TCN 4081

Telecommunication Network Security

Section: RVC

Internet/Fully Online

Spring Term 2026

Course Time Zone: Eastern Time (ET). Course due dates and times are according to this time zone.

Professor Information

Yu Du

Roles: Primary Instructor

Email: ydu@fiu.edu

Phone: 305-348-2886

Office Hours: By appointment

Office Location: EC3832

Website: yudu.fiu.edu

Department or Academic Unit: Electrical and Computer Engineering

Course Prerequisites

Course prerequisites, if any, are listed below.

Prerequisites: (TCN4211 or permission of the instructor)

Course Description

Introduction and overview of security issues for engineering applications. Topics include design, implementation, and management of security in networks.
(3 credits)

Textbook and Course Materials

EBK COMPTIA SECURITY+GDE TO NETWORK..

Required/Recommended: Required

Authors: CIAMPA

Publisher: VST

Publication Date: August 5, 2014

Copyright Date: August 5, 2014

ISBN 10: 1305093917

ISBN 13: 9781305093911

Chapters/Pages: chapter 1~15

EBK COMPTIA SECURITY+GDE TO NETWORK..

Required/Recommended: Required

Authors: CIAMPA

Publisher: VST

Publication Date: August 5, 2014

Copyright Date: August 5, 2014

ISBN 10: 1305093917

ISBN 13: 9781305093911

Notes: You can buy an e-book or hardcopy of it

Chapters/Pages: Chapter 1~15

Panther Book Pack

Get all required course materials for $20.50 per undergrad credit hour through Panther Book Pack. You'll be charged automatically unless you opt out within 3 days after the add/drop deadline.

For more details, to compare costs, and to learn how to access your course materials, visit the Panther Book Pack information page on FIU OneStop.

Readings, Materials, and Open Educational Resources (OER)

To successfully participate in this course, students are required to have access to the following hardware and software:

Hardware:

A computer has reliable internet connection for accessing course materials, participating in virtual sessions, and submitting assignments.

A webcam and microphone for virtual meetings, presentations, and office hours.

Software:

Zoom (or equivalent video conferencing tool) for virtual meetings.

Canvas (course management system) access.

Student Learning Outcomes/Objectives

- **Level I – Remembering (Knowledge): o Recall the vulnerabilities associated with network attacks. o Identify types of malware and social engineering attacks. o List various cryptographic methods. o Recognize key concepts in number theory related to cipher techniques.**

- **Level II – Understanding: o Explain the vulnerabilities that make networks susceptible to attacks. o Describe the characteristics of different types of malware and social engineering techniques. o Summarize the requirements for securing wireless networks. o Explain the principles behind cryptographic methods and their applications. o Describe how steganography is used to conceal information in various mediums**

- **Level III – Applying: o Apply cryptographic methods to secure data. o Use number theory concepts in the creation and analysis of cipher techniques. o Conduct vulnerability assessments and implement attack mitigation strategies. o Implement steganography techniques to hide information across different mediums.**

- **Level IV – Analyzing: o Analyze the impact of network vulnerabilities on system security. o Evaluate the effectiveness of various cryptographic methods in protecting data. o Assess different techniques for mitigating vulnerabilities in wireless networks. o Analyze the role of steganography in maintaining data secrecy.**

- **Level V – Evaluating: o Critique the effectiveness of different malware and social engineering prevention strategies. o Evaluate the suitability of**

various cryptographic methods for different security requirements. o Assess the challenges of maintaining wireless network security in diverse environments.

•Level VI – Creating: o Design strategies for mitigating network vulnerabilities and attacks. o Develop innovative methods using number theory for secure cipher techniques. o Propose new applications for steganography in digital security. o Create comprehensive security solutions for wireless networks.

Expectations of this Course

This is an online course, which means most (if not all) of the course work will be conducted online. Expectations for performance in an online course are the same as a traditional course. In fact, online courses require a degree of self-motivation, self-discipline, and technology skills which can make these courses more demanding for some students.

Students are expected to:

- **review the getting started page located in the course modules;**
- **introduce yourself to the class during the first week by posting a self-introduction in the appropriate discussion;**
- **take the practice quiz to ensure that your computer is compatible with the learning management system, Canvas;**
- **interact online with instructor and peers;**
- **review and follow the course calendar and weekly outlines;**
- **log in to the course 4 times per week;**

- **respond to discussions by the due date specified. No late work will be accepted;**
- **respond to emails within 2 days;**
- **submit assignments by the corresponding deadline.**

The instructor will:

- **log in to the course 3 times week;**
- **respond to emails within 72 hours;**
- **grade assignments and/or provide feedback within 5 days of the assignment deadline.**

Assignments & Assessments

Discussion Forums

Keep in mind that your discussion forum postings will likely be seen by other members of the course. Care should be taken when determining what to post.

Discussion Forum Expectations:

Introduce Yourself Forum

- Please introduce yourself during the first week of class.
- Please follow the guidelines in the forum.

Chapter Discussion Forums

- There will be discussion topics posted by the professor in every module.
- The professor will review student discussion posts and grade them according to the grading criteria.

- Student discussion board posts will be part of the final course grade.
- Please follow the guidelines listed in the Discussion Participation Rubric posted in the course.
- The approximate length of a posting should be no less than 200 words, and a student response no less than 100 words.
- In discussion forum, you need 1 primary + 2 peer reviews to qualify a full credit.
- Your 2 peer reviews must be detailed.
- Student discussion board posts will be worth 15% of the student grade.

Group Research Project

Please review the following:

- Group Research / Project Instructions
- Group Research / Project Rubric

Samples for this assignment are provided in the course.

Deadlines:

- Groups must be formed by 1**/18 at 11:59 PM**
- Group Research / Project Proposal - **Due 1/25 at 11:59 PM**
- Group Research / Project Draft - **Due 3/29 at 11:59 PM**
- Final Group Research / Project (submitted via Turnitin.com) - **Due 4/18 at 11:59 PM**

Quizzes

In order to mitigate any issues with your computer and online assessments, it is very important that you take the "Practice Quiz" from each computer you will be using to take your graded quizzes and exams. It is your responsibility to make sure your computer meets the minimum hardware requirements.

All assessments will auto-submit when (1) the timer runs out OR (2) the closing date/ time is reached, **whichever happens first**. For example, if a quiz has a closing time of 5:00 pm but the student begins the exam at 4:55 pm, the student will only have 5 minutes to complete the quiz.

Self-Assessment Expectations:

- Self-Assessments are provided primarily for students to check comprehension of course material.
- Students will complete 20-question assessments based on weekly content.
- Students will be allowed one attempt.
- Once started, the assessment must be completed in one sitting.
- The assessment will save and submit automatically when time expires.
- No late submissions will be permitted.
- Self-Assessments will be available **Monday – Sunday.**

Grading

Grading Scheme

Assignment	Weight
Group Project	15%
Discussion Posts	15%

Assignment	Weight
Self-Assessments	10%
Midterm Exam	30%
Final Exam	30%
Total	100%

Grading Scale

Letter	Range (%)	Letter	Range (%)	Letter	Range (%)	Letter	Range (%)	Letter	Range (%)
A	100-94	**B+**	87-89	**C+**	74-79	**D**	60-69	**F**	0-59
A-	90-93	**B**	84-86	**C**	70-73				
		B-	80-83						

Proctored Exams

Exam Expectations:

- The midterm and final exams will be completed online via Honorlock.
- Students will have 60 minutes to complete the assessment.
- The assessment will save and submit automatically when time expires.
- Students will be allowed one attempt.
- The scores will be available immediately upon completion.
- **The Midterm Exam will cover Modules 1~8 and will be available 3/1 at 12:00 am - 3/1 at 11:59 PM.**

- **The Final Exam will cover Modules 9~15 and will be available 4/18 (Saturday) at 12:00 am - 4/18 (Saturday) at 11:59 PM**

Schedule of Topics

Module 1-Chapter 1 - Introduction to Security | 1/5 - 1/11

Module 2-Chapter 2 - Malware and Social Engineering Attacks | 1/12 - 1/18

Module 3-Chapter 3 - Application and Network Attacks | 1/19 - 1/25

Module 4-Chapter 15 - Vulnerability Assessment | 1/26 - 2/1

Module 5-Chapter 4 - Host, Application and Data Security | 2/2 - 2/8

Module 6-Chapter 5 - Basic Cryptography | 2/9 - 2/15

Module 7-Chapter 6 - Advanced Cryptography | 2/16 - 2/22

Module 8-Chapter7- Network Security Fundamentals | 2/23 - 3/1

Module 9-Chapter 8 - Administering a Secure Network | 3/2 - 3/8

Module 10-Chapter 9 - Wireless Network Security | 3/9 - 3/15

Module 11-Chapter10 - Mobile Device Security | 3/16 - 3/22

Module 12-Chapter11 - Access Control Fundamentals | 3/23 - 3/29

Module 13-Chapter 12 - Authentication and Account Management | 3/30 - 4/5

Module 14-Chapter 13 - Business Continuity | 4/6 - 4/12

Module 15-Chapter 14 - Risk Mitigation | 4/13 - 4/18(Saturday)

Module 15-Final Project/Final Exam | 4/18 (Saturday)

Course Communication

Communication in this course will take place via **the Canvas Inbox**. Check out the Canvas Conversations Tutorial or Canvas Guide to learn how to communicate with your instructor and peers using Announcements, Discussions, and the Inbox.

I will respond to all correspondence within **5 days.**

Policies & Resources

Before starting this course, please review the Policies & Resources Page in Canvas, which includes comprehensive information on various University and Course Level Policies, such as:

- **University Policies**
- **Accessibility and Accommodations**
- **Online Etiquette**
- **Technical Requirements and Skills**
- **Computer & Digital Literacy Skills**
- **Course Technology Accessibility Statements and Privacy Policies**
- **Academic Integrity**
- **Copyright Statement**
- **Nondiscrimination Statement**
- **Panthers Care & Counseling and Psychological Services (CAPS)**
- **Fair Use Policy**

Zoom Video Conference

Zoom is a video conference tool that you can use to interact with your professor and fellow students by sharing screens, chatting, broadcasting live video/audio, and taking part in other interactive online activities.

Zoom meetings can be accessed via the Zoom link in the course navigation menu.

Once you click on the Zoom link, it will route you to join the meeting for the respective class session. You will also be able to view upcoming meetings, previous meetings that you have already joined, and meeting recordings. Before joining an actual class session:

• Reference the Zoom Student Tutorials to learn about the tool, how to access your meeting room, and share your screen.

• Access the Zoom Test Meeting Room to test out the software before joining an actual session.

If you encounter any technical difficulties, please contact the FIU Canvas Help Team. Please ensure you contact support immediately upon the issue occurring.

Nondiscrimination Statement

The **Office of Civil Rights Compliance and Accessibility** (CRCA) is responsible for ensuring that FIU maintains a workplace and learning environment free from discrimination, where current and prospective faculty, staff, and students are treated equitably. If any student, employee, or applicant has a sincere and reasonable belief that they have been discriminated against or harassed based on age, color, disability, marital status, ethnic or national origin, race, religion, retaliation, sex, or any other protected category, they can report their concerns to the CRCA team through report.fiu.edu.

Course Awards

This course met Quality Matters review standards.