Networks and Systems Security II - Winter 2025

Sambuddho Chakravarty

February 20, 2025

Assignment 2: Needham Shcroeder Based PDF Print Server (total points: 140)

Due date: March 15. Time: 23:59 Hrs. [Hard deadline, no extensions]

The objective of the assignment is to develop a PDF print server which converts a text or an image file to a PDF and sent it back to client. The server must be a multithreaded server that can handle multiple requests simultaneously (from multiple clients).

The requires you to design and implement a KDC server as well. The clients connect to the KDC server that provide them (*i.e.*, the clients with a signed ticket that they use when connecting to the print server.

The client (Alice) connects to the KDC and authenticates itself using a challenge response protocol that relies on Alice's long term secret (derived from a passphrase/password). Once authenticated, the KDC sends back to Alice a signed ticket that only the printer server (lets call it `PrnSrv`) can decrypt and verify, along with the session key K_{AP}, all of which are encrypted with Alice's long term secret so that it cannot be eavesdropped. You must also rely on ciphers like AES-GCM that can be also have inherent message authentication, that Alice must use to not only decrypt but also verify the messages. Thereafter, Alice then relies on a challenge response protocol, involving the signed ticket, to authenticate itself to `PrnSrv`.

After successfully authenticating to `PrnSrv`, Alice sends to it a file (either image or text) that the `PrnSrv` converts to a PDF using command line utilities like `img2pdf`, `enscript`, `ps2pdf` *etc.* to convert such files to PDF. Once converted, `PrnSrv` must send the encrypted files back to the Alice. The communication between Alice and `PrnSrv` must be encrypted using the session key K_{AP}.

All the entities, *i.e.* clients, `PrnSrv` and the KDC must be multi-threaded. These must be implemented in C. The encryption, message authentication, key derivation *etc.* must rely on `OpenSSL`'s `libssl` library.

What you need to submit:

You need to submit:

1. Complete source code the client, the KDC server and the `PrnSrv`, along with a simple `bash` script or command line instructions to run and test all of them (100 points).

2. Makefiles to compile and link the above programs thereafter generating binaries (10 points).

3. Details of the setup used to test the programs, run the individual programs (including appropriate command line arguments/files required if any), and `wireshark`/`tcpdump`/`tshark` captures as evidences corresponding to the various parts of the communication (30 points).