Contribution ID: **24** Type: **Poster Presentation**

Design and Implementation of Unified Authentication Management System of IHEP

High energy physics network computing environment has the characteristics of complex and heterogeneous, and the projects researched by high energy physics are mostly carried out in the way of international cooperation. These factors increase the complexity of the management infrastructure and application services system. Therefore, reasonable and efficient management of resources, taking into account the scientific application service flexibility requirements, has become the core issue of protecting information and resources. The traditional application and service authentication method is to save the user information in each application system and establishes an independent authentication mechanisms with independent authentication in their respective identity authentication modules. This traditional method of identity authentication makes the user's security identity fragmentation when using the application. These fragmented identity fragments consist of one to one customer service relationship in all the authentication modules, which implies a huge security risk. From the perspective of the user, each access to a system to verify the login once when the user needs frequent access to different systems, which will lead to the user needs to remember a large number of account information, while causing unnecessary time consumption.

The Institute of high energy physics, has all kinds of information system and service resources, such as personnel information management system, data sharing service, performance management system, conference system, and each user has an account in these systems. The traditional management mode is configured different permissions for each account on each system. It is easy to be wrong because the system is too much, for example users are assigned permissions without modifying high timely which eventually lead to the information divulgence and the system safety risk increasing. At the same time each user needs to remember their own user name and password on each system that is not only more troublesome but also easy to appear lost password.

It then proposes the unified authentication solution under the IHEP network environment. This solution uses LDAP directory services for storing user information, builds a unified authentication mechanism by using OAuth2.0 protocol. This approach eventually combines a variety of applications and enables the secure access to these applications.

Primary authors: Mr QI, Fazhi (Institute of High Energy Physics,CAS); Ms WANG, Li (Institute of High Energy Physics, CAS, China); Mr XU, Zhen (Institute of High Energy Physics, CAS, China)

Presenter: Ms WANG, Li (Institute of High Energy Physics, CAS, China)

Track Classification: Networking, Security, Infrastructure & Operations