Cryptographic RBAC Compiler

Fifth Sprint

11/12/18 - 23/12/18

FONDAZIONE BRUNO KESSLER

Layout of the slides by Coman Catalin Andrei

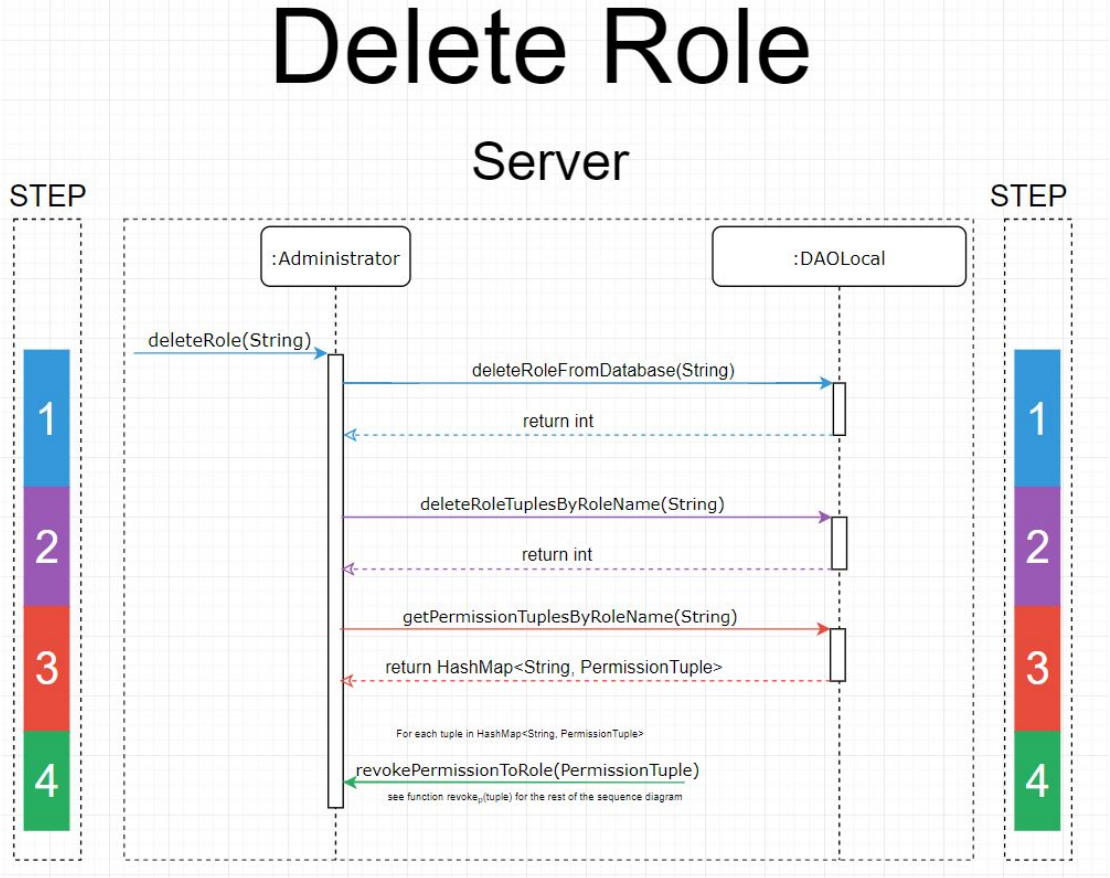
Agenda

- Recap
- Sprint Backlog
- UMLs modification
- Next Sprint
- Questions

- Creation of the **Gitlab project** (Code, graphs, documentation, ...) to be shared it with Adam
- Creation of a simple **storage solution** for managing keys
- Definition and implementation of **scenario** as sequence of operations (AddUser, AddRole, AssignUserToRole, AddFileFromUser, ...)
- Refactoring, test implementation and “TODO” resolution

Sprint Backlog

- 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`**


Delete Role
Server
STEP
STEP
:Administrator
:DAOLocal
deleteRole(String)
deleteRoleFromDatabase(String)
return int
deleteRoleTuplesByRoleName(String)
return int
getPermissionTuplesByRoleName(String)
return HashMap<String, PermissionTuple>
For each tuple in HashMap<String, PermissionTuple>
revokePermissionToRole(PermissionTuple)
see function revoke$_p$(tuple) for the rest of the sequence diagram
1
2
3
4
1
2
3
4

Next Sprint Backlog

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

- Finish to modify UML diagrams according to CryptoAC Table

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