Homework 7

HTTPS

Objective 1: Certificate Generation

Generate a self-signed certificate. Save the public certificate and private key as files in your project directory. You do not have to generate your cert in your server code, or even write any code to accomplish this (Ie. command line openssl is recommended).

Objective 2: HTTPS Redirect

Grading Note: This objective exists as a partial credit opportunity. If you complete Objective 3 you do not have to add a redirect and you will get full credit for this objective (Ie. You can assume all traffic is HTTPS and skip this objective, but if you can't get objective 3 to work, add a redirect to get the 3 from this objective)

When your server receives an HTTP request, respond with a redirect to the same host and path, but using HTTPS. This will involve detecting which protocol is being used whenever a request is received.

This redirect must be functional no matter where your server is hosted (Ie. Do not hardcode "localhost:<port>" anywhere in your redirect. You should read the "Host" header of the request to redirect to the correct host. For example, if you change the port of your TCP server you should not have to change any of your redirect code.

Note: In the real world you will listen for HTTP and HTTPS requests on different ports instead of detecting which protocol is being used.

Objective 3: HTTPS

When you receive an HTTPS request, apply your certificate and respond with the expected encrypted response. You may use any libraries you'd like to handle the SSL/TLS aspect of this objective, but no libraries for the HTTP aspect of the protocol. You must use some code from another assignment to handle the HTTP request after it is decrypted.

For this objective you only need a single path that can serve any content, even if it's plain text.

Objective 4: HTTPS Site

Host an entire site with HTTPS. The site must include at least 3 files (Ie. HTML, JavaScript, and an image or CSS).

Bonus Objective: WSS

Bonus Grading: Any points earned on this objective will be distributed across other objectives in the way that will maximize your final grade. This distribution applies across all HW assignments (Ex. If your HW1 grade was 3/3/2/1, you have all 3's on all other assignments, and you earn a 3 on this objective, your HW1 grade will be 3/3/3/3).

Apply SSL/TLS to your WebSockets from HW6. In your JavaScript, use wss instead of ws when you make the connection and have your server respond appropriately.

Submission

To earn credit for this homework you must complete all 3 submissions.

1. Submit all the files of your site to AutoLab in a **zip** file
2. Submit your report to AutoLab as a **txt** file
3. Fill out the [homework self-grading form](#)