Web Authorization Protocols

4

Demetrios Georgios Syropoulos-Harissis
Greek Molecular Computing Group, Greece

Apostolos Syropoulos
https://orcid.org/0000-0002-9625-1482
Greek Molecular Computing Group, Greece

BACKGROUND

Web applications were designed so to be a simple and friendly way for humans to interact with a machine. Initially, they were custom made and could solve a few problems. However, as the technology evolved, it was possible to create Web applications that could solve an even bigger range of problems. Nowadays, Web applications can virtually do almost anything. Apps are stand-alone applications that implement the full functionality of a Web page/application (Ater, 2017). These apps are typically installed on a mobile device (e.g., a smartphone or a tablet). There are simple but useful applications (e.g., apps that provide information about the weather) and more complicated ones (e.g., the Facebook and the LinkedIn apps). Most of these apps have something in common: They require some sort of account creation in order to personalize the data that they will offer to the user. Of course, this is a major development for apps. In the past, one could select a city and see the weather forecast in detail. One question that comes into our mind is: Why has the weather forecast has been so personalized and why Facebook needs to know my location at any given moment?

Most people are very sensitive about their personal data. Not all people consider the same kind of data, personal. Nevertheless, there are data that are definitely personal. For example, one's location or personal messages are definitely personal data. Apps require some of these personal data in order to provide a fully personalized experience. But this is something that makes people very suspicious. There are two problems here:

i. How is this information going to be used?
ii. How can be sure this information will not end up in wrong hands?

Fortunately or unfortunately, in the end, most users give access to their personal data. People do that because they trust their information to apps and whoever is behind them (e.g., a company, a developer, etc.). Typically, people who have "adopted" *stereotypes* (Neil Macrae, Stangor, & Hewstone, 1996), assume that developers have taken every precaution so that an app uses the data in a safe and sound way. Naturally, this is not always the case… Although the data management problem has been relatively easily solved in the past, still there are other more complicated problems that have come up after it. With so many personalized apps, anyone has typically an account for each app that she is using. If someone wants to use n apps, then that person needs n different accounts! [This is a major problem that was examined quite early, for example see (Adams & Sasse, 1999).] Having many accounts implies the use of many *authentication* systems. An authentication system makes sure that when a user attempts to login to a system or an app, she will be granted access only when she enters a valid user name and the

DOI: 10.4018/978-1-7998-3479-3.ch035

corresponding (secret) password. After user authentication, a system proceeds with *user authorization*, which is a process that verifies that the right person has access to the right data. A simple example for the discrimination of authentication and authorization is the following. Consider a student who enters the library. She shows her membership card to the security officer and enters. This procedure can be thought of as an authentication process. Next, the student is searching for a book. She finds the book and takes it to the reading room that is guarded by someone. Our student is asked for her membership card, but her *credentials* are not adequate as the reading room is for teachers only. The second check can be thought of as an authorization procedure. So the problem with many accounts and different authorization systems for a single app is solved with the *authorization protocols*. These protocols give us the ability to use one, two, or more accounts to connect to any number of applications in a secure and safe way. In this article we give an overview of authorization protocols and safe data transfer between apps.

INTRODUCTION

When we hear the term "protocol" what comes first in mind is a number of rules someone has to follow in a certain occasion. These rules have been given by someone who created this protocol and it is considered that these rules, if followed, are the best way to deal with this occasion. For example, think of banquet protocol and how one has to arrive at such an event, how she is supposed to dine, etc. An authorization protocol is definitely a protocol but differs slightly with what we described so far. In particular, a protocol is supposed to be unchanged and strict. However, the authorization protocols are being upgraded every time some security error occurs. We have introduced two new very important terms now: *upgrade* and *security*. The first term, upgrade, shows the flexibility of these protocols and it is being implemented

Figure 1. Authentication process. PR is a reliapble partner and OP is an OpenID provider