Abstract

Today, Single Sign-On (SSO) solutions for major enterprises as well as on the Internet (e.g. “Sign me in through Facebook/Google”) are flourishing. The large distribution of SSO is mainly driven by usability, cost savings, and performance. However, the security aspect is often overlooked. SSO systems provide a valuable single point of attack: If the SSO solution exhibits a flaw, all federated websites may be affected. Therefore, the security of SSO systems should be guaranteed under all common and even sophisticated attack scenarios.

This thesis analyzes the security of SSO by focusing on the Security Assertion Markup Language (SAML). The XML-based SAML standard is prevalently used in major enterprises and has been adopted by many high-profile services, such as Google Apps, Salesforce, and several e-Government systems. The thesis is divided into three main parts.

First, it analyzes common SSO threats and investigates two different functionalities of SAML-based Identity Provider (IdP): Issuing of SAML assertions, and security as a web application. By analyzing six different real-world IdPs, it shows that all are susceptible to at least one attack type. The IdPs are vulnerable either to a novel hijacking attack (called ACS Spoofing), or to specific attacks stealing HTTP session cookies. All attacks allow an attacker to impersonate the victim to thousands of websites accepting assertions from these IdPs.

Second, it discusses different channel bindings, which utilize the cryptographic capabilities of the Transport Layer Security (TLS) protocol as a holistic countermeasure. It presents the first practical implementation of the SAML Holder-of-Key SSO Profile in the popular SimpleSAMLphp framework. Furthermore, it proposes and implements a novel variant of this Profile, which binds authentication requests and assertions to TLS client certificates, and broadens this binding to session cookies. This combined countermeasure mitigates all attacks described in the first part.

Third, it presents several practical and highly critical attacks on SAML messages. An in-depth analysis of 14 major SAML frameworks reveals that eleven of them including Salesforce, Shibboleth, and IBM XS40, could be broken with different XML Signature Wrapping (XSW) attack techniques. These attacks circumvent the integrity protection of XML Signature and allow one to log in to any federated website of the SSO domain as an arbitrary user.

In summary, the work described in this thesis has influenced many SAML frameworks and systems, which were fixed to mitigate the found attacks. Furthermore, the proposed channel binding variant is generic and can be applied to other SSO protocols (e.g. OAuth or OpenID). This can be seen as one step towards a holistic solution to harden web authentication and SSO without changing existing infrastructure.