Abstract

The advent of message-level security raised with the upcoming popularity of multi-party application architectures, in which securing messages only during transport does not fulfill the demands. Security features are directly added to the exchanged messages so that they can be forwarded to further entities without losing their protection, even if an untrusted party is involved in between. This thesis analyzes message-level security in two widely-used application areas: web services and Single Sign-On (SSO). Through the described methodology, numerous security issues in various software libraries and websites were identified, reported and fixed.

The first part of the thesis analyzes the security of SOAP-based web services. This work found novel attack techniques with the focus on automatic detection and circumvention of existing countermeasures. With WS-Attacker, a software developed in this context, the first fully-automatic penetration test software for web service security is designed and implemented. Its application led to the discovery of numerous vulnerabilities in well-known web service frameworks, such as Apache CXF, and in the IBM DataPower Security Gateway. The issues were reported to the developers and the implementation flaws were fixed.

The second part of the thesis examines the security of SSO systems. Generic attack concepts applicable to arbitrary SSO protocols are developed and then applied to the protocols (1.) OpenID, (2.) OpenID Connect, and (3.) Security Assertion Markup Language (SAML). These attack concepts are based on a newly introduced SSO Attacker Paradigm which is founded by the question whether the Identity Provider (IdP) in an SSO protocol can always be viewed as a Trusted Third Party (TTP). The research results in this thesis show that in modern SSO systems, an attacker may integrate his malicious IdP and, thus, they reveal that the answer is no. The malicious IdP can then be used for the detection of security vulnerabilities and for their exploitation.

Based on the SSO Attacker Paradigm, the attack techniques are evaluated. Vulnerabilities are identified in different OpenID, OpenID Connect, and SAML implementations. The security of widespread systems, such as Software-as-a-Service Cloud Providers (SaaS-CPs), can be broken. We show how to successfully log in to foreign accounts, read out local files stored on the server, and to efficiently execute Denial-of-Service (DoS) as well as complex Server-Side Request Forgery (SSRF) attacks.

The work described in this thesis influenced the development of many web service frameworks and SSO systems. Within this context, attacks on the specification of OpenID Connect are shown that allow to break the main target of the protocol – the authentication of the End-User – regardless of the underlying implementation. A countermeasure has been proposed in collaboration with the official OAuth and OpenID Connect workgroups of the Internet Engineering Task Force (IETF). Due to the attacks, the specifications of OAuth and OpenID Connect are currently being updated and adjusted.