Common Criteria Evaluation and Validation Scheme

National Information Assurance Partnership (NIAP)

Title: Essential Security Requirements for Transport Layer Security (TLS)

Maintained by: US NIAP and UK CESG

Unique Identifier: 42

Version: 1.0

Status: draft

Date of issue: 31 Aug 2016

Approved by:

Supersedes:

Background and Purpose

This Essential Security Requirements (ESR) document describes a core set of security requirements for implementations of Transport Layer Security. The resulting Extended Package (EP) will permit evaluation of such functionality through the Common Criteria paradigm. The resulting EP is intended to serve as a consistent "building block" for evaluation of TLS functionality in application software, operating systems, mobile devices, and other IT products.

Use Cases

Several versions of the TLS protocol are in widespread use in applications such as web browsers, email, instant messaging, and voice-over-IP (VoIP). Major web sites use TLS to protect the communications from their servers. TLS is also commonly used to protect communications between hosts and network infrastructure devices for administration.

Resources to be protected

The TLS protocols provide confidentiality and integrity for the data transmitted between two communicating endpoints on Internet Protocol networks. This also includes the Datagram TLS protocol (DTLS), which is a connectionless version of TLS.

Attacker access

The attacker is expected to engage in the following general classes of attack against TLS implementations:

- Network eavesdropping, in which an attacker may monitor and attempt to gain access to data exchanged between the product and other endpoints.
- Network attack, in which an attacker may initiate malicious communications with the product or alter communications between the product and other endpoints.

Essential Security Requirements

Functionality-related requirements are:

- Confidentiality for transmitted data.
- Integrity for transmitted data.
- Identification and authentication of the server-side endpoint, and optionally the client-side endpoint.

Assumptions

The following assumptions are made for the TLS implementation and its operational environment:

- The private key of the TLS server has not been compromised. Compromise of this key implies compromise of any data transmitted over the TLS connection, as well as an inability to identify and authenticate the server. Similarly, any compromise of a client private key implies an inability to identify and authenticate that client.
- System administrators and users are not malicious in nature, and do not inadvertently or intentionally misconfigure the TLS software (e.g. null cipher).