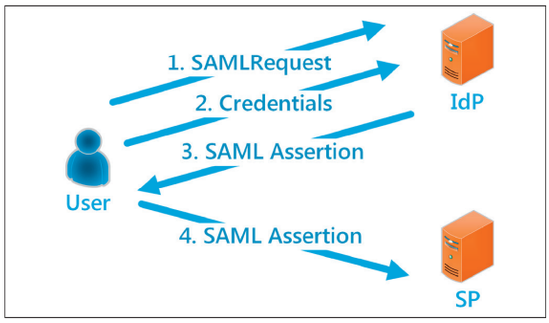
Roland Bischofberger

Emanuel Duss

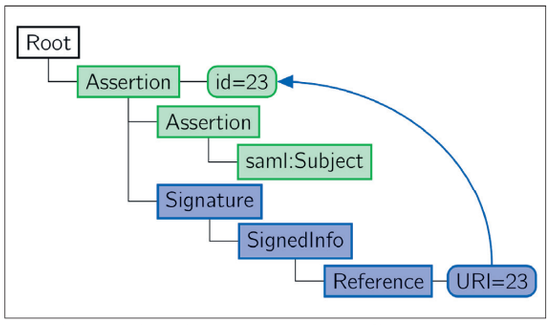
Diplomanden	Roland Bischofberger, Emanuel Duss
Examinator	Cyrill Brunschwiler
Experte	Thomas Risch, Swiss Reinsurance Company Ltd., Zürich, ZH
Themengebiet	Internet-Technologien und -Anwendungen

SAML2 Burp Plugin

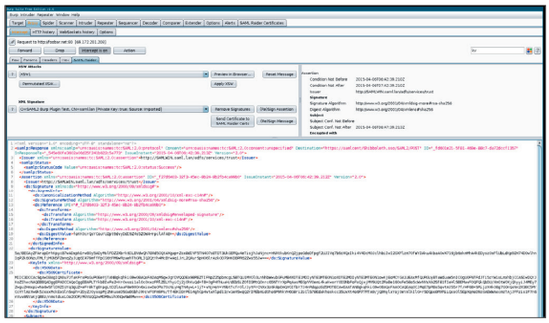
«SAML Raider»



Login mit SAML



Zu den Technologiestudien gehörten auch XML-Signaturen



SAML Raider Message Editor GUI

Ausgangslage: Security Assertion Markup Language (SAML) ist ein Standard für die verteilte Authentifizierung und geteilte Identitäten über mehrere Organisationen. Dieser Standard wurde in Produkten wie Shibboleth oder Microsoft ADFS implementiert. Diese Implementationen werden von Penetration-Testern auf ihre Sicherheit geprüft, was ein aufwendiger Prozess ist mit Dekodieren, Manipulieren, Signieren und wieder Zurückkodieren von SAML-Nachrichten, der ziemlich anfällig für Fehler ist. Der Tester darf keine Fehler machen, sonst funktioniert der Test nicht. Da eine SAML-Nachricht nur eine kurze Gültigkeitsdauer hat, müssen diese Schritte unter Zeitdruck durchgeführt werden, was ein korrektes, sorgfältiges Prüfen zusätzlich erschwert. Um die notwendigen Schritte zu automatisieren, soll ein Plugin für die Burp Suite geschrieben werden. Burp Suite ist eine von vielen Penetration-Testern genutzte Software ohne spezielle SAML-Funktionen, weshalb eine Erweiterung geschrieben werden soll. Um zu verstehen, wie der SAML-Standard funktioniert, sollen die Technologiegrundlagen zu SAML erarbeitet und dokumentiert werden. Dazu gehören ein Studium der Funktionsweise von SAML sowie eine Recherche über mögliche Angriffe.

Vorgehen/Technologien: Wir haben eine Projektplanung anhand des RUP-Projektmanagementmodells erstellt und uns Wissen zur Funktionsweise von SAML und möglichen Angriffen angeeignet. Nachdem die Anforderungen an das Plugin mit dem Projektpartner definiert waren, begann die Planung der Architektur, die auf das bekannte Model-View-Controller-Pattern setzt. Bei der Entwicklung entschieden wir uns für die Programmiersprache Java, die für die Benutzung des Plugins in Burp keine weitere Software benötigt. Um das Plugin auf korrekte Funktionsweise in einer realen Umgebung zu testen, wurde eine Testumgebung aufgesetzt.

Ergebnis: Anhand der Anforderungen entstand ein zweiteiliges Tool: Teil 1 dient der Verwaltung von Zertifikaten, Teil 2 der Manipulierung der SAML-Nachrichten. Von 20 funktionalen Anforderungen decken wir 14 ab. Alle mit der Priorität «sehr hoch» und die meisten der Priorität «hoch» sind erfüllt. Einige nicht hoch priorisierte Anforderungen wurden ebenfalls implementiert. Während der Entwicklung und der Zwischenpräsentation kamen weitere Anforderungen dazu, die wir ebenfalls implementierten. Die Implementation ist sehr nahe an der geplanten Architektur. Zusammenfassend wurden die grössten bzw. wichtigsten Teile des Plugins funktionstüchtig implementiert. Wir mussten nur kleine Abstriche bei den Funktionen machen. Ein Penetration-Tester kann unser Plugin bereits einsetzen und die wichtigsten Aufgaben durchführen. Das Plugin wird nach Abschluss der Arbeit von uns weiterentwickelt.