Contribution ID: **74** Type: **Oral Presentation**

Importance of User Deprovisioning from Services

Tuesday, March 15, 2016 2:40 PM (20 minutes)

Every service uses an authorization process to determine the access rights of individuals. Lots of services do authorization decisions only during the authentication process and by that the information about access rights is valid for the whole session. The other common approach is to run authorization process for each request from the user.

Both of the described approaches are commonly used and they are sufficient for most services. However there are services which enable users to work with persistent resources. An example of such services are cloud infrastructures which enable users to start virtual machines or use data storages for storing large amounts of data. Apart from the normal authorization done whilst user is interacting with the service, there is a need to know that the user is still authorized to use the resources, even though the user is not interacting with the service. Such knowledge enables services to free the persistent resources which were occupied by the user who is no longer authorized.

Deprovisioning is the process which enables service to know about users who are no longer authorized. It is the opposite of the well-known provisioning process, which is used in cases where the services need to know the users in advance of their first usage of the service.

In this paper we will describe the importance of deprovisioning process on real use-cases and services. Moreover we will focus on possible options to implement deprovisioning in existing infrastructures. That requires a well-defined user life-cycle process in the identity management system or a proper connection to the primary sources of user identities, in order to detect if the user is no longer authorized to use the service.

Last but not least, we will describe similarities between standard deprovisioning process and suspension of the users on the services due to security incidents. Based on those similarities, we will demonstrate on a real system how to utilize the deprovisioning process to automate mitigation of security incidents.

Primary authors: PROCHAZKA, Michal (Masaryk University); LICEHAMMER, Slavek (Masaryk University)

Co-author: Dr MATYSKA, Ludek (CESNET)

Presenter: LICEHAMMER, Slavek (Masaryk University)

Session Classification: Networking, Security, Infrastructure & Operations I

Track Classification: Networking, Security, Infrastructure & Operations