Release Date: 23 Sep 2020
Source: Application Security Division

Need of SSL/TLS certificate for all Websites

Overview

Websites are viewed in popular browsers (like Chrome, Mozilla Firefox, Safari, Opera etc.) by Users. The services and telemetric used in these popular browsers have in-built browsing safety features such as safe-browsing and website trust etc. The compliance to these browsers safety features requirement needs to be met from a broader perspective to establish the breach of trust.

Impact

1) Browsers trust the websites based on SSL certificate. If the website is hosted over plain http, the browser will show that website is **not-trusted**. SSL certificate is mandatory for establishing trust with the website in popular browsers to serve.
   In HTTP communication, the web server served pages are transferred in plain text. Malicious attackers may monitor the network traffic to capture website details.
2) Looking into the perceptive of privacy content of website users, attackers could likewise target anyone who visits an unprotected website.

Solution

1) The incorporation of SSL certificate in a website provides Certificate Authority details like signed authority, Domain information which is a major source of trust. Based on these information, browser checks the details in Online Certificate Status Protocol (OCSP) for validation. This also provides transport layer security to the browsed content.
   The website communication between the client's browser and SSL based website's Server is ensured to be secure.
2) **Enabling Static website over HTTPS would likewise build trust as well, as connection would be encrypted between website and client's browser.**
3) **It is recommended to host a site over https (i.e. using valid SSL/TLS certificate of latest updated version) for all Websites.**