Tutorial 8 (TLS - Transport Layer Security)

In this tutorial, we will program a primitive TLS-based application. First, we will run a TLS server using OpenSSL and then write a Python client to interact with it.

1) Self-signed Digital Certificates

To run a TLS server, we will need a certificate. Recall that digital certificates are usually signed by trusted third parties such as Certificate Authorities (CAs). This allows us to verify whether the public key contained in the certificate belongs to the correct party. However, for experimentation, we cannot use these certificates since they must be purchased from a CA. Therefore, in development and lab settings, we use self-signed certificates.

A self-signed certificate is a digital certificate issued by the person or entity creating the certificate rather than by a trusted third-party certificate authority. This means the certificate is not backed by a well-known and trusted third party, so it may not be considered as secure as a certificate issued by a trusted authority.

Simply put, a self-signed certificate is neither privately nor publicly certified by a CA. Instead of seeking the certificate from a public or private CA, it is signed using its own private key; i.e., the signature in the certificate can be validated by the public key contained within the certificate itself.

We have already created a certificate for you—*certificate.crt*—which is available in the tutorial folder.

Use the `openssl` command you learned last week to inspect the certificate's contents.

- What is the public key algorithm used in the certificate?
- What is the email address associated with the certificate?
- What is the Common Name (CN)? We will need it later.

In [1]:
```
!openssl x509 -in ./certificate.crt -text -noout
```

```
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number:
            4a:b8:c9:37:9f:bb:52:34:06:96:25:48:5d:2a:f8:1a:d0:1f:ed:80
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=AU, ST=NSW, L=Sydney, O=The University of Sydney, OU=The
School of Computer Science, CN=localhost, emailAddress=support@cs.usyd.ed
u.au
        Validity
            Not Before: Apr 19 01:39:46 2024 GMT
            Not After : Oct 10 01:39:46 2029 GMT
        Subject: C=AU, ST=NSW, L=Sydney, O=The University of Sydney, OU=Th
e School of Computer Science, CN=localhost, emailAddress=support@cs.usyd.e
du.au
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:d1:df:d8:19:4a:22:80:0e:b0:e4:3e:1f:5a:60:
                    91:81:af:43:53:b6:b5:45:33:b3:22:cc:b1:55:4f:
                    3f:29:32:49:b9:b5:3b:7b:bb:4c:fd:90:86:d1:44:
                    a8:a4:f9:c6:25:a1:47:5c:a2:36:3a:40:bf:d3:0c:
                    23:ff:12:e6:b7:11:10:03:fe:52:39:9f:7b:a9:ef:
                    cc:9d:c1:3f:79:54:e1:d4:97:be:5a:b0:4e:8c:d8:
                    af:47:dd:ff:f7:7d:00:18:01:30:aa:c0:5c:0e:4d:
                    5b:5f:7e:10:3e:de:73:b0:83:11:3f:cf:b5:b6:26:
                    91:e6:24:73:92:5c:92:a6:2b:f1:cd:23:6a:34:87:
                    19:89:7a:ed:3d:19:20:69:0d:51:f1:2d:f6:8f:b0:
                    30:8e:14:bf:f8:42:29:0c:5c:59:c3:bb:63:ad:ce:
                    9a:2e:a0:00:b7:34:42:60:5d:94:3f:c1:4d:ac:fa:
                    cd:5c:01:38:b1:2a:d0:f8:22:6c:b7:83:88:d6:14:
                    6c:91:b5:23:de:de:38:15:98:3d:e9:6e:5f:65:fc:
                    15:b7:5f:ba:d1:38:af:56:00:7e:ed:f1:a6:8c:de:
                    38:89:63:d9:21:35:ff:98:2b:c4:10:cd:1a:4d:2b:
                    34:9b:36:4a:0b:25:38:72:dd:3a:3a:5d:2a:19:7f:
                    8f:f7
                Exponent: 65537 (0x10001)
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        9a:47:a6:70:c0:60:3e:3e:09:2f:54:11:72:f2:de:53:8d:00:
        d7:f9:db:d5:10:c6:5f:18:4a:38:ff:9f:7a:01:5e:31:35:14:
        da:7f:cc:e6:7d:88:44:d5:63:c7:d6:6e:f5:70:da:4f:7c:de:
        42:d5:e9:c3:23:92:96:cd:9e:dd:98:3c:57:fe:ca:38:c5:6f:
        e9:4a:7b:c6:3d:c9:e9:1b:b3:7d:e4:a4:68:a6:5c:ca:2f:6b:
        b8:e5:9f:9d:c1:13:9d:79:20:9f:60:ba:2f:36:29:0f:13:27:
        6a:8d:a5:7a:e8:cd:40:af:5a:32:9e:e5:35:fe:3b:75:76:8c:
        ec:d9:6c:19:29:80:82:1d:63:a8:64:90:ab:48:d2:c3:45:fa:
        6c:4f:e4:cd:04:90:ae:5f:f2:ca:14:45:a4:93:8e:0f:d1:ac:
        ac:6e:57:f1:83:29:ac:04:40:e2:6e:c3:bb:b3:99:64:55:d7:
        c4:39:dc:08:48:1c:31:c6:b8:dc:fa:69:30:6e:06:0b:de:73:
        87:24:4c:88:d0:67:22:11:b2:49:c1:0d:f2:11:b2:44:86:e0:
        cd:99:ef:d8:03:ec:6a:2a:33:23:66:06:c0:21:94:70:59:aa:
        e2:bf:d3:1f:ca:8f:be:71:ff:bd:45:5d:23:06:82:37:76:4b:
        0b:11:15:a1
```

Solution:

- What is the public key algorithm used in the certificate? **RSA**

- What is the email address associated with the certificate? **support@cs.usyd.edu.au**
- What is the Common Name (CN)? We will need it later: **localhost**

2) A Quick and Dirty TLS Server for Debugging Purposes

The `openssl s_server` command allows you to run a TLS server on a specified port. This server will perform TLS handshakes as required and display anything the client sends. However, you need to pass a few arguments to make it work.

- Open a new SSH connection to the VM.
- Run the following OpenSSL command to start the server:
  - **sudo openssl s_server -accept 4443 -cert certificate.crt -key private.key**
- You will be prompted to enter the access code for the private key. Enter `usyd`.
- If everything is running correctly, you will see the message `"Using default temp DH parameters ACCEPT"` in the command line.
- If you get an error like `"Address already in use"`, try using a different port number.
- **Do not close this terminal window** while the server is running.

3) Complete the TLS Client Code

Let's begin writing our TLS client. You will find starter code in the cell below. Read it carefully, then refer to the API documentation as needed (https://docs.python.org/3/library/ssl.html) to complete the code.

- How do you create a socket and initiate a connection?
- What is an SSL Context, and what parameters does the context require?
- How do we use the context with the connection?

In [ ]:
```
import ssl
import socket
import time

hostname = 'localhost'  # TODO - Set hostname to localhost
port = 4444             # TODO - Set the port number you are listening on

# This function handles communication once the TLS connection is establis
# TODO: Read and understand what it does. Nothing to change here.
# Understand what the server needs to do to close the connection.

def handle(conn):
    KEEP_ALIVE = True
    while KEEP_ALIVE:
        print("PING...")
        conn.write(b'PING...')
        time.sleep(1)
        res = conn.recv().decode().strip()
```

```
        if res == "HELLO" and KEEP_ALIVE:
            print("Received HELLO, sending CLIENT ALIVE...")
            conn.write(b'CLIENT ALIVE...')
        elif res != "HELLO" and KEEP_ALIVE:
            KEEP_ALIVE = False
            print("No HELLO received, closing the connection")
            conn.write(b'CLIENT CLOSING...')
            conn.close()

# TODO - Refer to https://docs.python.org/3/library/ssl.html
# TODO - Complete the code below

def main():
    sock = socket.create_connection((hostname, port))  # TODO add the con
    context = ssl.create_default_context(ssl.Purpose.SERVER_AUTH)  # TODO
    context.load_verify_locations("certificate.crt")  # TODO specify the
    context.verify_flags &= ~ssl.VERIFY_X509_STRICT # TODO - Disable stri
    conn = context.wrap_socket(sock, server_hostname=hostname)  # Wrap th
    try:
        handle(conn)
    except Exception as e:
        print(e)
    finally:
        conn.close()

main()
```

Run the code. In the server side you can type replies to the client in the command line.

Solution:

- How do you create a socket and initiate a connection?
  - Define the host (IP address or localhost) and port
  - Create an SSL Context
  - Create the connection
- Explain what an SSL Context is and what parameter the context needs?
  - It contains parameters related to the TLS connection
  - See: https://docs.python.org/3/library/ssl.html#ssl-contexts
  - `SERVER_AUTH` — Authenticate only the server; i.e., the server sends a certificate and the client verifies it.
- How do we use the context with the connection?
  - We wrap the socket with the SSL context using the `wrap_socket` method

4) Extension - Improving Security

Back to the client. Modify it such that:

- It verifies that the Organization and Organizational Unit in the server certificate have the correct values:
  - O (Organization) = The University of Sydney
  - OU (Organizational Unit) = The School of Computer Science

Why is it necessary for `localhost` to appear in the Common Name (CN) field?

In [5]:
```
import ssl
import socket
import time

hostname = 'localhost' ### TODO - Set hostname to localhost
port = 4444 ### TODO - Set the port number you are listening in openssl

### This function handles the communication the TLS connection is establi
### TODO Read and understand what it does. Nothing to change here. Unders

def handle(conn):
    KEEP_ALIVE=1
    while KEEP_ALIVE==1:
        print("PING...")
        conn.write(b'PING...')
        time.sleep(1)
        res = conn.recv().decode().strip()
        if res == "HELLO" and KEEP_ALIVE==1:
            print("Received HELLO, sending PING")
            conn.write(b'CLIENT ALIVE...')
        elif res != "HELLO" and KEEP_ALIVE==1:
            KEEP_ALIVE=0
            print("No HELLO received, Closing the connection")
            conn.write(b'CLIENT CLOSING...')
            conn.close()

### TODO - Have a look here https://docs.python.org/3/library/ssl.html
### TODO - And complete the codes

def main():
    sock = socket.create_connection(("localhost", port)) ### TODO add the
    context = ssl.create_default_context(ssl.Purpose.SERVER_AUTH) ### TOD
    context.load_verify_locations("certificate.crt") ### TODO Give the pa
    context.verify_flags &= ~ssl.VERIFY_X509_STRICT # TODO - Disable stri
    conn = context.wrap_socket(sock, server_hostname = hostname) ### Give
    cert = conn.getpeercert() ### TODO - Use the getpeercert() method to

    subject = dict(x[0] for x in cert['subject'])
    organizationName = subject['organizationName'] ### TODO - Extract org
    organizationalUnitName = subject['organizationalUnitName'] ### TODO -

    print(organizationName)
    print(organizationalUnitName)

    if (organizationName=='The University of Sydney' and organizationalUn
        try:
            handle(conn)
        except Exception as e:
            print(e)
        finally:
```

```
            conn.close()

main()
```

```
The University of Sydney
The School of Computer Science
PING...
```

```
---------------------------------------------------------------------------
KeyboardInterrupt                         Traceback (most recent call last)
Cell In[5], line 53
     49             print(e)
     50         finally:
     51             conn.close()
     52
---> 53 main()

Cell In[5], line 51, in main()
     47             handle(conn)
     48         except Exception as e:
     49             print(e)
     50         finally:
---> 51             conn.close()

Cell In[5], line 17, in handle(conn)
     13     while KEEP_ALIVE==1:
     14         print("PING...")
     15         conn.write(b'PING...')
     16         time.sleep(1)
---> 17         res = conn.recv().decode().strip()
     18         if res == "HELLO" and KEEP_ALIVE==1:
     19             print("Received HELLO, sending PING")
     20             conn.write(b'CLIENT ALIVE...')

File /usr/lib/python3.14/ssl.py:1285, in SSLSocket.recv(self, buflen, flags)
   1281     if flags != 0:
   1282         raise ValueError(
   1283             "non-zero flags not allowed in calls to recv() on %s" %
   1284             self.__class__)
-> 1285     return self.read(buflen)
   1286 else:
   1287     return super().recv(buflen, flags)

File /usr/lib/python3.14/ssl.py:1140, in SSLSocket.read(self, len, buffer)
   1138         return self._sslobj.read(len, buffer)
   1139     else:
-> 1140         return self._sslobj.read(len)
   1141 except SSLError as x:
   1142     if x.args[0] == SSL_ERROR_EOF and self.suppress_ragged_eofs:

KeyboardInterrupt:
```

5) Capturing Packets

Next, we are going to use the packet capture tool `tshark` to capture the packets exchanged between your client and the TLS server running in the VM.

- Go to the `/tmp` directory and run the command: `sudo tshark -i lo -w ./capture.pcap`
- Here, `lo` refers to the loopback interface on which our server is listening.
- While `tshark` is running, execute your client code again, then press `Ctrl+C` to stop capturing.
- If everything is working correctly, you will see an output like: `Capturing on 'Loopback: lo'`
- Download the capture file to your local machine.
- Download and install **Wireshark** on your computer from www.wireshark.org.
- Open the `capture.pcap` file using Wireshark.
- Find the communication between your client and the OpenSSL server.
- **Hint:** A TLS communication starts with a `Client Hello` message. Do a regular expression search.
- Once you find the packet, right-click and use the **Follow TCP Stream** option to get the full message flow.
- Inspect the **payload** tab for the packet content.

Question

- What TLS version does the communication use?
- What is the selected Cipher Suite?

> **Solution:**
>
> In Wireshark the message flow will appear as this.
>
> PCAP Trace
>
> - What TLS version does the communication use? **TLS1.3**
> - What is the selected Cipher Suite? **TLS_AES_256_GCM_SHA384**

4) Homework – Try the Above with Your Own Self-Signed Certificate

Use the link below to learn how to create your own self-signed certificate in Ubuntu:

- https://learn.microsoft.com/en-us/azure/application-gateway/self-signed-certificates
- Verify that when you specify a different hostname in the certificate, the code above no longer works.