Office of the Chief Information Security Officer
Risk Advisory: Transport Layer Security

Intended audience: IT staff, anyone interested in cybersecurity

What is Transport Layer Security?

Communication via the Internet is made possible by data exchanges between properly functioning endpoints. Each individual communication has two endpoints: usually a server, router, or other infrastructure device on one end, and either another server or an end user device (a **client**, such as a smartphone or a computer) on the other. The exchanges between endpoints are susceptible to eavesdropping at any point in the path between them. In order to prevent someone from listening in to your Internet activities, endpoints have rules when they talk to each other, and those rules are referred to as **protocols**.
A protocol that is specifically designed to ensure security between endpoints is Transport Layer Security, or TLS. TLS enables a secure connection by allowing a server and client:

- to authenticate or verify one another's identity,
- to agree upon a method of **encryption**, which is a way to obfuscate data from attackers, and
- to ensure reliable transmission of data by including a message authentication code.

TLS is often used interchangeably with SSL (Secure Sockets Layer), which was first developed in 1995. TLS came along a few years later and became known as a more secure version of SSL. While they are two distinct protocols with different rules, the term "SSL" is still associated with encrypted connections, as in the term "SSL certificates," which verifies a website or server's identity. When you see "HTTPS," rather than "HTTP" at the beginning of a URL, the "S" refers to the SSL certificate, and implies that the connection is secure.
Within each protocol version, there are **cipher suites**, which can be thought of as the underlying encryption algorithms used. The two endpoints must agree on which cipher suite to use. In addition to disabling obsolete protocols, you should also disable cipher suites which have become insecure, where possible.

Why should you care?

Understanding the TLS protocol and keeping servers, browsers, and websites configured and updated to the latest version is an important part of securing UW's institutional systems. Check the resources below for guidance.

Risks of using deprecated protocols and cipher suites

Using a deprecated version of TLS or an insecure cipher suite provides users with a false sense of security. Like WEP and WPA Wifi encryption, deprecated protocols and cipher suites are easy enough to subvert or "crack" that they offer little or no practical protection against eavesdropping. Endpoints which use deprecated protocols and cipher suites put at risk the data transmitted for interception or manipulation by cyber attackers.

Things to do

- Ensure that you see "https" (not http) on any websites in which you enter information, particularly login credentials, and be aware that "http" web pages are highly vulnerable to attacks, such as eavesdropping and injection of unwanted advertisements.
- Enable TLS 1.2 or 1.3 on all web browsers that you use.
    - You can test your browser here.
- Server administrators should disable TLS 1.0, 1.1 and require connections to use TLS 1.2 or above.
    - You can test your servers and view best practices and other documentation here.

- Review the list of cipher suites which your clients and servers support, and consider disabling those which are insecure. This can be complex and has risks (many older or embedded systems will become unreachable if you disable the only supported cipher suites), so consult with your vendor or product documentation and test carefully. For detailed guidance on deprecated cipher suites, visit the NSA Advisory.

Resources

Qualys SSL Labs
https://www.ssllabs.com/index.html
Test Your Browser
https://clienttest.ssllabs.com:8443/ssltest/viewMyClient.html
SSL Server Test
https://www.ssllabs.com/ssltest/
Qualys SSL/TLS deployment best practices
https://www.ssllabs.com/projects/best-practices/index.html
Verisign: Everything you need to know about SSL certificates
https://www.verisign.com/en_US/website-presence/online/ssl-certificates/index.xhtml
Modernizing TLS connections in Microsoft Edge and IE 11 (updated 8/2020)
https://blogs.windows.com/msedgedev/2018/10/15/modernizing-tls-edge-ie11/
NSA Guidance to eliminate obsolete TLS 1.0 Protocol Configurations
https://media.defense.gov/2021/Jan/05/2002560140/-1/-1/0/ELIMINATING_OBSOLETE_TLS_UOO197443-20.PDF