Das Design und die Analyse der sicheren Kommunikationsprotokolle

Yong Li

Informationssicherheit spielt eine wichtige und entscheidende Rolle in der heutigen digitalen Gesellschaft. Integrität und Authentizität von Daten muss sichergestellt werden können und Informationen müssen vertraulich gesendet werden können. Kryptographische Protokolle zur authentischen Schlüsselvereinbarung (AKE-Protokolle) bilden einen wichtigen Baustein, um eine sichere Kommunikation zu gewährleisten. Diese Protokolle werden von mehreren Parteien in einer unsicheren oder nicht vertrauenswürdigen Kommunikationsumgebung, wie dem Internet, ausgeführt um anschließend Daten authentisch, integritätsgeschützt und vertraulich übertragen zu können. Etwas genauer erlauben sie einer Partei, etwa Alice (A), einen Kommunikationspartner, beispielsweise Bob (B), zu authentifizieren und einen gemeinsamen, "sicheren" Sitzungsschlüssel zu generieren. Die Kommunikation wird anschließend mit diesem Sitzungsschlüssel geschützt.

Das Design und die Analyse der sicheren Kommunikationsprotokolle haben sich als nichttriviale Aufgabe erwiesen. Der Beweis der Sicherheit einfacher kryptographischer Protokolle ist üblicherweise sehr komplex. Viele Protokolle wurden ohne theoretische Rechtfertigung, d.h. ohne formalen Sicherheitsbeweis, entwickelt. Dies umfasst etwa die Protokolle TLS/SSL, IPSec oder Kerberos. Aus diesem Grund gibt es in regelmäßigen Abständen Angriffe auf diese Protokolle. Daher ist die Analyse bstehender Protokolle, sowie der Entwurf theoretisch fundierter kryptographischer Protokolle von großer Wichtigkeit, wenn man solche Angriffe vermeiden möchte.

Diese Arbeit beschäftigt sich mit dem Design und Analyse kryptographischer Protokolle in den aktuell gängisten Sicherheitsmodellen. Wir zeigen wie man die Kommunikationsprotokolle systematisch konstruieren und analysieren kann, insbesondere für authentifizierte Schlüsselaustauschprotokollen in realitätsnahen Modellen. Protokoll entwickeln und analysieren kann. Diese Arbeit besteht aus zwei Teilen.

Im ersten Teil dieser Dissertation erweitern wir existierende Sicherheitsmodelle, um zusätzlich praktisch relevante Angriffe zu simulieren, die durch existierende Modelle noch nicht berücksichtigt wurden. Außerdem diskutieren wir die vorgeschlagenen Sicherheitsmodelle und zeigen die Beziehungen zu vorherigen Modellen auf.

Im zweiten Teil dieser Dissertation beschreiben wir die Ergebnisse mit den folgenden Schwerpunkten:

- In einem ersten Schritt erforschen wir zwei neue effiziente Transformationen, die sichere Schlüsselaustauschprotokolle gegen passive Angreifer in effiziente sichere AKE-Protokolle gegen aktive Angreifer überführen.

- Wir konstruieren generisch das erste AKE-Protokoll mit einer "scharfen Reduktion" (tight reduction). Der Sicherheitsbeweis verliert nur einen konstanten Faktor.

- Wir analysieren die Sicherheit des TLS-PSK Protokolls. TLS-PSK ist ein sehr wichtiges Sicherheitsprotokoll, welches häufig für den Remotezugriff auf eine Smartcard eingesetzt wird. Um die Sicherheit des Protokolls zu beweisen haben wir das bekannte ACCE Modell erweitert.

- Die Dissertation schließt mit einen neuen generischen Angriff gegen AKE-Protkolle ("No-Match Attacks"). Wir zeigen, dass unser Angriff auf viele existierende AKE-Protokolle durchgeführt werden kann. Wir betonen, dass unsere Angriffe nicht das Modell verletzen, in dem die Sicherheit dieser Protokolle bewiesen wurde. Schließlich geben wir einige Lösungen an mit deren Hilfe unser Angriff verhindert werden kann.