Brandon Hudson

30 June 2020

CS447 Network and Data Communication

# *Project 3 Report: TLS*

## Intro:

In this report, I am going to walk you thru the process of sending and receiving emails in my application down to every command. I will walk thru how to start the server and client, how to authenticate and how to send an email in detail.

**For the sender server and client(**Send emails after authentication**)**:

First how to start the server type "make senderserver PORT=" and type the port number after the '=' "make senderserver PORT=9000" and type the port number after the '='

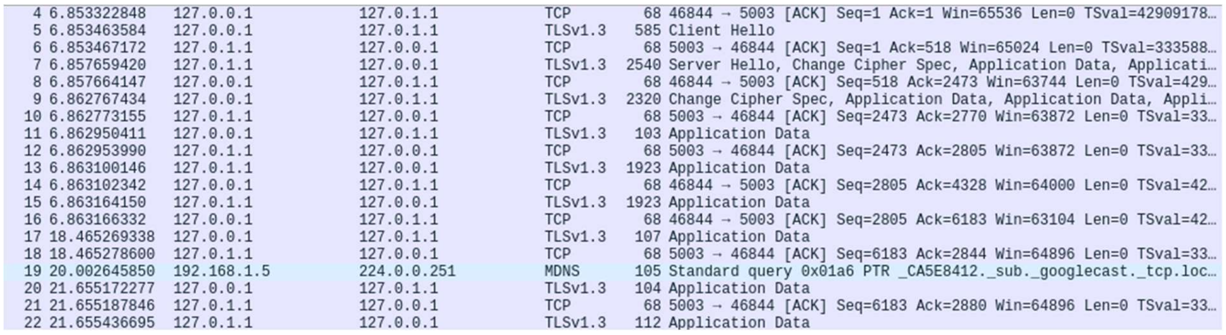
Do the same in a separate terminal for the client type "make senderclient PORT=" e.g. "make senderclient PORT=9000". The number that you pick MUST match up.

## Limitation:

To start one of the most prevalent limitations of this implementation of TLSv1.3 STMP Is that when using Python, you must enter the PEM password to verify their certificates. The password I used and that you need to type in Is "cs447". This is the same password anytime you are prompted to type in a PEM password. I believe to get around this in Python You need to use Pem formatting instead of the .key and .crt. If I had more time, I would try out different certificate formats, but due to major time limitations I had to stick with what was working for me at the time. Also, for limitation in implementation, the receiver server (I think should be called retriever instead) does not auth the users but it does fetch the emails based on user. It is also not multi-threaded. This could have been easily implemented because it's the exact same as the sender but due to the time constraint I didn't want to break what was already running perfectly in TLSv1.3 which is the major focus in this project. I did not want to risk not being able to get my program to compile for a minor requirement when I have the major requirement working with valid proof.

When correctly starting their server and client as stated above and entering the correct PEM password then you will be asked as a client to type "Connect" after doing so you will be prompted with the menu. This menu corresponds to SMTP commands that was referenced in the RFC. these commands should be entered in the correct order RFC explains. If a command is entered out of sequence error code 503 is shown. Otherwise a 200 OK is printed in the server log. The client must first type the command “HELO” after receiving the welcome message from the server the client next must authenticate he or her user email with the server that cross references new and returning users with the hidden file in password given to you upon first authenticating. to authenticate type the command “AUTH” and follow through the prompt. The first time you authenticate you will be given a random 5-digit number password that ends in “447” Making it 8-digit password altogether. You MUST reconnect both client and server to a NEW PORT at this point. Do this by typing. "make senderserver PORT=9001" for server and "make senderclient PORT=9001" for client and typed the same password for each. Go thru the same steps as before and when AUTH enter your same email and password that was given to you. Follow the order of command for SMTP (MAIL FROM, RCTP TO, DATA). After which a status code 250 SENT should be sent as well as your message to the specify user email that was giving in the command “RCTP TO”.

Here is the screenshot of the above process improve of the protocol that is use while doing this process in Wireshark format.



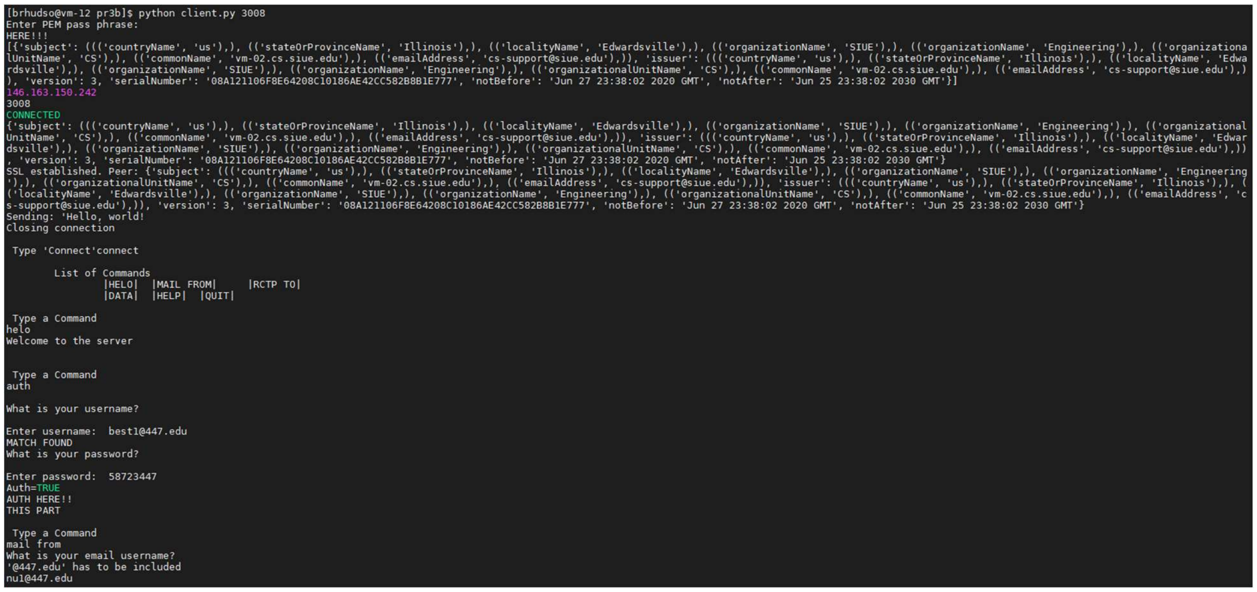
```
 4 6.853322848   127.0.0.1          127.0.1.1          TCP       68 46844 → 5003 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=42909178…
 5 6.853463584   127.0.0.1          127.0.1.1          TLSv1.3  585 Client Hello
 6 6.853467172   127.0.1.1          127.0.0.1          TCP       68 5003 → 46844 [ACK] Seq=1 Ack=518 Win=65024 Len=0 TSval=333588…
 7 6.857659420   127.0.1.1          127.0.0.1          TLSv1.3 2540 Server Hello, Change Cipher Spec, Application Data, Applicati…
 8 6.857664147   127.0.0.1          127.0.1.1          TCP       68 46844 → 5003 [ACK] Seq=518 Ack=2473 Win=63744 Len=0 TSval=429…
 9 6.862767434   127.0.0.1          127.0.1.1          TLSv1.3 2320 Change Cipher Spec, Application Data, Application Data, Appli…
10 6.862773155   127.0.1.1          127.0.0.1          TCP       68 5003 → 46844 [ACK] Seq=2473 Ack=2770 Win=63872 Len=0 TSval=33…
11 6.862950411   127.0.0.1          127.0.1.1          TLSv1.3  103 Application Data
12 6.862953990   127.0.1.1          127.0.0.1          TCP       68 5003 → 46844 [ACK] Seq=2473 Ack=2805 Win=63872 Len=0 TSval=33…
13 6.863100146   127.0.1.1          127.0.0.1          TLSv1.3 1923 Application Data
14 6.863102342   127.0.0.1          127.0.1.1          TCP       68 46844 → 5003 [ACK] Seq=2805 Ack=4328 Win=64000 Len=0 TSval=42…
15 6.863164150   127.0.1.1          127.0.0.1          TLSv1.3 1923 Application Data
16 6.863166332   127.0.0.1          127.0.1.1          TCP       68 46844 → 5003 [ACK] Seq=2805 Ack=6183 Win=63104 Len=0 TSval=42…
17 18.465269338  127.0.0.1          127.0.1.1          TLSv1.3  107 Application Data
18 18.465278600  127.0.1.1          127.0.0.1          TCP       68 5003 → 46844 [ACK] Seq=6183 Ack=2844 Win=64896 Len=0 TSval=33…
19 20.002645850  192.168.1.5        224.0.0.251        MDNS     105 Standard query 0x01a6 PTR _CA5E8412._sub._googlecast._tcp.loc…
20 21.655172277  127.0.0.1          127.0.1.1          TLSv1.3  104 Application Data
21 21.655187846  127.0.1.1          127.0.0.1          TCP       68 5003 → 46844 [ACK] Seq=6183 Ack=2880 Win=64896 Len=0 TSval=33…
22 21.655436695  127.0.1.1          127.0.0.1          TLSv1.3  112 Application Data
```

As you can see, I am running the program on a localhost because my hard drive was wiped doing a failed attempt of dual booting Linux on my windows machine. the dual boot now works but due to partitioning errors all my hard drive data was wiped. Luckily I have backup copies when the schools server I could retrieve but SSH tunneling was not set up anymore so for quick proof I ran the program on my local machine what should be more than efficient enough to prove be protocol that is being run. As you can see TLSv1.3 is definitely being run by my application without a doubt. In the screenshot above the first TLS message being “Client Hello” followed by the “Server Hello”. You can see full detailed captures in the file “Wiresharkcaptures.txt”. In the same file you can see the same process being run As TCP a not TLS. I will only provide 1 example because you can simply look in the “Wiresharkcaptures.txt” for more.

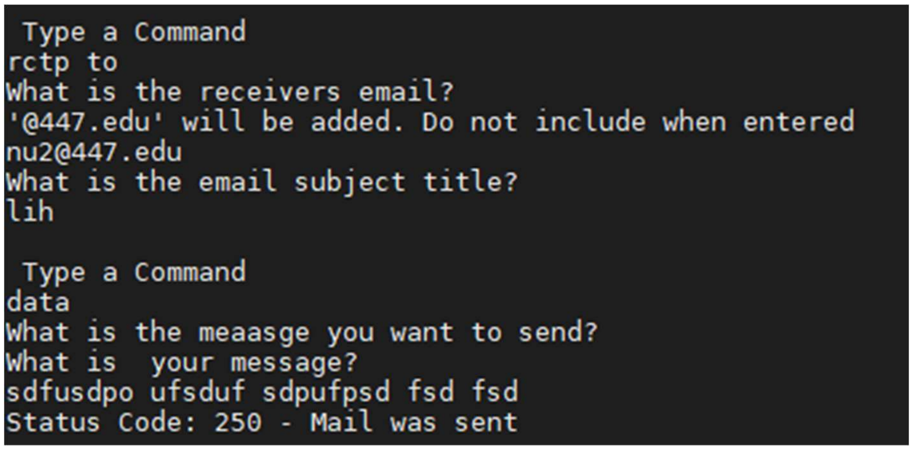
```
No.     Time           Source                Destination           Protocol Length Info
     27 26.691387077   127.0.0.1             127.0.1.1             TCP      68     46844 → 5003 [ACK] Seq=2916 Ack=6272
Win=65536 Len=0 TSval=4290937728 TSecr=3335900898
Frame 27: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface any, id 0
Linux cooked capture
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.1.1
Transmission Control Protocol, Src Port: 46844, Dst Port: 5003, Seq: 2916, Ack: 6272, Len: 0
```

## Output of sample run:

Here are Screenshots of me running the exact same process myself



```
[brhudso@vm-12 pr3b]$ python client.py 3008
Enter PEM pass phrase:
HERE!!!
[{'subject': ((('countryName', 'us'),), (('stateOrProvinceName', 'Illinois'),), (('localityName', 'Edwardsville'),), (('organizationName', 'SIUE'),), (('organizationName', 'Engineering'),), (('organizationa
lUnitName', 'CS'),), (('commonName', 'vm-02.cs.siue.edu'),), (('emailAddress', 'cs-support@siue.edu'),)), 'issuer': ((('countryName', 'us'),), (('stateOrProvinceName', 'Illinois'),), (('localityName', 'Edwa
rdsville'),), (('organizationName', 'SIUE'),), (('organizationName', 'Engineering'),), (('organizationalUnitName', 'CS'),), (('commonName', 'vm-02.cs.siue.edu'),), (('emailAddress', 'cs-support@siue.edu'),)
), 'version': 3, 'serialNumber': '08A121106F8E64208C10186AE42CC582B8B1E777', 'notBefore': 'Jun 27 23:38:02 2020 GMT', 'notAfter': 'Jun 25 23:38:02 2030 GMT'}]
146.163.150.242
3008
CONNECTED
{'subject': ((('countryName', 'us'),), (('stateOrProvinceName', 'Illinois'),), (('localityName', 'Edwardsville'),), (('organizationName', 'SIUE'),), (('organizationName', 'Engineering'),), (('organizational
UnitName', 'CS'),), (('commonName', 'vm-02.cs.siue.edu'),), (('emailAddress', 'cs-support@siue.edu'),)), 'issuer': ((('countryName', 'us'),), (('stateOrProvinceName', 'Illinois'),), (('localityName', 'Edwar
dsville'),), (('organizationName', 'SIUE'),), (('organizationName', 'Engineering'),), (('organizationalUnitName', 'CS'),), (('commonName', 'vm-02.cs.siue.edu'),), (('emailAddress', 'cs-support@siue.edu'),))
, 'version': 3, 'serialNumber': '08A121106F8E64208C10186AE42CC582B8B1E777', 'notBefore': 'Jun 27 23:38:02 2020 GMT', 'notAfter': 'Jun 25 23:38:02 2030 GMT'}
SSL established. Peer: {'subject': ((('countryName', 'us'),), (('stateOrProvinceName', 'Illinois'),), (('localityName', 'Edwardsville'),), (('organizationName', 'SIUE'),), (('organizationName', 'Engineering
'),), (('organizationalUnitName', 'CS'),), (('commonName', 'vm-02.cs.siue.edu'),), (('emailAddress', 'cs-support@siue.edu'),)), 'issuer': ((('countryName', 'us'),), (('stateOrProvinceName', 'Illinois'),), (
('localityName', 'Edwardsville'),), (('organizationName', 'SIUE'),), (('organizationName', 'Engineering'),), (('organizationalUnitName', 'CS'),), (('commonName', 'vm-02.cs.siue.edu'),), (('emailAddress', 'c
s-support@siue.edu'),)), 'version': 3, 'serialNumber': '08A121106F8E64208C10186AE42CC582B8B1E777', 'notBefore': 'Jun 27 23:38:02 2020 GMT', 'notAfter': 'Jun 25 23:38:02 2030 GMT'}
Sending: 'Hello, world!
Closing connection

 Type 'Connect'connect

        List of Commands
                |HELO|  |MAIL FROM|     |RCTP TO|
                |DATA|  |HELP|  |QUIT|

 Type a Command
helo
Welcome to the server


 Type a Command
auth

What is your username?

Enter username:  best1@447.edu
MATCH FOUND
What is your password?

Enter password:  58723447
Auth=TRUE
AUTH HERE!!
THIS PART

 Type a Command
mail from
What is your email username?
'@447.edu' has to be included
nu1@447.edu
```



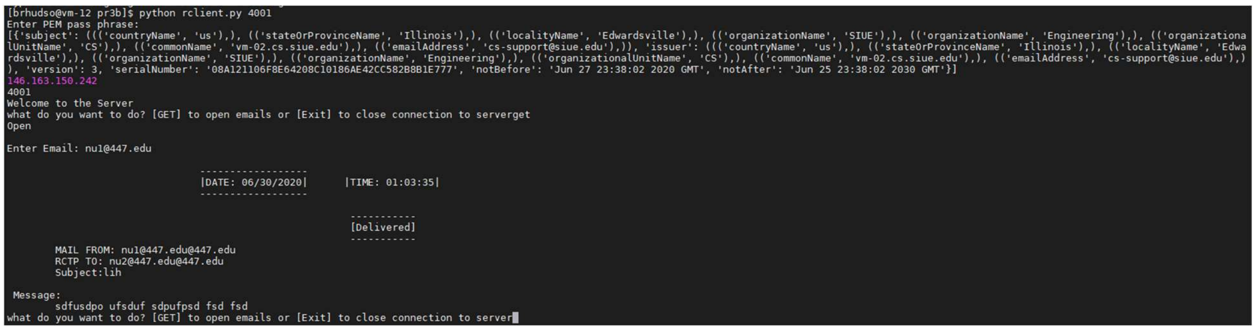
```
 Type a Command
rctp to
What is the receivers email?
'@447.edu' will be added. Do not include when entered
nu2@447.edu
What is the email subject title?
lih

 Type a Command
data
What is the meaasge you want to send?
What is  your message?
sdfusdpo ufsduf sdpufpsd fsd fsd
Status Code: 250 - Mail was sent
```

**For the receiver server and client (**To retrieve sent emails open a new terminal**):**

Start the server by typing “make receiverserver PORT=” and type the port number after the ‘=’ “make receiverserver PORT=9100” and type the port number after the ‘=’

Do the same in a separate terminal for the client type “make receiverclient PORT=” e.g. “make receiverclient PORT=9100”. The number that you pick MUST match up.

To retrieve your emails from here is simple. Type the HTTP(now HTTPS) “GET” command and you will prompted to enter you email that you want to read emails from as shown below.



```
[brhudso@vm-12 pr3b]$ python rclient.py 4001
Enter PEM pass phrase:
[{'subject': ((('countryName', 'us'),), (('stateOrProvinceName', 'Illinois'),), (('localityName', 'Edwardsville'),), (('organizationName', 'SIUE'),), (('organizationName', 'Engineering'),), (('organizationa
lUnitName', 'CS'),), (('commonName', 'vm-02.cs.siue.edu'),), (('emailAddress', 'cs-support@siue.edu'),)), 'issuer': ((('countryName', 'us'),), (('stateOrProvinceName', 'Illinois'),), (('localityName', 'Edwa
rdsville'),), (('organizationName', 'SIUE'),), (('organizationName', 'Engineering'),), (('organizationalUnitName', 'CS'),), (('commonName', 'vm-02.cs.siue.edu'),), (('emailAddress', 'cs-support@siue.edu'),)
), 'version': 3, 'serialNumber': '08A121106F8E64208C10186AE42CC582B8B1E777', 'notBefore': 'Jun 27 23:38:02 2020 GMT', 'notAfter': 'Jun 25 23:38:02 2030 GMT'}]
146.163.150.242
4001
Welcome to the Server
what do you want to do? [GET] to open emails or [Exit] to close connection to serverget
Open

Enter Email: nu1@447.edu

                                ------------------
                                |DATE: 06/30/2020|      |TIME: 01:03:35|
                                ------------------

                                                         -----------
                                                         [Delivered]
                                                         -----------
        MAIL FROM: nu1@447.edu@447.edu
        RCTP TO: nu2@447.edu@447.edu
        Subject:lih

 Message:
        sdfusdpo ufsduf sdpufpsd fsd fsd
what do you want to do? [GET] to open emails or [Exit] to close connection to server
```