Report on TLS 1.3

Aarav Varshney[1]

[1]**Ashoka University**, aarav.varshney@alumni.ashoka.edu.in

Abstract

Writeup on TLS and with focus on version 1.3.

1. Introduction

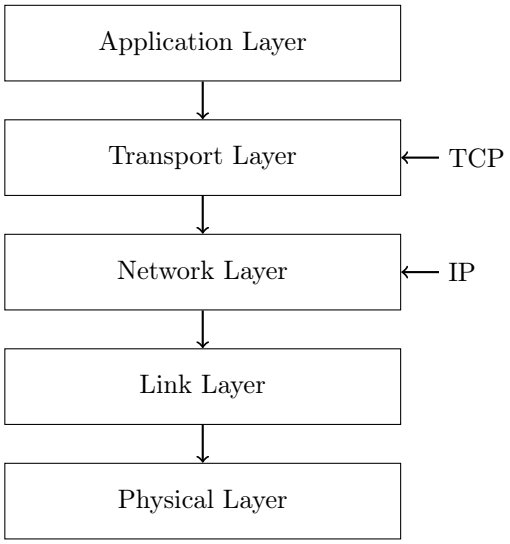

Figure 1. The TCP/IP Reference Model [1]

When two computers want to send data to each other, they may use the **Internet Protocol** (IP) [2] directly. IP fragments data into blocks of data called *packets* (also called datagrams) and transmits them from the source to the destination. The sources and destinations are computers identified by fixed length addresses. However, IP is a low-level protocol that does not interact directly with application data and may cause unreliable data transmission.

In the TCP/IP Reference Model [1], the IP protocol works in the network layer, which is two layers below the application layer (see Figure 1). This layer provides an unreliable, connectionless delivery system (there is no direct connection between two hosts) which does not provide any functionality for error recovery for datagrams that are either duplicated, lost or arrive at the remote host in another order than they were sent. The transport layer, which is the layer above the network layer, is responsible for fixing the unreliable data transmission with transport protocols like **Transmission Control Protocol (TCP)** [3]. TCP is the most commonly used transport protocol on top of IP and includes strategies for packet ordering, retransmission, and maintaining data integrity.

TCP is a connection-oriented protocol, which means that before any data can be sent, a connection must be established between the two hosts. This connection is established by a three-way handshake between the two hosts. The first computer sends a packet with the SYN (a field in the TCP header) bit set to 1. The second computer responds with a packet with the SYN and ACK (another field in the TCP header) bits set to 1. The first computer then sends a packet with the ACK bit set to 1. Once the connection is established, the two hosts can start sending data to each other.

Now that we have established a connection between two hosts and have the ability to reliably send data across, we can further improve the transmission by using **Transport Layer Security (TLS)** [4] (original [5]). TLS protocol allows two hosts to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery. While TCP provides reliable data transmission, the data in the packets is unencrypted and can be read by anyone who has access to the network. This is acceptable when the data is not sensitive, but when the data is sensitive, TLS is used to *encrypt* the data. TLS also provides *authentication* of the remote host, which means that the remote host can be trusted to be the host it claims to be.

TLS is primarily used in a client/server setting where the client initiates the connection and the server responds. Setting up a TLS connection requires a handshake between the client and the server. At the end of the handshake, the client and the server have agreed upon a shared secret key which is used to encrypt the data, the encryption schemes and their parameters, and the client is also assured of the server's identity (not without issues [6, 7]).

In this report, we discuss TLS 1.3 [4], which is the latest version of TLS in two sections. Section 1 covers the *handshake protocol* in TLS 1.3. Section 2 discusses the *record protocol* that uses the parameters established by the handshake protocol to protect traffic between the communicating hosts.

2. TLS Handshake Protocol

H

$$(k_{\text{sh}}, k_{\text{sm}}, k_{\text{ch}}, k_{\text{cm}}) := H_1\left(g^{\alpha\beta}, u, \mathcal{N}_{\text{c}},\ \text{offer}\ , v, \mathcal{N}_{\text{s}},\ \text{mode}\ \right)$$
$$(k_{\text{c}\to\text{s}}, k_{\text{s}\to\text{c}}) := H_2\left(g^{\alpha\beta}, u, \mathcal{N}_{\text{c}},\ \text{offer},\ v, \mathfrak{N}_{\text{s}},\ \text{mode}\ , c_1, \ldots, c_4\right)$$

References

[1] A. S. Tanenbaum and D. J. Wetherall, *Computer Networks*, 5th ed. USA: Prentice Hall Press, 2010.

[2] "Internet Protocol," RFC 791, Sep. 1981. [Online]. Available: https://www.rfc-editor.org/info/rfc791

[3] "Transmission Control Protocol," RFC 793, Sep. 1981. [Online]. Available: https://www.rfc-editor.org/info/rfc793

[4] E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.3," RFC 8446, Aug. 2018. [Online]. Available: https://www.rfc-editor.org/info/rfc8446

[5] C. Allen and T. Dierks, "The TLS Protocol Version 1.0," RFC 2246, Jan. 1999. [Online]. Available: https://www.rfc-editor.org/info/rfc2246

[6] B. Laurie, A. Langley, and E. Kasper, "Certificate Transparency," RFC 6962, Jun. 2013. [Online]. Available: https://www.rfc-editor.org/info/rfc6962

[7] A. Parsovs, "Practical issues with tls client certificate authentication," 01 2014.