Department of Computer Science and Engineering

Course Title: Computer Networks

Course Code: CSE 319

Date of submission: **31/10/2021**

Submitted by: _____

Name: Ayman Hasib

Reg. No.: 18201065

Section: B1

Submitted to: _____

Name: Dr. A S M Touhidul Hasan

Designation: Assistant Professor

TLS 1.3

Introduction:

It has been almost eight years since the last encryption protocol update. But the final version of TLS 1.3 has been published recently in 2018. TLS 1.3 includes a lot of security and performance improvements. TLS 1.3 in 2018, encrypted connections are now more secure and faster than ever.

What is TLS?

The full form of TLS is Transport Layer Security. And it came after the SSL (Secure Sockets Layer). And it is the successor to SSL. TLS provides the encrypted or secure communication between web browsers and servers. It can provide the security in the connection because it uses the symmetric cryptography to encrypt the data transmissions. There are unique keys generated for building up each network by this TLS, and method is known as TLS handshaking.

Benefits of using TLS 1.3:

- **Speed of TLS 1.3:**
  This encrypted connection always add up the performance when it comes to web performance. It helps HTTP to solve the performance, but this TLS 1.3 enhances the speed up encrypted connections with more features such as TLS false start and Zero Round Trip (0-RTT). It requires only one round-trip, which in turn cuts the encryption latency in half. Another advantage of this, it can remember**.** On sites users have previously visited, so that he can send data on the first message to the server.

- **Improve Security:**
  TLS 1.3 came up with extra security, where that other encryption method leaves the connection on vulnerable to attacks. It removes the insecure features from TLS 1.2 as following:
  (a)SHA-1, (b) RC4, (c) DES, (d) 3DES, (e) AES-CBC, (f) MD5

  Because this protocol it is more simplified that this makes it less likely for administrators and developers to misconfigure the protocol. And it increases the extra security.

- **Browser Support:**
  As there are various browsers available, for these browsers there are different versions of TLS 1.3 available. Such as Chrome 70, Firefox 63. This TLS 1.3 gives the extra security and encryption to the browser during communication and browsing.

- **Block unauthorize user:**
  It can block the unknown unencrypted traffic from entering or leaving the network. So that the network can stay safe from untracked users.

- **Server Support:**
  TLS 1.3 can provide better encryption than other security protocols. Such as, TLS1.2, 1.2, 1.0, SSL. So that the communication or data transmission between host and servers are always secure.

Summary:

Just Like other security layers TLS 1.3 is another important protocol from which we can get benefit for many years. It doesn't provide the encrypted connection to become faster, but also it provides the secure connection more than that. So, that users can get a delightful experience from this security protocol TLS 1.3.