Kurzfassung der Dissertation "Binding Credentials – Securing (SSO) Authentication" von Florian Feldmann

Diese Dissertation beschäftigt sich mit der Authentifizierung von Benutzern in Web-Umgebungen, speziell in Single Sign-On Szenarien. Zunächst wird – anhand des Beispiels von Software-as-a-Service Cloud Anbietern – ein theoretisches Modell des für die Authentifizierung zuständigen Moduls eines Cloud Services erläutert. Anhand dieses Modells werden drei mögliche Angriffsklassen definiert, die sich in den benötigten Fertigkeiten des angenommenen Angreifers unterscheiden. Darauf aufbauend werden mögliche Angriffe identifiziert und diesen Angriffsklassen zugeordnet. Für jeden Angriff werden entsprechende Gegenmaßnahmen empfohlen. Eine anschließende Feldstudie, bei der alle identifizierten Angriffe gegen die SAML-Authentifikations-Schnittstellen von insgesamt 22 realen Cloud Service Providern getestet wurden, zeigt, dass in der Praxis hier teils gravierende Sicherheitsprobleme existieren: 20 der 22 getesteten Anbieter waren jeweils gegen mindestens einen der identifzierten Angriffe anfällig.

Um die Sicherheit der Authentifizierung in solchen Szenarien zu erhöhen, werden verschiedene kryptographische Bindings diskutiert. Speziell das TLS-Unique Channel Binding, bei dem Authentisierungsinformationen an einen spezifischen TLS-Kanal gebunden werden, wird eingehend untersucht. Es wird dargelegt, wie dieses Binding sowohl in herkömmlichen (z.B. Passwort-basierten) als auch in Single Sign-On Protokollen eingesetzt werden kann, um die Sicherheit gegen Man-in-the-Middle Angriffe und anderweitigen Diebstahl der Authentisierungsinformationen deutlich zu erhöhen.

Weiterhin wird dieses Binding auch auf den Bereich der Mobiltelefonie übertragen: Hier steht mit der SIM-Karte ein hardware-basiertes Mittel zur Verfügung, das bislang jedoch nur vom entsprechenden Mobile Service Provider sinnvoll zu Authentifikationszwecken eingesetzt werden kann. Es wird in dieser Dissertation gezeigt, wie die Authentifikation mittels SIM-Karte mit dem bereits vorher analysierten TLS-Unique Channel Binding kombiniert werden kann, um eine sichere Authentifizierung eines Nutzers gegenüber einem Webservice-Anbieter (z.B. einem Cloud Provider) zu realisieren.

In der Praxis erfolgt nach der initialen Authentifikation eines Nutzers (über Nutzername/Passwort-Kombinationen, SSO Authentifikationsverfahren o.ä.) eine Persistentmachung dieser Authentifikation mittels Session Cookies. Diese unterliegen technisch ähnlichen Gefährdungen wie die Zugangsdaten bei der initialen Authentifikation und sollten ebenfalls abgesichert werden. Die Arbeit diskutiert daher die Anwendbarkeit verschiedener kryptographischer Bindings zur Absicherung von Session Cookies.

Neben einer Authentifikation der Teilnehmer sollen moderne sichere Kommunikations-protokolle oft auch eine sichere, d.h. unter anderem vertrauliche, Kommunikation dieser Teilnehmer untereinander ermöglichen. Zu diesem Zweck müssen meist kryptographische Schlüssel zwischen den Teilnehmern ausgetauscht oder vereinbart werden. Die Dissertation zeigt daher eine Möglichkeit, wie das Authentisierungsframework SAML standardkonform erweitert werden kann, um den sicheren Austausch solcher Schlüssel oder Teilschlüssel zu gewährleisten.