Jericho Perdon
Prof Scrivnor
Comp 429
12 May 2021

Lab 11

1) Submit your root-ca folder zipped up on Canvas.
2) db/index contains a database of certificates signed by your private CA. What does the first column mean? What are the possible values of the first column?

The first column tells if the certificate is verified or revoked. Possible values of the first column are “V” and “R”.

3) Looking at the first certificate in your db/index, the third field is the serial number for the certificate. What is this numbers relationship to db/serial?

The relationship between the serial number in index and serial number in serial is that the serial numbers (third column) in index are just slightly modified serial numbers.

4) Looking at the serial number for the first certificate, can you find it in certs/? If so, which *.crt file does it match in your root-ca directory?

The .crt file that matches my first certificate in the certs folder is the root-ca.crt file.

5) We have revoked the last certificate due to key compromise. How will a browser know that the certificate is no longer valid?

A browser will know that the certificate is no longer valid because the browser will not be able to verify the certificate.