Cryptographic RBAC Compiler

Sixth Sprint

7/01/19 - 20/01/19

FONDAZIONE BRUNO KESSLER

Layout of the slides by Coman Catalin Andrei

Agenda

- Recap
- Sprint Backlog
- User Stories
- Design
- Implementation
- Testing
- Nex Sprint

- Refactoring of
  - Cache (from HashSet to HashMap)
  - Log system
  - Not null parameters checks server-side
  - Tuples signing and verifying process (to adapt for function **`addP`**$_u$)
- Implemented
  - **`AssignPermissionToRole`**
  - Protocol for query admin's public key and symmetric key encrypted by admin
  - Delete functions in server DAOLocal, both entities and tuples
- Communication schemes for client-server-cloud
- Modified UML diagrams for CryptoACTable (the one describing the binding between the sequence of operations in Adam's paper and in mine implementation). Still missing **`revokeUser`**, **`revokePermission`**, **`Read`**, **`Write`**

Sprint Backlog

- Add other low-level functionalities
  - **`revokeUserFromRole`**
  - **`deleteUser`**
  - **`deleteFile`**
  - **`revokePermissionFromRole`**

- Finish to modify UML diagrams according to CryptoAC Table

11. As the **Administrator**, I want to delete a user from the system so that he cannot access files anymore TO IMPLEMENT EVERYTHING

12. As the **Administrator**, I want to delete a file from the system to remove all the tuples related to it THERE'S UML BUT IS TO IMPLEMENT

13. As the **Administrator**, I want to delete a role from the system to remove all the tuples related to it THERE'S UML BUT IS TO IMPLEMENT

TODO

- TODO

Next Sprint Backlog

- Add other low-level functionalities
  - **`revokeUserFromRole`**
  - **`deleteUser`**
  - **`revokePermissionFromRole`**
  - **`readFile`**
  - **`writeFile`**
- Development of other scenarios
  - User read file
  - User write file

Questions

- How does the Admin handle tuples with invalid signature?
- Do we encrypt socket communication?
- Do we encrypt PKI keys files with a Master Key?

Thanks

Layout of the slides by Coman Catalin Andrei