Fall 2021

Section 1: TTh 3:30pm - 4:45pm - JFSB B092 (changed from MARB 130)

Project 6: TLS

Objectives

- Learn how websites you frequently use establish TLS connections.
- Learn about the openssl TLS debug utility

Background

The following openssl command can be used to debug TLS connections. It will output information regarding the TLS handshake. Port 443 is the default port for HTTPS connections. Run this command and notice the key exchange method that is used for this particular BYU website.

```
openssl s_client -connect booklist.byu.edu:443
```

Use control-c to break out of the TLS connection established by this command.

Consider also using the SSL Labs test too, and other command line options to openssl s_client. for instance, you can examine server certificates, see how they are signed, by what 3rd parties etc. Also testssl.sh may also be a helpful tool

Requirements

- Use the openssl command to connect to ten secure websites that you regularly use (email, social networking, banking, etc.)
- Write a brief report that lists the key cryptographic properties used by these websites to establish TLS connections. Put relevant information in a table, such as:
    - key exchange method
    - (message) authentication algorithm
    - symmetric encryption algorithm, key size, and mode
- Summarize any interesting differences or common features that you observe
- Explain what cryptographic guarantees are given by which portions of at least 3 of your samples.
- List questions about any information you don't understand or would like to know more about

See this document for examples of the TLS cipher suite options

- up to 5 bonus points for examining at least two NON-HTTP tls protected services (e.g. pop, imap, rtsp, ldap, sip, smtp, ...)

Submission

Submit a PDF of your report on Learning Suite.