Cryptology ePrint Archive: Report 2013/049

Lessons Learned From Previous SSL/TLS Attacks - A Brief Chronology Of Attacks And Weaknesses

Christopher Meyer and Jörg Schwenk

Abstract: Since its introduction in 1994 the Secure Socket Layer (SSL) protocol (later renamed to Transport Layer Security (TLS)) evolved to the de facto standard for securing the transport layer. SSL/TLS can be used for ensuring data confidentiality, integrity and authenticity during transport. A main feature of the protocol is its flexibility. Modes of operation and security aims can easily be configured through different cipher suites. During its evolutionary development process several flaws were found. However, the flexible architecture of SSL/TLS allowed efficient fixes in order to counter the issues. This paper presents an overview on theoretical and practical attacks of the last 15 years, in chronological order and four categories: Attacks on the TLS Handshake protocol, on the TLS Record and Application Data Protocols, on the PKI infrastructure of TLS, and on various other attacks. We try to give a short ”Lessons Learned” at the end of each paragraph.

Category / Keywords:

Publication Info: SSL, TLS, Handshake Protocol, Record Layer, Public Key Infrastructures, Bleichenbacher Attack, Padding Oracles

Date: received 31 Jan 2013

Contact author: christopher meyer at rub de