RBAC(Role Based Access Control) 솔루션

RBAC(Role Based Access Control) Solution

역할기반 접근제어(RBAC: Role Based Access Control)

역할기반 접근제어 정책은 정보에 대한 사용자의 권한 부여 여부를 각 사용자의 식별자나 이미 정의된 규칙에 의해 판단하지 않고, 사용자가 소속된 조직내에서의 역할에 의해 결정하는 특징을 가지고 있습니다. 즉, 역할기반 접근제어 시스템에서는 정보에 대한 접근 권한이 사용자에게 직접 부여되지 않고, 조직에서 규정된 역할들에게 배정됩니다.

역할 기반 접근 제어의 구성요소

역할 (Role)

주어진 환경에서 정의된 업무의 기능으로서, 각 역할이 수행 가능한 권한들로 구성됩니다.

역할 계층(Role hierarchy)

역할에 배정된 권한들 사이에 포함관계가 있는 역하들 간의 부분 순서 관계입니다.

사용자 (User)

컴퓨터 시스템을 통하여 시스템내의 정보를 사용하는 객체로서 한 사용자는 한 명의 사람에 대응됩니다.

권한 (Permission)

정보 객체에 대해 실행 가능한 연산의 집합으로 구성됩니다.

세션 (Session)

한 사용자와 여러 개의 역할로 구성된 집합으로 구성되며 사용자는 세션을 통하여 자신에 배정된 역할들 중 일부 또는 전체를 수행할 수 있습니다.

제약조건 (constraint)

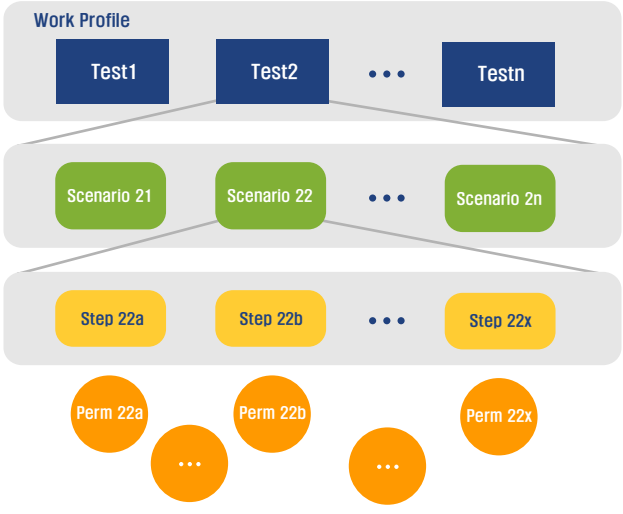
각 구성요소가 가지는 특성을 제한사항이나 조건으로 기술합니다. 최소, 최대 사용자 수(Cardinality), 임무 분리(Separation of duty), 선수역할(Prerequisite roles), 시간제약(temporal constraint)등이 있습니다.

Role Engineering

Role Engineering은 Role Based Access Control(RBAC)를 위한 Roler과 Permission, Constraints, Role-hierarches들을 정의하는 프로세스입니다. Role은 Functional Role과 Organization Role로 구분됩니다.

Scenario Driven Role Engineering

Composition of Work Profile



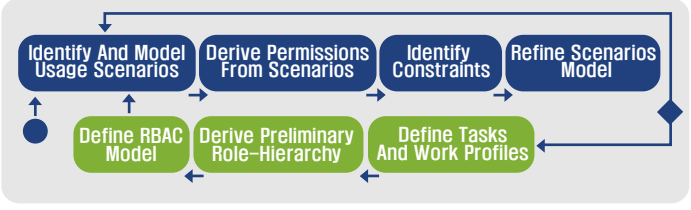
Derive preliminary role hierarchy

Work profiles 과 permission catalog을 이용하여 반자동으로 초기버젼의 Role hierarchy를 정의 합니다. 명시적으로 상 하위 Role이 정의되고 계층구조가 정립됩니다. 중복 가능 성이 있는 Role들은 재검토 되도록 합니다.

Derive permissions from scenarios

각usage 시나리오 Step을 수행하기 위하여 필요로 되는 Permission을 도출합니다.

Role Engineering Process



Identify and model usage scenario

UML Usecase 뷰에 해당하는 모델링 단계로 먼저 기능적인 Usage시나리오를 찾아내어(Identify) 간단한 문장으로 기술합니다.

Identification of permission constraints

Constrains를 도출한다. 먼저 어떤 유형의 Constraints 가 모델링 되어야 하는지를 정의합니다. 가장일반 적인 두가지 Constraints는 "separation of duties"와 "cardinalities"가 있습니다.

Refine scenario model

현재 모델링 된 시나리오를 재검토 하여 상세하게 모델링합니다. 서브 프로세스는 기본적으로 두개의 Activity(Concretion, Generalization)로 구성됩니다.

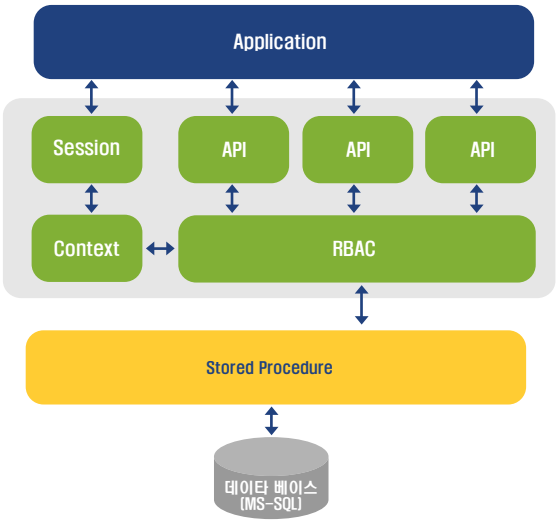
Define tasks and work profiles

논리적으로 연결되어 수행되는 시나리오를 Task(직무)로 통합하고, 정의된 Task를 사용하여 Work Profile 을 정의합니다.

Engine API의 RBAC 적용

응용 프로그램 또는 웹 응용프로그램에서 데이터베이스의 정보를 질의하는 시스템입니다.관리자를 포함하여 모든 사용자에게는 수행할 작업에 대한 역할을 부여받게 되며, 수행가능한 작업의 분류에 따라 역할이 정의됩니다. 각 역할는 최소단위의 작업의 집합으로 이루어 집니다.

구성도



모듈 설명

Application

Library모듈을 이용하는 응용 프로그램입니다. 응용프로그램에서는 Login과정에서 사용자의 Session이 생성됩니다. 하나의 Session은 사용자 정보(사용자 기본 정보, 소속, Role, Permission 등)를 담고있는 Context정보를 생성합니다.

API

Application에서 호출하는 Library의 API들을 의미합니다.

RBAC

API호출되어 저장 프로시를 수행하기 전에, RBAC는 현재 사용자가 호출된 API를 수행할 권한이 있는가를 검사합니다. RBAC는 현재 Session의 사용자 Context에 호출된 API에 대한 실행 permission을 담고있는가를 조사함으로서 수행 권한 여부를 판단합니다.

Role, Permission관리

Permission의 유추는 최소 단위의 step이 Library에서 하나의 API에 해당함으로 API와 1:1대응 관계를 갖도록 하였습니다. Permission의 집합에 대한 Role은 관리자에 의해 구성됩니다. 관리자는 사용자의 역할에 따라 부여된 Role을 정의하고, Role에 사용자의 역할에 필요한 최소단위의 작업 즉, Permission을 적용합니다.

RBAC의 유용성

역할 기반 접근 제어 정책은 정보 시스템에 의해 관리되는 정보의 단순한 보호기능 뿐만 아니라, 기업환경의 관리 체계를 자연스럽게 모델링하는 장점과 함께 다수의 사용자와 정보객체들로 구성된 환경에서 효과적인 권한관리 기능을 제공하는 특징을 가지고 있습니다.

시스템 요구사항

- 운영체제 : Windows 2000이상
- 프레임워크 : .Net Framework
- 데이터베이스 : MS-SQL Server 2000
- 웹 서버 : IIS 5.0이상
- 웹 브라우저 : IE5.5이상

연락처

Nehom

회 사 명 : 내홈닷컴
전화번호 : 1566-6346
FAX 번호 : 02) 6008-3876
홈페이지 : http://www.nehom.com
주 소 : 443-400 경기도 수원시 영통구 망포동 558번지 LG 탑프라자 5층
연 구 소 : 305-350 대전시 유성구 가정도 34번지 #105