



VHA RBAC Program Manager
Chuck Brown
Chuck.Brown@med.va.gov

VHA/IHS RBAC TF Chair
Dr. Robert O'Hara, MD
Robert.Ohara@med.va.gov

VHA Deputy Chief Architect,
RBAC Project Manager
Steve Wagner
Steve.Wagner@med.va.gov

VHA Security Architect,
RBAC Architect
Mike Davis, CISSP
Mike.Davis@med.va.gov

VHA Security Architect,
RBAC Architect
Ed Coyne, PhD
Ed.Coyne@med.va.gov

VHA Software Security
Architect, RBAC Project Lead
Amy Page
Amy.Page@med.va.gov

VHA/IHS RBAC TF
Functional Analyst Lead
Dawn Rota, RN
Dawn.Rota@med.va.gov

GATHERING ANCILLARY HEALTHCARE INFORMATION FOR HEALTHCARE SCENARIO ROADMAP

The Veterans Health Administration (VHA)/Indian Health Service (IHS) Role-Based Access Control (RBAC) Task Force (TF) continues its efforts to expand the Healthcare Scenario Roadmap spreadsheet to include licensed and non-licensed ancillary healthcare roles and responsibilities. The Healthcare Scenario Roadmap, a task identification questionnaire tool, and department distribution letter were developed by the VHA RBAC TF Permission Definition Subcommittee and are being distributed to ancillary healthcare departments within the Department of Veterans Affairs (VA), IHS, Department of Defense (DoD) and Kaiser Permanente. Results will be analyzed, harmonized, and modeled in accordance with the RBAC Role Engineering Process with the purpose of deriving standard healthcare permissions. The roadmap is already complete in the identification and representation of clinical activities for physicians and nurses and other licensed roles in clinical capacities.

The Healthcare Scenario Roadmap was developed during weekly discussions with clinicians on the VHA/IHS RBAC TF clinicians initially using the American Society for Testing and Materials (ASTM) E1986 Standard Guide for Information Access Privileges to Health Information list of "Healthcare Personnel that Warrant Differing Levels of Access Control" as the initial basic role names. The roadmap can function as a foundational tool to assist in defining the scope of the RBAC modeling effort, as well as be utilized as a quick reference of healthcare scenarios. The roadmap presents scaleable management of user permissions in the form of a list of tasks as a healthcare standard and is available on the RBAC website.

PERMISSION CATALOG DEVELOPMENT

A Permissions Catalog is being developed for licensed healthcare roles with tasks identified on the Healthcare Scenario Roadmap in accordance with the VHA-developed "Role-Based Access Control (RBAC) Role Engineering Process". Associated scenario steps and {operations, objects} are paired and then harmonized to create a standardized set of permissions. The preliminary Permissions Catalog will be presented at the January Health Level Seven (HL7) Working Group Meeting.

REVERSE ENGINEERING VISTA ROLES

The VHA RBAC TF Functional Role/Business Rule Sub-committee has developed a process to reverse engineer healthcare roles within VistA, the legacy health information system for VHA. The process document entitled "Guidance for Mapping VHA RBAC Roles and Abstract Permission to VistA Derived Roles" is currently undergoing internal review.

Inside this issue:

- Roadmap Continuation
- Permission Catalog Development
- Reverse Engineering VistA Roles
- "Evaluation of XML Technologies as Applied to Access Control" by David Staggs, Chief Systems Engineer, VHA OI AAIP Lab
- Upcoming Meetings

EVALUATION OF XML TECHNOLOGIES AS APPLIED TO CONTROL, SECTIONS 1 AND 4

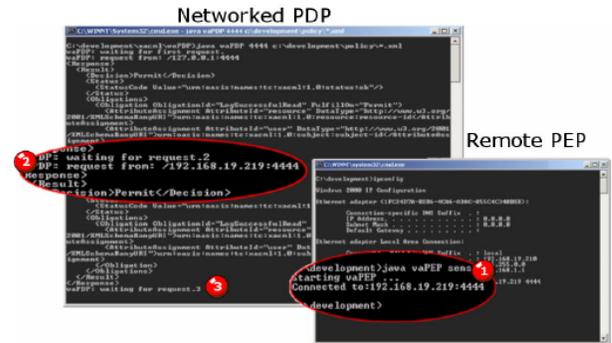
David Staggs, Chief Systems Engineer
September 13, 2004

1. Introduction

This document summarizes efforts by the Authentication and Authorization Infrastructure Project (AAIP) lab to explore the use of emerging XML (eXtensible Markup Language) based technologies for controlling access to protected information resources. Our central focus is on providing solutions to meet the VHA business requirement of implementing role based access control (RBAC). RBAC is an approach to controlling access to protected resources on an information system. The National Institute of Standards and Technology (NIST) identified RBAC as the predominant model for advanced access control because it reduces the complexity and cost of security administration in large networked applications. Consequently, the AAIP lab is reviewing several XML-based technologies that may be useful in implementing RBAC.

Since XML is a relatively new technology, the AAIP has relied on the guidance of industry-recognized standards groups. Several XML standards have been promulgated by the Organization for the Advancement of Structured Information Standards (OASIS). XACML (eXtensible Access Control Markup Language) is an OASIS standard useful in expressing and evaluating access control decisions on a protected system resource, such as a patient's medical record. The OASIS XACML Technical Committee has provided guidance on using XACML with several XML-based technologies. Specifically, "XACML Profile for Role Based Access Control (RBAC)," "LDAP (Lightweight Directory Access Protocol) Profile for Distribution of XACML," and "Service Provisioning Markup Language (SPML)," as discussed below.

Although using XML-based access control technologies in a Service Oriented Architecture (SOA) is still in its infancy, the technology shows promise in providing a non-proprietary, industry-wide methodology for RBAC implementation. Based on our initial experiences with XACML in the AAIP laboratory, we believe additional effort in developing XML-based technologies for RBAC is justified.



Screen Shots of Testing Networked XACML Implementation

4. Summary

Our investigation has demonstrated that an XML-based implementation of RBAC in the healthcare sector is technically feasible. In addition, there are several other recent technologies that can be leveraged using XACML. The XML-based Security Assertion Markup Language (SAML) protocol can provide access control information between security domains. The SPML offers a system for populating XACML policies in LDAP. In addition, XACML requests and responses can be transmitted using the Simple Object Access Protocol (SOAP), providing end-to-end security.

It appears that this confluence of standards will bring forward the technology to support the adoption of XML-based applications. Therefore, we see the use of XACML as a viable technology in providing an XML-based RBAC implementation for the healthcare sector. Although still in its infancy, XACML and related technologies may provide the means to simplify the complexities inherent in managing individual user access permissions in large organizations.

The article is available in its entirety via: http://www.va.gov/rbac/docs/Veterans_Administratio_n_Lab_Eval_of_XML_Technologies.pdf

UPCOMING MEETINGS

- ASTM Committee E31 on Healthcare Informatics, November 8 – 10, 2004, Omni Shoreham Hotel, Washington, D.C.
- HL7 Working Group Meeting, January 23-28, 2005, The Hilton in Walt Disney Resort, Orlando, FL.