Auditable Authorization

Abstract

Bearer tokens are vulnerable at rest and in transit when an attacker is able to intercept a token to illegally access private information. In order to mitigate some of the risk associated with bearer tokens, the Authorization Audit Trail (AAT) may be used instead of bearer tokens in the authorization process. AAT consists of cryptographically chained blocks of data bearing a chronological tamper-resistant records of all their possessors and the changes that have been made by them. A nested, chained MAC construction (e.g., HMAC) is used to ensure the authenticity and integrity of AAT. All sensitive information are encrypted to preserve confidentiality. The access control relies on a real-time auditability of AAT by the authorization server. The AAT concept is compatible with existing OAuth2 and UMA protocols.

Introduction

Bearer tokens are easy to use and easy to integrate with any client, server, and mobile device. Once they have been minted on the authorization server, they don't require additional processing on the client, and token validation on the resource server is trivial. While existing technology standards are acceptable for many use cases, they have been harder adopt in the healthcare industry and financial sector, where higher degree of authenticity and integrity of authorization process is required. An auditable authorization mechanism allows Identity and Access Management (IAM) systems to authorize resource access using AAT that can simultaneously ensure compliance with financial and legal regulations.

Concept

The auditable authorization concept is based on a verifiable tamper-resistant audit trail created by authenticated participants (authorization server, client, resource server) during the respective stages of the authorization process.

Conclusion

By utilizing simple cryptographic techniques, the AAT mechanism may be used instead of bearer tokens during the authorization process. This concept of auditable authorization mitigates the risk associated with bearer tokens to illegally access private information. In a broader scope of AAT, there is the possibility of using the recorded data for forensic analysis and verification of legal compliances.

Acknowledgment

Credits go to WG - User-Managed Access, Google Research Publications and Audit in OAuth 2.0