CNS: TLS Programming Assignment

Note: Group assignment with max of 2 students per group.

Let us assume that IITH going to have many web services inside the campus which would be accessed among the IITH community. In this case, we may not need to have server certificates to be issued by a public Certificate Authority, we can have our own Certificate Authority to have secured services. This assignment is about creating such infrastructure and services by completing the following four tasks.

Task 1 (20 Points) - Creating a Public Key Infrastructure (PKI) for IITH: Let us have one root CA for IITH who would certify the intermediate CA for each department i.e., CSE, EE, ISAC. When each department wants to host their web servers then can get their server certificate signed by the intermediate CA of their own department. All the IITH community can configure their system to trust the IITH root CA. You need to create this PKI for IITH. You can use any cloud services such as Google Cloud or your own laptop to create VMs for each entity i.e., root CA, CSE CA, EE CA and ISAC CA. Server certificates for each department can be certified by only the respective intermediate CAs. Ensure that you provide realistic meta-data while creating certificates like values for CN, OU, L, Country, etc.

How to communicate among the multiple VMs?
You can use the Linux based commands like SCP for transferring the files.
You have to be sure about the integrity and clearly, show that the files transferred are indeed sent by the intended sender and received by the intended receiver.
For example, if you send the CSR to the Signing Authority, then the signing authority should be able to verify that it is sent by the intended sender and similarly when receiving the certificate back it should be verified that it is indeed signed and sent by the actual authority. You can use signing and encryption concepts for this.

Task 2 (10 points) - Creating a webserver with HTTPS support: The web server inside a particular department creates their own certificate and get it signed by the department's intermediate CA. The web server should allow only HTTPS connections to it. Configure the web server accordingly and configure the browser to trust the root CA and intermediate CA that you have created in Task 1. Host a web service that collects user profile for registration for a particular service. The user suppose to fill a form with some personal information. You need to show using wireshark that the connection between the client and server happens over HTTPS. You can either use a public cloud service such as Google Cloud or VMs on your own laptop/desktop.

Task 3 (30 Points) - Secure Peer-to-Peer application using PKI: Let us assume that the IITH community wants to create a secure application (e.g., chat application / gaming / file transfer / etc.) using the PKI of IITH in Task 1. You can pick up any application of your choice and code it in C/C++ by using OpenSSL or GnuTLS library. You need to use the PKI of IITH to get the user certificates and use SSL based communication between the users. Create your application using socket programming using SSL socket and show that the communication between the users is secure by using either TLS 1.2 or 1.3. You get bonus marks if you show performance improvement in TLS 1.3 compared to TLS 1.2 for your application.

Report (20 Points): The report should be a detailed assignment report and self sufficient to understand what you have done. You can add screenshots to show the working of the system. All the tools and softwares used should be mentioned with reference.

Deliverables: You need to submit all your source codes (well documented), configuration files, README file, wireshark traces and a detailed report in a single tar ball with filename as <your_roll_number>.tgz

Late Submission Policy: 20 % penalty for each late day submission.

PLAGIARISM STATEMENT <Include it in your report>

We certify that this assignment/report is our own group's work, based on our personal study and/or research and that we have acknowledged all material and sources used in its preparation, whether they be books, articles, reports, lecture notes, and any other kind of document, electronic or personal communication. We also certify that this assignment/report has not previously been submitted for assessment in any other course, except where specific permission has been granted from all course instructors involved, or at any other time in this course, and that we have not copied in part or whole or otherwise plagiarised the work of other students and/or persons. We pledge to uphold the principles of honesty and responsibility at CSE@IITH. In addition, we understand my responsibility to report honour violations by other students if we become aware of it.

Names of the Students in the group:

Date:

Signature: <keep your initials here>