CS 471–02 Security & Info Assurance

Instructor: Christopher Smith
Email: christopher.smith@csueastbay.edu **Phone:** 510 885-4300 (CS Department)

Office Hours

Office Location:

Zoom conference Wednesdays.
In-person Thursdays in North Science Building Room N154

Office Hours:

Wednesday(Zoom) 2:00-3:00pm and
Thursday(N154) 12:30-1:30pm

Office Hour Zoom Link:
https://csueb.zoom.us/j/83616322133?pwd=bVg3RlczM1c3MSswYkRYYm1xUGw4QT09

Class Meeting Time and Location

Time: Monday and Wednesday 5:00PM – 6:15PM
January 17 -- May 13 2023
Location: Zoom Conference
https://csueb.zoom.us/j/89819309377?pwd=disvdEZORVVROVozUCtrSS9jSHpaZz09

Course Format

Class lectures are held over Zoom video conference and will be structured as synchronous class meetings. All students are expected to show up on time, share your video, and participate in class discussion. Lecture attendance and video sharing is required.

Catalog Description

Fundamentals of network and computer security. Security services and mechanisms, models, cryptography, network and wireless security, digital forensics, security threats and vulnerabilities, risk analysis and management models, security attacks and policies, and legal and regulatory issues. Programming projects.
Prerequisites: CS 301 with grade C- or better. Grading: A-F grading only.
Equivalent Quarter Course: CS 4525 or CS 4526 or CS 4527.

Prerequisites

CS 301 with grade C- or better.

Required Text

William Stallings, Network Security Essentials Applications and Standards, 6th Edition.
ISBN: 978-0134527338

STUDENT LEARNING OUTCOMES

Students will be able to:

1. Describe key network security requirements

2. Present main concepts of symmetric cryptography (DES, AES algorithms)

3. Present main concepts of asymmetric cryptography (RSA, Diffe-Hellman, ECC)

4. Present an overview of the basic structure and usage of cryptographic hash functions (SHA-1, MD5)

5. Present an overview of techniques for remote user authentication using symmetric encryption (Kerberos)

6. Describe Web security threats and security approaches

7. Present an overview of Secure Socket Layer (SSL/TLS)

8. Present an overview of the operation of PGP (Pretty Good Privacy)

9. Understand the functionality of S/MIME and security threats it addresses

10. Present an overview of IP security (IPsec)

11. Present an overview of Firewalls, Viruses and Intrusion Detection Systems

12. Practice different Hacking Techniques

13. Apply critical thinking and problem solving skills by analyzing security problems, designing solutions, and evaluating results.

14. Demonstrate communication skills in both written and oral form, and work in a team environment. (WIKI, EP and Discussion group activities)

15. Independently and collaboratively acquire new network sec security skills through analysis of current computer science literature and industrial practices. (EP)

Advice and Consultation

All programming projects are to be individual efforts, not group efforts. This means that there should be no sharing of code; such sharing constitutes academic dishonesty, as described below and in the CSUEB catalog. Only submit your own original work.

Academic honesty is expected from each student. If a student is academically dishonest, the student will receive a 0 for the assignment or exam and an academic dishonesty report will be filed as required by the department. This will occur on the first offense. Note: I am required to report ANY EVIDENCE of academic dishonesty. You will be notified via email and Canvas. Once you have been notified a report has been filed, your recourse is to contest the report with the appropriate committee using the procedures outline in the link below. By enrolling in this class the student agrees to uphold the standards of academic integrity described at http://www20.csueastbay.edu/academic/academic-policies/academic-dishonesty.html

Only submit your own original work.

Canvas

This course makes extensive use of Canvas. Assignments, sample problems, solutions, announcements, etc are submitted and/or posted through Canvas. Be sure to check it often!

Course Schedule

Week #	Monday	Wednesday	Reading	Weekly Topic	Due	Assigned
1	01/16/23	01/18/23		Getting started		
2	01/23/23	01/25/23	Chapter 1	Introduction		Assignment 1
3	01/30/23	02/01/23	Chapter 2	Symmetric Encryption	Assignment 1	Assignment 2
4	02/06/23	02/08/23	Chapter 3	Asymmetric Encryption	Assignment 2	Assignment 3
5	02/13/23	02/15/23	Chapter 4	Key Distribution and Authentication	Assignment 3	
6	02/20/23	02/22/23	Chapters 1-4	Review : **Midterm 1**		
7	02/27/23	03/01/23	Chapter 5	Network Access Control		Assignment 4
8	03/06/23	03/08/23	Chapter 6	Transport Level Security	Assignment 4	Assignment 5
9	03/13/23	03/15/23	Chapter 7	Wireless Network Security		
10	03/20/23	03/22/23	Chapter 8	DNS and Email Security	Assignment 5	
11	03/27/23	03/29/23		Spring Break		
12	04/03/23	04/05/23	Chapters 1-8	Review : **Midterm 2**		
13	04/10/23	04/12/23	Chapter 9	IP Security		Assignment 6
14	04/17/23	04/19/23	Chapter 10	Malicious Software	Assignment 6	Assignment 7
15	04/24/23	04/26/23	Chapter 11	IDS		
16	05/01/23	05/03/23	Chapter 12	Firewalls	Assignment 7	
17	05/08/23	05/10/23		Finals Week		
	*No Meeting			Final Exam: **TBD**		

Dates in red are school holidays. There will be no lecture.

*Changes to the schedule may be required. This is a guide and is subject to changes.

Grading Breakdown

Homework 30% of final grade

Exam 1 20% of final grade

Exam 2 20% of final grade

Exam 3 (Final) 30% of final grade

Grading Scale

90 – 100% A

80 – 89% B

70 – 79% C

60 – 69% D

0 – 59% F

The top and bottom ranges of each grade level will earn pluses or minuses respectively.

Assessments

Homework

There will be 6-8 homework assignments. Assignments will a mix of programming, using security software or tools, and documenting your results. Most assignments will be directly based on demonstrations from lecture. Read, attend lecture, then complete the assignment for best results.

All assignments are submitted via Canvas. Due dates for assignments are posted on Canvas.

Submissions must be the result of the student's own work, using techniques discussed in class and the text book. Implementing solutions from code found on the internet will constitute a violation of the Academic Dishonesty Policy. Base your solutions from examples in the text and concepts discussed in class. If in doubt, ask.

Homework assignments are worth 50-100 points. Partial credit will be awarded for programs, where each minor defects will result in a small point deduction each and major defects will result in multiple point deductions.

No late assignments will be accepted.

No extra credit assignments will be made available.

It is the student's responsibility to keep current on all due dates.

Exams

There will be two midterm exams and one final exam.

All exams will be held using Canvas and the Respondus Lockdown Browser. For these exams, a video camera or web cam will be required. For more information about the Respondus Lockdown Browser, see Canvas.

It is the student’s responsibility to make any special scheduling arrangements in advance of exams. No make up exams will be given without prior arrangements.

Final Exam Schedule

Please review the CSUEB final exam schedule here:
https://www.csueastbay.edu/students/academics-and-studying/finals/fall.html

The final exam for this course is scheduled for **TBD**

University policies regarding cheating and academic dishonesty

By enrolling in this class the student agrees to uphold the standards of academic integrity described at http://www20.csueastbay.edu/academic/academic-policies/academic-dishonesty.html

Accommodations for students with disabilities

If you have a documented disability and wish to discuss academic accommodations, or if you would need assistance in the event of an emergency evacuation, please contact me as soon as possible. Students with disabilities needing accommodation should speak with the Accessibility Services.

Emergency Information

California State University, East Bay is committed to being a safe and caring community. Your appropriate response in the event of an emergency can help save lives. Information on what to do in an emergency situation (earthquake, electrical outage, fire, extreme heat, severe storm, hazardous materials, terrorist attack) may be found at:

http://www20.csueastbay.edu/af/departments/risk-management/ehs/emergency-management/index.html

Please be familiar with these procedures. Information on this page is updated as required. Please review the information on a regular basis.

Discrimination, Harassment, and Retaliation (DHR)Title IX and CSU policy prohibit discrimination, harassment and retaliation, including Sex Discrimination, Sexual Harassment or SexualViolence

CSUEB encourages anyone experiencing such behavior to report their concerns immediately. CSUEB has both confidential and non-confidential resources and reporting options available to you. Non-confidential resources include faculty and staff, who are required to report all incidents and thus cannot promise confidentiality. Faculty and staff must provide the campus Title IX coordinator and or the DHR Administrator with relevant details such as the names of those involved in an incident. For confidential services, contact the Confidential Advocate at 510-885-3700 or go to the Student Health and Counseling Center. For 24-hour crisis services call the BAWAR hotline at 510-845-7273. For more information about policies and resources or reporting options, please visit the following websites:

http://www.csueastbay.edu/af/departments/risk-management/investigations/register-complaints.html
http://www.csueastbay.edu/titleix

Safe and healthy living

The University is committed to maintaining a safe and healthy living and learning environment for students, faculty, and staff. Each member of the campus community should choose behaviors that contribute toward this end

http://www.csueastbay.edu/studentconduct/student-conduct.html