Project - Flexible, Risk Aware Authentication System

Introduction

Nowadays, many Service Providers (SP) rely on external identity Providers (IdPs) for authenticating end-users and providing selected identity attributes of them. The widespread use of IdPs has several advantages, being one of them a kind of backup system for end-users, when they forget their credentials in those SPs, or an extra factor of authentication (to increase robustness against impersonation attacks).

Also, they can implement multiple authentication factors, in a dynamic manner, in order to increase the robustness and security of the authentication process.

Identity Providers are called whenever an authentication is required, therefore, they can have better understanding of the user behavior across multiple applications. They constitute corner stones for a solution using user behaviour analysis coupled with Multi Factor Authentication.

Project Description

The work consists on developing an IdP supporting services with different criticalities, and applying multi-factor authentication methods, in a dynamic manner according to the service requirements and user perceived risk. It will also aim at addressing the issue of MFA fadigue, by tailoring the authentication process in order to keep the security level, while not burdening the user too much.

The IdP shall support the definition of services, consisting of web applications that use the IdP to authenticate their users. When defining a service, a set of policies based on aspects such as risk, session time, location, or any other constrain should be defined. This set of policies will influence how the IdP actually authenticates the user in each session..

As an example, critical applications may imply the need for additional validation by means of MFA or stricter behavior checks. The IdP may require higher number of authentications if the user risk score is high, or a password spray is active. It may relax the authentication requirements if the user or service risk score is low. The authentication methods used are also flexible and defined by the IdP according to the current perceived risk. Implicit methods, such as IP Address, User-Agent or Time of Day (to name a few), can be used in risk assessment.

A set of plausible authentication methods and policies and behaviors must be set by the students. Then, a clear risk based authentication process should be presented, by defining the different states and how observed actions can influence this process.

At least three services need to be integrated. They can reuse the same applicational code, but must exist as three different clients. They will have different policies and risk profiles, allowing the validation of the entire process.

These services will have some resources that are protected, thus bound to authentication and authorization. The access control approach should consider Roles in granting access to resources, with principles from both Bell–LaPadula and Biba. A simple message billboard mapped to a Role based structure may suite this purpose.

The communication between the services and the IdP shall be achieved by means of an adequate OAuth2 Flow. In line with the objective of this work, the IdP shall use the Refresh Tokens to finelly control the session duration.

Project development and delivery

This project is to be implemented by groups of 2 students. The project can be coded in any language but must use OAuth2.0.

Development should be done in a Github Classroom repository as provided by your professor.

An initial report, with no more than 10 pages, must be provided with the architecture, description of the services, general authentication and authorization flows, and general risk tracking model.

A final report, with no more than 30 pages, describing the system implemented. Such description must include the data structures stored, the structure of the messages exchanged and the message flows, the interfaces used and their parameters, some relevant implementation details (not complete copies of the code!), the MFA and risk tracking approach, and the results achieved.

The results should demonstrate the effectiveness of the system to correctly authenticate users under different risk situations.

The final report must state the percentage of effort devoted by each group member to the project.

Evaluation

This project will be evaluated as follows:

- IdP implementation with adequate user attributes: 20%
- 3 MFA methods: 10%
- A risk based approach with scalable authentication: 20%
- Support for OAuth2.0 between services and the IdP: 10%
- Integration of three distinct services: 10%
- Written final report 2, with complete explanations of the strategies followed and the results achieved: 20%
- Written initial report 1, with the architectural diagram and authentication flows defined 10%
- Bonus: 10% if an MFA method relies on a Hardware Secure Module

References

- https://oauth.net/2/
- https://oauth.net/code/python/

2024

PREVIOUS

Lab - 1 - Linux files' access control

Last updated on 11 Mar 2022