CMPUT 333, Assignment 2, Winter 2021

(sliding part - 25%)

University of Alberta / Department of Computing Science

Instructor: Ioanis Nikolaidis (nikolaidis@ualberta.ca)

(certificates, certificate authorities)

Part 4 (25%)

From the earlier part of the assignment, you have set up an http server on your virtual Linux host. You will now add an `https` service on your Linux (only) host. That's additional to the `http` service already running) which means you will have to add a certificate for the `https` server, to enable encrypted access to it. The problem is you do not have the luxury for a Certificate Authority (CA) to sign your public key. So, you will become your own CA. It is recommended that you read about `openssl` and how you can use it to generate private keys, etc.

1. Each group will create its own public/private key pair (at least 1024 bit long private key) and create a self-signed root certificate (this is your CA certificate). The certificate's organization name should be `GroupXX_W21` where `XX` is your group number. Your `.crt` and `.key` files are to be submitted as part of the deliverables, as well as the password used to encrypt your private key. Note that you will have files for both your own CA as well as, in the next steps, for the server certificate. All of those files need to be submitted as part of the deliverables.
2. Generate a certificate request where the organization name is `GroupXX_W21_Web_Services` (again `XX` is your group's number). The certificate request `.csr` and the `.key` file is part of the deliverables.
3. Sign the certificate request with your "CA" private key. The policy should be set to `policy_anything`. You will have at this point a `.crt` file which is also part of the deliverables. In your writeup explain what would have been the impact if the policy was not set to `policy_anything`.
4. The next steps require that you configure your web server to use the `GroupXX_W21_Web_Services` certificate that was just signed, as well as your self-signed root GroupXX_W21 `CA` certificate. Describe how you accomplished this step.
5. Use the web browser on the virtual Windows host to access your Linux `https` server. Verify that it does **not** recognize the certificate authority that signed the certificate (for the deliverables, take a screenshot of this behavior). Then show how to install your root CA so that Internet Explorer trusts it. Try again to access your server's content and show that it is now successful (for the deliverables, take a screenshot of this behavior).
6. The above may sound simple but they have to be performed in the right order and with due care for details. In your report explain (using accompanying screenshots as necessary) what are the different file types you encountered and what is each type used for and why it is needed at a particular step. Outline any problems you encountered trying to achieve your goal. After you have completed this task:
7. Find how you can use your new power as CA to sign code, and in particular Java `jar` files. Write up the process of how to generate signed Java code and explain what is the purpose of each step (emphasizing the 'why' each step is needed). What (if any) are the differences with respect to the web server certificates?

You do not need to sign any code as this part of the task is mostly a reading exercise, but going through the steps using some example code and the appropriate tools could help you understand the process better.

8. **NOTE** The firewall rules applicable to your `https` server should be set to be exactly the same applicable to your Linux `http` service. Provide the additional (or changed) `iptable` commands necessary for treating the `https` service as the `http` service.

Deliverables

Only one of the group members need to submit on behalf of the entire group (in the event of more than one submission, the last one will be considered). Your report (in plaintext, markdown, or pdf format) should include answers to the questions posed in the specification. You should cite any resources that you used to produce your answers. Your report should be accompanied by all relevant files, e.g., private key and certificate files, screenshots, dump of `iptables` rules, etc. By default it is assumed that all group members equally contribute to the assignment. If you need to deviate from this model of cooperation, explain why and indicate who was responsible for what.

(This is the sliding part of Assignment 2 and will be submitted separately from the non-sliding part by the deadline for Assignment 3.)

Friday, March 12, 2021