# Modellierung und Analyse von Kryptographischen real-world Protokollen

Florian Bergsma

In der nahen Vergangenheit ist die beweisbare Sicherheit von kryptographischen Protokollen, die täglich eingesetzt werden, mit in den Fokus der kryptographischen Forschung gerückt. Sicherheitsanalysen von sogenannten „real-world“ Protokollen stellen Forscher vor eine neue Herausforderung: Die echte Welt muss in einem theoretischen Modell so präzise wie möglich abgebildet werden. Doch zwischen Theorie und Praxis besteht offenbar eine Lücke, denn trotz gültiger Sicherheitsbeweise in der Theorie gibt es praktische Angriffe auf – als sicher bewiesene – Protokolle. In dieser Arbeit wird ein Schritt gemacht, die Lücke zwischen Theorie und Praxis zu schließen.

Zuerst wird die Modellierung von kryptographischen Protokollen untersucht. Die unterschiedlichen Modelle werden je nach Anwendbarkeit motiviert und dargestellt. Ein Fokus hierbei liegt auf dem sogenannten ACCE Modell, welches das am besten geeignete kryptographische Werkzeug zu sein scheint, um „real-world“ Protokolle zu analysieren.

Die Ergebnisse dieser Arbeit lassen sich dann in die folgenden Schwerpunkte gliedern:

1. In einem ersten Schritt wird das ACCE Modell erweitert um die Neuverhandlung von kryptographischen Parametern zu modellieren. Diese Entwickelung wird durch einen Angriff auf den Renegotiation Mechanismus von TLS motiviert, der genau in die Lücke zwischen Theorie und Praxis fällt.
   Die Standardisierte Lösung dieser Sicherheitslücke wird kryptographisch analysiert. Hierbei fällt auf, dass die Lösung nicht das gewünschte Maß an Sicherheit liefert, was auch durch einen 2014 publizierten erneuten Angriff auf TLS-Renegotiation, in Verbindung mit dem Session-Resumption Mechanismus von TLS, gezeigt wurde. Eine in dieser Arbeit Vorgeschlagene Sicherheitslösung kann auch den neuen Angriff abwehren.
2. Dann wird die Sicherheit von SSH, dem Secure Shell Protokoll, analysiert. SSH ist ein sehr wichtiges Sicherheitsprotokoll, welches häufig für den Remotezugriff zur Serverkonfiguration eingesetzt wird. In einem ersten Schritt wird die Sicherheit von SSH bewiesen, wenn kryptographische Parameter nur einmal pro Sitzung ausgehandelt werden. Dann wird das erweiterte ACCE Modell verwendet und die Neuverhandlung (bei SSH Re-Exchange genannt) kryptographisch untersucht.
3. Die Arbeit schließt mit einer sehr effizienten Konstruktion eines Zwei-Nachrichten Protokolls, welches ein hohes Maß an Sicherheit liefert. Dieses Protokoll garantiert Sicherheit, selbst wenn der langlebige geheime Schlüssel oder der kurzlebige geheime Sitzungsschlüssel der beiden Parteien kompromittiert sind. Protokolle mit diesen Sicherheitseigenschaften haben insbesondere durch die aktuelle Spionageaffäre an Bedeutung gewonnen.