Cybersecurity MSc: Identification, Authentication and Authorization 2021-22

Project (2nd part): Authentication of players' with CMD (Chave Móvel Digital)

May 18, 2022 Due date: Jun 23, 2022

Changelog

- v1.1 - Changed the delivery date.
- v1.0 - Initial version.

1 Introduction

Nowadays, many Service Providers can benefit from existing Identity Providers (IdPs) to get attributes of their client users. In this project, we will use the Portuguese IdP Chave Móvel Digital (CMD) to identify players within the Reputation Manager (RM). The CMD IdP should be accessed either using OAuth2.0 (without OpenID Connect) or SAML (Security Assertion Markup Language).

Foreign students can also activate their CMD, so they can implement and test this project just by themselves as well.

2 Homework

The work consists on adapting the RM to use CMD as an external IdP. The adaptation should provide the following features:

- Creation of a personal reputation profile. Obviously, each person should have a single profile, and therefore the external IdP (CMD) must be used to query for attributes such that each person could not have more than one instance (e.g. an email address cannot be used). Also, colliding attributes should not be used alone.

  Upon the creation of personal profile, you should create an alternative set of access credentials, formed by a username + password. The username acts as a long-term pseudonym.
- Authenticate in the RM using the external IdP. Complementary, you should also allow players to authenticate in the RM with their username + password credentials.
- Change the profile password upon a CMD-based authentication.

Since a single person cannot have multiple identities when these are provided by CMD (you can have multiple identifiers and attributes, but they are normally constant for what they stand for), you could not test your system just by yourself. Therefore, keep whatever system you developed for authenticating players for the 1st part, and just allow people to create pseudonyms and authenticate with CMD for the second part.

For security reasons, the RM should not keep any personal attributes in cleartext. One-way transformations of the set of attributes provided by the IdP should be kept instead. Do not forget to implement transformations capable to stand against off-line exhaustive (or dictionary-based) search attacks.

2.1 Access to the external IdP

The CMD IdP can be accessed using OAuth2.0 (without OpenID Connect) or SAML. Any of these standards can be used.

SAML Service Providers, which are IdP clients, must be identified by a certified asymmetric key pair. This key pair and the certificate of its public key is the same for all students, and is available in Elearning.

If using OAuth2.0, the CMD IdP uses the implicit flow. In this flow, you do not have to have a (public) redirection endpoint for the OAuth2.0 client. The redirection endpoint can be any endpoint accessible from the player's User Agent.

In the integration with CMD you should follow the public manual and code, available at `https://github.com/amagovpt/doc-AUTENTICACAO`. Please do not interact with the project contributors without first discussing your problems/suggestions/etc. with the teachers. You are going to use the pre-production settings. You do not have to register to use the CMD services; we already did that for all students, as a whole.

3 Project development and delivery

This project is to be implemented by groups of 2 students and as a complement of the previous one (1st part). The project can be coded in any language but must use the CMD IdP.

Send your code to the course teachers through Elearning (a submission link will be provided). Include a 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!) and the results achieved.

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

As an add-on (not to be evaluated!), please provide a feedback note about the materials provided through `git-hub` to CMD developers; these will be included in an anonymized feedback report.

4 Evaluation

This 2nd part of the project will be evaluated as follows:

- CMD setup and use: 55%;
- CMD-based management of profiles: 25%;
- Written report, with complete explanations of the strategies followed and the results achieved: 20%