Contribution ID: **135** Type: **Sectional reports**

Passwordless Authentication Using Magic Link Technology

Friday, 9 July 2021 11:30 (15 minutes)

Nowadays, the problem of identification and authentication on the Internet is more urgent than ever. There are several reasons for this: on the one hand, there are many Internet services that keep records of users and differentiate their access rights to certain resources; on the other hand, cybercriminals' attacks on web services have become much more frequent lately. At the same time, in many cases, the weak point of systems exposed to attacks is precisely the authentication system.
Many different authentication methods have been developed and are in use today. For their classification, the factor on which their principle of operation is based is mainly used - the knowledge factor, the ownership factor, or the inherence factor.
Authentication methods based on the knowledge factor (e.g. password protection) are the most common and are applied almost everywhere. Their advantages are ease and low cost of implementation. On the other hand, such systems are often vulnerable to various kinds of attacks. It is estimated that up to 80% of successful hacker attacks (including attacks on the largest services with millions of users) succeeded precisely because of the weakness of the password protection system.
In this paper,passwordless authentication methods are considered. Systems based on such methods have a number of advantages –ease of use, protection against many common types of attacks, and the lack of need to create a large number of passwords. Passwordless authentication technologies are increasingly widespread, and are already in use by a number of large companies –Google, Medium, etc.
In particular, the magic link technology is considered. Using it, the end user does not need to use a password to register or log in to the system –just to enter an email address and follow the link sent by the authentication system. The link is unique, and authorization with its help is possible only for a specific user and only for a limited time. This approach not only greatly simplifies the process of registering new users and relieves them of the need to remember passwords, but also provides reliable protection against a number of attacks related to password theft or brute-force attacks.
An authentication system has been implemented using Keycloak. Keycloak is an open-source software product that implements single sign-on technology, in which a user can switch from one system to another connected to the first one without re-authentication.
Thus, this paper presents a solution to the problem of passwordless authentication, which can be applied in a number of online services and systems. In the future, it is possible to further improve the system, in particular, using adaptive authentication, which allows switching between different authentication mechanisms depending on certain factors.

Summary

Primary author: MATIUSHIN, Iurii (Saint Petersburg State University)

Co-author: KORKHOV, Vladimir (St. Petersburg State University)

Presenter: MATIUSHIN, Iurii (Saint Petersburg State University)

Session Classification: Data Management, Organization and Access

Track Classification: 6. Data Management, Organisation and Access