Smart-M3 security project status description

Main security mechanism for smart space Smart-M3 platform

1. Smart space (SS) users access control mechanism, identification and authentication mechanism of the SS users. Mechanism to provide and control access to the SS for all of its users.
2. Access control mechanism to SS information, authorization mechanism. Distribution and control user access to the information of the SS.

Implementation details of the security mechanisms

For adding the security mechanisms to the SS Smart-M3 platform will be redesigned piglet module, which is responsible for working with the SS database and all of its operations.

Identification and authentication mechanisms will be implemented with the HIP (Host Identify Protocol). After his investigation was suggested a solution of HIP-agent, which identifies and authenticates the subjects of the space.

Authorization mechanism planned to implement by mapping SS RDF-graph to the virtual file system (VFS), SS triples converted to a pre-defined directory structure. After implementation of the VSF to the platform and replace all of its operations, will be given a standard access control mechanism for information based on the access attributes of VFS. Also, this mechanism can be implemented on the basis of named graphs, which also provide the necessary mechanisms by extending RDF-graph.

To simplify the configuration of access rights of a new model necessary to develop the interface (tool) for editing SS permissions, which will set up access rights for all SS users.

The scenario of the security system in the Smart-M3 platform

1. Restricting access to the SS.
   Access to the SS have only those users, who have been proof of identity. For this procedure monitors the administrator of the SS.
2. Access control to information of SS.
   For each SS user defined access rights (while reading and writing). Based on this rights will be taken decision on access to the SS information and all its users. Access rights restrict the range of the user in a SS.

What was done

In the course of the project was implemented:

1. the mechanism of authorization and SS subjects access control by mapping RDF-graph to the virtual file system is developed; mechanism tested in a Smart-M3 platform;
2. analyzed and designed the HIP protocol-based mechanism of identification and authentication;
3. the process of implementation mapping mechanism to the Smart-M3 platform is started;
   3.1. piglet proxy creation for new extensions - done;
   3.2. replacement of all SS database operations to mapping VFS operations - in progress;
   3.3. determine and verify client access permissions - in progress;
   3.4. testing operations on the client side - in progress.

What is planned for FRUCT 12

1. A prototype of the identification and authentication mechanism based on HIP protocol;
2. A prototype of the authorization and access control mechanism for the SS.

Future research and development

The next step in developing a security model for SS is:

- HIP-agent development;
- implementation of mapping model to Smart-M3 platform;
- set permissions tool development for mapping FS;

Also planned for the future:

- named graph authorization system development;
- adding developed mechanisms to new version of Smart-M3 platform (Redland);