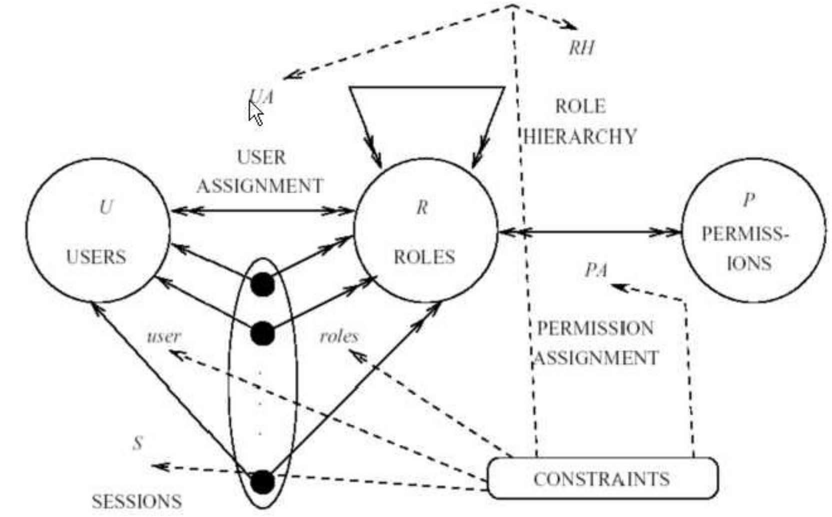
Implementation and Interoperability of Role Based Access Control

RBAC Implementation and Interoperability Standard (RIIS)

INCITS CS1.1 RBAC Task Group
INCITS 459 Draft Standard



Ed Coyne
Chair, INCITS CS1.1
RBAC Task Group

Info About Ed

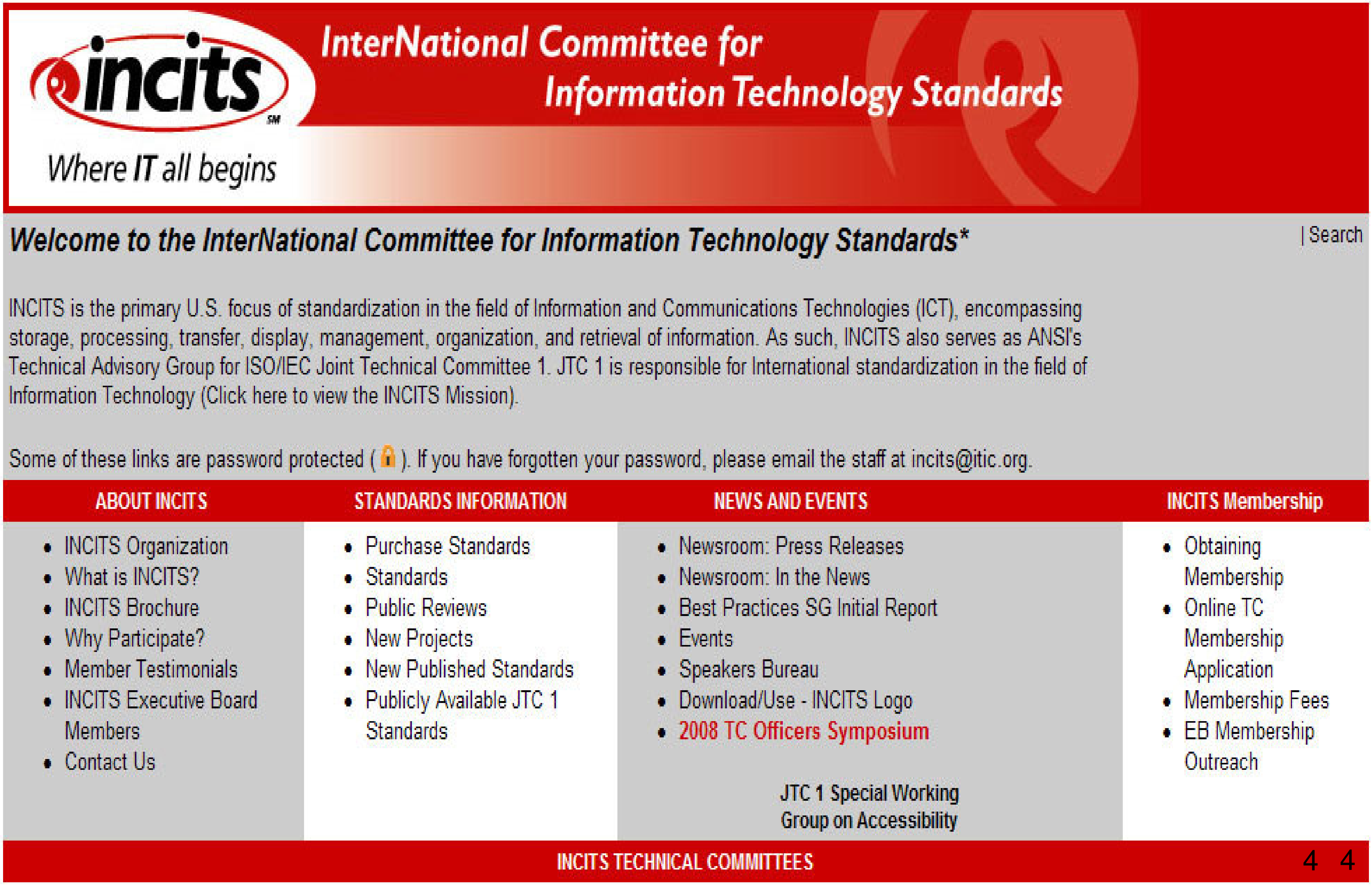
- Evaluator of security products since 1987
  - National Computer Security Center
  - SAIC Common Criteria testing laboratory
- Developer of RBAC specifications since 1995
  - NIST
  - INCITS
- Role engineering analyst since 2003
  - Veterans Health Administration
  - Health Level 7
- Author of *Role Engineering for Enterprise Security Management*

INCITS is the sponsor

- The InterNational Committee for Information Technology Standards (INCITS) is the forum of choice for developers, producers, and users for the creation and maintenance of formal *de jure* information and communications technology (ICT) standards.

- INCITS and the Information Technology Industry Council (ITI) are jointly accredited by, and operate under the rules approved by, the American National Standards Institute (ANSI). These rules are designed to ensure that voluntary standards are developed by the consensus of directly and materially affected interests.

INCITS – http://www.incits.org



InterNational Committee for Information Technology Standards

Welcome to the InterNational Committee for Information Technology Standards*

INCITS is the primary U.S. focus of standardization in the field of Information and Communications Technologies (ICT), encompassing storage, processing, transfer, display, management, organization, and retrieval of information. As such, INCITS also serves as ANSI's Technical Advisory Group for ISO/IEC Joint Technical Committee 1. JTC 1 is responsible for International standardization in the field of Information Technology (Click here to view the INCITS Mission).

Some of these links are password protected (🔒). If you have forgotten your password, please email the staff at incits@itic.org.

ABOUT INCITS

- INCITS Organization
- What is INCITS?
- INCITS Brochure
- Why Participate?
- Member Testimonials
- INCITS Executive Board Members
- Contact Us

STANDARDS INFORMATION

- Purchase Standards
- Standards
- Public Reviews
- New Projects
- New Published Standards
- Publicly Available JTC 1 Standards

NEWS AND EVENTS

- Newsroom: Press Releases
- Newsroom: In the News
- Best Practices SG Initial Report
- Events
- Speakers Bureau
- Download/Use - INCITS Logo
- 2008 TC Officers Symposium

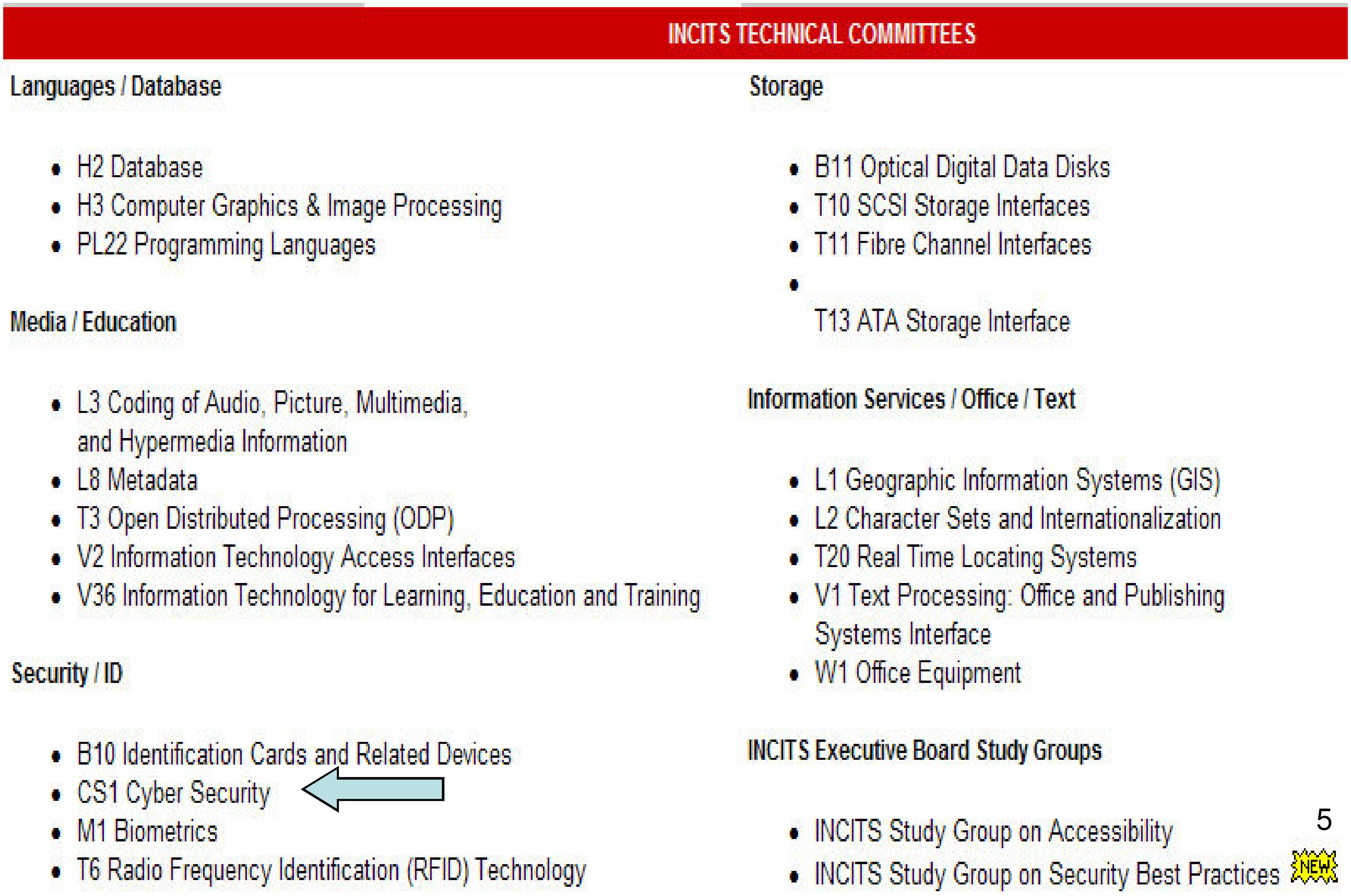
JTC 1 Special Working Group on Accessibility

INCITS Membership

- Obtaining Membership
- Online TC Membership Application
- Membership Fees
- EB Membership Outreach

INCITS TECHNICAL COMMITTEES

INCITS CS1.1 is the Role-Based Access Control working group under CS1 Cyber Security (http://cs1.incits.org)



INCITS TECHNICAL COMMITTEES

Languages / Database

- H2 Database
- H3 Computer Graphics & Image Processing
- PL22 Programming Languages

Media / Education

- L3 Coding of Audio, Picture, Multimedia, and Hypermedia Information
- L8 Metadata
- T3 Open Distributed Processing (ODP)
- V2 Information Technology Access Interfaces
- V36 Information Technology for Learning, Education and Training

Security / ID

- B10 Identification Cards and Related Devices
- CS1 Cyber Security
- M1 Biometrics
- T6 Radio Frequency Identification (RFID) Technology

Storage

- B11 Optical Digital Data Disks
- T10 SCSI Storage Interfaces
- T11 Fibre Channel Interfaces
- T13 ATA Storage Interface

Information Services / Office / Text

- L1 Geographic Information Systems (GIS)
- L2 Character Sets and Internationalization
- T20 Real Time Locating Systems
- V1 Text Processing: Office and Publishing Systems Interface
- W1 Office Equipment

INCITS Executive Board Study Groups

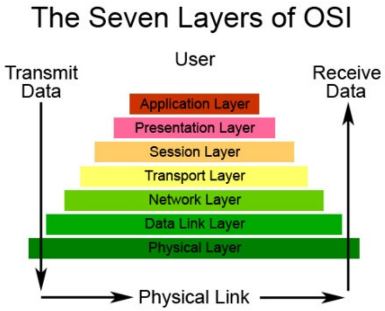
- INCITS Study Group on Accessibility
- INCITS Study Group on Security Best Practices NEW

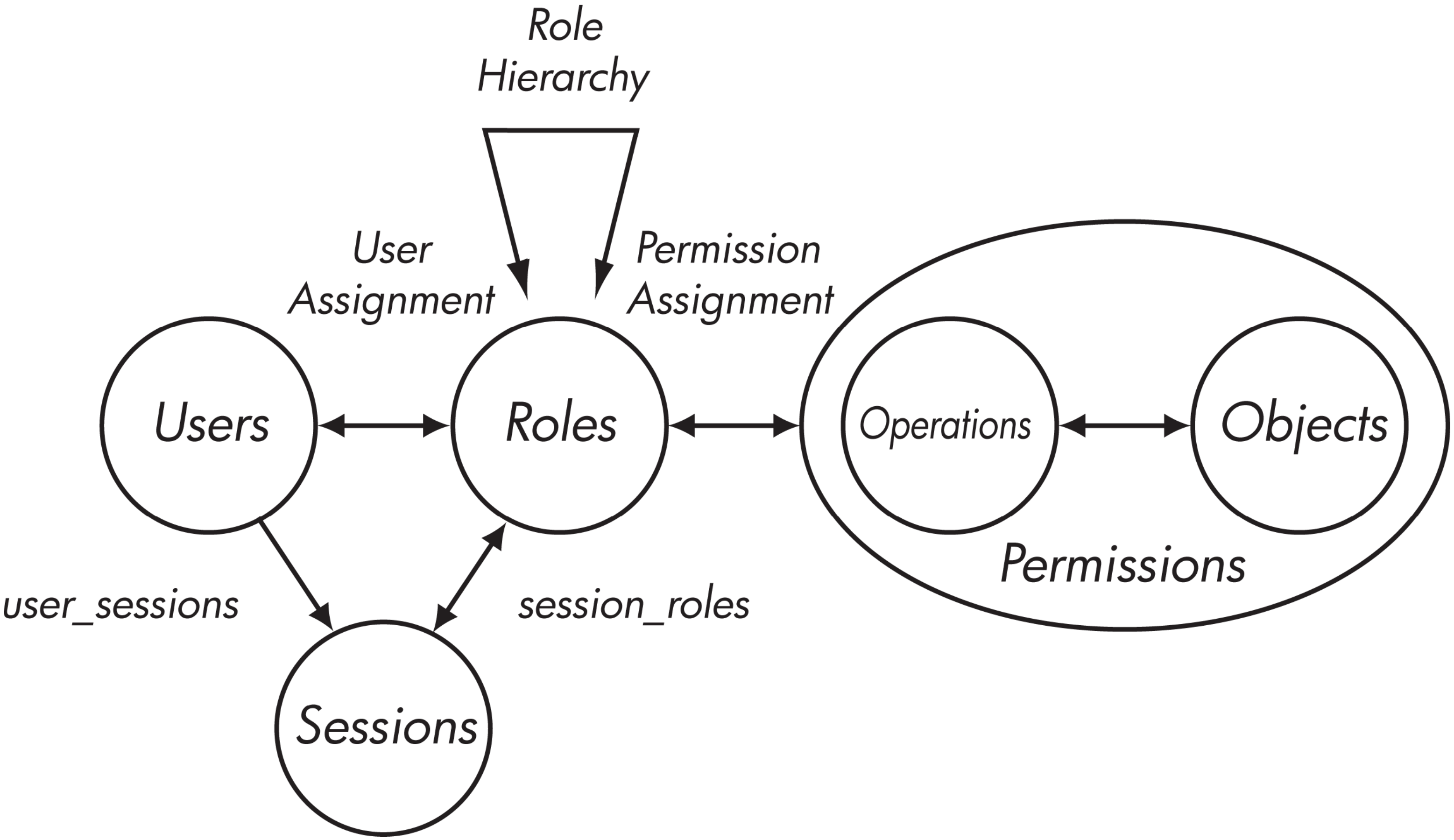
What do we mean by RBAC?

- Permissions are assigned to roles rather than to individual users
- Users are assigned to roles rather than directly to permissions
- This level of indirection facilitates user-permission management and provides additional security benefits
- See the NIST RBAC website

http://csrc.nist.gov/rbac

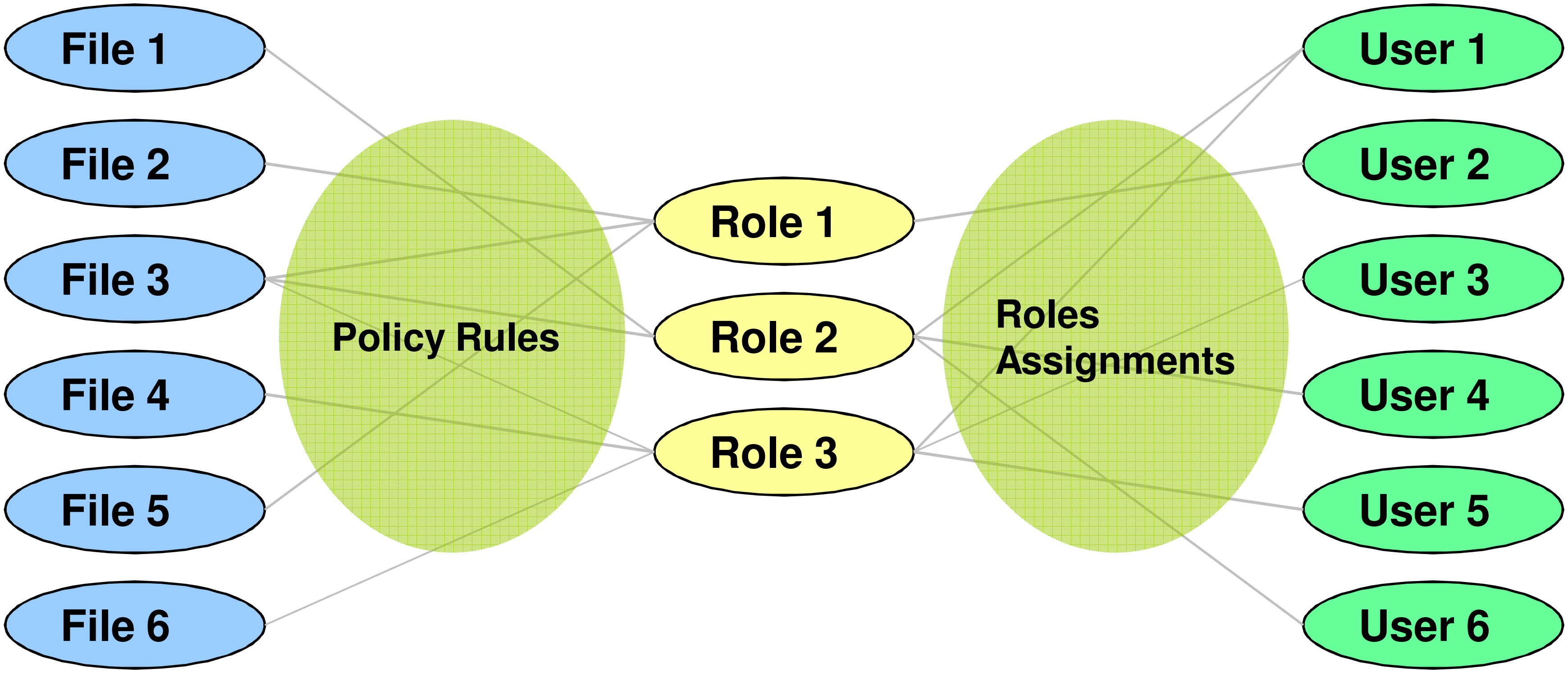
NIST RBAC Model





RBAC Privilege Management

- With RBAC, privileges are managed indirectly through roles



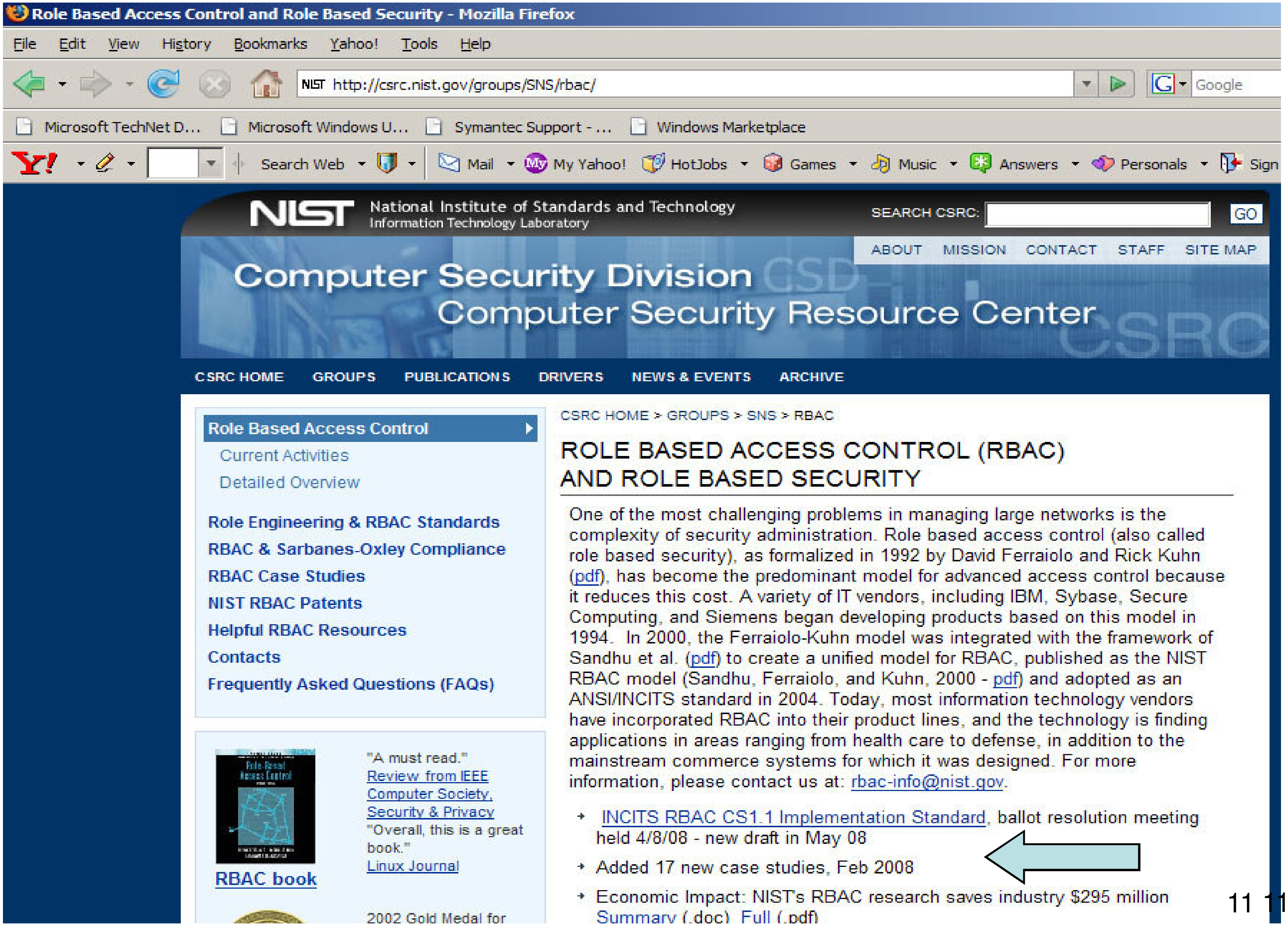
ACM symposium on access control models and technologies (SACMAT)

SACMAT 2009 is the Fourteenth of a successful series of symposiums that continue the tradition, first established by the ACM Workshop on Role-Based Access Control, of being the premier forum for presentation of research results and experience reports on leading edge issues of access control, including models, systems, applications, and theory. The missions of the symposium are to share novel access control solutions that fulfill the needs of heterogeneous applications and environments and to identify new directions for future research and development.
SACMAT gives researchers and practitioners a unique opportunity to share their perspectives with others interested in the various aspects of access control.

NIST Supports RBAC Research and Standards

- **National Institute of Standards and Technology**
  - **RBAC Model**
  - **Policy Machine**
  - **RBAC Book**
  - **RBAC Prototype**
  - **RBAC Economic Study**
  - **RBAC and Related Research Papers**

NIST RBAC Portal - http://csrc.nist.gov/rbac


Role Based Access Control and Role Based Security - Mozilla Firefox
File Edit View History Bookmarks Yahoo! Tools Help
http://csrc.nist.gov/groups/SNS/rbac/
Google
Microsoft TechNet D...
Microsoft Windows U...
Symantec Support - ...
Windows Marketplace
Search Web
Mail
My Yahoo!
HotJobs
Games
Music
Answers
Personals
Sign
NIST National Institute of Standards and Technology
Information Technology Laboratory
SEARCH CSRC:
GO
ABOUT
MISSION
CONTACT
STAFF
SITE MAP
Computer Security Division
Computer Security Resource Center
CSRC HOME
GROUPS
PUBLICATIONS
DRIVERS
NEWS & EVENTS
ARCHIVE

CSRC HOME > GROUPS > SNS > RBAC

ROLE BASED ACCESS CONTROL (RBAC) AND ROLE BASED SECURITY

One of the most challenging problems in managing large networks is the complexity of security administration. Role based access control (also called role based security), as formalized in 1992 by David Ferraiolo and Rick Kuhn (pdf), has become the predominant model for advanced access control because it reduces this cost. A variety of IT vendors, including IBM, Sybase, Secure Computing, and Siemens began developing products based on this model in 1994. In 2000, the Ferraiolo-Kuhn model was integrated with the framework of Sandhu et al. (pdf) to create a unified model for RBAC, published as the NIST RBAC model (Sandhu, Ferraiolo, and Kuhn, 2000 - pdf) and adopted as an ANSI/INCITS standard in 2004. Today, most information technology vendors have incorporated RBAC into their product lines, and the technology is finding applications in areas ranging from health care to defense, in addition to the mainstream commerce systems for which it was designed. For more information, please contact us at: rbac-info@nist.gov.

- INCITS RBAC CS1.1 Implementation Standard, ballot resolution meeting held 4/8/08 - new draft in May 08
- Added 17 new case studies, Feb 2008
- Economic Impact: NIST's RBAC research saves industry $295 million Summary (.doc) Full (.pdf)

Role Based Access Control
- Current Activities
- Detailed Overview

Role Engineering & RBAC Standards
RBAC & Sarbanes-Oxley Compliance
RBAC Case Studies
NIST RBAC Patents
Helpful RBAC Resources
Contacts
Frequently Asked Questions (FAQs)

RBAC book

"A must read."
Review from IEEE Computer Society, Security & Privacy
"Overall, this is a great book."
Linux Journal

2002 Gold Medal for

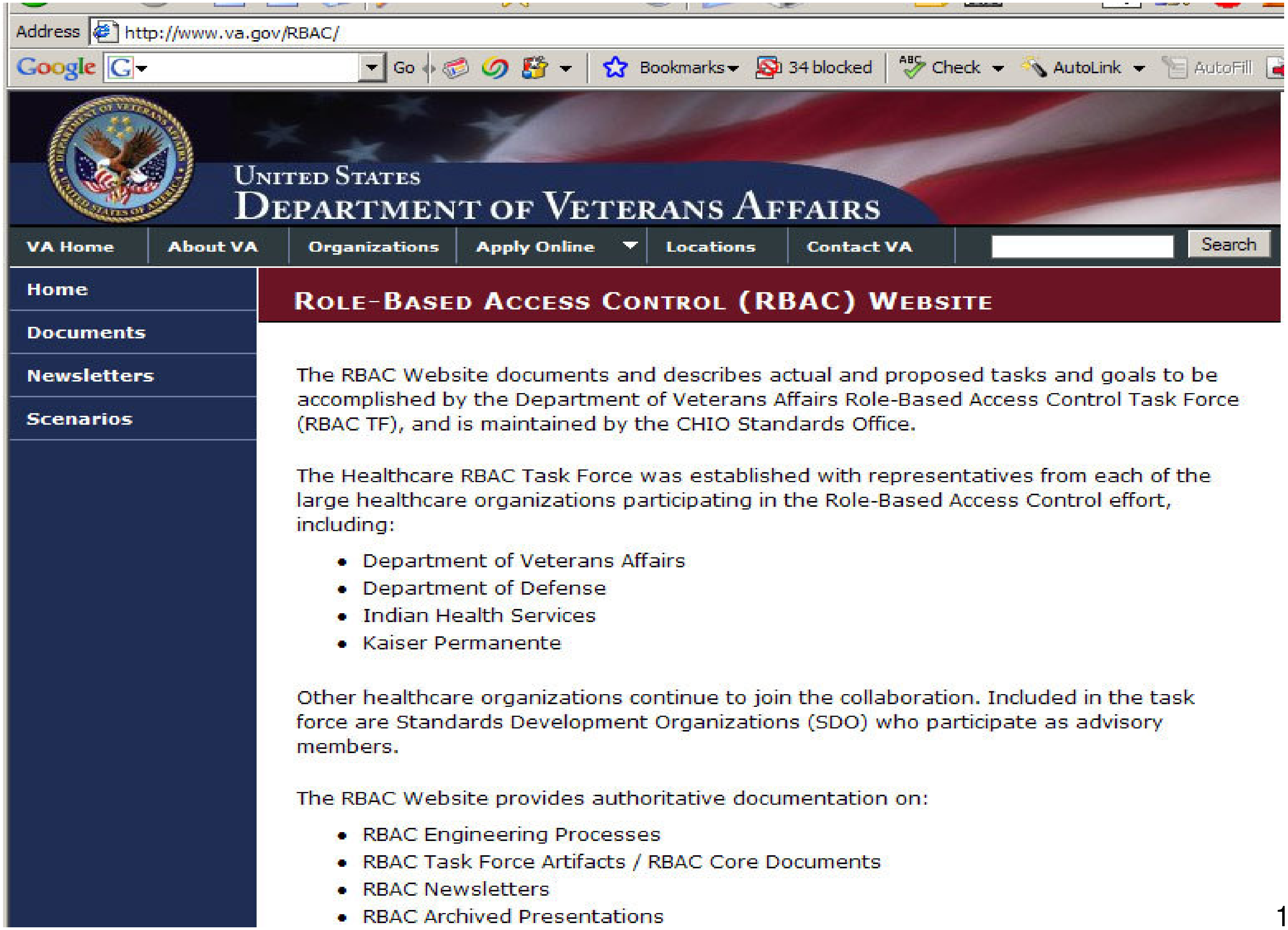
Veterans Health Administration

- RBAC Task Group
- Healthcare Task Group
- Role engineering process
- Permission catalog
- Handoff for continuation in HL7

VA RBAC Website

- http://www.va.gov/rbac

US Department of Veterans Affairs – RBAC Initiatives



Role-Based Access Control (RBAC) Website

The RBAC Website documents and describes actual and proposed tasks and goals to be accomplished by the Department of Veterans Affairs Role-Based Access Control Task Force (RBAC TF), and is maintained by the CHIO Standards Office.

The Healthcare RBAC Task Force was established with representatives from each of the large healthcare organizations participating in the Role-Based Access Control effort, including:

- Department of Veterans Affairs
- Department of Defense
- Indian Health Services
- Kaiser Permanente

Other healthcare organizations continue to join the collaboration. Included in the task force are Standards Development Organizations (SDO) who participate as advisory members.

The RBAC Website provides authoritative documentation on:

- RBAC Engineering Processes
- RBAC Task Force Artifacts / RBAC Core Documents
- RBAC Newsletters
- RBAC Archived Presentations

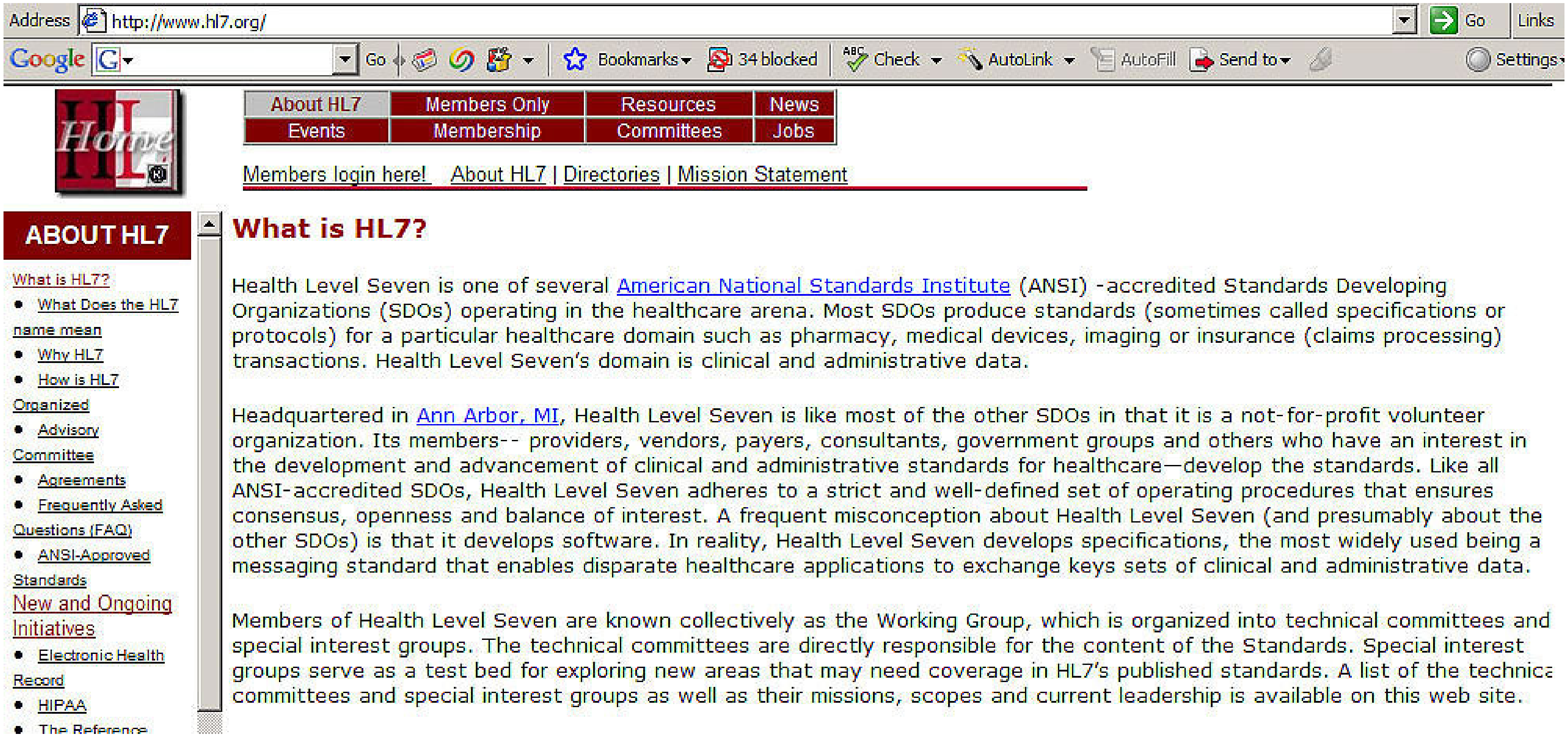
Health Level 7 (HL7)

- Healthcare permission catalog
- Healthcare constraint catalog
- Role engineering process

HL7 Website

- http://www.hl7.org

HL7 – IT Standards for the Healthcare Community



What is HL7?

Health Level Seven is one of several American National Standards Institute (ANSI) -accredited Standards Developing Organizations (SDOs) operating in the healthcare arena. Most SDOs produce standards (sometimes called specifications or protocols) for a particular healthcare domain such as pharmacy, medical devices, imaging or insurance (claims processing) transactions. Health Level Seven's domain is clinical and administrative data.

Headquartered in Ann Arbor, MI, Health Level Seven is like most of the other SDOs in that it is a not-for-profit volunteer organization. Its members-- providers, vendors, payers, consultants, government groups and others who have an interest in the development and advancement of clinical and administrative standards for healthcare—develop the standards. Like all ANSI-accredited SDOs, Health Level Seven adheres to a strict and well-defined set of operating procedures that ensures consensus, openness and balance of interest. A frequent misconception about Health Level Seven (and presumably about the other SDOs) is that it develops software. In reality, Health Level Seven develops specifications, the most widely used being a messaging standard that enables disparate healthcare applications to exchange keys sets of clinical and administrative data.

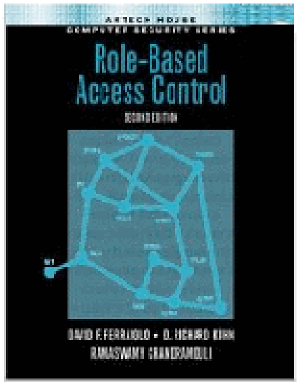
Members of Health Level Seven are known collectively as the Working Group, which is organized into technical committees and special interest groups. The technical committees are directly responsible for the content of the Standards. Special interest groups serve as a test bed for exploring new areas that may need coverage in HL7's published standards. A list of the technica committees and special interest groups as well as their missions, scopes and current leadership is available on this web site.

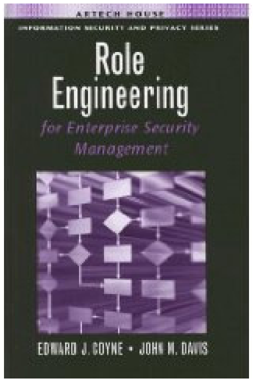
HL7 RBAC Initiatives

RBAC has a natural fit with many health care applications. Standards are being developed under er the HL7 Standards Development Organization. The Department of Veterans Affairs is leading a number of these activities. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) mandates use of RBAC to protect patient information. The HL7 RBAC activities are oriented toward application level systems that are built using the services defined in the general purpose RBAC standards.

What RBAC standards exist?

1. INCITS 359-2004 “The RBAC Standard”
2. Draft INCITS 459 RBAC Implementation and Interoperability Standard (RIIS)
3. HL7 Healthcare Permission Catalog
4. HL7 Role Engineering Process
5. RBAC Book
6. Role Engineering Book



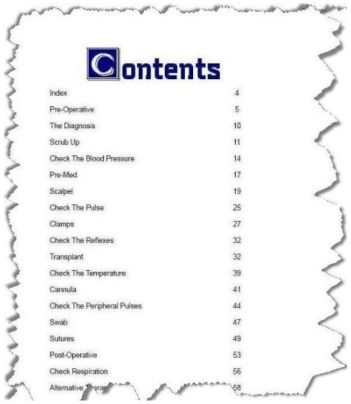

ARTECH HOUSE
INFORMATION SECURITY AND PRIVACY SERIES
Role Engineering
for Enterprise Security Management
EDWARD J. COYNE • JOHN M. DAVIS

NEW

Why was a new standard needed?

- Existing standard was useful for definitions but not intended as guidance to implementers and evaluators
- Existing standard's "academic" nature deters some readers
- Existing standard does not address interoperability

What does the RIIS provide?



- Provides guidance on packaging of RBAC features
  - Role Names, Permissions, Hierarchies, Constraints
- Defines mechanisms (function definitions) that provide an interface to transfer RBAC definitions from one implementation to another
  - The two systems need not be operational
- Provides standard terminology for the components of RBAC systems

CS1.1 – Implementation Component Model

Component	Fundamental (F)	Organizational (O)	User Limiting – Universal (ULU)	User Limiting – Operational (ULO)
1. Core RBAC	X	X	X	X
2. Hierarchical RBAC		X		
3. Static Separation of Duty (SSD) Relations			X	
4. Dynamic Separation of Duties (DSD) Relations				X

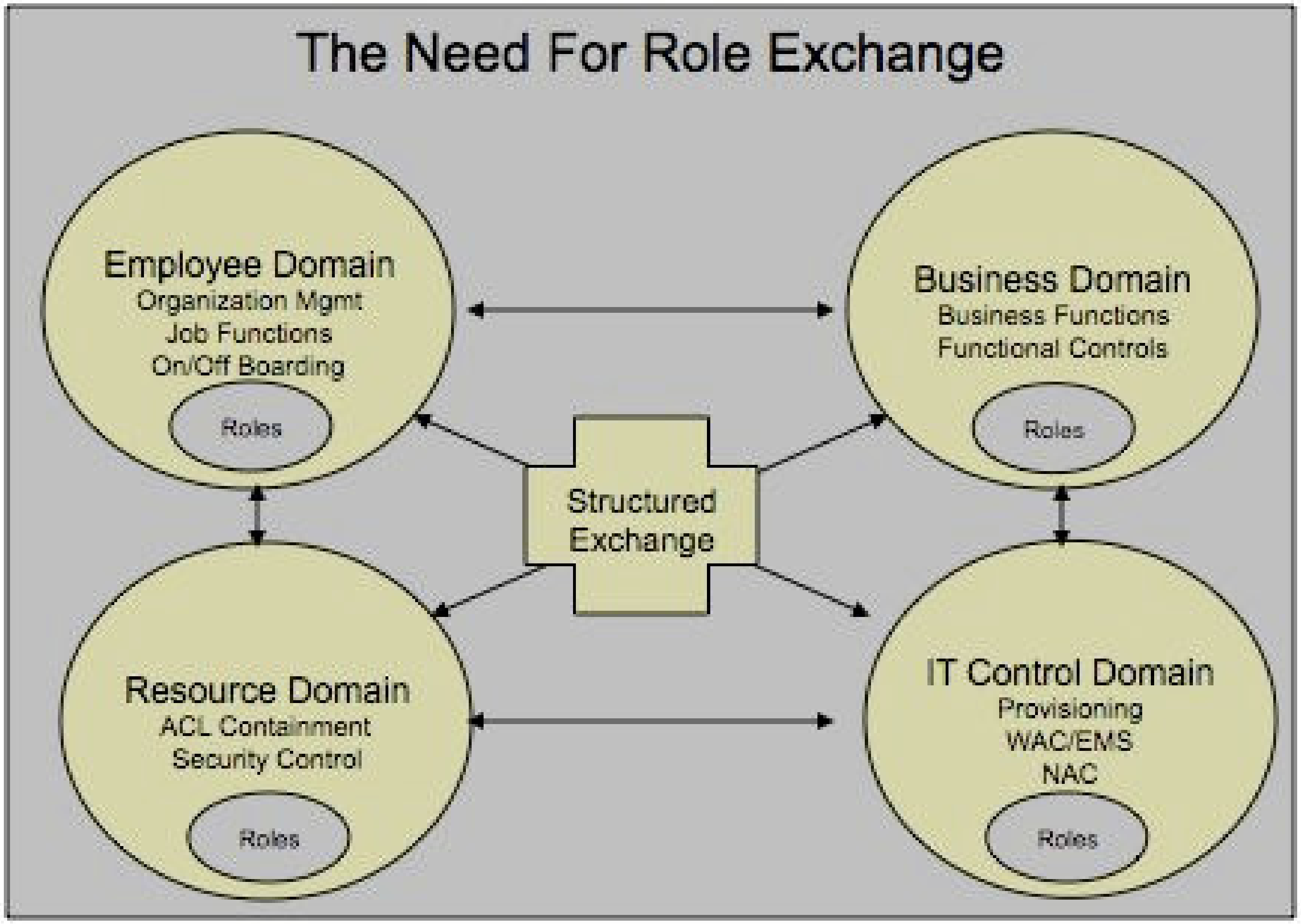
Fundamental refers to core RBAC with no hierarchies or constraints;

Organizational refers to RBAC with role hierarchies,

User Limiting Universal refers to RBAC with static constraints

User Limiting Operational refers to RBAC with run-time constraints.

RBAC Interoperability (Enterprise Security Management)



The Need For Role Exchange

Employee Domain
Organization Mgmt
Job Functions
On/Off Boarding
Roles

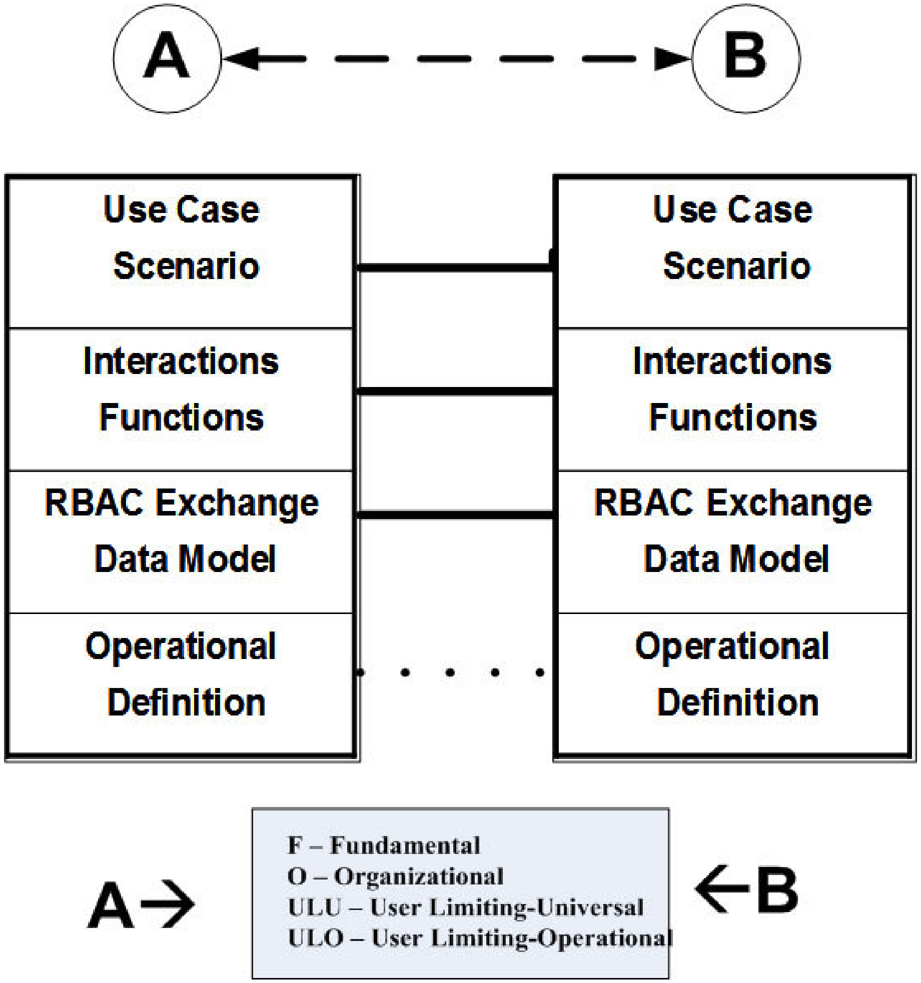
Business Domain
Business Functions
Functional Controls
Roles

Structured Exchange

Resource Domain
ACL Containment
Security Control
Roles

IT Control Domain
Provisioning
WAC/EMS
NAC
Roles

CS1.1 Annex –Conceptual Model (Interoperability)



A ←– – – – –→ B

Use Case Scenario	Use Case Scenario
Interactions Functions	Interactions Functions
RBAC Exchange Data Model	RBAC Exchange Data Model
Operational Definition	Operational Definition

A→

F – Fundamental
O – Organizational
ULU – User Limiting-Universal
ULO – User Limiting-Operational

←B

Two Security (or Identity Management) domains are depicted. Within each system, the RIIS interoperability model segments into four areas defined as Use Case Scenarios, Interaction Functions, RBAC Exchange Data Model and Operational Definition

CS1.1 – Management Interaction Functions (1 of 2)

Interaction Function	Meaning	Options
PostRoleSet	Inform of current set of roles	F, O, ULU, ULO
GetRoleSet	Obtain current set of roles	F, O, ULU, ULO
PostRoleName(rolename)	Inform of a new role name	F, O, ULU, ULO
GetRoleName(rolename)	Obtain new role name	F, O, ULU, ULO
PostUserSet	Inform of current set of RBAC users	F, O, ULU, ULO
GetUserSet	Obtain current set of RBAC users	F, O, ULU, ULO
PostRoleUsers(role name)	Inform of users currently assigned to a given role	F, O, ULU, ULO
GetRoleUsers(rolename)	Obtain users currently assigned to a given role	F, O, ULU, ULO
PostUserRoles(user)	Inform of roles currently assigned to a given user	F, O, ULU, ULO
GetUserRoles(user)	Obtain roles currently assigned to a given user	F, O, ULU, ULO
PostUserAssignment(user, role)	Inform of user assignment to a role	F, O, ULU, ULO
GetUserAssignment(user, role)	Obtain user assignment to a role	F, O, ULU, ULO
PostPermissionAssignment (role,permission)	Inform of permission assignment to a role	F, O, ULU, ULO
GetPermissionAssignment (role,permission)	Obtain permission assignment to a role	F, O, ULU, ULO
PostPermissionSet	Inform of current set of permissions	F, O, ULU, ULO
GetPermissionSet	Obtain current set of permissions	F, O, ULU, ULO

F – Fundamental	O – Organizational
ULU – User Limiting-Universal	ULO – User Limiting-Operational

CS1.1 – Management Interaction Functions (2 of 2)

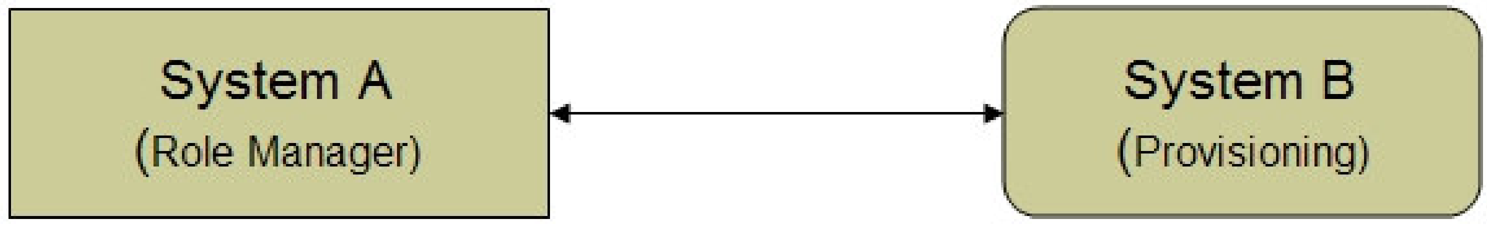
Interaction Function	Meaning	Options
PostRolePermissions(role)	Inform of permissions currently assigned to a given role	F, O, ULU, ULO
GetRolePermissions(role)	Obtain permissions currently assigned to a given role	F, O, ULU, ULO
PostPermissionRoles (permission)	Inform of roles to which a given permission is assigned	F, O, ULU, ULO
GetPermissionRoles (permission)	Obtain roles to which a given permission is assigned	F, O, ULU, ULO
PostUserAssignmentConstraintStatic (user,role)	Inform of a given user's static assignment constraint	ULU
GetUserAssignmentConstraintStatic (user,role)	Obtain a given user's static assignment constraint	ULU
PostUserAssignmentConstraintDynamic (user,role)	Inform of a given user's dynamic assignment constraint	ULO
GetUserAssignmentConstraintDynamic (user,role)	Obtain a given user's dynamic assignment constraint	ULO
PostInheritanceRelationship (role,role)	Inform of an inheritance relationship between two given roles	O
GetInheritanceRelationship (role,role)	Obtain an inheritance relationship between two given roles	O

F – Fundamental	O – Organizational
ULU – User Limiting-Universal	ULO – User Limiting-Operational

CS1.1 Use Case – Continuous Synchronization of External Role Model

Problem Statement (affecting RBAC)

An enterprise has deployed a Role Management solution (depicted as Systems A) to develop and maintain its role models. As this model changes over time, System A needs to publish these changes out to the operational infrastructure for use and implementation in the user on-board / off-boarding process.



Scope

One time load (Role Model Provisioning) has occurred

Repeating cycle of synchronization continues in which System A is seen as authoritative over the model used in System B.

Assumptions

Both systems, denoted System A and System B, are fully RBAC capable.

System A has posed all current configurations to System B and System B is assumed to be in a consistent steady state.

For performance reasons, System A may choose to batch process change notification to System B.

Trust model exists between System A and System B.

System A has a defined Role model and tracks changes make to it in order to relay them to System B

CS1.1 Use Case – Management Interaction Functions

Interaction Function	Meaning
PostRoleSet	Inform of current set of roles
PostUserSet	Inform of current set of RBAC users
PostUserRoles(user)	Inform of roles currently assigned to a given user
PostUserAssignment(user, role)	Inform of user assignment to a role
PostPermissionAssignment (role,permission)	Inform of permission assignment to a role
PostPermissionSet	Inform of current set of permissions
PostPermissionRoles (permission)	Inform of roles to which a given permission is assigned

RBAC Data Exchange Model

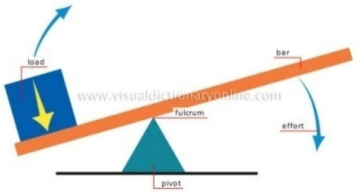
Extract, Transform and Load (ETL)

Roles Sets, Role Names, User Set, User Assignments,

Permission Assignments

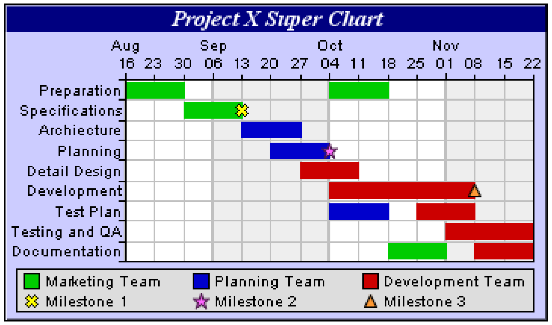
What doesn’t the RIIS do?

- RIIS does not provide implementation details (although examples are provided)
- RIIS does not address interoperability between running systems (static rather than dynamic)



What benefits does the RIIS provide?

- Promotes ability to compare two RBAC implementations if these adhere to the RIIS
  - Standard concepts and terminology
- Facilitates transfer of definitions of an RBAC implementation from one system to another or to the design process for a proposed system
  - Standard interfaces and definitions of data content



What is the status of the RIIS?

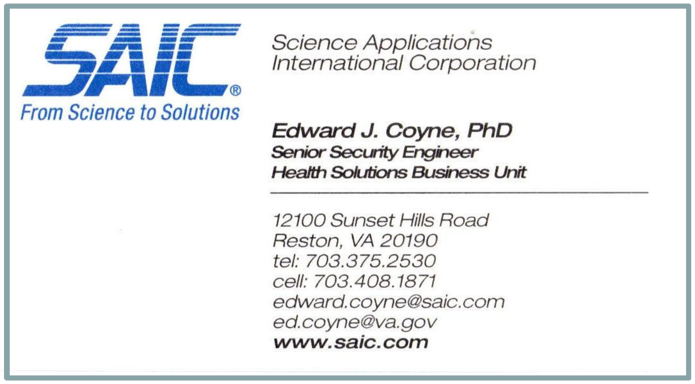
- Approved by INCITS Secretariat
- Initial public comment period began this month

What are the current activities of INCITS CS1.1?

- Addressing public comments on RIIS
- Updating the INCITS 359-2004 standard
- Development of a role engineering standard

Additional volunteers are needed for these activities!

Thank you for joining us!

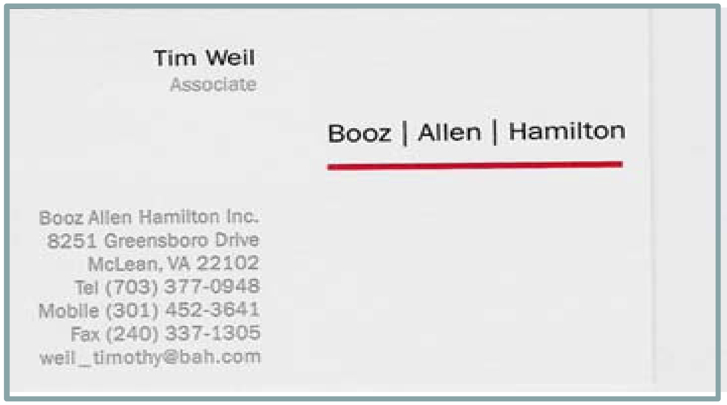


SAIC®
From Science to Solutions

Science Applications
International Corporation

Edward J. Coyne, PhD
Senior Security Engineer
Health Solutions Business Unit

12100 Sunset Hills Road
Reston, VA 20190
tel: 703.375.2530
cell: 703.408.1871
edward.coyne@saic.com
ed.coyne@va.gov
www.saic.com



Tim Weil
Associate

Booz | Allen | Hamilton

Booz Allen Hamilton Inc.
8251 Greensboro Drive
McLean, VA 22102
Tel (703) 377-0948
Mobile (301) 452-3641
Fax (240) 337-1305
weil_timothy@bah.com

- **Draft Copy of the CS1.1 (RIIS) Standard**

  http://csrc.ncsl.nist.gov/groups/SNS/rbac/documents/draft-rbac-implementation-std-v01.pdf

- **Call for CS1.1 Use Case Development**

  http://csrc.nist.gov/groups/SNS/rbac/documents/rbac-use-cases.html

- **How to Join CS1.1**

  http://csrc.nist.gov/rbac/how-to-join-CS1.1.pdf

Contact Info

- Ed Coyne – CS1.1 Chair
  - SAIC
  - 703-375-2530
  - coynee@saic.com
- Tim Weil - CS1.1 Vice Chair
  - Booz Allen Hamilton, Inc
  - 703-377-0948
  - weil_tim@bah.com
- INCITS – incits.org