SecureChat Project Report

Part 2: Testing Report

Ibraheem Farrukh
Student ID: 22i-1111

December 4, 2025

Contents

1 Test Suite Overview

The project includes automated and manual tests validating security properties.

Test File	Type	Purpose
`test_invalid_cert.py`	Automated	Certificate validation
`test_tampering_client.py`	Semi-automated	Message integrity
`test_replay_client.py`	Semi-automated	Replay attack prevention
`run_all_tests.bat`	Runner	Execute all tests
`run_tests.py`	Runner	Python test orchestrator

Table 1: Overview of Test Files

2 Test Cases

2.1 Invalid Certificate Test

Objective: Verify server rejects clients with untrusted certificates.

- **Procedure:**
  1. Generate self-signed certificate (not signed by CA).
  2. Attempt connection to server.
  3. Verify connection is rejected.
- **Expected Result:** `BAD_CERT: Self-signed certificate rejected`
- **Status:** PASS ✓

2.2 Message Tampering Test

Objective: Verify tampered messages are detected and rejected.

- **Procedure:**
  1. Client A sends encrypted message to Client B.
  2. Intercept and modify ciphertext bytes.
  3. Forward tampered message to recipient.
  4. Verify signature verification fails.
- **Expected Result:** Message rejected with signature/integrity error.

2.3 Replay Attack Test

Objective: Verify duplicate messages are rejected.

- **Procedure:**
  1. Capture valid encrypted message.
  2. Resend exact same message (same nonce/timestamp).
  3. Verify server rejects duplicate.
- **Expected Result:** `REPLAY_DETECTED: Nonce already used`

3 Security Validation Matrix

Attack Vector	Mitigation	Test	Status
Man-in-the-Middle	TLS + Certificate Pinning	`test_invalid_cert.py`	✓
Message Tampering	Digital Signatures + GCM Tag	`test_tampering.py`	Manual
Replay Attack	Nonces + Timestamps	`test_replay.py`	Manual
Eavesdropping	AES-256-GCM Encryption	Implicit	✓
Impersonation	Client Certificates	`test_invalid_cert.py`	✓

Table 2: Security Validation Matrix

4 Running Tests

Prerequisites:

- MySQL running (Docker or local).
- Database initialized: `python setup_database.py`
- Server running: `start_server.bat`

Execute All Tests:

```
.\run_all_tests.bat
```

Or individually:

```
python test_invalid_cert.py
python test_tampering_client.py
python test_replay_client.py
```

5 Known Issues

Issue	Cause	Resolution
`CryptographyWarning`	Deprecated datetime properties	Update `pki.py` to use `not_valid_before_utc`
`Can't connect to MySQL`	MySQL not running	Start MySQL via Docker

6 Test Environment Requirements

- **Python:** 3.12+
- **MySQL:** 8.x (via Docker recommended)
- **Dependencies:** `cryptography`, `pymysql`, `python-dotenv`
- **OS:** Windows 10/11