SSL Details

SSL is a security standard used to encrypt data before transmission over HTTP requests. This is an HTTPS request. SSL uses a public-private key system. The server has a private key, and sends out an authentication message to the client, which uses a public key to decrypt the authentication token. This allows the client to make sure the packet’s data or origin is not being impersonated.

The OPEnS lab has written a wrapper for SSL: SSLClient. This allows an arduino-ide compatible microcontroller to integrate HTTPS requests with an already existing network interface script (e.g. ethernet, wifi).

Sapflow Project

The Sapflow project uses an Ethernet Featherwing & Feather M0 to communicate with a server via get requests. We want to show encryption capability of the project.

Roadblocks to SSL Implementation at OSU

Our current server is hosted on web.engr.oregonstate.edu. The primary domain name field (subject) for the certificate being sent by web.engr.oregonstate.edu is always engineering.oregonstate.edu, with web.engr.oregonstate.edu in a secondary field (subject alternative names). The OPEnS SSLClient library is based on BearSSL, which does not support verification based on this alternate field. Thus, a mismatch (web.enrg.oregonstate.edu != engineering.oregonstate.edu) occurs, causing the connection to fail.

Solutions

There are two solutions that maintain the present server hosting domain:

1. Having a system administrator change the domain returns
2. Develop support in SSLClient (and BearSSL) for the alternate domain field.

The first option has already been rejected when this issue came up in the past. OSU has too much infrastructure around the certificates being presented, making changing them a difficult process.

The second option would require an inordinate amount of effort by members of the OPEnS lab.
With these two options exhausted we believe that the best option is to change hosting entirely. Switching to non-engineering hosting would allow for more control over certificates and network configurations.