Name: Nicholas Mason

Course: CS445 – Internet Security

Date: March 28th, 2018

CS 445 – Internet Security Technical Report

Introduction

SSL certificates

SSL certificates were originally created in order to provide an additional layer of security when a private party is attempting to communicate on the internet, specifically connecting to websites where confidential information may be passed between each party. A website where confidential information is needed to complete a transaction or process, involving such information as a user’s name, password, banking information, or social security number, must now have a SSL certificate. Having such a certificate allows the website to obtain a distinct public and private encryption key, further providing a higher level of security online.

A SSL certificate can be obtained by a given website by going through the process of finding a 3rd party Certificate Authority, also called a CA. The CA will possess the ability to authenticate and legitimize the intent of the website. If the website passes the qualifications of the CA, the website will gain access to their own unique public and private encryption keys for their specific IP address or domain name of their website. To a user on the internet, the lock icon next to the URL and the URL starting with the symbols HTTPS ensures the user that the website has obtained some sort of SSL certificate from a Certificate Authority, resulting in their personal information being encrypted.

Creating a certificate for a given website

Conclusion