Introduction to Computer Security Module – G6077

-

Introduction to OpenSSL

Contents

Client-Server architecture.....2

OpenSSL Tutorial: An Introduction to Internet Security.....2

Abbreviations Key.....2

Task 1 install OpenSSL.....3

Task 2 start the openssl.....3

Task 3 version of openssl.....4

Task 4 standard commands.....4

Task 5 inspect ciphers.....4

Task 6 verities of AES/DES.....4

Task 7 online book.....4

OpenSSL is among the most popular cryptography libraries. It is most commonly used to implement the Secure Sockets Layer and Transport Layer Security (SSL and TLS) protocols to ensure secure communications between computers. In recent years, SSL has become basically obsolete since TLS offers a higher level of security, but some people have gotten into the habit of referring to both protocols as "SSL."

Client-Server architecture

If you don't know about client-server architecture, have a quick read on this link.

OpenSSL Tutorial: An Introduction to Internet Security

When a client requests a secure connection to a server, the server, in turn, requests information to figure out which types of cryptographic security the client can support. Once it determines the most secure option, the following takes place:

1. The server sends a security certificate that is signed with the server's public key.
2. Once the client verifies the certificate, it generates a secret key and sends it to the server encrypted with the public key.
3. Next, both sides use the secret key to create two sets of public-private keys. At last, secure communication can commence.

SSL and TLS are two of many security protocols used to accomplish these steps. To implement these protocols, we need library like OpenSSL.

Abbreviations Key

You'll come across tons of abbreviations and other OpenSSL tutorials. For quick reference, here is a short list of some terms you might encounter:

- **CSR:** Certificate Signing Request

- **DER:** Distinguished Encoding Rules
- **PEM:** Privacy Enhanced Mail
- **PKCS:** Public-Key Cryptography Standards
- **SHA:** Secure Hash Algorithm
- **SSL:** Secure Socket Layer
- **TLS:** Transport Layer Security

Task 1 install OpenSSL

Install OpenSSL

- Read the author comments in red when you open the link below – third comment is interesting and of course funny
- Untick the donation option when you are installing
- Make sure that you know where you have installed the OpenSSL. I have installed it in Program Files, in C drive.
- Once installed open the command prompt and navigate to the OpenSSL folder to be able to run OpenSSL commands as shown in the image below.

Install link. Make sure that you install the correct version

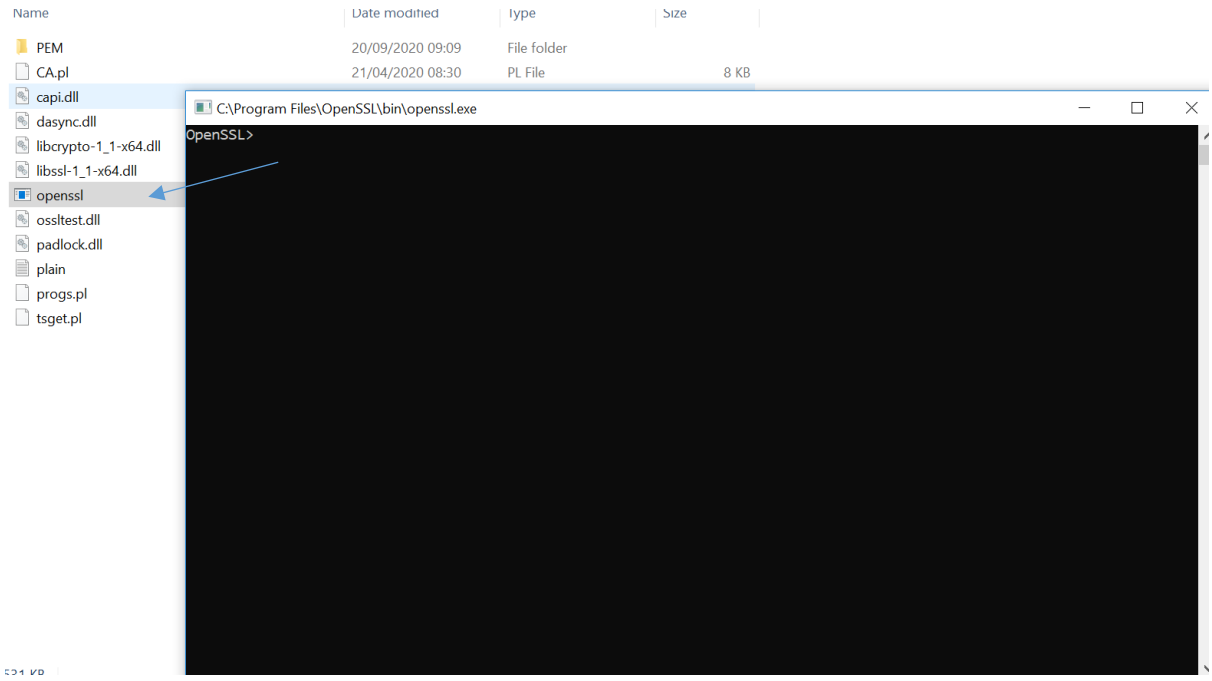
https://slproweb.com/products/Win32OpenSSL.html

Task 2 start the openssl

Important note:

In my examples, you will notice the word openssl. It refers to the openssl prompt. You do not need to type openssl while writing commands.

In the bin folder in OpenSSL, you will find openssl application file. Open the



Task 3 version of openssl

```
openssl version -a
```

```
OpenSSL 1.0.2h  3 May 2016
built on: reproducible build, date unspecified
platform: darwin64-x86_64-cc
options:  bn(64,64) rc4(ptr,int) des(idx,cisc,16,int) idea(int) blowfish(idx)
compiler: clang -I. -I.. -I../include  -fPIC -fno-common -DOPENSSL_PIC -DZLIB_SHARED -DZLIB -DOPENSSL_THREAD
S -D_REENTRANT -DDSO_DLFCN -DHAVE_DLFCN_H -arch x86_64 -O3 -DL_ENDIAN -Wall -DOPENSSL_IA32_SSE2 -DOPENSSL_BN
_ASM_MONT -DOPENSSL_BN_ASM_MONT5 -DOPENSSL_BN_ASM_GF2m -DSHA1_ASM -DSHA256_ASM -DSHA512_ASM -DMD5_ASM -DAES_
ASM -DVPAES_ASM -DBSAES_ASM -DWHIRLPOOL_ASM -DGHASH_ASM -DECP_NISTZ256_ASM
OPENSSLDIR: "/usr/local/etc/openssl"
```

Is any of these words familiar to you? Note the word DAES, blowfish and whirlpool.

Task 4 standard commands

Entering "help" or any random string is a way to list all commands supported in OpenSSL.

OpenSSL categorises commands into three. What are those three categories?

Task 5 inspect ciphers

Using the help command, inspect the following for its structure and different options that can be used with it

a) enc b) genrsa c) x509 d) md5 e) aes-128-cbc

Task 6 verities of AES/DES

List all the verities of aes. In all the variations of aes command, you will notice the following structure:

aes-Number-cbc/ecb [note cbc and ecb, it will be covered in a lecture]

What does the number represent in aes commands?

Make a list of des variations. You will notice that there is no number. Do you know why?

If you don't figure it out, that is fine. After the lecture of DES/AES, I will expect you to know the reason.

Task 7 online book

Cryptography is tricky business, and OpenSSL has too many features to cover it. The link below is to an online book about the OpenSSL which looked OpenSSL in a little more detail. You can read it online. We will be covering chapter1 mainly next week. You are free to complete chapter 1 this week.

https://www.feistyduck.com/library/openssl-cookbook/online/