CSIS-160: INFORMATION SECURITY SYSTEMS

Effective Term
Fall 2025

BOT Approval Date
12/17/2024

Discipline
CSIS - Computer Sci/Info Systems

Course Number
160

Course Title
Information Security Systems

Short Title
Info Security Systems

Credit Status (CB 04)
D - Credit - Degree applicable

Units

Lecture Units
3.00

Total Units
3.00

Hours

Lecture Contact Hours
3.00

Out of Class Hours Lecture
96-108

Total Contact Hours
48 - 54

Total Out of Class Hours
96 - 108

Total Student Learning Hours
144 - 162

Distance Education
Yes

Distance Education

Distance Education Type
Both Fully Online and Hybrid Online

Fully Online Delivery Requirements:
a. Students must be notified via the college schedule of classes and the syllabus for the class if proctored tests are required for this course
b. Any planned face-to-face meetings, such as an orientation or study session, must be optional

c. The MSJC curriculum committee requires the use of accessible, asynchronous discussion as a component of every fully online course

Are you using publisher content?

No

Regular Substantive Interaction

Instructor-to-student, student-to-student, and student-to-content contact shall be distributed in a manner that will ensure regular substantive interaction (RSI) is maintained not only weekly but also for the duration of the course. Instructor interactions should be equivalent in time, quality and consistency to the engagement students would receive in a face-to-face course—for example, through announcements, discussion participation, personalized feedback, video messages, or other instructional communications. Instructors are expected to be responsive to student inquiries within a 24-72 hour time frame excluding holidays. RSI will be maintained through a variety of methods: • Orientation - Students must be oriented to the online and face-to-face portions at the start of the course. • Announcements - Announcements using the course management system must be posted at least weekly to keep students current on course events, due dates, materials, etc. • Discussion Forums - Content-related discussion forums within the designated CMS will include appropriate instructor participation and will be initiated and maintained, with timely feedback provided. Instructors are required to monitor the discussions and related activities to provide guidance and direction. Open-ended discussion boards may be used to further learning and interaction. • MSJC Communication – Instructor will use MSJC-administered communication tools (such as email or the designated CMS communication tools) to regularly communicate with and provide ease of access to students. • Timely Feedback - Timely feedback on student work will be provided by the instructor, which may include comments and/or rubrics, within the Grades area of the designated CMS. • Scheduled Meetings – Hybrid and synchronous courses will meet at regularly scheduled times. ADA Compliance - All course interactions and content must be designed with accessibility in mind and meet ADA requirements.

Catalog Description

This course is a survey of Network/Internet security. It will help prepare students for the CompTIA Security+ Exam. Topics will cover Authentication, Malicious Code, Web Security, Intrusion Detection, Cryptography, and Biometrics. The class will have lecture and hands-on components.

Codes

TOP Code (CB 03)

0708.10* - *Computer Networking

CIP Code

11.1003 - Computer and Information Systems Security/Information Assurance.

Repeatability Code

No

Grading Option

Letter grade OR P/NP

Learning Objectives

Learning Objectives

Learning Objective
1. Analyze the role of security protocols in data networks.
2. Assess network security and propose methods for improvment.
3. Illustrate the devices and services used to support securing data networks and Internet access.
4. Evaluate fundamental security concepts such as secure sockets layer, digital certificates, digital signatures, one-way hashing, and encryption.
5. Compose a security configuration to deal with specific threats against the data communications network.
6. Analyze the type of security threats that threaten a network to determine best practices policies that need to be implemented.
7. Construct a security plan for protecting business assets like servers, data, and business rules.
8. Appraise new security devices and security protocols for applicability of implementation for specific security threats.
9.Explore the impact of diversity, equity, and inclusion on information security, addressing cultural, social, and economic influences on threat landscapes

10. Develop strategies to foster diversity, equity, and inclusion within security practices, enhancing effectiveness through diverse perspectives.

Learning Outcome Information

Course Learning Outcomes

Learning Outcome
1. The student will analyze a data communications security implementation strategy for protecting a company's digital assets.
2. The student will develop a data communications security implementation strategy for protecting a company's digital assets.
3. The student will assess a data communications security implementation strategy for protecting a company's digital assets.

Program Learning Outcomes

Learning Outcome
Research and apply industry reference models and best practices in order to improve process designs. Apply systems concepts in the investigation, evaluation, and resolution of information technology problems.

Institutional Learning Outcomes

Information and Technology Literacy: The student will access, interpret, evaluate, and apply relevant information sources and digital media effectively, and in an ethical and legal manner.
Scientific Awareness: The student will apply the scientific method of inquiry to assess potential solutions for real-life challenges by employing science-based knowledge and methodologies in daily life.

Content

Course Lecture Content

1. Network Security
   a. Network Devices and Technology
   b. Secure Network Administration Principles
   c. Network Design Elements and Compound
   d. Network Protocols
   e. Ports
2. Compliance And Operational Security
   a. Risk Analysis
   b. Risk Mitigation Strategies
   c. Incident Response Procedures
   d. Security Awareness and Training
   e. Business Continuity
   f. Environmental Controls
   g. Recovery Plans and Procedures
3. Threats And Vulnerabilities
   a. Malware
   b. Varieties of Attacks
   c. Social Engineering Attacks
   d. Wireless Attacks
   e. Application Attacks
   f. Mitigation and Deterrent Techniques
   g. Security Threats and Vulnerabilities
   h. Penetration Testing
4. Application, Data And Host Security
   a. Application Security
   b. Host Security Procedures
   c. Importance of Data Security
5. Access Control And Data Management

a. Authentication Services
b. Authentication, Authorization and Access Control
c. Account Management

6. Cryptography
   a. Concepts
      i. Tools and Products
      ii. Public Key Infrastructure
      iii. Certificate Management
      iv. Associated Components
7. Understanding Racial Bias in Information Security
   a. Historical Context of Racial Bias in Technical Fields
   b. Analysis of Racial Bias in Information Security Systems
   c. Implications of Racial Bias on Diversity and Inclusion

Methods of Instruction

Method

Discussion

Integration

Weekly discussion will be conducted as a means to compare and contrast various security vulnerabilities, threat Analysis plans, and Intrusion Event Categories.

DE Adaptations for MOI

Discussions will take place through the course management system's (CMS) discussion tool, which is designed with accessibility in mind. Features such as screen reader support, adjustable text size, and keyboard navigation ensure that all students can actively participate. Feedback on discussion contributions will be provided via the CMS within one week, ensuring timely and accessible engagement for every student.

Method

Lecture

Integration

Lecture, with supporting visual materials (presentation or multimedia) will introduce conceptual and practical skills such as assessing different access control models, rating the effectiveness of various data ciphers, and the appraisal of different Antimalware and Antivirus software tools.

DE Adaptations for MOI

The CMS will serve as a central hub for online students, providing accessible recorded lectures, online presentations, and supplementary materials.To ensure inclusivity, all lectures—including live and recorded ones—will be conducted with closed captioning (cc). Live online lectures will allow for real-time interaction and discussions.

Method

Lab Activities

Integration

Guided practice and demonstration will illustrate lecture principles and reading assignments, with a focus on Intrusion Analysis, security attacks, and threat analysis

DE Adaptations for MOI

Guided practice and demonstrations will be available within the CMS, utilizing accessible closed-captioned videos, web-based tutorials, and hands-on activities. Interactive software simulations hosted within the CMS will offer students opportunities for real-time engagement and practice, ensuring accessibility and active learning for all users.

Methods of Evaluation

Method

Exams/Tests

Integration

A midterm and final exam will be given. The exams will be composed of short answer and multiple choice questions designed to evaluate the mastery of such topics as incident response teams, intrusion analysis, security attacks, and access control models. Exams will be evaluated based on the correct answer given.

DE Adaptations for MOE

The midterm exam will be administered through the course management system (CMS), consisting of multiple-choice, true/false, and short-answer questions. Students will submit their completed exams directly through the CMS. Immediate feedback will be provided for objective questions (such as multiple-choice and true/false), while feedback on short-answer responses will be given within 48 hours. This ensures timely reinforcement of learning and clarity on areas for improvement.

Method

Homework

Integration

Weekly assignments will be given that apply important concepts and skills to the student's experience outside the classroom. The focus might be on network security devices, access control models, or Antimalware and Antivirus software tools. Homework will be evaluated based on a pre-established rubric for correctness, completeness, and how well directions were followed. The resulting score and instructor feedback (when applicable) will be posted in the College CMS.

DE Adaptations for MOE

Homework will be evaluated based on correctness, completeness, and adherence to instructions. Assignments will be submitted using the assignment editor within the course management system (CMS). Students will receive detailed feedback through the CMS grading tool, which will include comments on areas of improvement and strengths. Feedback will be provided within one week of the submission deadline. Additionally, students can submit assignments via discussion boards, blogs, or wiki tools within the CMS, depending on the task requirements.

Method

Quizzes

Integration

Weekly multiple choice / short answer quizzes will be given as a means to test the students knowledge of Intrusion event categories, threat analysis, cipher effectiveness, and security vulnerabilities. Quizzes will be evaluated based on the correct answer given.

DE Adaptations for MOE

Quizzes will be delivered and submitted through the Quiz tool within the course management system (CMS). Once submitted, students will receive immediate feedback for automatically graded questions, such as multiple-choice or true/false. For short-answer or more detailed questions, feedback will be provided within 48 hours through the CMS, allowing students to review their performance and areas for improvement in a timely manner.

Assignments

Assignment Type

Reading

In-class and/or outside of class

Outside of class

Formative or Summative

Summative

Assignment

Background:
The United Kingdom's National Cyber Security Centre (NCSC) recently replaced racially charged terms like "whitelist" and "blacklist" with more inclusive alternatives, sparking discussions on inclusivity in cybersecurity. This assignment explores the implications of this change from a diversity, equity, and inclusion (DEI) perspective, aiming to help students critically evaluate the role of language in shaping professional environments.

Assignment Overview:
For this project, you will analyze the historical context of racially charged terminology in cybersecurity and its broader implications for diversity and inclusion. You will provide a detailed examination of the impact such language can have on marginalized communities and propose actionable solutions to create a more inclusive industry.

Tasks:
Analysis of Racial Bias:
Investigate the historical origins of terms like "whitelist" and "blacklist" and how these terms may reinforce racial stereotypes.
Discuss the potential harm such terminology might have on marginalized communities in the information security sector.
Examine the broader implications of using racially charged language within technical and professional discourse.
Implications for Diversity:
Analyze how insensitive language can create an unwelcoming environment for diverse professionals in the information security field.
Evaluate how terminology influences perceptions of inclusivity and diversity within organizations.
Discuss the benefits of adopting more inclusive language in cybersecurity discourse and how it can foster a more welcoming professional environment.
Proposed Actions:
Propose steps that could be taken to address racial bias in information security terminology. Consider solutions such as updating terminology, training programs, or policy changes, and analyze their potential impact on promoting inclusivity within the industry.

Reading: "Are these Common Cybersecurity Terms 'Racist'?" by SecureWorld News Team

Criteria for Evaluation: Grading and feedback by following criteria
1. Depth of analysis regarding the causes and implications of bias.
2. Feasibility and innovativeness of proposed solutions.
3. Clarity, coherence, and structure of the written assignment

How assignment will be adapted in online format

This assignment will take place through an online discussion board. Students will submit their analyses and proposed actions as initial posts on the board, followed by responses to at least two classmates' posts to foster peer discussion. The assigned article will be available via the course management system (CMS), either as a PDF or a link. Submissions will be made directly through the CMS discussion board.Feedback on your work will be provided through the CMS within one week of submission. instructor will evaluate both the initial submission and the interaction in the discussion, providing detailed feedback on the depth of your analysis, the innovativeness of your solutions, and the quality of your writing. This will ensure that feedback is timely and constructive, enabling you to reflect on your learning effectively.

Assignment Type

Writing

In-class and/or outside of class

In-class
Outside of class

Formative or Summative

Formative

Assignment

Throughout this course, you will complete a series of case projects, review questions, and hands-on activities to develop practical skills and reinforce your understanding of key information security systems concepts. These assignments will help you apply theoretical knowledge to real-world scenarios and evaluate your comprehension of course material.

Assignment Overview:

In this project, you will assume the role of an intern at Bay Point Ridge Security (BPRS), a managed service provider (MSP) that manages networks, computers, cloud resources, and information security for small-to-medium enterprises (SMEs). BPRS has asked you to prepare a presentation on common web application attacks and write a report on a specific security vulnerability.

Tasks:
PowerPoint Presentation on Web Application Attacks:
Create a PowerPoint presentation that covers the following four types of web application attacks:
Cross-Site Scripting (XSS)
SQL Injection (SQLi)
Cross-Site Request Forgery (CSRF)
Server-Side Request Forgery (SSRF)
Compare and contrast these attacks, discussing how they exploit web applications and how they can be mitigated.
Your presentation should be between 10-12 slides and include detailed information about each attack, examples, and recommendations for preventing them.
One-Page Report on Race Conditions:
Following your presentation, write a one-page report on race conditions, a security vulnerability that occurs when multiple operations execute simultaneously in a way that leads to unintended outcomes.
Use online resources to research race conditions and discuss how they occur and how they can be mitigated or addressed in information security systems.

Grading and Feedback: Evaluate the students' performance on projects and review questions within the domain of information security systems. Assess the technical accuracy of their solutions, ensuring thoroughness and effectiveness. Recognize their efforts in problem-solving and critical thinking, regardless of the final outcome. Provide unbiased feedback that respects the diverse cultural, racial, and gender backgrounds of all students, focusing on constructive criticism related to the task at hand rather than personal attributes. Grades for case projects and review questions will be provided within a week.

How assignment will be adapted in online format

This course will integrate case projects, review questions, and hands-on activities within the online learning environment. You will access course materials and submit your PowerPoint presentation and report electronically through the course management system (CMS). The PowerPoint presentation will be submitted as a file upload, and your one-page report will be submitted through a text or PDF upload in the same CMS. Simulations and discussion forums will be available for hands-on activities related to the case projects, and virtual communication tools will facilitate discussions and feedback. Instructors will provide feedback through the CMS within one week of submission, offering comments on your presentation content, report structure, and technical accuracy. Virtual office hours will be available for students who need additional guidance or clarification, ensuring timely and supportive feedback throughout the course.

Assignment Type

Writing

In-class and/or outside of class

In-class
Outside of class

Formative or Summative

Summative

Assignment

Complete a final project that demonstrates your understanding of information security systems concepts and your ability to apply these concepts in a real-world scenario. The final project will involve designing, implementing, and managing an information security system or network, and will require the integration of various skills and knowledge gained throughout the course.

Example Final Project: Design and implement an information security system for a medium-sized organization, including network security measures, access controls, encryption protocols, intrusion detection systems, and incident response procedures. Document the setup process, the rationale behind design choices, and provide a user guide for the system.

Grading and Feedback: Evaluate the technical completeness and correctness of the information security configurations, protocols, scripts, or solutions proposed. Examine the quality of the project report, ensuring it's comprehensive, structured, and well-documented. For projects that require a presentation, evaluate clarity, confidence, and the ability to answer questions. Ensure that feedback is objective, unbiased, and recognizes the diverse backgrounds and perspectives students bring to their projects. The final project will be graded by finals week.

How assignment will be adapted in online format

The final project will be submitted through the course management system, along with any supporting documentation and files. Instructors will provide feedback and guidance during the project development process, and students will receive a comprehensive evaluation of their final submission, including feedback on both technical and documentation aspects. Final feedback will be delivered through the CMS within one week of the project submission, ensuring students receive timely and detailed insights into their performance.

Course Materials

Textbooks

CompTIA Security+ Guide to Network Security Fundamentals
by Mark Ciampa

8th Edition | Copyright 2025
ISBN-13: 9798214000633

Class Size Information

Class Size

35

Class Size Category

B - Facilitated learning 35

Diversity and Inclusion

Explain how diversity and inclusion(e.g., gender, culture/race, sexuality, etc.) is infused into the course.

Diversity and inclusion are integral to our Information Security Systems class, ensuring every student feels valued. Through diverse perspectives in our curriculum, inclusive pedagogy, and supportive classroom environment, we cultivate respect and understanding. Faculty receive training to enhance cultural competence, and students engage in critical discussions on ethics and bias. By infusing diversity and inclusion, we empower students to become inclusive security professionals ready to navigate global challenges. For example, Dr. Suranjit Kumar Sippy, a security researcher, made significant contributions to information security through his work on intrusion detection systems.

Describe how assignments, instruction, evaluation, course content, and interactions are contextualized for diverse learners promoting an equitable course.

Representation in course materials: The course content will be carefully curated to ensure representation of diverse individuals and groups. Case studies, examples, and images featured in the course materials will highlight the contributions and experiences of people from various cultural, ethnic, and socio-economic backgrounds. This approach aims to promote inclusivity and ensure that all students feel acknowledged and able to relate to the material, fostering a sense of belonging in the classroom. For example the course content includes the following selections:
#Historical Context of Racial Bias in Technical Fields
#Analysis of Racial Bias in Information Security Systems
#Implications of Racial Bias on Diversity and Inclusion

Real-world scenarios: The assignments and projects within the course will emphasize real-world scenarios that involve diverse populations and contexts in the realm of Information Security Systems. This approach enables students to understand the importance of considering diversity and inclusion when designing and implementing security measures and networks.

Addressing bias and stereotypes: The course will discuss potential biases and stereotypes that may exist within the field of Information Security Systems, with a focus on how they manifest in system administration and network security. By acknowledging these issues, students can become more aware of their own biases and work towards creating a more inclusive and equitable environment in their professional practice.

Encouraging diverse perspectives: Group discussions, collaborative projects, and peer evaluations will be structured to encourage the sharing of diverse perspectives and experiences within the realm of Information Security Systems. This approach promotes open-

mindedness, empathy, and a greater understanding of the importance of diversity and inclusion in the field of security administration and network management.

Cultivating an inclusive learning environment: The instructor will establish a safe and supportive learning environment where students feel comfortable expressing their thoughts and ideas without fear of judgment or discrimination in the realm of Information Security Systems. This includes setting clear expectations for respectful communication, providing opportunities for anonymous feedback, and actively addressing any incidents of discrimination or bias that may arise during the course of study.

Interactions

Explain how the course will incorporate student-to-student interaction.

a. Collaborative Projects: Students will engage in group work for the final project, where they design and implement a comprehensive information security system, incorporating network security measures, access controls, encryption, and intrusion detection systems. By working in groups, students will collaboratively discuss design strategies, divide tasks, and present solutions, fostering teamwork and peer-to-peer problem-solving. This interaction directly aligns with the Guided Practice and Demonstration (MOI), allowing students to learn from each other as they tackle complex security challenges similar to those in their formative web application attack presentation and race conditions report.
b. Interactive Classroom Sessions: In lecture-based sessions, students will participate in group discussions that apply the content covered in class, such as exploring strategies to prevent specific types of web application attacks (XSS, SQLi, CSRF, SSRF). These group activities, facilitated through the Lecture (MOI), require students to collaborate on applying theoretical concepts, enabling them to compare methods for securing web applications. Working together, students can build upon each other's knowledge, linking these discussions to their formative assignment content.
c. Online Discussion Platforms: The "Student Lounge" within the CMS will allow informal interactions where students can share additional resources and tips for tackling assignments like the presentation on web application attacks. Formal discussion boards will focus on specific security concepts, like race conditions, facilitating in-depth discussions on vulnerability mitigation. This peer interaction encourages students to engage with each other's insights and problem-solving approaches, promoting a collaborative atmosphere that enhances understanding of formative assignments.

Explain how the course will incorporate instructor-to-student interaction.

a. Course Introduction Package: At the start of the course, students will receive a welcome letter and orientation video introducing the Lecture (MOI) and setting expectations for both formative and summative assignments. The package outlines the approach to the formative assignment on web application attacks, ensuring students understand how to structure their presentation and report submissions. Additionally, it provides guidance on how to engage with the instructor for assignment feedback, helping students feel prepared and supported.

b. Weekly Updates: Each week, the instructor will post CMS updates with reminders about project deadlines, including those for the final project and the web application attack presentation. Weekly reminders help keep students on track with their assignments, align with the Homework and Quizzes (MOE) schedule, and clarify instructor expectations. This consistent communication ensures students stay engaged with both formative and summative assignments.

c. Interactive Discussion Platforms: Dedicated discussion boards for each unit allow students to ask assignment-related questions, such as those about the formative web application attack presentation. The instructor will regularly participate in these discussions, offering clarifications and guidance. For instance, if students are unsure about specific technical terms in their report on race conditions, the instructor will provide timely responses to deepen their understanding, aligning with Guided Practice and Demonstration (MOI).
d. Accessible Support Channels: Virtual office hours and email support enable personalized, one-on-one interaction between the instructor and students, particularly during the final project phase. As students work on designing their information security systems, they can consult the instructor for feedback on their network security measures or encryption protocols, ensuring alignment with course objectives. This support offers students tailored feedback, enhancing their grasp of complex security concepts.

Explain how the course will incorporate student-to-content interaction.

a. Interactive Lecture Sessions: Online lectures will include "test your knowledge" segments on topics such as security vulnerabilities and race conditions. These interactive sections, part of the Lecture (MOI) and weekly Quizzes (MOE), prompt students to actively engage with course content, providing real-time feedback on their comprehension. This continuous engagement prepares students for more in-depth tasks, such as their formative assignment on web application attacks.

b. Educational Video Clips: Short video clips reinforcing lecture content will demonstrate specific attacks like SQL Injection and XSS. These clips are directly linked to the web application attack presentation, providing a visual supplement to the hands-on task of analyzing and presenting these attacks. This pairing of content with assignment requirements ensures that students are actively engaging with course materials in a meaningful way.

c. Application Exercises and Practice Materials: Various application exercises, such as case studies on threat analysis and vulnerability mitigation, reinforce the Homework (MOE) and Guided Practice (MOI) approaches. These exercises build on lecture content, preparing students for more comprehensive assignments, including the final project. Consistent practice enhances students' ability to apply theoretical knowledge and fosters a deeper understanding of key security concepts.

Explain how the course will incorporate student-to-self interaction (metacognitive).

a. Reflective Self-Evaluation: After completing assignments, such as the report on race conditions, students will submit reflective self-assessments. These reflections encourage critical thinking about their learning process and prompt students to consider the implications of inclusivity in information security. This metacognitive activity aligns with both formative and summative assignments, fostering self-awareness and deeper comprehension of course material.

b. Diverse Problem-Solving Approaches: Throughout the course, students will be encouraged to reflect on the effectiveness of various problem-solving strategies they used in assignments, including their approach to mitigating web application attacks. Reflecting on these strategies will help students identify which techniques worked best, cultivating metacognitive awareness of their learning processes. This self-reflection is particularly useful for completing the final project, as students adapt their strategies to tackle complex tasks in their security systems.

Key: 1063