Network Working Group Internet-Draft Intended status: Informational Expires: September 1, 2019

Security is a function, not a layer draft-kuehlewind-security-is-not-a-layer-00

Abstract

This document argues that security functions should be implemented on each layer as needed. Especially security functions should not be separated in its own layer. Having security scoped to the needs of each layer makes it possible to separate different functions correctly without the risk of impacting security on another layer. Note that this does not mean that each layer needs to maintain and negotiate it's on security context.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of <u>BCP 78</u> and <u>BCP 79</u>.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <u>http://datatracker.ietf.org/drafts/current/</u>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on September 1, 2019.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to <u>BCP 78</u> and the IETF Trust's Legal Provisions Relating to IETF Documents (<u>http://trustee.ietf.org/license-info</u>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in <u>Section 4</u>.e of

Expires September 1, 2019

Internet-Draft

security is not a layer

the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

<u>1</u>. Introduction

Today, encryption and (server) authentication in the web is mostly provided by TLS. TLS is a security protocol on top of (usually) TCP. However, a TLS session might possible not be end-to-end, where an end-point is associated with the actual user at the application level, but could be interrupted by an immediate device that e.g. terminates the TCP connection, so-called TCP proxies. Further, intermediate devices might block TLS negotiation, as a side effect when higher layer in-network functions are preformed. This effect has been often observed in e.g. mobile network which a connection failure rate of up to 20% when TLS is used [CROWD].

[More information to follow... this 00-draft is a place-holder only.]

- **2**. Definitions
- 3. Discussion
- **<u>4</u>**. Informative References
 - [CROWD] Mandalari, A., Bagnulo, M., and A. Lutu, "Informing Protocol Design Through Crowdsourcing: The Case of Pervasive Encryption", 2015.

Author's Address

Mirja Kuehlewind ETH Zurich Gloriastrasse 35 8092 Zurich Switzerland

Email: mirja.kuehlewind@tik.ee.ethz.ch

Kuehlewind

Expires September 1, 2019 [Page 2]