulate principles of computer and network security.
* Define main terminology such as confidentiality, integrity, availability, and security fundamentals of computer networks, network security, basics of cryptography, mobile device security, access control mechanisms, and vulnerability assessment.
* Design for privacy and security constraints.
* Create and manage security networks applications in health and wellness.
* Design and manage a security policy.
* Create and manage data security policies.
* Create and manage virtual environments, particularly in health and wellness.
* Analyze and use the information generated from healthcare computing applications.
* Integrate information from ubiquitous computing applications with health information systems.

Course Topic Schedule

The course will roughly cover the following topics by week and unit, which are associated with the following [Knowledge Areas](https://www.cybok.org/knowledgebase1_1/) (KAs) of the [Cybersecurity Body of Knowledge](http://cybok.org/). Depending on class progress, the units might be adapted.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Unit** | **Week/**  **Module** | **Topic** | **CyBOK KA Coverage** | |
| 1 | 1 | Introduction & Motivation: Introduction to Security | I.2 | Risk Management & Governance |
| 2 | Malware and Social Engineering Attacks | I.3  II.6  II.7  II.8 | Law & Regulation  Malware & Attack Technologies  Adversarial Behaviours  Sec. Operations & Incident Mgmt |
| 3 | 2 | Application and Networking-Based Attacks | III.11  III.14 | Op. Systems & Virtualisation Sec.  Authentication, Authorisation & Accountability |
| 4 | Host, Application, Data Security | II.9  III.10 | Forensics  Cryptography |
| 5 | 3 | Basic Cryptography | III.13  V.18 | Formal Methods for Security  Applied Cryptography |
| 6 | Network Security Fundamentals | III.12  V.19  V.22 | Distributed Systems Security  Network Security  Physical Layer & Telecommun. |
| 7 | 4 | Administering a Secure Network | IV.15 | Software Security |
| 8 | Mobile Device Security | IV.16 | Web & Mobile Security |
| 9 | 5 | Access Control Fundamentals | I.5 | Privacy and Online Rights |
| 10 | Authentication and Account Management | III.14 | Authentication, Authorization & Accountability |
| 11 | 6 | Vulnerability Assessment and Penetration Testing | II.6  II.7  II.8  IV.17 | Malware & Attack Technologies  Adverarial Behaviours  Sec. Operations & Incident Mgmt  Secure Software Lifecycle |

Assignments

You must complete an assignment and a quiz by the end of each learning module, sometimes more frequently, to show your familiarity with the principles and concepts discussed in that module. These assignments will consist of questions, exercises, lab exercises, or writings based on the readings.

Assignments will be distributed and submitted through Blackboard Learn. There will be a **strict deadline** – if you **neglect to submit** your assignment sheet by the time posted, **you will receive zero points** on that assignment sheet. There won’t be any make-up assignments.

Class Project

A class project will accompany the entire course. More information on the class project will be given in class.

Exams

There will be no exams. Successful completion of the course will be assessed by assignments, project, and online discussion participation.

Learning Activities

ALL students enrolled in the course are required to:

* Complete and submit the Course Pre-Work.
* Log into the course site at least 3 times during each module to review announcements, download materials, and keep track of asynchronous discussions in the Discussion Forums.
* Submit all assignments on time. There will be no tolerance on late submissions.
* Contribute at least 1 substantive message and 2 replies in each week's Discussion Forum that:
  + are related to the assigned readings
  + compare/contrast perspectives
  + support ideas with concepts, theories or examples
  + the first post is expected between Monday and Wednesday, and the two peer responses between Wednesday and Saturday.
* Keep an online journal of thoughts and insights relating course topics to your professional practices or interest area.

The learning activities for this course include the following:

***Quizzes.*** You are required to attempt quizzes on a weekly basis. Quizzes will be based on the assigned readings. Note that each quiz would only allow a limited number of attempts. The quizzes will consist of questions/implementation based on the readings and your programming skills which is a prerequisite for successful completion of this course.

***Assignments.*** You must complete an assignment at the end of each learning module to show your familiarity with the principles and concepts discussed in that module.

***Peer Feedback.*** You must post your solutions to assignment sheets in the discussion forums, thereby submitting it to peer review feedback. You must also provide (substantial!) comments on at least three other students to provide peer review feedback.

***Discussion Forum Participation.*** You are required to post at least 1 substantive message and 2 replies to classmates’ messages during each week's discussion forum that:

* are related to the assigned readings
* compare/contrast perspectives
* support ideas with concepts, theories, or examples

Keep in mind that some of the modules last longer than one week, however you are still expected to participate as frequently as above for each week in the module. Please check your writing for spelling and grammar. Use appropriate references and citations in assignments where required. Please refer to the benchmarks for a good message posted under Grading Scheme for reference on how to construct a good message posting. **You must make a substantive message contribution (i.e., create a discussion thread) before you will be able to reply to someone else’s thread.**

Grading

The following grading scheme will be used:

|  |  |  |  |
| --- | --- | --- | --- |
| **Learning Activity** | **Individual Score** | **Total Score** | **Relative Score** |
| Course Pre-Work | 4 points | 4 points | 4 % |
| Discussion Forum Participation | 3 points per week | 18 points (+2 points extra credit for extraordinary contribution) | 18 % |
| Quizzes | 4 points per week | 22 points | 22 % |
| Assignments & Peer Feedback | 5 points per week (2 points for completion and posting,  3 points for providing feedback) | 20 points | 20 % |
| Final Project Report | 18 points | 22 points | 22 % |
| Presentations & Style | 10 points | 10 points | 10 % |
| Course End Work | 4 points | 4 points | 4 % |
|  | **TOTAL** | **100 points** | **100 %** |

Final Grades will be determined using the following scale and honoring +/- designations: A > 90%

B > 80% D > 60%

C > 70% E < 60%

Learning Activities Requirements

***Course Pre-Work.*** You will be required to:

* Complete the intellectual integrity quiz online.
* Complete a pre-course survey regarding your technical skills, study skills, work environment, and expectations for this course.
* Submit a practice assignment.
* Present yourself in the discussion forum for this week.

***Discussion Forum Participation.*** The online learning experience depends on active participation and high-quality contributions from all participants. This is the primary criterion upon which grades are determined and learners exchange ideas. Writing a message is different from writing a term paper or essay. It is a form of communication that has its own limitations and advantages. Below are benchmarks of a good message that will be helpful to you so that you may work effectively in an online environment.

Your message posts will each be **graded out of one (1) point for every two criteria that it meets out of the five benchmarks** below:

* **Substantial**. Messages in your classes should relate to the subject matter and provide information, opinions, interpretations, or questions about that subject matter. They may relate the subject matter to something personal, but they should remain academic in their focus.
* **Concise**. Studies have shown that messages that are several screens long do not get many replies. To write an effective message attempts to use a single screen if possible. Try to get to the point and focus your message so that it is clear what you are saying.
* **Thought-provoking**. The Discussion Forum is an interactive medium. The more interaction, the better. A good message is one that prompts others to reply or object. A focused and pointed message that produces replies from other learners in the class moves the discussion forward and has an impact on the learning environment.
* **Timely.** A good message appears in the context of similar messages in the Discussion Forum. If you get online irregularly, your message will appear late and out of context to what is currently happening in the Forum. Get online regularly and reply to messages in a timely fashion.
* **Logical.** A good message that is not a question should contain a logical argument. This means it should contain a clearly stated conclusion or thesis supported by premises, reason, evidence, or grounds of belief. This encourages critical thinking in the discussion.
* **Grammatical.** A good message should be well-written using standard English and syntax. This means you must review both quality of content and writing of messages. You may find it helpful to draft your contributions outside of the course site in your word processing software to check grammar and spelling, and then cut and paste your posting into a message window.

***Journal Writing.*** You are required to keep an online journal of weekly insights relating course topics to your professional practices or interest area. **These will be reviewed periodically during the course by the instructor.**

***Quizzes.*** You must complete a quiz at the end of each learning module to show your familiarity with the principles and concepts discussed in that module. **Quizzes are graded based on answer correctness by the instructor.**

***Assignments.*** You must complete an assignment at the end of each learning module to show your familiarity with the principles and concepts discussed in that module. The assignments in this class take the form of a series of case studies. Each case study will comprise the following components:

* problem comprehension
* proposed solution

The assignment will have a technical component using software tools to practice security concepts in a practical manner. **Assignments will be graded through peer review, for which you will receive one (1) point for completing the assignment (i.e., by uploading it to the Blackboard assignment dropbox); one (1) point for posting your solution in the discussion forums; and up to three (3) points for providing feedback to others’ solutions with comments that meet the above message criteria.**

***Final Project with Report*.** The project consists of two parts:

1. conducting a penetration test of a vulnerable system
2. a report outlining the vector of attack.

The report shall contain an analysis portion that gives comments, concerns, questions raised, and evaluations of the security of the attacked system. Note that there is no exact format required, however emphasis on clear and successful communication of the findings. In your report, do not expect to get a 100% unless you have perfect grammar, good writing style, excellent summaries, as well as a thorough and critical analysis of the attack you conducted.

***Course End-Work.*** You will be required to:

* Complete a learner-centered course evaluation online.
* (Extra Credit) Submit a one-page reflection paper.

Required Texts

The following texts are **required**. Additional texts will be made available in class. You will be expected to read and study all material as it is discussed, without explicit assignment of readings.

* Rashid, Awais; Chivers, Howard; Lupu, Emil; Martin, Andrew; Schneider, Steve (Eds.): CyBOK The Cyber Security Body of Knowledge v1.1.0. University of Bristol, 2021. Available at: <https://www.cybok.org/media/downloads/CyBOK_v1.1.0.pdf>
* Ciampa, Mark: CompTIA Security+ Guide to Network Security Fundamentals , 5th Edition. <https://www.amazon.com/CompTIA-Security-Network-FundamentalsCertBlaster/dp/1305093917>

Recommended (but not required) books:

* Pfleeger, Charles; Lawrence Pfleeger, Shari; Margulies, Jonathan: Security in Computing, 5th edition, Prentice, Hall. ISBN: 978-0132390774.
* Pfleeger, Charles; Lawrence Pfleeger, Shari: A Threat / Vulnerability / Countermeasure Approach, Prentice Hall. ISBN: 9780132789462.

Disability Statement

If you have a disabling condition, which may interfere with your ability to successfully complete this course, please contact the Office of Accessibility Resources at oar@oswego.edu and x3358. Additional resources can be found here: <http://www.oswego.edu/student/services/disabilities.html>

Intellectual and Academic Integrity

This course will strictly adhere to the university’s policy. **A student found to be in violation of this policy will receive negative the maximum score for the learning activity in question and will be officially reported.** Repeated violations and cases of particularly deceitful behavior may also receive a failing grade for the course, at the discretion of the instructor, and judicial charges may be filed. SUNY Oswego’s policy may be found at:

<http://catalog.oswego.edu/content.php?catoid=1&navoid=12#inte_inte>

Copyright Statement

Unless otherwise noted, all course material is copyrighted and made available for personal use of students enrolled in this course for the purpose of education only. All commercial use or distribution of the material, or excerpts thereof, in any form, for example by uploading it to online course websites (including, but not limited to Oneclass.com, Gradebuddy.com, Studyblue.com, coursehero.com, studysoup.com, chegg.com, Quizlet.com, or comparable websites) is strictly prohibited, will be considered an intellectual integrity violation, and will be prosecuted to the fullest extent of the law.

Changes to the Syllabus and the Course

Changes to the syllabus or the course can occur at any point and will be announced.