

REPORT

Problem Statement :

Cryptography Simulation with mbedTLS/OpenSSL Library Usage and User Interaction.

Team Name

Adventurers

Team Size

2 (TWO)

Team Member 1

Karthikeyan A

Team Member 2









Sri Ganesh R

College Name : Sairam Group of Institutions

Topics:

1. Created Digital Certificates.
2. Implemented CryptoWrapper.
3. Secured the custom protocol.

1. CREATED DIGITAL CERTIFICATES :

Name	Date modified	Type	Size
 alice	25-06-2024 09:04	Security Certificate	2 KB
 alice.csr	25-06-2024 09:03	CSR File	2 KB
 alice.key	18-06-2024 08:47	KEY File	3 KB
 bob	25-06-2024 09:04	Security Certificate	2 KB
 bob.csr	25-06-2024 09:04	CSR File	2 KB
 bob.key	18-06-2024 08:50	KEY File	3 KB
 rootCA	18-06-2024 08:27	Security Certificate	2 KB
 rootCA.key	18-06-2024 08:26	KEY File	3 KB

2. IMPLEMENTED “CryptoWrapper” :

All 5 unit test cases have passed.

```
testHMAC PASSED!  
The plaintext is the same - This is a secret plaintext that we want to protect  
testSymmetricEncryption PASSED!  
Error in finalizing digest verify at verifyMessageRsa3072Pss  
testRsaSigning PASSED!  
testDh PASSED!  
Error in checking host at checkCertificate  
Error in verifying store context at checkCertificate  
testCertificateChecking PASSED!
```

3. SECURED THE CUSTOM PROTOCOL :

Starting the server :

```
udp_party\x64\Debug>udp_party -port 60000 -key alice.key -pwd alice -cert alice.crt  
-root rootCA.crt -peer Bob.com  
Server: Starting listening...
```

Starting the client :

```
udp_party\x64\Debug>udp_party -ip 127.0.0.1 -port 60000 -key bob.key -pwd bobkey
-cert bob.crt -root rootCA.crt -peer Alice.com
Session started with Alice.com
Received response:"HI! I'M ELIZA. WHAT'S YOUR PROBLEM?"
|
```

View Packets from wire shark :

The image shows a Wireshark packet capture window titled "Adapter for loopback traffic capture". The packet list on the left shows two packets. The first packet is selected, showing details for an IPv4 packet and a UDP payload. The packet data is displayed in the packet bytes pane on the right.

No.	Time	Source	Destination	Protocol	Length	Info
6	19.047023	127.0.0.1	127.0.0.1	UDP	85	65114 → 60000 Len=53
7	19.048100	127.0.0.1	127.0.0.1	UDP	101	60000 → 65114 Len=63

Packet 6 details:

- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 81
- Identification: 0xccc58 (52312)
- 000. = Flags: 0x0
- ...0 0000 0000 0000 = Fragment Offset: 0
- Time to Live: 128
- Protocol: UDP (17)
- Header checksum: 0x0000 [validation disabled]
- [Header checksum status: Unverified]
- Source Address: 127.0.0.1
- Destination Address: 127.0.0.1
- User Datagram Protocol, Src Port: 65114, Dst Port: 60000
- Source Port: 65114
- Destination Port: 60000
- Length: 61
- Checksum: 0xf76f [unverified]
- [Checksum status: Unverified]
- [Stream index: 2]
- [Timestamps]
- UDP payload (53 bytes)
- Data (53 bytes)
- Data: 010000000300000006000000025000000539b56225b20d7a6afc2195c6d989dbc962689848cf697482acdcdcdcdcd

Packet 7 details:

- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 101
- Identification: 0xccc58 (52312)
- 000. = Flags: 0x0
- ...0 0000 0000 0000 = Fragment Offset: 0
- Time to Live: 128
- Protocol: UDP (17)
- Header checksum: 0x0000 [validation disabled]
- [Header checksum status: Unverified]
- Source Address: 127.0.0.1
- Destination Address: 127.0.0.1
- User Datagram Protocol, Src Port: 60000, Dst Port: 65114
- Source Port: 60000
- Destination Port: 65114
- Length: 85
- Checksum: 0xf76f [unverified]
- [Checksum status: Unverified]
- [Stream index: 2]
- [Timestamps]
- UDP payload (63 bytes)
- Data (63 bytes)
- Data: 010000000300000006000000025000000539b56225b20d7a6afc2195c6d989dbc962689848cf697482acdcdcdcdcd

