Building End-to-End Multi-Client Service Oriented Applications

Module 07

Services & Engines – Part 2

Securing & Unit Testing the Service Layer

pluralsight
hardcore developer training

Highlights

- Standard WCF-based security
- User-data Authorization
- Unit Testing

Security

- **Special windows group (role) for the admin functions**
  - Users of desktop app will be members
- **Special windows user for non-admin functions (still secure)**
  - Site will run under this user
- **Admin functions will NOT be accessible to web users**
  - Rent car to customer
  - Accept car return
- **Non-admin functions will NOT be open to outside world**
- **Simple to assign using PrincipalPermission attribute**

User-Data Authorization

- **Principal permission is NOT enough**
- **All web site users will have access to all non-admin operations**
- **One user should NOT be able to see data from another**
  - In many cases, a WCF service's reach is extended with Web API
- **Problem**
  - Windows authentication passes caller identity to service
  - Caller identity is IIS user
  - Need actual user (person logged into site) without coupling to web
- **Solution**
  - Receive a user login name in every operation
  - Use SOAP header to avoid adding to operation contracts
  - **IAccountOwnedEntity** will finally be made clear !

Summary

- **Used both standard principal/identity security and custom solution for user-data-authorization**
  - User name of application user sent through SOAP header
  - **IAccountOwnedEntity** interface finally used
  - Unit test needed to fake credentials in order to execute

End of module