Jericho Perdon
Prof Scrivnor
Comp 429
7 May 2021

Lab 10

Exploring SSL

Qanda

1) What is the OPENSSLDIR?

   The OPENSSLDIR is “usr/lib/ssl”.

2) What files are contained in this path?

   The files contained in this path are “certs”, “openssl.cnf”, private, and misc.

3) Where are most of the files actually located? (use ls -l)

   Most of the files are located in the “misc” folder.

Most Encountered Use Case

Qanda

1) Submit your CSR to canvas in the human readable format AND in the csr format. Make sure the field for Common Name is YOUR name.
2) Encrypt a text file that has your name in it with the public key above.
   - Use openssl rsautl --help to see the rsautl command options
   - The options you will need to provide are an infile, outfile, keyfile, public key flag, and encrypt flag
   - Submit your own encrypted file

3) Submit the encryption command you used as well.

openssl rsautl -encrypt -inkey fd.key -in encryptThis.txt -out encrypt.txt

4) Verify that this file was signed by me: http://429.scrivnor.ckileys.com/signed
   - I “signed” this file with my private key. Since only I can do that, you should be able to view the file in plaintext using my public key.
   - Submit the command used and contents of the file

5) Why can we not truly verify that the file was signed by me?

We cannot truly verify that the file was signed by Kevin because the private key can only be verified by the correct public key.