Browserbasierte Identitätsföderation

Browserbasierte Identitätsföderation etabliert eine Dreiparteienauthentifikation mit einem Standard-Webbrowser als Client. So das Forschungsgebiet der Dreiparteienauthentifikation auch gut etabliert ist, lassen sich dessen Resultate nicht direkt auf browserbasierte Protokolle anwenden. Ein Standard-Webbrowser ist nicht unmittelbar in der Lage, die vorherrschende Methode des sicheren Sitzungsschlüsselaustausches für Identitätsföderation einzusetzen. Stattdessen verwendet ein Webbrowser einen bereits etablierten server-authentifizierten Kanal, um den Berechtigungsnachweis einer dritten Partei zu übertragen. Mit diesen zwei Schritten wird ein beidseitig authentifizierter Kanal aufgebaut. Diese Doktorarbeit behandelt das Problem, den Kanalaufbau durch browserbasierte Identitätsföderation als sicher zu beweisen.

Wir tragen zweierlei Forschungsergebnisse zu dem Gebiet bei: (i) Zunächst führen wir detaillierte Protokollanalysen von Standards des Gebiets durch, mit denen wir eine Reihe potentieller Sicherheitslücken bei einem realistisches Angreifermodell aufzeigen. (ii) Während sich jedoch frühere Beiträge zu diesem Gebiet auf die Suche nach Angriffen beschränkt haben, gehen wir einen Schritt weiter. Wir zeigen den ersten rigorosen *Sicherheitsbeweis* für standardisierte Identitätsföderation mit einem *formalen Browsermodell*. Dazu führen wir *Channel Authenticity* als neue Sicherheitseigenschaft browserbasierter Protokolle ein, die stärkere Garantien bietet als die verbreitete Entity Authentication. Im Prinzip garantiert Channel Authenticity einen sicheren Kanal zwischen dem identifizierten Benutzer und einem akzeptierenden Dienstleister.

Diese Promotion umfasst drei Arten von publizierten Forschungsbeiträgen: (i) Wir veröffentlichten die erste Sicherheitsanalyse der standardisierten Security Assertion Markup Language (SAML). Unsere Analyse bewirkte signifikante Verbesserungen in SAML und wurde vom Standardkomitee anerkannt. Wir entwarfen auf der Grundlage von Geheimnisverteilung neue Schutzmaßnahmen, die eine höhere Effizienz und Sicherheit im Vergleich zu bestehenden Maßnahmen bieten. (ii) Wir entwickelten ein formales Modell für browserbasierte Protokolle, welches auf dem Reactive-Simulatability-Rahmenwerk (RSIM) basiert. Unser Modell stellt eine neue, an die Unified Modelling Language angelehnte, Spezifikationssprache für das RSIM-Rahmenwerk bereit. (iii) Wir erstellten einen rigorosen Sicherheitsbeweis für das browserbasierte WS-Federation Passive Requestor Interop Profile. Dies ist der erste Beweis eines standardisierten Identitätsföderationsprotokolls. Er beruht auf unserem formalen Browsermodell, wohldefinierten Annahmen und protokollspezifischen Maschinen im RSIM-Ramenwerk.