Authentication systems in IT solutions based on web architectures

Luca Di Bello
luca.dibello@student.supsi.ch
Computer Science, SUPSI, Lugano, Switzerland

Abstract

The web over the years has spread to all areas of our lives, from the most basic to the most complex thus being more and more connected to the Internet. This led to the necessity of having a secure and reliable authentication system to protect users and the system itself. In this article will be presented the most common authentication techniques used in web applications and the advantages and disadvantages of each one, followed by real-world study cases. The main goal is to present the most common authentication systems and their respective characteristics, so that the reader can have a better understanding of the subject and be able to choose the best authentication system for their project.

json web tokens; oauth2; saml

1 Introduction

Authentication systems are one of the most important parts of a web application. This system is responsible for identifying the user and granting access to the system. This process comprises a series of steps that are performed in order to verify the identity of the user. It is usually divided into two phases: the first phase is the authentication itself, and the second phase is the client authorization.

Authentication Authentication is the process of verifying the identity of a user. It is the first step of the authorization process, which is the process of verifying that the user has the rights to perform the action they are trying to perform. The authentication process is performed by a system or service, which in the case of web applications is the web server.

A user can authenticate on a web server by entering a username and password, which is the most common method, but there are other methods that will be presented later in this article. The web server receives the username and password and then verifies them, and if they are correct, the user is authenticated and the server returns an authentication token to the client. The authentication process is usually performed by the user, but in some cases, the system can perform the authentication process automatically, for example, when the user is already logged in.

Authorization Authorization is the process of verifying that the user has the rights to perform the action they are trying to perform. The authorization process is performed by a system or service, which in the case of web applications is the web server. The web server receives an authenticated session signature and verifies if the user has the rights to perform the action they are trying to perform. Usually, if the user is authorized to perform a certain action, the server returns the operation result to the client, and in the other hand, if the user is not authorized, the server returns an error to the client and the operation is not performed.

2 Authentication system types

Authentication systems can be categorized into two main groups: session-based and token-based.

Session-based authentication Session-based authentication is a method of stateful-authentication[1] that uses a session identifier to identify the user. The session identifier is a unique token, stored by the server, to ensure that a specific user has been authenticated and authorized to perform certain actions. It is stored in the server's memory

[1]Stateful Authentication is a way to verify users by having the server or backend store much of the session information, such as user properties.**website:1**

Token-based authentication

3 Study cases

3.1 PostFinance - Mobile ID

3.2 Cembra Money Bank - mTAN

3.3 PostFinance - Photo-TAN

Supplementary Files (optional)

Any supplementary/additional files that should link to the main publication must be listed, with a corresponding number, title and option description. Ideally the supplementary files are also cited in the main text. Note: supplementary files will not be typeset so they must be provided in their final form. They will be assigned a DOI and linked to from the publication.