Smart-M3 Security Model

Kirill Yudenok
Saint-Petersburg Electrotechnical University
Saint-Petersburg, Russia
kirill.yudenok@gmail.com

Abstract

The main goal of the project is to develop a security model for smart spaces, design access and control algorithms and test the components on the Smart-M3 platform.

The current task is the creation of a discretionary (matrix) security model within the smart space Smart-M3 platform. This model is simple to implement and allows to achieve full access control over the space, by maintaining the access control list (access matrix), but also has disadvantages, such as:

- the administration security procedure is complicated, which can lead to errors.
- low-level (too much of details) model and because of this the complexity of full implementation of the model;

The main element of this model is the access matrix. In terms of the matrix model, the state of protection system is described by a triple (S, O, M), where M [S, O] defines the access rights of the subject (client, S) to the object (space, O). The access rights regulate the management methods of the subject to different types of access objects, such as read (R), write (W) and delete (D).

The basis implementation of the access control is the analysis of the access matrix rows, when subject referring to the object. It checks the matrix row, which corresponds to an object and analyzes whether it allowed access rights to the subject or not. Based on this, the decision to grant an access.

The primary proposed solution based on the principles of discretionary model. Namely, the implementation of access matrix as a component of the platform, which will store the access right to the space and verification and access control algorithms (mechanisms) to the smart space in accordance with the matrix.

The proposed scenario of the security model is:

1. Access matrix configuration, the administrator sets access rights for all prospective clients of the smart space (SIB).
2. Knowledge Processor (KP) sends a connection request to the SIB.
3. The request is sent to a special service (ACS), a server-side component, responsible for granting of access rights for KP.
4. ACS analyzes the access matrix rows and returns a triplet, containing information with KP access rights to the SIB, if there are none, the connection request is rejected.
5. KP is connected to the SIB with issued rights.

Follows that the space control security is fall on the access matrix administrator and occurs on the SIB side. The model implementation wouldn't conflict with the basic principles of smart spaces, but rather will improve its safety.

It is also well applicable access control model based on roles, where each space user is assigned the role, which defines its capabilities in the system. Creation of this model will allow more easier and flexible configure the access to the space. As a basis has been chosen discretionary model and its implementation can be easily extended to the role model in the future.

For a complete understanding a model simulation process try to reveal the main points of the functioning of the model.

Suppose that the "SIB-DB" is a file system (directory tree) that has certain access rights "R, W, X". R - read a triple, extract its components (S, P, O). W - write (insert) relation in

the triple. X - get a list of relationship objects in RDF. The matrix identifies only those operations that are allowed to perform a subject for an objects.

At the time of connection the subject to the space will be determined all valid operations for this subject. The admissibility of any operation is checked when it is committed.

Assume the following list of control options rights:

1. Get a list of rights on the connection. In certain operations, it is checked in the list of his rights, if it is enabled, the operation is confirmed, if not, rejected.
2. Entity subscribes to its operations on the connection. Once the subject begins to perform the operation, the operation is checked in its subscription, if the operation is absence, it is rejected.

In terms of checking access to the SIB, the access operation may occur locally, unnecessarily no matter where subjects located, they are connect to the SIB, which is posted on the particular machine of the network, where checking and issuance rights to a specific subject.

SIBs can also be distributed in the network, but presented as a single entity for all subjects and access during the passage of local operation on the SIB side. If SIBs distributed, there should be a single "access service" through which all subjects receive the rights to the space.

Access matrix (AMX) should be store near the data on the same device, where the processing procedure takes place, in the metadata form, which will be taken decisions to access control. To search for each SIB, it must be assigned a unique identifier. The identifier assignment issue is still open. Options for storing the access matrix in the SIB and a separate service are eliminated, because there is a bottleneck in the system, namely, in the event of unavailability the safety control process becomes impossible. Access is assigned to a particular user (the administrator). Appointed special user, which monitors the matrix. A copy of the AMX is stored on each subject client.

Based on the principles of the storing and working with objects in smart spaces is assumed that the image of the object (general representation of the object in a few spaces) can be stored in multiple SIB-DB simultaneously. In this case, introduced the appropriate relations, defines their identity in a different SIBs. The identity attitude determines whether of one concept is identical to another. For this case creates a "dictionary" of common concepts.

The solutions and proposals are supposed and require further investigation. In the process, it was also decided to use the ”internal mechanism" of access control and refuse to create an access control ontology, because in intensive access to the ontology will be greatly reduced access time to the system objects. Although the use of ontology is possible, but in this case is not the best solution.

The next step is the development of a smart space access control mechanisms and algorithms based on the Smart-M3 platform for a decision to limit client access to information of the smart space.

Index Terms: Smart-M3, Smart Space, security model, access control.