Cybersecurity – Identity Management
Prof. Dr. Anja Lehmann

Master Project | Winter Term 23/24

Security Analysis of Assertion Tokens in Single Sign-On Solutions

Description

Single Sign-On (SSO) is an increasingly popular authentication method that leverages a trusted Identity Provider (IdP) to allow users to conveniently authenticate to multiple service providers using a single set of credentials. A crucial aspect of most SSO protocols is the creation and handling of *assertion tokens*. These tokens assert the identity of a user and are created by the IdP after the user has authenticated to the IdP. The token is then transmitted to a Relying Party (RP). After validating the token, the RP may grant the user access to restricted resources based on the user's verified identity and possibly additional attributes.

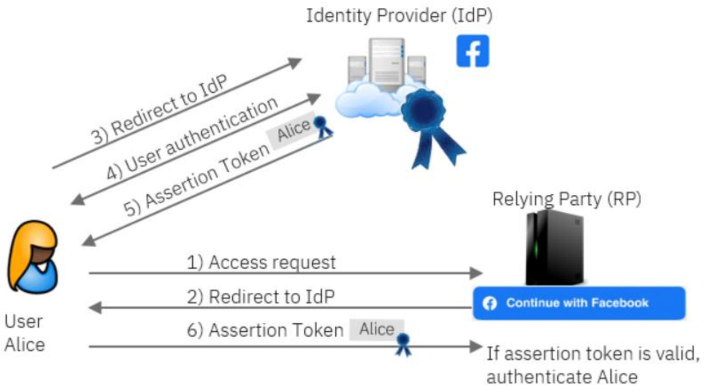

Figure 1: Schematic Overview of Authentication in an SSO protocol. The user Alice tries to login at the RP, and is then redirected to the IdP. After authenticating the user, the IdP creates an assertion token which is passed to the RP. The figure depicts the front-channel setting, where the token is sent via the user to the RP.

Current standards and guidelines define various approaches for the IdP to generate assertion tokens and transmit them to the RP. These tokens can be conveyed through either the front-channel (via the user) or the back-channel (between IdP and RP directly). They may be encrypted or unencrypted, and can take the form of bearer tokens (where possession of the token is sufficient for authentication) or holder-of-key tokens (where knowledge of a secret key is required for authentication). The chosen design options have implications for the security assurances provided.

The NIST Digital Identity Guidelines for Federation and Assertions [1] categorizes three federation assurance levels (FAL) with the following minimum requirements:

FAL1: Bearer assertion, signed by IdP.
FAL2: Bearer assertion, signed by IdP and encrypted to RP.
FAL3: Holder-of-key assertion, signed by IdP and encrypted to RP.

Interestingly, no formal security analysis of the concrete security guarantees provided by these levels has been conducted, and the latest OIDC standard [2] does not include explicit support for holder-of-key assertions which would be needed for the highest security level FAL3.

Goals

The objective of this master project is to conduct a formal security analysis of the different design choices for assertion tokens.

First, we need to establish a framework for SSO protocols that captures the different communication and cryptographic settings (front-channel vs back-channel, signed vs signed & encrypted, etc) and allows us to analyze existing protocols such as OpenID Connect. Subsequently, we will formally define the desired security guarantees for an assertion token, such as unforgeability and confidentiality, considering different corruption capabilities of the adversary. As the model and the possible security therein will most likely vary for each setting, we will also study the relations among them. Finally, we will analyze the security of the existing protocols in our model and prove their security from (hopefully) well-established assumptions. Ideally, we will be able to establish a clear correlation between the security levels defined by the NIST guidelines and concrete (game-based) security properties, thereby demonstrating the level of security attained by the proposed levels. Ultimately, the goal of the project is to produce a research paper suitable for publication at a cryptographic conference.

Requirements

We expect a solid understanding and interest in cryptography in general, and provable security in particular. You should have attended the “Introduction to Cryptography”, and the “Advanced Cryptography” courses (or similar) and passed with very good grades.

Contact

You’re welcome to visit us in building G-3 (first floor), or send us an email:
Dennis Dayanikli dennis.dayanikli@hpi.de
Anja Lehmann anja.lehmann@hpi.de

References

[1] NIST Special Publication 800-63C - Digital Identity Guidelines - Federation and Assertions https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63c.pdf

[2] OpenID Connect Core 1.0: https://openid.net/specs/openid-connect-core-1_0.html