On Message-Level Security

Über Nachrichtensicherheit

Christian Mainka

Die vorliegende Dissertation beschäftigt sich mit dem Thema Nachrichtensicherheit in Webservices und Single Sign-On (SSO) Systemen. Durch die in der Dissertation beschriebene Methodologie sind zahlreiche Sicherheitslücken in verschiedenen Softwarebibliotheken und Webseiten identifiziert, gemeldet und behoben worden.

Im ersten Teil der Dissertation wird die Sicherheit von SOAP-basierten Webservices untersucht. Mithilfe der in diesem Rahmen entwickelten Software *WS-Attacker* ist es möglich vollautomatische Penetrationstests durchzuführen. In der Dissertation sind neuartige Angriffstechniken mit dem Fokus auf automatischer Erkennung und Umgehung von existierenden Gegenmaßnahmen entwickelt worden. Dadurch konnten zahlreiche Schwachstellen in bekannten Webservice-Frameworks sowie in der *IBM DataPower* und dem *Axway Security Gateway* festgestellt werden. Diese sind den Herstellern gemeldet und durch die Mithilfe des Autors behoben worden.

Im zweiten Teil der Dissertation wird die Sicherheit von SSO Systemen untersucht. Es werden generische Angriffskonzepte entwickelt, die anschließend auf die Protokolle *OpenID*, *OpenID Connect* und *SAML* angewendet werden. Diese Konzepte beruhen auf einem neuen Angriffsparadigma, das durch die Dissertation eingeführt wird. Das Paradigma basiert auf der Frage, ob der Identity Provider (IdP) in einem SSO Protokoll stets als vertrauenswürdige dritte Partei angesehen werden kann. Die Dissertation zeigt, dass in modernen SSO Protokollen ein Angreifer seinen eigenen, bösartigen IdP verwenden kann. Dieser kann für das Auffinden von Schwachstellen (Vulnerability Detection) und für dessen Ausnutzung (Vulnerability Exploitation) verwendet werden.

Auf Basis des Paradigmas werden die entwickelten Angriffstechniken evaluiert. Dabei werden Schwachstellen in verschiedenen *OpenID*, *OpenID Connect* und *SAML* Implementierungen identifiziert. Die Sicherheit von weit verbreiteten Systemen, wie Software-as-a-Service Cloud Anbietern, konnte vollständig gebrochen werden. Es wird gezeigt, wie die Anmeldung in fremden Accounts, das Auslesen von lokalen auf dem Server gespeicherten Dateien, effiziente *Denial-of-Service* sowie komplexe *Server-Side-Request-Forgery* Angriffe erfolgreich durchgeführt werden konnten.

Im Rahmen der Dissertation werden darüber hinaus Angriffe auf die Spezifikation von *OpenID Connect* gezeigt. Diese ermöglichen es, das Hauptziel des Protokolls – die Authentifizierung des Endbenutzers – unabhängig von der genutzten Implementierung zu brechen. Gemeinsam mit den offiziellen *OAuth*- und *OpenID Connect*-Arbeitsgruppen der Internet Engineering Task Force (IETF) ist eine Gegenmaßnahme entwickelt worden. Auf Grund der Angriffe werden die Spezifikationen von *OAuth* und *OpenID Connect* zur Zeit erneuert und angepasst.