50th IAA SYMPOSIUM ON SAFETY, QUALITY AND KNOWLEDGE MANAGEMENT IN SPACE ACTIVITIES (D5)
Cyber-security threats to space missions and countermeasures to address them (4)

Author: Dr. Nadine Perera
DLR (German Aerospace Center), Germany, nadine.perera@dlr.de

PERFORMING IDENTITY AND ACCESS MANAGEMENT WITH GART (GSOC ACCESS REQUEST TOOL)

Abstract

Performing Identity and Access Management (IAM) for space mission ground systems is essential to ensure operational security. Establishing an IAM Tool (IAMT) in addition to a manual process is a powerful countermeasure to address cyber-security threats. Informing the mission managers at a glance which users currently have access to mission (IT) resources improves transparency and diminishes the risk for identity theft. For instance, transparency leads to a more prompt and strict deletion of users, who no longer need access to resources, thereby eliminating their login data as an attack surface. Access Management is demanded by information security regulations, e.g., ISO-27001. Space operations companies need to show compliance with regulations, which require controls to enforce the need-to-know-principle. At the same time, organizations want to help users to gain quick and secure access to the (IT) resources they need. The observation of the defined process can be established much more efficiently by a tool than via a manual and error-prone organizational process. This paper describes the approach taken at GSOC to enforce the access management process for all ground systems by implementing an IAMT. A role-based workflow, governing (IT) resources, provides accountability and traceability in addition to transparency. The first implementation covers the physical door entry system and the OpenLDAP systems. Other directory services may be added in a modular fashion, e.g., DLR's Active Directory. Identity Management introduces transparency across a user's different access data, such as login names and passwords, in different directories within the organization. The more directories and heterogeneous types of resources exist in an organization, the more important it is to provide an overview of a user's accounts, passwords, and responsibilities, such as changing the password at regular intervals and choosing safe passwords according to different rule sets. Challenges for the approach were the multi-mission character of GSOC, since several missions share personnel and resources, and the integration of several directory services into one system, among them two separate OpenLDAP trees with overlapping user entries, and a physically separated database with door access information. Thanks to the established IAMT, access changes are recorded and traceable, both during the review process and afterwards. A future step is to use the IAMT to detect unauthorized changes in directories by regularly polling and comparing the data over time. The IAMT will generate a warning if changes are found without a corresponding approved request, for better control and monitoring of privileged users.