NJIT New Jersey Institute of Technology

Network Protocols Security/CS646 Syllabus

Fall 2025

Course Modality:
This is an online course, which will be conducted fully online, asynchronously via Canvas. For more information on using Canvas and other supported learning tools, visit the IST Service Desk Knowledgebase.

Instructor Information

Instructor	Email	Office Hours
Asad Raza	asad.raza@njit.edu	Available by appointment via Webex. To schedule an appointment for a one-on-one meeting, please email me.

I will typically respond to direct communications, such as email, within 48 hours. Allow up to 2 weeks for feedback on submitted assignments. This feedback will be provided in Canvas.

General Information

Course Description

This course covers the security of network protocols currently used on the internet. It seeks to familiarize students with common threats and network attacks, and provides an in-depth study of methods used to secure network communication. The course includes an applied component, which will help students gain practical experience in attacking and defending networked systems. Topics include authentication systems, and routing security, firewalls, intrusion detection, honeypots, wireless network security, malware, propagation and detection, and web security.

Prerequisites/Co-requisites

CS 656 or ECE 637 (Internet and Higher Layer Protocols) and an ability to program in Java and C/C++.

Course Learning Outcomes

By the end of the course, you will be able to:

1. Identify the appropriate security primitives that should be used to achieve specific security goals for communication over insecure networks.

2. Analyze the security of the main mechanisms used on the Internet to secure communication between computer systems at various network layers, including datalink, network, transport, and application layers.
3. Describe common attacks against wired and wireless network protocols using standard terminology, allowing them to communicate effectively with other security professionals.
4. Assess whether a given communication protocol achieves the desired security goals.
5. Implement communication protocols that achieve one or more specific security goals.
6. Evaluate the impact of attacks against network protocols, web applications, and design principles for effective defenses.
7. Analyze a scientific article that focuses on the security of network protocols.

Required Materials

Due to the dynamic and evolving nature of the network security field, the course will feature a mixture of material based on the optional recommended textbook, instructor notes, and scientific articles in order to reflect recent developments in this area.

Optional Textbook

- Network Security: Private Communication in a Public World (Prentice Hall Series in Computer Networking and Distributed Systems) 3rd Edition by Charlie Kaufman, Radia Perlman, Mike Speciner and Ray Perlner
  Publisher: Addison-Wesley Professional; 3rd edition (September 26, 2022)
  ISBN-10: 0136643604
  ISBN-13: 978-0136643609

Software Tools Required

- Vmware Workstation Player (For Windows Users) - Free
- Vmware Fusion (For MAC Users) - Free
- Cisco Packet Tracer - (create a Cisco account to log in and access the resource hub downloads) Free
- GNS3 - Open Source
- Wireshark - Open Source
- Kali Linux Operating System (Will be Running in Vmware as Guest OS) - Open Source

Recommended Laptop/PC Configurations Required for the course

- RAM: 16 GB or more
- Processor: Corei5/Corei7

Grading Policy

NJIT Grading Legend

Note: It is up to the discretion of the instructor to apply either absolute or curve grading.

Final Grade Calculation

Final grades for all assignments will be based on the following percentages:

Quizzes	**10%**
Discussions	**10%**
Assignments	**10%**
Projects	**20%**
Project 1	10%
Project 2	10%
Midterm Exam	**20%**
Final Exam	**30%**

Course Work

Quizzes: (10% of grade) There will be questions with multiple-choice, matching, short-answer, and scenario questions. They are meant to help you practice course concepts and prepare for the exams.

Discussions: (10% of grade) You are expected to participate in weekly discussion forums in Canvas. When all students participate in a discussion, it creates an active learning environment that will help you better understand the materials and be more successful in the class. Discussions will be research-oriented, so refer to the course Library Services page for guidance. You will post your initial response to the discussion prompt by Friday at 11:59 pm and respond to two classmates by Sunday at 11:59 pm the module they are listed.

Assignments: (10% of grade) Practical assignments will be given regularly, and these are an opportunity to apply course concepts in a hands-on way. These activities are designed to help you practice and prepare for the projects.

Projects: (**20% of grade**) There will be two projects in this course that cover the practical aspects of specific network protocols and their security. The first focuses on setting up virtual machines, evaluating the impact of ARP poisoning attacks, and defending against such attacks. The second focuses on the design and implementation of defensive technologies to prevent attacks against systems, services, and protocols.

Midterm Exam: (**20% of grade**) The Midterm Exam will be conducted in Module 8. It will cover content from Modules 1-7 and include a range of question types, including multiple-choice, scenario-based, and short-answer questions. You will be required to use Respondus LockDown Browser & Monitor.

Final Exam: (**30% of grade**) The Final Exam will be conducted in Module 15. It will cover content from Modules 9-14 and include a range of question types, including multiple-choice, scenario-based, and short-answer questions. You will be required to use Respondus LockDown Browser & Monitor.

Feedback

I will deliver feedback on each assignment, project, and exam using the comments feature in Canvas. I can also arrange one-to-one online meetings with you to discuss your feedback, if deemed necessary.

Letter to Number Grade Conversions

A	B+	B	C+	C	F
90-100	86-89	80-85	76-79	70-75	0-69

Exam Information and Policies

Both the Midterm and Final Exams will be conducted online on Canvas using Respondus Lockdown Browser & Monitor:

- LockDown Browser: A locked browser used to prevent students from printing, copying, going to another URL, or accessing other applications during an assessment in Canvas.
- Monitor: Used in conjunction with LockDown Browser, Monitor is the usage of a webcam to record a user during the exam session.

Technical Requirements include:

- High-speed internet connection
- Windows or Apple Operating System
- Webcam (internal or external)
- Microphone and Audio (internal or external)
- NJIT ID or Photo-Issued ID
- To perform an environment check

Per the NJIT Online Course Exam Proctoring Policy, all midterm and final exams must be proctored, regardless of delivery mode, in order to increase academic integrity. Detailed instructions about Respondus LockDown Browser & Monitor are provided in Canvas.

Policy for Late Work

It is highly recommended to avoid any late submissions because it will reflect negatively on your grades. Below is the late submission policy/penalty.

Category	Penalty for submissions within 24 hours after the deadline	Penalty for submissions 2-3 days after the deadline
Assignment	20%	50 %
Project	20%	50 %
Presentation	20%	50 %
Quiz	No retake	No retake
Midterm and Final Exams	No retake	No retake

Submissions are not accepted 3 days after the deadline. If you are not able to take the Midterm or Final Exam under exceptional circumstances (e.g., emergencies, medical reasons, etc.), you can contact the Dean of Students and Campus Life with official and verifiable documentation to be considered for retake. If you need to request reasonable accommodations and support services, you must apply and get approval from the Office of Accessibility Resources and Services before the exam date.

Academic Integrity

"Academic Integrity is the cornerstone of higher education and is central to the ideals of this course and the university. Cheating is strictly prohibited and devalues the degree that you are working on. As a member of the NJIT community, it is your responsibility to protect your educational investment by knowing and following the NJIT academic code of integrity policy.

Please note that it is my professional obligation and responsibility to report any academic misconduct to the Dean of Students Office. Any student found in violation of the code by cheating, plagiarizing or using any online software inappropriately will result in disciplinary action. This may include a failing grade of F, and/or suspension or dismissal from the university. If you have any questions about the code of Academic Integrity, please contact the Dean of Students Office at dos@njit.edu"

Netiquette

Throughout this course students are expected to follow NJIT's Code of Student Conduct, You are expected to be courteous and respectful to classmates by being polite, active participants. You should respond to discussion forum assignments in a timely manner so that your classmates have adequate time to respond to your posts. Please respect opinions, even those that differ from your own, and avoid using profanity or offensive language.

Weekly Expectations

This course is organized into 15 weekly modules. Each week, you will complete reading assignments, watch lecture videos, and submit tasks (including quizzes, discussions, assignments, and projects) per the course schedule below. Please note that your participation in the course will be closely monitored.

Course Schedule

Week	Topic	Assignments	Due Dates
1	Module 1: Fundamental Concepts of Network Security	1. Module 1 Knowledge Check: Fundamentals of Network (Optional) 2. Introduce Yourself	1. Due by Sunday at 11:59 pm 2. Due by Sunday at 11:59 pm
2	Module 2: Network Fundamentals	1. Module 2 Discussion: Securing TCP/IP Communications: Challenges and Best Practices 2. Module 2 Practice Assignment: Build a Switch and Router Network 3. Project 1: ARP Poisoning Assigned	1. Initial post due by Friday at 11:59 pm; replies to peers due by Sunday at 11:59 pm 2. Due by Sunday at 11:59 pm 3. Due by the end of Module 6
3	Module 3: Layer 2 Security: Attacks on Layer Protocols	1. Module 3 Quiz 2. Module 3 Discussion: Secure Switching Technologies for Data Link Layer 3. Module 3 Practical Assignment 1: Implementing Switch Security	1. Due by Sunday at 11:59 PM 2. Initial post due by Friday at 11:59 pm; replies to peers due by Sunday at 11:59 pm 3. Due by Sunday at 11:59 PM
4	Module 4: Layer 2 Security: Port-Based Access Control	1. Module 4 Quiz 2. Module 4 Discussion: Analyzing an STP Scenario 3. Module 4 Reflection: Create a Mind Map (Extra Credit)	1. Due by Sunday at 11:59 PM 2. Initial post due by Friday at 11:59 pm; replies to peers due by Sunday at 11:59 pm 3. Due by Sunday at 11:59 PM
5	Module 5: Layer 3: IPV4 and IPV6	1. Module 5 Discussion: IPV6 Security Podcast 2. Module 5 Practical Assignment 2: Addressing and OSPF Configuration	1. Initial post due by Friday at 11:59 pm; replies to peers due by Sunday at 11:59 pm 2. Due by Sunday at 11:59 PM
6	Module 6: Layer 3: Protocol Attacks and Countermeasures	1. Project 1: ARP Poisoning	1. Due by Sunday at 11:59 PM
7	Module 7: Layer 3 Security: IPSec and ACLs	1. Module 7 Quiz 2. Module 7 Discussion: The Role of IPSec in Securing Modern Networks 3. Module 7 Bonus Practical Assignment: Configuring Extended ACLs (Optional)	1. Due by Sunday at 11:59 PM 2. Initial post due by Friday at 11:59 pm; replies to peers due by Sunday at 11:59 pm 3. Due by Sunday at 11:59 PM

8	**Module 8: Midterm Exam**	**Midterm Exam**	**Available from Sunday at 12:01 am to 11:59 pm (time limit is 1 hour and 30 minutes)**
9	Module 9: Layer 4 Security: Transport Layer Attacks & TLS	1. Module 9 Discussion: Secure Web Communication With SSL/TLS 2. Module 9 Practical Assignment 3: Implementation and Analysis of SSL/TLS 3. Project 2: Design and Implementation of Defensive Technologies to Prevent Attacks Against Systems, Services, and Protocols Assigned	1. Initial post due by Friday at 11:59 pm; replies to peers due by Sunday at 11:59 pm 2. Due by Sunday at 11:59 PM 3. Due by the end of Module 13
10	Module 10: Layer 7 Security: DHCP and DNS	1. Module 10 Quiz 2. Module 10 Discussion: Attacks and Countermeasures for Application Layer Protocol	1. Due by Sunday at 11:59 PM 2. Initial post due by Friday at 11:59 pm; replies to peers due by Sunday at 11:59 pm
11	Module 11: Authentication Protocols: PAP, CHAP, Needham-Schroeder Protocol, Kerberos	1. Module 11 Discussion: Comparison Between NTLM and Kerberos Authentication 2. Module 11 Practical Assignment 4: PAP and CHAP Configuration	1. Initial post due by Friday at 11:59 pm; replies to peers due by Sunday at 11:59 pm 2. Due by Sunday at 11:59 PM
12	Module 12: Firewalls & Intrusion Detection Systems	1. Module 12 Discussion: Comparative Analysis of NTFW and UTM with Traditional Firewalls	1. Initial post due by Friday at 11:59 pm; replies to peers due by Sunday at 11:59 pm
13	Module 13: Malware Propagation and Containment	1. Project 2: Design and Implementation of Defensive Technologies to Prevent Attacks Against Systems, Services, and Protocols	1. Due by Sunday at 11:59 PM
14	Module 14: Wireless Network Security	1. Module 14 Quiz 2. Module 14 Discussion: KRACK Attack: Breaking WPA2 by Forcing Nonce Reuse	1. Due by Sunday at 11:59 PM 2. Initial post due by Friday at 11:59 pm; replies to peers due by Sunday at 11:59 pm
15	**Module 15: Final Exam**	**Final Exam**	**TBD**

Additional Information and Resources

Accessibility:

This course is offered through an accessible learning management system. For more information, please refer to Canvas's Accessibility Statement and Respondus’s Accessibility Statement.

Requesting Accommodations:

The Office of Accessibility Resources and Services works in partnership with administrators, faculty, and staff to provide reasonable accommodations and support services for students with disabilities who have provided their office with medical documentation to receive services.

If you are in need of accommodations due to a disability, please contact the Office of Accessibility Resources and Services to discuss your specific needs.

Resources for NJIT Online Students

NJIT is committed to student excellence. To ensure your success in this course and your program, the university offers a range of academic support centers and services. To learn more, please review these Resources for NJIT Online Students, which include information related to technical support.