Single Sign-On Sicherheit

Vladislav Mladenov
vladislav.mladenov@rub.de

Single Sign-On (SSO) ist ein Konzept mit dessen Hilfe sich ein Benutzer einmalig an einer zentralen Instanz, dem Identity Provider (IdP), anmeldet und diese Authentifikation anschließend benutzt, um sich bei weiteren Dienstleistern (Service Providern, SPs) anzumelden. Zu diesem Zweck erstellt der IdP ein Authentifizierungstoken, welches dann vom SP überprüft und für den Login genutzt wird. Es existieren unterschiedliche SSO Protokolle, die in opensource Bibliotheken und kommerziellen Produkten implementiert sind. Zu den bekanntesten SSO Anbietern in Internet gehören Google, Facebook, Microsoft und PayPal.

Die vorliegende Dissertation stellt eine umfassende Sicherheitsuntersuchung von verschiedenen SSO Protokollen und deren Implementierungen vor. Ausgangsbasis für diese protokollübergreifende Untersuchung ist die Entwicklung eines neuartigen Konzepts *(malicious IdP, mIdP)*, das erstmals die Benutzung eines bösartigen IdPs für Angriffe einführt. Der *mIdP* ist in der Lage, valide wie invalide Nachrichten und Authentifizierungtokens an verschiedene SPs zu senden. Darauf aufbauend werden generische Angriffsklassen entwickelt, die entsprechend ihrer Voraussetzungen und ihrer erreichten Ziele kategorisiert werden. Anschließend werden diese Angriffsklassen auf verschiedene SSO Protokolle angewendet, was zur Entdeckung zahlreicher kritischen Schwachstellen in Software-as-a-Service Cloud Anbietern, eCommerce Produkten, web-basierten Nachrichtenportalen, Content-Management Systemen und opensource Bibliotheken führt. Die gefundenen Schwachstellen ermöglichen den unerlaubten Zugang zu fremden Accounts, das Auslesen von geschützten Ressourcen sowie das Aussetzen von Dienstanbietern mithilfe von Denial-of-Service Techniken.

Um die Sicherheit von SSO Systemen zu verbessern und einen erhöhten Schutz gegen Angriffe zu erlangen, werden in dieser Dissertation Technologien beschrieben, die die Authentifizierungstoken während des Transports zusätzlich absichern und einen Diebstahl verhindern bzw. erkennen. Diese Technologien nutzen einen vorliegenden TLS Kanal und binden ihn kryptografisch an den Authentifizierungstoken.

Die Dissertation hat die Entwicklung vieler SSO Bibliotheken und Systeme, die SAML, OpenID oder OpenID Connect einsetzen, beeinflusst. Die gefundenen Schwachstellen wurden mit den Entwicklern kommuniziert, die bei der Behebung unterstützt wurden. Ein weiteres Ergebnis dieser Arbeit ist die Änderung der OpenID Connect und OAuth Spezifikation, die aufgrund zweier neu aufgedeckter Angriffe angepasst werden musste. Eine entsprechende Gegenmaßnahme wurde in Zusammenarbeit mit der OpenID Connect und OAuth Arbeitsgruppe veröffentlicht.