20 Jahre Forschung an SSL/TLS - Eine Anaylse der Basistechnologie für Internet Sicherheit

Christopher Meyer

Entwickelt 1994, etablierte sich SSL/TLS im Laufe der vergangenen Jahre zum de facto Standard für sichere Kommunikation im Internet. Das Protokoll unterliegt der stetigen Weiterentwicklung und ist bis zum jetzigen Zeitpunkt in 5 verschiedenen Versionen verfügbar. Durch die flexible Architektur können einerseits die jeweiligen Sicherheitsziele für einen Kommunikationsablauf dem Anwendungsszenario (auch zur Laufzeit) angepasst werden, andererseits ist somit eine unkomplizierte Modifikation der verwendeten kryptografischen Algorithmen möglich.

Die eingereichte Dissertation analysiert die Sicherheit des Protokolls, zeigt neue, bisher unveröffentlichte Angriffe praktischer und theoretischer Art und beschreibt eine neuartige Technik zur Identifizierung von SSL/TLS Implementierungen aus der Ferne. Weiterhin wird die zur Zeit umfangreichste Liste bekannter Angriffe präsentiert. Im Rahmen der Dissertation wurde ein umfangreiches Test-Framework - T.I.M.E. - zur Evaluierung/Penetration des Protokolls und der Interaktion im gesamten Protokollverlauf implementiert, das direkten Zugriff auf alle Phasen, Nachrichten und deren Inhalte ermöglicht. Hierdurch erübrigt sich die Notwendigkeit verschiedenste SSL/TLS Software verstehen und dem Testszenario anpassen zu müssen. Die Verwendung des Frameworks wird anhand der Referenzimplementierung zur vorgestellten Fern-Identifizierung von SSL/TLS Implementierungen verdeutlicht. Durch die Referenzimplementierung kann, unter Verwendung des T.I.M.E.-Frameworks, die SSL/TLS Software (Hersteller/Version) eines Servers durch gezielte Provokation signifikanter Systemzustände analysiert und identifiziert werden.

Die bisher unveröffentlichten Angriffe auf das SSL/TLS Protokoll basieren auf bekannten Angriffstechniken und wurden auf neue Anwendungsszenarien adaptiert. Hierbei kommen sowohl Techniken im Zusammenhang mit der gezielten Herbeiführung von Fehlerzuständen auf Seiten des Servers, als auch die Beobachtung von Abarbeitungszeiten durch die Server Software zum Einsatz. Desweiteren wird eine praktische Untersuchung von (Pseudo-) Zufallszahlengeneratoren und der Gleichverteilung der hiermit generierten Zufallszahlenfolgen vorgestellt. Aufgrund der besonderen Bedeutung von Zufallszahlen für SSL/TLS sind die Ergebnisse für alle SSL/TLS Implementierungen, die fehlerhafte oder schwache (Pseudo-) Zufallszahlengeneratoren verwenden, von praktischer Relevanz.

Die während dieser Dissertation gewonnenen Erkenntnisse und Fehlerberichte führten zu Korrekturen bestehender Produkte und beeinflussten nachhaltig die Implementierungen weitverbreiteter Software. Hierbei wurde (vor Veröffentlichung der Fehlerberichte) eng mit den Herstellern zusammengearbeitet um die Probleme dauerhaft zu beheben. Aus diesem Grund finden sich in dieser Ausarbeitung bisher unveröffentlichte Forschunsgergebnisse, für die vom Hersteller erst in naher Zukunft Updates verfügbar sein werden.