Lab2Milestone2

Jump to bottom

sethnielson edited this page 2 days ago · 1 revision

Lab 2 Milestone 1: Finalize Secure Layer

Assigned	11/14/2019
Due	11/22/2019
Points	100

Overview

You should already have a working cryptographic handshake that does an ephemeral key exchange. In this milestone, we are going to do two things.

1. Implement Certificate Verification
2. Implement bulk data transfer.

Certificate Generation, Certificate Verification

To ensure that your diffie-hellman keys are not generated by an unauthorized party with a false identity, you must modify your handshake to sign these keys by a long-term certificate. The PRFC needs to specify what is signed, the signature algorithms used, and other certificate details.

The one requirement for this lab that the PETF cannot change is that identity must follow playground addresses.

Unlike the real Internet, we are going to create some playground address hierarchies. Each team will "own" a block of addresses based on team number. Team 1, for example, will own all `20194.1.x.y` addresses. The staff will own team number 0.

To secure addresses, each team will create a CSR with a common name for `20194.<team number>.` . Each team will submit this to the staff via email (professor and TA please). We will send back a signed certificate.

Each team can generate any number of certificates for various addresses. For example, to use an address of `20194.1.100.200` , team 1 would generate a CSR with a common name of `20194.1.100.200` and sign it with the private key associated with their `20194.1.` certificate. The secure protocol must chain these certificates together so that anyone in the class can establish the chain of trust.

Bulk Data Transfer

In addition to verifying the certificate, you must also define a key-derivation protocol based on the key-agreement from the handshake. With these keys, you must arrange to secure transport to and from the peer. The PETF must agree on an algorithm and algorithm parameters.

Grading

Official testing will be derived from github as per recent updates posted by the TA. Please follow those instructions for submitting your official *individual* graded submission.

For self-testing, the auto-grader will be available shortly:

```
python autograder_lab2_client.py 20194.0.0.19000 <team_number> <email> milestone2 submit
```

NOTES: The autograder is running on the reliable class switch and is on port 19102

▼ Pages 26

Find a Page...

Home

BackgroundOverlayNetworks

- Creating an unreliable switch
- Exercise10MonitorPlayground
- Exercise1GettingStarted
- Exercise2EscapeRoomSockets
- Exercise3EscapeRoomAsyncio
- Exercise4EscapeRoomAsychUserInput
- Exercise5EscapeRoomPlayground
- Exercise6EscapeRoomPackets
- Exercise7EscapeRoomAdmission
- Exercise9StandardizeEscapeRoom
- Lab1Milestone1
- Lab1Milestone2
- Lab1Milestone3

Show 11 more pages…

Clone this wiki locally

```
https://github.com/CrimsonVista/20194NetworkSecurity.wiki.git
```