Semester Project: Advanced Secure File Transfer System with Low-Level IP Processing & Network Performance Analysis

📌 **Title:**

"Advanced Secure File Transfer System: Encryption, Low-Level IP Processing, and Network Performance Analysis"

🗓 **Duration:**

- **Deadline:** 09 June 2025 / 23.59
-
- **Project Milestones:**
  - **31 March 2025 / 23.59:** Initial project proposal (The proposal for this project will be made through the 'Tübitak 2209 Project Proposal draft'.)
  - **28 April 2025 / 23.59:** Project interim report
  - **09 June 2025 / 23.59:** The final report submission deadline

👥 **Team Size: 1 student**

📌 Project Overview

In this project, students will develop a **secure file transfer system** that ensures **encrypted transmission, authentication, and integrity validation**. The system will involve **manual low-level IP header manipulation** (flags, fragmentation, checksum, TTL) to deepen students' understanding of network protocols. Additionally, students will analyze **network performance metrics** (latency, bandwidth, packet loss) under various conditions using **Wireshark, iPerf, and traffic control (tc)**.

The project will provide hands-on experience with **computer networking concepts, security measures, and network performance analysis** in a real-world scenario.

📌 Project Requirements

1. Core Features (Mandatory)

✅ **File Transfer System**

- Supports **sending and receiving** files over a network.
- Uses **manual packet fragmentation & reassembly** to handle large file transfers.
- Implements **error detection and correction mechanisms**.

✓ **Security Mechanisms**

- Uses **AES/RSA encryption** to protect files during transmission.
- Implements **client authentication** before allowing a transfer.
- **Ensures integrity** using cryptographic hashing (SHA-256).

✓ **Low-Level IP Header Processing**

- Manually **modifies and processes IP headers** (flags, TTL, checksum, fragmentation).
- Computes and verifies **IP checksum** before transmission.
- Analyzes **packet reassembly** on the receiver side.

✓ **Network Performance Measurement**

- Measures **latency** (ping, RTT calculations).
- Measures **bandwidth** using iPerf and packet analysis.
- Simulates **packet loss & network congestion** using tc.
- **Compares different network conditions** (Wi-Fi vs. wired, local vs. remote).

✓ **Security Analysis & Attack Simulation**

- **Intercepts and analyzes packets** using Wireshark.
- Simulates **man-in-the-middle (MITM) attacks** and packet injection.
- Ensures encryption makes data unreadable in packet captures.

---

2. Tech Stack (Suggested Technologies)

- **Programming Languages:** Python (Scapy) or C (raw sockets)
- **Encryption Libraries:** OpenSSL, PyCrypto, hashlib
- **Network Analysis Tools:** Wireshark, iPerf, netstat, ping, tc
- **Packet Manipulation:** Scapy (Python) or raw sockets (C)

---

3. Additional Features (Bonus Points)

✓ **Hybrid TCP/UDP Switching** – Adapt file transfer method based on network conditions.
✓ **Dynamic Congestion Control** – Implement rate adaptation for efficient bandwidth usage.
✓ **Graphical User Interface (GUI)** – Build a simple UI for file transfer visualization.
✓ **Advanced Attack Simulations** – Implement real-time packet filtering and intrusion detection.

📌 Grading Criteria (100 Points Total)

1. Functionality (18 points)

- **File Transfer Implementation (6 points):** The system correctly transmits files.
- **Encryption & Authentication (6 points):** Implements AES/RSA encryption to prevent unauthorized access.
- **Fragmentation & Reassembly (6 points):** Large files are properly divided and reassembled.

2. Low-Level IP Header Processing (12 points)

- **Manual IP Header Manipulation (6 points):** Customizes IP headers (TTL, flags, checksum).
- **Checksum Validation (6 points):** Detects transmission errors using computed checksum.

3. Network Performance Measurement (15 points)

- **Latency Measurement (3 points):** Ensures accurate round-trip time (RTT) calculations.
- **Bandwidth Analysis (3 points):** Compares actual versus theoretical transfer speeds.
- **Packet Loss Handling (6 points):** Simulates packet loss and verifies retransmission mechanisms.
- **Performance Comparison (3 points):** Evaluates performance across multiple network types (Wi-Fi, wired, VPN).

4. Security Analysis (9 points)

- **Encryption Validation (3 points):** Ensures that encrypted data is unreadable in network traffic analysis (e.g., Wireshark).
- **Attack Simulations (3 points):** Detects or mitigates MITM (Man-in-the-Middle) and packet injection attacks.
- **Secure Protocol Justification (3 points):** Compares various encryption and authentication mechanisms.

5. Code Quality & Documentation (40 points)

- **Code Readability & Comments (20 points):** Adheres to best coding practices and is well-documented.
- **Report Quality (20 points):** Provides a comprehensive analysis of the system's design, implementation, and performance evaluation.

Total: 100 points

Expected Learning Outcomes

✓ Hands-on experience with **low-level networking** (IP headers, sockets, packet handling).
✓ Practical understanding of **network performance metrics** (latency, bandwidth, loss).
✓ Exposure to **security risks** and defensive programming in networking.

Project Report Guidelines

All writing rules specified in this document must be followed when preparing the project report. The report should maintain a consistent format throughout, using a simple writing style, **12-point font size, 1.5 line spacing, and justified alignment on both sides**. Headings should be structured hierarchically. Points will be deducted if the report is not readable.

PROJECT PROPOSAL

In the first stage, you will submit a project proposal. This proposal should follow the same format as the **TÜBİTAK 2209-A Project Proposal Template**. Excluding sections irrelevant to your project, such as budget, all other sections must be detailed and explained as required. *(Prepare this proposal carefully, as if you were submitting it to TÜBİTAK.)* The project proposal must be uploaded to the designated section on **E-Campus by March 31, 2025, at 23:59**.

INTERIM REPORT

At the interim report stage, you must report your project's progress up to that point **following the rules specified in the FINAL REPORT section**. *(No video submission is required at this stage.)* The interim report must be uploaded to the designated section on **E-Campus by April 28, 2025, at 23:29**.

FINAL REPORT

The content should begin with the **'INTRODUCTION'** section, where the project is summarized.

The second section, **'TECHNICAL DETAILS'**, should describe all the methods and specifications used.

The third section, **'LIMITATIONS AND IMPROVEMENTS'**, should include all incomplete or planned-but-not-implemented aspects of the project under separate subheadings. If any additional features were implemented for the **Bonus Points** section, they should also be mentioned here.

The last section, **'CONCLUSION'**, should summarize the entire project. The video link should be shared in this section (details are provided below).

At the end of the document, a **'REFERENCES'** section must be included. Sources **should not** be shared as links only. If available, they should include the author's name, website name, topic title, and the link. *(Refer to the APA citation format!)*

Students are responsible for every sentence in this document while preparing the project assignment. Every rule, requirement, and obligation mentioned will be considered **read and acknowledged** by the student. The final report must be uploaded to the designated section on **E-Campus by June 9, 2025, at 23:59**.

YouTube Video Submission

- Record a **detailed project explanation video** of up to **10 minutes** and upload it to **YouTube**.
- Add the **video link** to the **end of your report**.
- Ensure the video is set to **public**. *(Test by sharing the link with friends; unplayable videos will not be reconsidered.)*

Additionally, **share your project video and final report on LinkedIn**.
