Über die Sicherheit von Web Single Sign-On

Andreas Mayer

Single Sign-On (SSO) Lösungen gewinnen derzeit besonders in großen Unternehmen und im Internet (z.B. Facebook Connect und Google+ Sign-In) sehr stark an Bedeutung. Die zunehmende Verbreitung von SSO wird hauptsächlich durch den erhöhten Benutzerkomfort, die möglichen Kosteneinsparungen und die Effizienz dieser Technologie angetrieben. Die Sicherheit dieser Systeme wird dagegen oft vernachlässigt. Gleichwohl stellt ein SSO-System aber ein besonders attraktives und lohnenswertes Angriffsziel dar. Eine einzige Schwachstelle kann alle föderierten Webseiten kompromittieren und den vollständigen Identitätsdiebstahl des Opfers bedeuten. Deshalb ist es unabdingbar, dass die verwendeten SSO-Technologien sehr sicher und selbst gegen komplexe Angriffe äußererst resistent ist.

Diese Dissertation beschäftigt sich mit der Sicherheit von Single Sign-On Systemen auf Basis der Security Assertion Markup Language (SAML). Der XML-basierte SAML-Standard erlaubt die Realisierung von SSO-Lösungen und zeichnet sich durch eine hohe technische Reife und große Industrieakzeptanz aus. Zudem wird SAML bei vielen bedeutenden Diensten wie Google Apps, Salesforce und verschiedenen E-Government Systemen eingesetzt. Diese Arbeit gliedert sich in drei Hauptteile.

Zuerst werden allgemeine Gefahren und Schwachstellen von webbasiertem SSO analysiert und zwei verschiedene SAML Identity Provider (IdP) Funktionalitäten untersucht: Das Ausstellen von SAML Assertions und die Sicherheit der IdP Webanwendung selbst. Die Analyse von sechs IdPs zeigt, dass alle in mindestens einer untersuchten Funktionalität Schwachstellen aufweisen. Es kann entweder ein neuartiger SAML-Angriff (ACS Spoofing) durchgeführt oder aber die HTTP Session Cookies gestohlen werden. Die gefundenen Angriffe erlauben einem Angreifer den vollständigen Identitätsdiebstahl bei allen föderierten Webseiten der SSO-Domäne.

Im folgenden Teil werden verschiedene Varianten von sogenannten *Channel Bindings* diskutiert, die die kryptographischen Fähigkeiten des Transport Layer Security (TLS) Protokolls als ganzheitliche Schutzmaßnahme verwenden. Es wird die erste praktisch einsetzbare Implementierung des SAML Holder-of-Key SSO Profiles für das weit verbreitete SimpleSAMLphp Framework vorgestellt. Darüber hinaus wird eine neuartige Variante dieses Profiles diskutiert und implementiert, welches Authentifizierungsanfragen und SAML Assertions an TLS Client-Zertifikate bindet. Diese kryptographische Verschränkung wird anschließend auf Session Cookies erweitert. Alle im ersten Teil vorgestellten Angriffsvarianten werden durch diese kombinierte Gegenmaßnahme verhindert.

Im dritten Teil werden mehrere praktische und sehr kritische Angriffe auf SAML-Nachrichten vorgestellt. Eine detaillierte Analyse von 14 weit verbreiteten SAML Frameworks zeigt, dass elf von diesen – einschließlich Salesforce, Shibboleth und IBM XS40 – mit verschiedenen XML Signature Wrapping (XSW) Angriffen komplett gebrochen werden können. Diese Angriffstechnik umgeht den Integritätsschutz von XML Signature und erlaubt es einem Angreifer, sich mit jeder beliebigen Identität an jeder föderierten Webseite anzumelden.

Zusammenfassend beeinflussen die Ergebnisse dieser Arbeit eine Vielzahl von SAML Frameworks und Systemen. Die gefundenen Schwachstellen wurden durch Updates behoben. Darüber hinaus ist die vorgeschlagene Channel Binding-Variante generisch und kann in jedem anderen SSO-Protokoll (z.B. OAuth oder OpenID), ohne tiefgreifende Änderung der bestehenden Infrastruktur, verwendet werden. Dies kann als ein Schritt hin zu einer ganzheitlichen Absicherung von webbasierten Authentifizierungslösungen und SSO-Systemen gesehen werden.