68th International Astronautical Congress (IAC), Adelaide, Australia, 25-29 September 2017.

IAC-17-F1.2.3

Identity and Access Management with GART (GSOC Access Request Tool)

Nadine Perera[a]

[a] *Quality, Configuration and Security Management, German Aerospace Center (DLR), Münchner Straße 20, 82234 Wessling-Oberpfaffenhofen, Germany,* Nadine.Perera@dlr.de

Abstract

Performing Identity and Access Management for space mission ground systems is essential to ensure operational security. Doing so using appropriate tool support via workflow-based granting and revoking of access privileges is a powerful countermeasure to address cyber-security threats. 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. This paper describes the approach taken at GSOC to enforce the access management process for all ground systems by designing and implementing an Identity and Access Management tool called GART, and discusses the challenges posed by an operational environment in a restrictive security setting.

Keywords: identity management, access management, information security, process, workflow

Acronyms/Abbreviations

AD	Microsoft Active Directory
CTA	Controlling & Acquisition
ECSS	European Cooperation for Space Standardization
GSOC	German Space Operations Center
IAM	Identity and Access Management
IAMT	IAM Tool
ISMS	Information Security Management System
LDAP	Lightweight Directory Access Protocol
LDIF	LDAP Data Interchange Format
PM	Project Manager

1. Introduction

Identity and access management (IAM) is, in computer security, the security and business discipline that "enables the right individuals to access the right resources at the right times and for the right reasons" [2]. It addresses the need to ensure appropriate access to resources across increasingly heterogeneous technology environments and to meet increasingly rigorous compliance requirements. Performing IAM for space mission ground systems is essential to ensure operational security. Establishing an IAM Tool (IAMT) in addition to a manual process for granting and revoking rights is therefore the very first countermeasure to address cyber-security threats. If mission managers can see at a glance which users currently have access to mission (IT) resources, transparency is improved and the risk for identity theft is diminished. 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. It also leads to a more selective granting of access privileges, avoiding dangerous misconfigurations in the first place. Access Management is demanded by information security regulations, e.g., ISO27001 [1]. 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 called GART, the GSOC Access Request Tool. 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 system(s). 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.

2. Material and methods

The main component of the IAMT is a workflow engine to grant and revoke access privileges. In Section 2.1., the underlying data model is explained with its entities, such as users, projects, roles and system resources. The user roles are detailed in Section 2.2. Section 2.3 entails the detailed use cases in which the

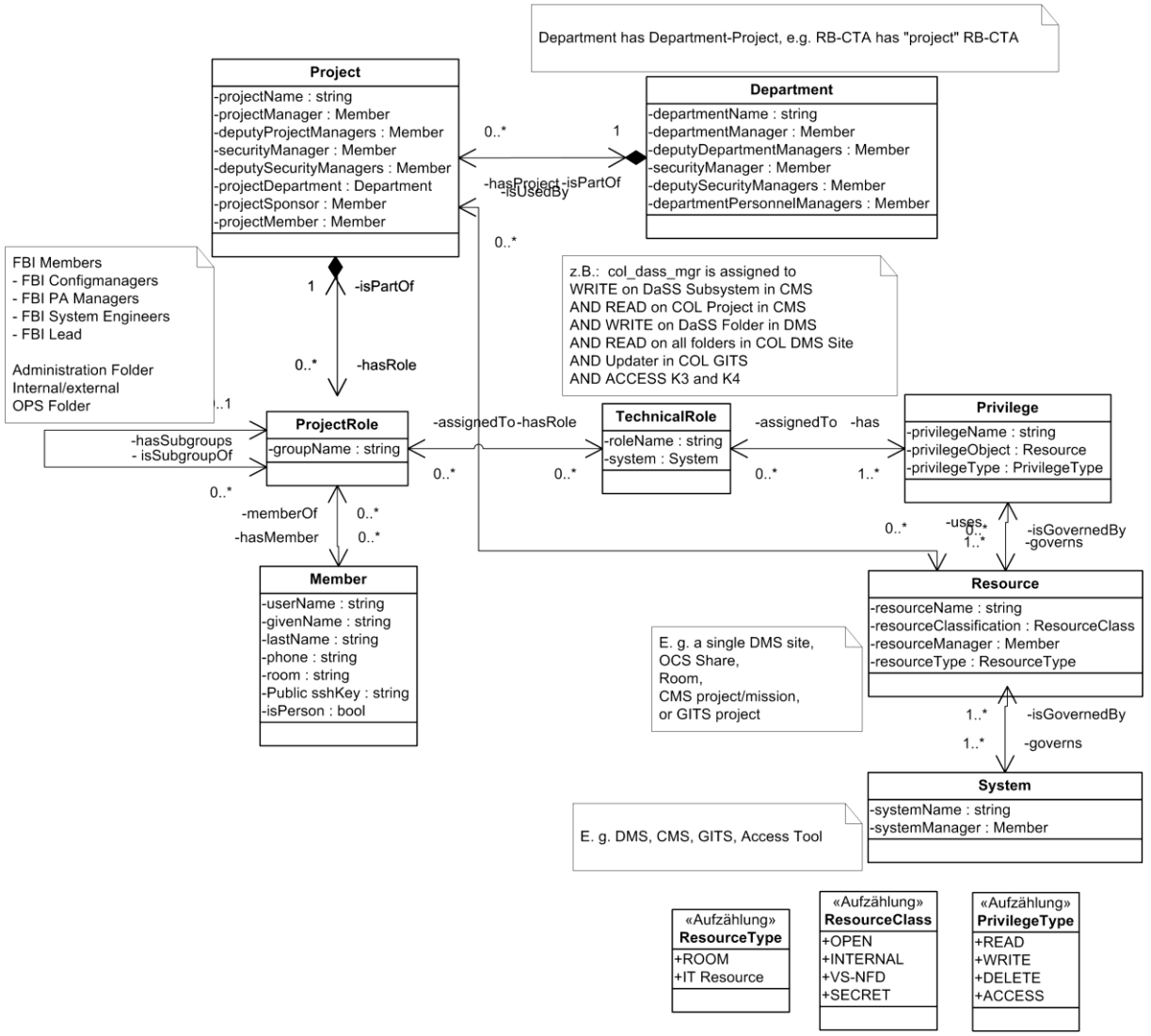

Figure 1: The Data Model (Entity Relationship UML Diagram)

entities interact, while Section 2.4 describes technical details. Specific configuration observations are described in Section 2.5, while Section 2.6 contains our approach to identity management including the unification of directory systems.

2.1 Concept and Data Model

The data model (see Fig. 1) shows an organization of access privileges consisting of a set of users, a set of system resources, a set of projects and a set of access privileges which a user has for projects and their system resources. In order to reflect our matrix structure, departments have matching department projects where general resources that belong to the department, and not to a satellite mission project, are governed. The bulk of the LDAP resources, however, are satellite mission specific or part of the Columbus project, i.e., belong to our only manned mission on the International Space Station. A project has a number of project roles that group one or more technical LDAP roles together. This project role is then assigned to users or project members, which results in the addition of these users to all the connected technical LDAP roles. The technical LDAP role is the one that has access privileges on resources assigned, the functional project role only relates to access privileges via the technical LDAP role(s). Resources are grouped into systems, i.e., the Documentation Management System (DMS) is a system in which all the projects have a project site, i.e., a project resource. The resource has a classification that can lead to additional steps in the approval process. The privileges that a technical role has on IT resources can be classified into READ, WRITE, DELETE, and ACCESS, if the resource is a room. It is important to

note that the LDAP system has no way of knowing where its groups are used. Anyone can poll the LDAP in the correct network and make use of the configured groups. The resources and systems within our data model are therefore documentation only; there is no means to get the information automatically.

2.2 User Characteristics

The IAMT shall be used by all staff members of DLR-RB (including contractor personnel). GSOC-external users (project partners external to DLR, other DLR institutes) can be administered in GART (via ID and email address), but can only login if they are on site and have an LDAP system login. Users will have a number of project roles, each combining membership in several LDAP groups. Some special GART roles are needed for the workflow administration etc. In general, more than one person shall be assigned to each role to provide suitable substitutes. The roles for GART are as follows:

2.2.1 GART User

A person with access to the central LDAP system, who needs an additional privilege or wants to revoke a privilege. The GART User can be any user with LDAP login, especially those not covered by any other role. Users who are persons have an isPerson flag set to true to discriminate users who are persons from functional users, since functional users shall not be able to log into GART, nor do they have telephone numbers etc. However, functional users shall also be governed with GART.

External User: a person who has no RB-LDAP account and therefore no access to GART, but who can be granted access to system resources via GART by a GART User.

2.2.2 Project Manager

A person in charge of a project, usually a satellite mission, who decides upon project privileges for her project members. The Project Manager is responsible for managing a project's day-to-day business and often also the room responsible for the room access request tool, since the rooms are assigned to projects.

2.2.3 Security Manager

A person in charge of a classified system resource, who decides upon privileges for persons according to their security classifications. The Security Manager reviews access requests with respect to information security aspects, and keeps a list of authorized personnel for classified resources (e.g., national and international security clearance levels).

2.2.4 LDAP Manager

The LDAP Manager is able to import LDIFs into the LDAP system (and to configure the LDAP system manually). He is in charge of the implementation of granted requests, as GART cannot write into the LDAP system directly due to security restrictions.

2.2.5 Door Access Manager

A person who can implement door access changes in the door access tool, typically security personnel at the GSOC main entrance.

2.2.6 Business Unit Manager

A person in charge of an organizational group, company or department, who decides upon group privileges for business unit members. A typical business unit is an RB department, e.g., RB-CTA, or a subcontracted company.

2.2.7 Personnel Manager

A person who informs upon leaving users, updates and reviews personnel system resources, e.g., a staff list website.

2.2.8 GART Administrator

A person with GART administrator privileges, i.e., to set up and configure projects.

2.2.9 System Resource Manager

A person responsible for a tool or system resource, such as the DMS/CMS/GITS/OCS, i.e., who needs to write emails to a system's users.

2.3 Process and Use Cases

A number of use cases for the IAMT have been defined. The central use cases, i.e., to grant or revoke access privileges, have been grouped into a workflow with four steps, cf. Figure 2. The following sections detail the use cases including the process steps for the revocation and granting of access privileges. Users are notified about an action resulting from a step or informed about decisions via email.

2.3.1 Use Case 1: Create User

An LDAP account can be requested for a new user by his/her Business Unit Manager or the Business Unit's Personnel Manager.

2.3.2 Use Case 2: Create Project Structure

Managing the project structure includes setting up and maintaining the project system resource structure; this includes naming the Project Manager. This is done by the GART Administrator on request. Information about the project's LDAP system Distinguished Names (DNs) shall be given.

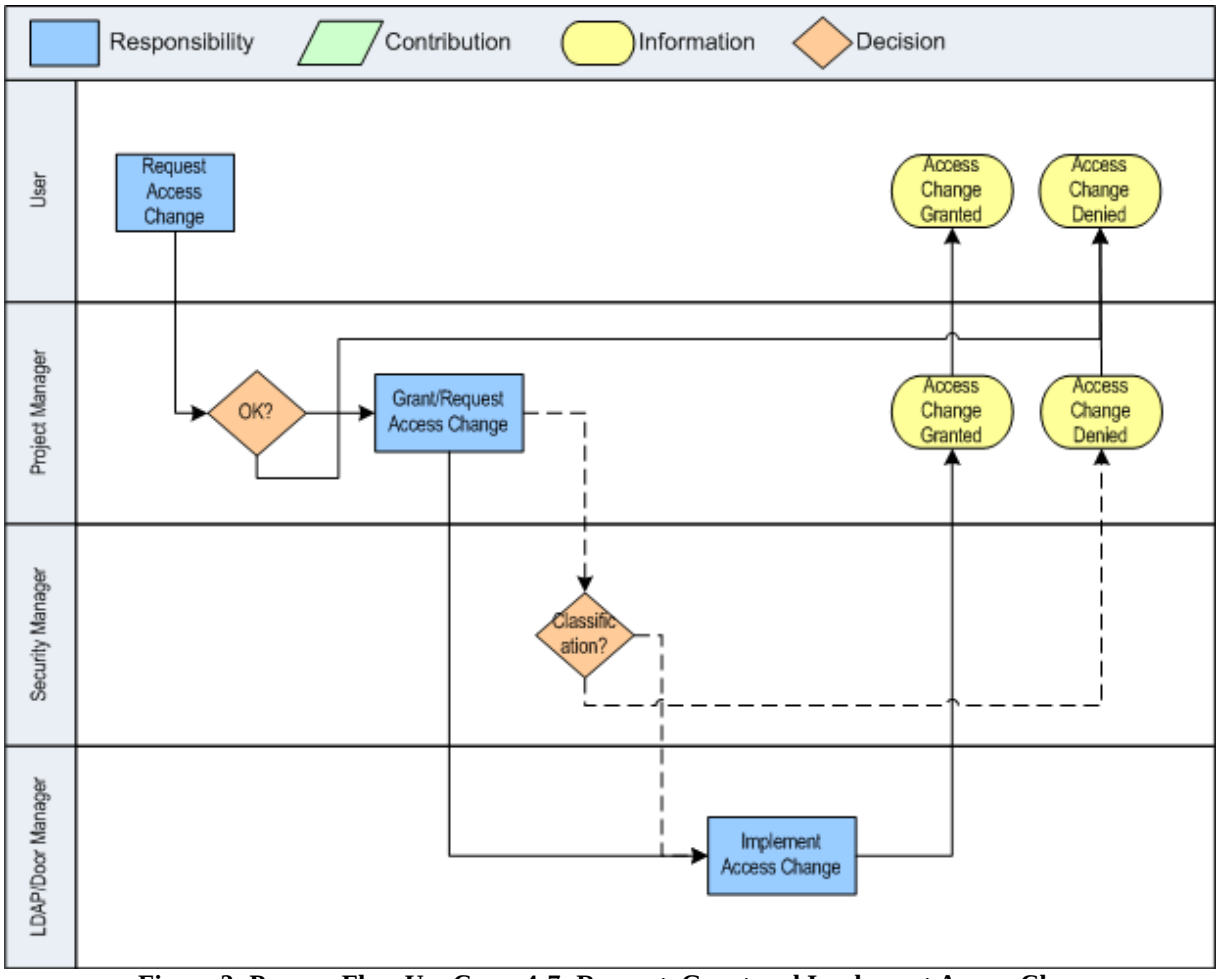

Figure 2: Process Flow Use Cases 4-7: Request, Grant and Implement Access Changes

2.3.3 *Use Case 3: Manage Project Roles and Technical Roles*

The bulk of the work in creating the project structure has to be done by the Project Manager, who must set up his or her functional project roles. This requires quite a bit of effort and thought.

Project roles are used to apply a combination of technical access privileges, typically on LDAP groups, to users in a project. Managing project roles consists of configuring and saving a combination of access privileges. Project roles can be defined without dedicated users. Project roles can be applied negatively and additively. Project roles are used to:

- Ensure high level of uniformity in access privilege combinations across users with the same tasks, e.g., configuration managers, project members, project system engineers.
- Ensure possibility to define project roles at the start of the project (according to Project Management Plan).
- Ensure ease of use for Project Manager

2.3.4 Use Cases 4-7: Request User Access Change

Requesting an access change means that a user with an LDAP account requests to receive additional access privileges, or wants to revoke his current access privileges to a system resource managed by GART. The revocation of access privileges takes place when a user leaves a project or a department. Access changes can be requested by the user (only for roles of projects to which he already has access) or his Project Manager for all access privileges of the project, or the Personnel Manager (mainly for new users and retiring users). Steps for Revoking Access Privileges are:

- Personnel Manager flags retiring user or Project Manager knows user is leaving project
- Project Manager is informed that user is leaving and requests to revoke project access for user.
- Emergency Access Revocation: All privileges are revoked, no granting of access removal by Project Manager required. Possibly, user is disabled in the LDAP system.

Steps for Requesting Access Privileges are:

- Determine project roles and system resources to which the user needs access to for a given project
- Give reason for access request

2.3.5 *Use Case 4: Request User Access Change*

The GART User can request access changes for herself, or the Project Manager can request access changes for members of her project.

2.3.6 Use Case 5: Grant or Request User Access Change

If an access change is requested by the user instead of the Project Manager himself, the Project Manager has to grant the access change, otherwise, the requested change is granted implicitly.

If the system resource to which access is requested is classified, the Security Manager also has to grant the access change.

2.3.7 Use Case 6: Implement Access Change (by LDAP Manager or Door Tool Manager)

If an access change is requested and granted, the LDAP Manager/Door Access Manager has to manually implement the technical access change, e.g., by downloading and entering an LDIF (LDAP Data Interchange Format) file produced by GART to the Management LAN LDAP system or by manually configuring the Door Access Tool. Upon implementation, the LDAP Manager can update GART such that the LDAP system is polled and the request can be marked as implemented, of the desired change is detected. Otherwise, the request will be marked as implemented automatically with the next LDAP sync. For the Door Access Tool, it is not possible to poll the information in the Door Access database, in this case, the implementation sets of an email that the request was implemented, but no automatic check can be performed.

2.3.8 Use Case 7: Receive Access Change Notifications

At regular intervals, the IAMT reminds the Project Manager to review the access privileges for all the system resources associated with his project, i.e., which users can access which resources of his project. This reminder consists of an email notification, optionally with an attached report of users and project resources.

Upon implementation of access changes on project resources, GART will send an email notification to the Project Manager, the System Resource Manager and to the user involved in the change.

The first implementation of GART has polled the LDAP regularly, but did not retain a copy of the data, such as which users are members of which groups. In order to note unauthorized changes, it was requested that GART keep track of the status of users in groups and notify the project manager or responsible of the LDAP group where a member appears or disappears without a corresponding GART request, in addition to verifying the implementation of a GART request as it is already implemented. This serves to notify resource responsibles about unauthorized or erroneous LDAP system changes. Only the membership of users in groups is monitored and email notified, i.e., there are no email notifications sent if a new LDAP system groups is created or deleted. In the case where a new LDAP group is created, GART has no way of knowing who the associated project manager is, in the case where an entire group that is already assigned to a project is deleted in the LDAP system, e.g., by accident, this would lead to several users being deleted from the group as well, which should again trigger email notifications. We have introduced a new table in the database to keep track of all users in every LDAP group associated with a project. This table can now be updated with every LDAP-sync, and if a change is detected where no request is present in GART, the Project Managers of the affected functional project roles as well as the affected user are notified by email. This table does not contain any historic data but is purely used to detect changes between each LDAP-sync, such that the notification email is only record of the incident in the case that the change gets reverted.

The user is also informed by GART when he has to renew his access privileges, e.g., to change his password, to which system resources, via email notification. This contributes to the identity management part of GART.

Functional users, i.e., system accounts used be more than one person or in inter-machine operations only, play a special role here. Once the password of such a functional user becomes invalid, all sorts of problems can arise in operations. It is therefore crucial that a Project Manager can access the user data of such functional accounts, to check and be informed upon password expiration dates. This special feature was built into GART. In summary, users receive access change notifications to:

- Ensure that the Project Manager reviews access privileges regularly
- Ensure that only the authorized users have access to project resources, and that even temporary changes without a GART request are recorded.
- Ensure that all the authorized users have access to project resources, and that even temporary changes without a GART request are recorded.
- Ensure that the Project Manager is informed on LDAP or Door Access Tool changes upon access privileges on his project resources.

2.3.9 Use Case 8: Review Access Privileges

The Project Manager can review the access privileges for all the system resources associated with

his project, i.e., which users can access which parts of his project.

The user can review the access privileges for all the system resources for which she has access, i.e., project resources she can access.

The System Resource Manager (e.g., the DMS Manager) can review the access privileges for his resources, e.g. to manage tool email distribution lists. Reviewing access privileges is done to

- Ensure that only the authorized users have access to project resources
- Enable Project Managers to request/revoke access to project resources for users
- Enable users to verify their access privileges
- Enable users to request/revoke access to project resources
- Enable Project Managers and users to view when a specific access privilege to a given project resource was requested, when it was granted, by whom it was requested and by whom or by which system it was granted, e.g. to answer the question: "Who had access to project resource between date1 and date2?" or "Which project resources had a given user access to between date1 and date2?"

2.3.10 Use Case 9: Review Personal Data

The user and the Personnel Manager can browse and edit a page containing the user's name, given name, email address, telephone number, office number, badge-number, personnel number, optional photo, company, public sshKey (used for Git).

One section of the page lists system resources with the user's login name for the system resource and a link to the site where the password can be changed, if possible also the date when the password has to be changed next. For functional users, i.e., users with isPerson flag set to false, the corresponding Project Manager can access the personal data page of the functional user.

2.3.11 Use Case 10: Mark Leaving User

The Business Unit Manager/Personnel Manager can mark a retiring or leaving user in GART to trigger a review/revocation of his access privileges at a certain date. This is strategically important to

- Ensure process for removing users from GART and for revoking access
- Emergency Process

Description/steps:

- Find user in GART
- Set user to retiring (with date)
- Triggers Use Case 4: Revocation of all access privileges, must be granted by Project Manager
- In the Emergency Process (when the revocation date is set to today), access revocation needs not be granted by the Project Managers, they shall however receive the information that all access has been revoked for a user.

2.3.12 Use Case 11: Delete Project

If a project is over and its resources are no longer needed, the project can be deleted in GART by revoking all access privileges for all users and all project resources.

2.4 Technical Details

GART consists of a database system, using the Yii PHP framework (http://www.yiiframework.com/). This framework was chosen to create a Look & Feel similar to GITS, the GSOC Issue Tracking System, that our designated users are all familiar with and that is also based on the Yii framework. Since the LDAP system is located in a secure network area, there is no direct connection between GART and the LDAP system. Changes are implemented by way of LDIF (LDAP Data Interchange Format) files, of the type “LDIF Change”, more specifically, as opposed to “LDIF Content”, such that only the relevant changes are imported by a human user, who can also read the file, as it only contains the part that shall be changed in the system. The Door Access System is located in another different network area and shall remain there for security objectives, no automatic interface will be permitted. This makes it hard to keep GART’s information up to date, since the real configuration of the system and what our IAMT thinks it should be will definitely differ over time. Unfortunately, there is no alternative solution at the moment than to perform regular audits at the time being.

2.5 GART Configuration and Practical Issues

The combination of technical LDAP groups to functional project roles is done in such a way that the users remaining in the functional role are the ones who are in all the technical LDAP groups, i.e., the *intersecting set* of all the LDAP groups. It has to be the intersecting set, since the planned use is for the project manager to add a new user to a project role, which leads to the user being added to all the underlying LDAP groups. Users who are only in one or some of the underlying LDAP rules obviously cannot fulfil the project role, as they are lacking access privileges. This intersecting set approach lead to slight confusion in cases where there was no means to configure a functional role, e.g., TSX FOM (TerraSAR-X Flight Operation Managers), without GART showing other users in the FOM project role, who are not actually FOMs in the project, but had the same access privileges. This is often due to the fact that many users have a

number of privileges and no one remembers why or when they were granted. One reason is that it was easier to copy combinations of privileges across persons, while the combination of privileges User A had was not exactly right for User B, and it was impossible to notice because the summary of the combination of access privileges was unreadable to the Project Managers.

A sensible structure of project roles can therefore prevent and excess of granted privileges and ensure that every user only has the privileges that she needs to fulfil her project role, thereby limiting the attack surface for possible misconduct, should the login data become compromised.

Due to the fact that users are added or removed from grouped intersecting sets, the programming and behaviour of the system had to be changed. For instance, if the project roles are laid out in such a way that one functional project role P1 combines several technical LDAP groups L1…n, but there is another project role P2 that has LDAP group L1 associated. If a user shall be removed from P1, he must be removed from all the LDAP groups L1…n, except for L1, since he still is a member of P2 which has L1 associated. This behaviour corresponds to the intuitive understanding of the users.

2.6 System integration for Identity Management

For historic reasons, we had two OpenLDAP systems at GSOC, in addition to the Active Directory system that DLR uses for all DLR employees, and where our email addresses are hosted. The two LDAP systems had two user branches, one for Columbus and one for the Satellite Missions. This lead to a rather confusing situation where many users had credentials for in both people-branches with an identical login name, but typically different passwords, such that it was very difficult for the users to remember which login/password combination to use for which IT system. Further, there were and are IT systems that are not connected to the central LDAP system, but have their own user management. Some of these systems, e.g., Jira, Git (BitBucket) have been reconfigured in order to connect to the now central LDAP system, such that the user access privileges can be governed by GART automatically, for other systems, this has proven too much effort for the time being. The problem with the two LDAP branches was solved by merging the branches. The operation was time consuming and a lot of effort went into it, but reduces the risk for further malfunctions and misconfigurations greatly.

3. Results and Discussion

We have successfully designed, developed and implemented an IAMT called GART. This tool enables and reminds Project Managers to review the users who can access their project resources. It also leads to a more selective granting of access privileges, avoiding dangerous misconfigurations in the first place. It increases transparency, accountability, and improves the maintenance of the directory system. The initial configuration event alone has lead to a massive cleansing of old accounts and restructuring of LDAP system groups, such that the system has become more manageable and better documented. The configuration of the Door Access could not be accomplished due to a proprietary and physically separated database system without automatic interfaces.

Thanks to the established IAMT, access changes are recorded and traceable, both during the review process and afterwards. The IAMT was further improved to detect and record unauthorized changes in the LDAP system by regularly polling and comparing the data over time. The IAMT will now generate a warning if changes are found without a corresponding approved request, for better control and monitoring also of privileged users.

4. Conclusions

As with all preventive measures, it is difficult to estimate the benefits of the IAMT compared to the security risks posed by not implementing it – how many sets of login data would have been disabled how much later, and whether and when any of them would have been used as an attack surface. However, one can say that transparency, accountability and maintainability have greatly increased and that users and administrators alike are less worried about discrepancies between the access database and the perceived actual access that users have to system resources. Especially the notification emails about unwanted or even malevolent changes directly to the LDAP system increase trust in the systems and in the IT landscape. The fulfilment of ISO27001 recommendations [1] puts us in a better position regarding audits. The observation of the defined process can be established much more efficiently by a tool than via a manual and error-prone organizational process.

Acknowledgements

We would like to thank Thomas Geppert for the very competent and efficient tool implementation, Dr. Thomas Bassler for conceptual advice, and Dr. Edith Maurer for frequent testing of the system and helpful comments.

References

[1] Gartner IT Glossary, Identity and Access Management (IAM). Gartner. Retrieved 2016-09-02.
[2] ISO/IEC 27002 - Information technology – Security techniques – Code of practice for information security management, 2013.