BAN-Analyse des Authentifizierungs-Schlüssel im MTProto Mobile Protocol

Anna-Katharina Wickert

13. April 2015

Mobile Endgeräte, wie das Smartphone, werden größtenteils für den Versand von Nachrichten verwendet. Aus diesem Grund wird es immer wichtiger, dass die verwendeten Protokolle auch kryptografisch sicher sind. Die Analyse ist aber ein komplexer Prozess, da durch eine unsichere Komponente das ganze System angreifbar sein kann.

Ein Ansatz ist die logikbasierte Analyse mit der BAN-Analyse. Dabei wird mit logischen Operatoren jeder einzelne Schritt des Protokolls dargestellt. Durch diese Abstraktion lässt sich das Protokoll in sprachlichen Phrasen ausdrücken. Ein Beispiel ist: Alice glaubt, dass der Nonce frisch erzeugt wurde (A glaubt frisch (N)). Auf die formalisierte Form des Protokolls werden anschließend Regeln nach der BAN-Analyse angewandt. Am Ende der Analyse sieht man formal, ob alle Ziele des Protokolls erreicht wurden.

Als Beispiel für die Analyse wird das MTProto Mobile Protocol (MTPMP) verwendet. Das MTPMP wird von Telegram verwendet und ermöglicht den Empfang von verschlüsselten Nachrichten auf mehreren Endgeräten. Telegram ist eine Anwendung, die es erlaubt über verschiedene Plattformen verschlüsselt und kostenlos Nachrichten zu versenden.

Die Idee der Erfinder ist es Short Messaging Service (SMS), als auch die E-Mail zu vereinen. Die Anwendung soll über die mobile Datenverbindung kommunizieren und dabei sicher sein. Konkret wird die Erzeugung des Authentifizierungs-Schlüssels abstrahiert und untersucht. Mit dem einmalig erzeugten Schlüssel ist es, möglich die Nachricht zu entschlüsseln und zu verschlüsseln.