What's in a Downgrade? A Taxonomy of Downgrade Attacks in the TLS Protocol and Application Protocols Using TLS

By [Submitted on 15 Sep 2018 (v1), last revised 26 Jan 2019 (this version, v2)]

Archived: 2026-04-05 19:57:24 UTC

View PDF

Abstract:A number of important real-world protocols including the Transport Layer Security (TLS) protocol have the ability to negotiate various security-related choices such as the protocol version and the cryptographic algorithms to be used in a particular session. Furthermore, some insecure application-layer protocols such as the Simple Mail Transfer Protocol (SMTP) negotiate the use of TLS itself on top of the application protocol to secure the communication channel. These protocols are often vulnerable to a class of attacks known as downgrade attacks which targets this negotiation mechanism. In this paper we create the first taxonomy of TLS downgrade attacks. Our taxonomy classifies possible attacks with respect to four different vectors: the protocol element that is targeted, the type of vulnerability that enables the attack, the attack method, and the level of damage that the attack causes. We base our taxonomy on a thorough analysis of fifteen notable published attacks. Our taxonomy highlights clear and concrete aspects that many downgrade attacks have in common, and allows for a common language, classification, and comparison of downgrade attacks. We demonstrate the application of our taxonomy by classifying the surveyed attacks.

Submission history

From: Eman Alashwali [view email]
[v1] Sat, 15 Sep 2018 09:22:50 UTC (132 KB)
[v2] Sat, 26 Jan 2019 10:58:37 UTC (132 KB)