Zero Round-Trip Time Key Exchange: Foundations and Applications

Sebastian Lauer

Schlüsselaustauschprotokolle werden verwendet, um zwei oder mehr Parteien die Möglichkeit zu geben, ein gemeinsames Geheimnis über einen unsicheren Kanal zu etablieren. Eines der ersten Schlüsselaustauschprotokolle wurde 1976 von Diffie und Hellman vorgestellt. Seitdem wurden verschiedene Protokolle entworfen, welche verschiedene Sicherheitsanforderungen erfüllen sollen. Neben dem Ziel einen sicheren Schlüssel zu etablieren, ist *Forward Security* eine weitere Sicherheitseigenschaft, die von moderne Protokolle angestrebt wird. Forward Security garantiert, dass selbst dann, wenn ein Angreifer Zugriff auf den privaten Schlüssel einer der beteiligten Parteien erhält, die zuvor ausgetauschten Sitzungsschlüssel sicher bleiben. Diese Eigenschaft wird in Protokollen wie dem Transport Layer Security-Protokoll (TLS) oder dem Internet Key Exchange-Protokoll (IKE) durch Interaktion zwischen den beteiligten Parteien erreicht. Diese Interaktion besteht in der Regel aus dem Austausch von Diffie-Hellman-Schlüsseln, was zu einer Latenzzeit führt, da Nachrichten über einen Kanal hin und her gesendet werden. Eine solche Latenz wird als Round-Trip-Time (RTT) bezeichnet. Moderne Protokolle erfordern in der Regel mehr als eine RTT für den Schlüsselaustausch. Um die Latenz zu verringern, schlug Google 2013 das Konzept des 0-RTT-Schlüsselaustausch vor. 0-RTT-Protokolle ermöglichen es einem Client, innerhalb der ersten Nachricht des Protokolls verschlüsselte Nachrichten an den Server zu senden. Der symmetrische Schlüssel, der zur Verschlüsselung der ersten Nutzlastnachricht verwendet wird, wird durch die Verwendung einer so genannten Server-Konfigurationsdatei abgeleitet, die einen öffentlichen Schlüssel des Servers enthält. In den nächsten Schritten des Protokolls wird durch den Austausch von Diffie-Hellman-Schlüsseln ein weiterer Schlüssel berechnet. Der zweite Schlüssel wird dann als Sitzungsschlüssel zur Verschlüsselung aller weiteren Nachrichten verwendet.

In dieser Thesis wird dieses Konzept aus einer akademischen Perspektive untersucht. Es werden Sicherheitsmodelle entwickelt, um zu analysieren, welche Sicherheitseigenschaften mit dem 0-RTT-Protokollen erreicht werden können. Zusätzlich werden einfache Konstruktionen von 0-RTT-Protokollen entworfen und analysiert. Lange Zeit war es eine offene Frage, ob es überhaupt möglich ist, Forward Security für die erste Nachricht zu erreichen. In dieser Thesis wird bewiesen, dass man diese Eigenschaft durch die Verwendung einer neuen kryptographischen Primitive erreichen kann. Auf Grundlage dieser Ergebnisse wird zusätzlich untersucht, ob 0-RTT-Protokolle in Onion-Routing-Netzwerken wie z.B. Tor genutzt werden kann. Tor ermöglicht anonymes Routing, indem Nachrichten über mehrere Routern gesendet werden. Jede Nachricht ist dabei mit den Schlüsseln der jeweiligen Router verschlüsselt. Dazu muss ein Benutzer einen geheimen Schlüssel mit jedem Router auf dem Pfad austauschen, was zu einer großen Menge an Nachrichten führt. Im Rahmen dieser Thesis wird gezeigt, dass mit Hilfe von 0-RTT-Schlüsselaustausch die Anzahl der benötigten Nachrichten für diesen Prozess drastisch reduziert werden kann.