Software Application Role Management
Through a unified cached “RoleSpace”

Version 1.0 final, 1/17/2005

Authors

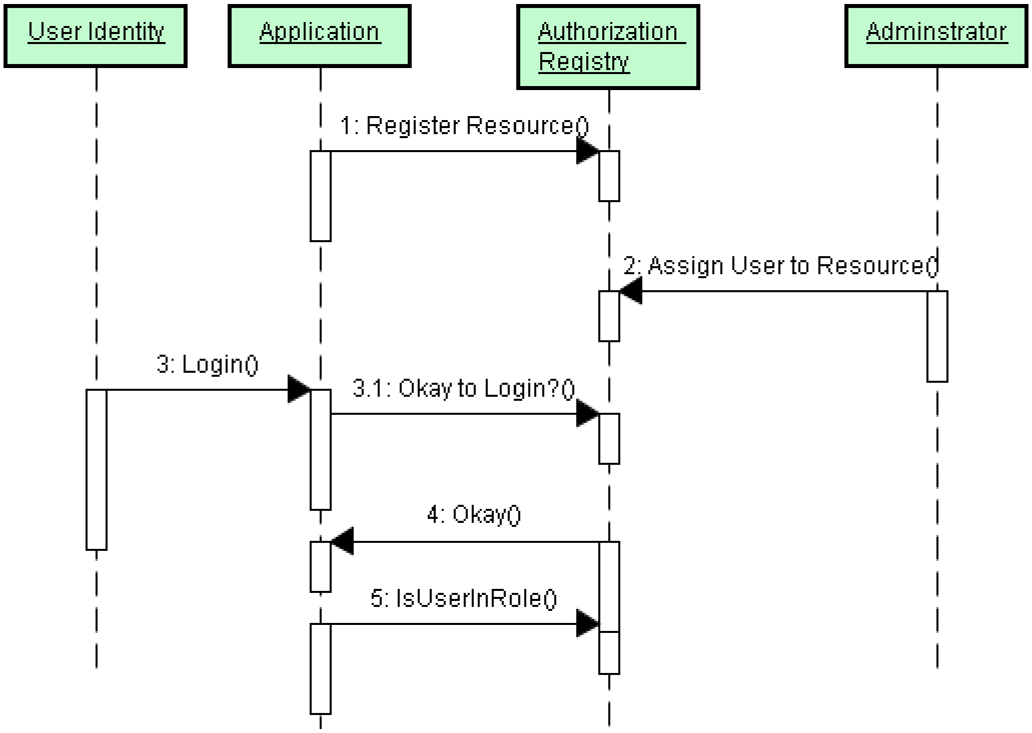
Michael Behrens, R2AD, LLC

Abstract

Assignment of features or resources to users is one of the functions that is currently provided by permission systems such as the APM software segment.[1]
This document proposes concepts for centralized administration of access rights and outlines the goals and requirements for a distributed authorization system that unifies the desktop client identity with the web based identity.

User Administration

Administrators desire a single mechanism to create and manage users. When a user comes to the system with an identity certificate and a request to establish an account, the administrator is notified and has the responsibility to verify the users role and purpose. Upon account creation, the administrator assigned roles to the account. The roles need to come from the variety of applications to which the user is accessing. These roles can also act as resources that can be allocated to users by the administrator.



[1] Account and Profile Manager (APM) provides centralized account and profile management across a collection of Solaris and Windows hosts called an APM administrative domain (AAD).

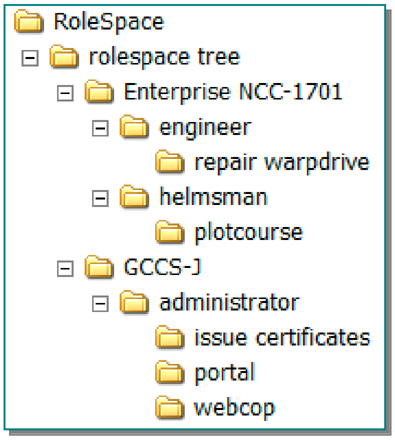
Roles & RoleSpace

> *Roles job-oriented titles for the overall job someone has or performs. Features are usually and represent actions that the computer operators do in a more specific sense, like the ability to delete a widget. A **Unified-RoleSpace** is defined such that a user can login and be authenticated and authorized via the same managed authority regardless of whether connecting from a thin (web) or thick (heavy) client.*

Segments (applications) need to specify roles that their application requires and role usage (semantics) should be uniformly interpreted (delete, create, etc). Some roles might be in common with the entire system and have a global scope. These are defined by the system and are prefixed with "system", i.e.: "System.Administrator". Case is ignored.

Applications would need to advertise (register at install time) their roles (or features) so that the administrators can assign capabilities to users. Deployment tools such as **J2EEDT** currently parses web.xml files and obtains the roles dynamically. A similar mechanism is also required for thick client applications. SAFE must be capable of knowing (by listening) when a feature is disabled (when the originating segment is de-installed) and re-enabled (when the segment is re-installed). This will help administrators maintain user access rights.

RoleSpace is a way to access a unique role within an enterprise. They basically is a period separate string such as "oracle.administrator" or "GCCS-J:portal.administrator". The words further to the right are more generic and should form a natural hierarchy in reverse order. This allows for quick manipulation on all "*.administrators" for example.



- RoleSpace
  - rolespace tree
    - Enterprise NCC-1701
      - engineer
        - repair warpdrive
      - helmsman
        - plotcourse
    - GCCS-J
      - administrator
        - issue certificates
        - portal
        - webcop

Developer guidance documentation would of course need to provide clear information on how segments can participate in the user management console and how to specify what can be assigned to users.

Related to this is the subject of configuration items, many of which are on a per-user basis (preferences). This is a topic in another paper however.

Cache

For thick clients especially, actions that a principal can take may be cached in a secure store on the client (secured using the owners encryption key). Doing so would enable and support the notion of "Disconnected Operations" where-in the client is able to use the software to visualize and even manipulate any cached data. It is important, for security reasons that any data modified in this manner be captured in transactions, which can be re-authenticated when a network connection is re-established. This way, the data source could only be manipulated by current authorized users.

PKI Usage (thick and thin)

Consider where PKIs are currently stored and how they are used today and compare that with Active Directory and window's domains or NIS+ on Solaris. End-User PKIs are maintained and stored by the user, not just in a centralized location. It is important to realize that the user presents their identity via a PKI certificate to the system, not the central domain controller. One should think that the user does not really have an "account", but rather is issued an identity which is portable and capable of being used by many mechanisms (operating system + servers, etc).

Single Login Prompt – Desktop User Keystores

Applications (both desktop/thick and web/thin) need to be capable of initially obtaining the user's public key from their certificate and using that as their identity. The browser does this for accessing our web applications. Software security libraries such as SAFE[2] provide the thick client with user keystore management capability analogous to that of the browser. Within this architecture, a single management console (ala SAFE) can assign privileges to identities that affect both the thick and thin clients, at the same time. SAFE can be coded to provide the XML declaratives for developers to specify their program's roles, similar to J2EE.

After user login, SAFE calls can be made to check authorized roles as needed to enable dialogs, buttons, menus, etc. This is handled very nicely by the middle tier (J2EE) when applications invoke the request.isUserInRole() method. However on the thick client, an equivalent API is provided by SAFE. SAFE in turn communicates over the network to provide authorization (via its own secure channel or via NCES web services).

When a user first attempt to access the system, a prompt for their keystore password should occur (thick and thin clients) and a network session is established once the user is authenticated. The "session" should remain alive so that the user would not have to login again unless the session is ended by a normal logout or a session timeout. Extending the concept of the browser session to other clients (thick) needs to be implemented. This goes beyond just Web Single-Sign on as presented in Sun's recent paper.[3]

Server Certificates and Trusts

The security library should automatically obtain the server certificates and ask the user if it should be trusted (just like the browser does). Trusted public server identities can then be stored in that users trust file on their client. Doing so will provide immediate relief on the client-side maintenance currently encountered during installation of the system.

[2] Northrop Grumman developed API

[3] Sun Identity Management

Terminology and Concepts

The following definitions outline the terminology and usage in this paper.

Role:
A role is generally a job task that a user can perform, such as "Mission Planner" or "Database Administrator" or "Briefing Editor".

RoleSpace:
A unique path to the role/resource being managed. Each application should prefix their specific roles with their application unique prefix or name.

Account:
A record of all the data about a principle to include current role assigments.

Profile:
A collection of resource assignments for an abstract principle.

Feature:
A feature is the smallest end-user selectable unit of software. In the COE context, features are resources.

Resource:
A software function that can be assigned or unassigned to a user.

Principle:
A principal represents an entity such as an individual user or a company. The user.

Group:
An organizational abstract construct to aid in sharing resources. With regard to accounts, a principle can be a member of a group and would therefore inherit the rights and privileges of that group. Groups can be used to efficiently assign features to users.

Segment:
An application developed with the intent of being part of a bigger system. Therefore segments tend to have dependencies and interactions with other segments.

Acknowledgements

Northrop Grumman's work on the SAFE and J2EEDT segments which provides PKI and install support for the GCCS-J system at the Defense Information Systems Agency (DISA).

References

[WS-Security]
http://www.oasis-open.org/committees/download.php/5531/oasis-200401-wsssoap-message-security-1.0.pdf
[Sun Identity Management: Technology Cornerstone of the Virtual Enterprise, October 2004]
http://www.sun.com/software/products/identity/wp_virtual_enterprise.pdf

The information contained in this document represents the current view of R2AD, LLC Corporation on the issues discussed as of the date of publication. Because R2AD must respond to changing market conditions, it should not be interpreted to be a commitment on the part of R2AD, and R2AD cannot guarantee the accuracy of any information presented after the date of publication.

R2AD, LLC MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

R2AD may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from R2AD, LLC, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

RESTRICTED RIGHTS: Use, duplication, or disclosure by the U.S. Government is subject to restrictions of FAR 52.227-14(g)(2)(6/87) and FAR 52.227-19(6/87), or DFAR 252.227-7015(b)(6/95) and DFAR 227.7202-3(a). THIS WHITEPAPER IS PROVIDED "AS IS". R2AD, LLC, BiblioTronix, LLC (COLLECTIVELY, THE "COMPANIES") MAKE NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR TITLE; THAT THE CONTENTS OF THIS WHITEPAPER ARE SUITABLE FOR ANY PURPOSE; NOR THAT THE IMPLEMENTATION OF SUCH CONTENTS WILL NOT INFRINGE ANY THIRD PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS. THE COMPANIES WILL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF OR RELATING TO ANY USE OR DISTRIBUTION OF THIS WHITEPAPER.