RUB

Über die Kryptografische Sicherheit Browser-Basierter Protokolle

hgi NDS

Florian Kohlar

Um Sicherheit im Internet gewährleisten zu können werden vor dem Austausch sensibler Daten sogenannte Authentikations- und Schlüsselaustauschprotokolle ('Authenticated Key Exchange', AKE) ausgeführt. Das wichtigste dieser Protokolle ist das **S**ecure **S**ocket **L**ayer (SSL) / **T**ransport **L**ayer **S**ecurity (TLS) Protokoll. Es wird unter anderem zur Absicherung von HTTP-Verbindungen benutzt wird, der Grundlage des World Wide Web. In allen aktuell existieren kryptografischen Sicherheitsmodellen konnte das TLS Protokoll bislang nicht bewiesen werden, sodass wir keine formalen Aussagen über die Sicherheit dieses Protokolls treffen konnten. Aufgrund der hohen Verbreitung von TLS ist dies ein besonders kritischer Mangel im Stand der Technik. Dieser Mangel wurde in der vorliegenden Arbeit behoben.

Die Ergebnisse lassen sich in drei Schwerpunkte gliedern:

1. Zuerst wird Konstruktion beweisbar sicherer Protokolle für Authentikation und Schlüsselaustausch untersucht. Hierbei wird gezeigt, wie man aus einem Schlüsselaustauschprotokoll mit niedrigen Sicherheitsanforderungen auf generische Art und Weise ein sicheres AKE Protokoll mit hohen Sicherheitseigenschaften konstruieren kann.

2. Dann wird ein Sicherheitsmodell für den sicheren Aufbau von authentischen und vertraulichen Kanälen ('Authenticated and Confidential Channel Establishment', ACCE) entworfen. Dieses Modell ermöglicht es, für alle im Standard vorgesehenen Kombinationen von kryptografischen Algorithmen erstmalig einen Sicherheitsbeweis für das komplette TLS Protokoll zu geben. Daber werden sowohl Varianten für beidseitige Authentikation als auch serverseitige Authentikation betrachtet. Alle Ergebnisse fußen auf allgemein akzeptierten kryptografischen Annahmen und kommen ohne die Verwendung sogenannter *Random Oracles* aus.

3. Zuletzt wird die Sicherheit des TLS Renegotiation Protokolls untersucht, welches ermöglicht, über einen vorher ausgehandelten, sicheren Kanal frische Sicherheits-Parameter auszutauschen. Bisher war unklar, wie ein solcher Anwendungsfall formal modelliert werden kann, weshalb zuerst ein geeignetes Sicherheitsmodell für Multi-Phasen Protokolle und sichere Neuverhandlungsprotokolle entworfen wird. In diesem Modell wird dann die Sicherheit des TLS Renegotiation Protokolls sowohl mit als auch ohne zusätzliche Sicherheitsmaßnahmen gegen spezifische Angriffe analysiert. Schließlich wird eine neue Sicherheitsmaßnahme vorgeschlagen, welche es erlaubt, TLS Renegotiation auch im stärksten der eingeführten Sicherheitsmodelle als sicher zu beweisen.