Ryan Stearns  
Final Project Abstract  
Second Submission  
CNA 432

As security threats are growing exponentially in numbers every year, there is a primary goal for companies to provide privacy, as well as data integrity between two communicating applications. [1] Transport Layer Security aims to provide these security needs, while eliminating many of the vulnerabilities apparent in its predecessor, Secure Socket Layers. This paper will discuss the fundamentals of the Transport Layer Security (TLS) Protocol, its predecessor Secure Socket Layers (SSL), as well as examining both past and present vulnerabilities of TLS and SSL. There are many factors that make Transport Layer Security a necessity for businesses, and average end users alike. TLS is made up of two subsystems, the TLS Record Protocol, and the TLS Handshake protocol. TLS uses “symmetric cryptography for data encryption,” and keeps the connections private. [1] Another benefit of using TLS is it also makes the connection more reliable, and it is “application protocol independent and higher-level protocols can layer on top of the TLS Protocol transparently.” [1] SSL 3.0 was the predecessor of TLS 1.1, and Google Chrome, as well as Microsoft Internet Explorer, have plans to disable SSL 3.0 Support in the very near future. [2] Furthermore, this paper will discuss the future outlook of Transport Layer Security, primarily in terms of adapting to vulnerabilities that could potentially be exposed within TLS.