RACF and z/OS Security Server Update

Walt Farrell, CISSP
z/OS Security Server Design
IBM Corporation MS P388
2455 South Road
Poughkeepsie, NY 12601
(845) 435-7750
wfarrell@us.ibm.com

RUG Mar. 6, 2003

Disclaimer

The information contained in this document is distributed on an "as is" basis without any warranty either express or implied. The customer is responsible for use of this information and/or implementation of any techniques mentioned. IBM has reviewed the information for accuracy, but there is no guarantee that customers using the information or techniques will obtain the same or similar results in their own operational environments.

In this document, any references made to an IBM licensed program are not intended to state or imply that only IBM's licensed programs may be used. Functionally equivalent programs may be used instead. Any performance data contained in this document was determined in a controlled environment and therefore, the results which may be obtained in other operating environments may vary significantly. Users of this document should verify the applicable data for their specific environments.

It is possible that this material may contain reference to, or information about, IBM products (machines and programs), programming, or services that are not announced in your country. Such references or information must not be construed to mean that IBM intends to announce such IBM Products, programming or services in your country.

IBM retains the title to the copyright in this paper as well as title to the copyright in all underlying works. IBM retains the right to make derivative works and to republish and distribute this paper to whomever it chooses.

Trademarks

- **The following are trademarks or registered trademarks of the International Business Machines Corporation:**
  - IBM, CICS, DB2, z/OS, OS/390, RACF, S/390, Tivoli
- **UNIX is a registered trademark of The Open Group in the United States and other countries.**
- **Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.**
- **Other company, product, and service names may be trademarks or service marks of others.**

Agenda

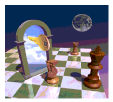
- **OS/390 Version 2 Release 10**
  - Selected Security Server enhancements
    - RACF:
      - ✓Program control usability enhancement
      - ✓Application identity mapping
      - ✓Mixed case profiles
    - New Security Server Component: Network Authentication Service
  - Selected Communications Server enhancements
    - TN3270
    - SERVAUTH controls

Agenda...

- **z/OS Release 2 Enhancements**
  - Security Server
    - RACF:
      - ✓UNIVERSAL groups
      - ✓SAF Trace
      - ✓Cross-system VLF
      - ✓Coupling Facility error toleration
    - Network Authentication Service
      - ✓New encryption methods
      - ✓New client commands
      - ✓Additional exploiters
  - Communications server
    - Express Logon
    - Network authentication
    - Intrusion detection
    - FTP

Agenda...

- **z/OS Release 3 Security Server Enhancements**
  - UNIX Access Checking Enhancements
    - **Access Control Lists**
    - RESTRICTED User ID Support
  - New PKI Services Component
  - Support for IBM Policy Director Authorization Services
- **z/OS Release 4 Security Server Enhancements:**
  - UNIX Security Management Usability
  - Program Control and PADS Usability and Security
  - Enterprise Identity Mapping Support
  - Network Authentication Services Enhancements
  - LDAP Server Enhancements
  - Firewall Technologies Enhancements
- **z/OS Release 4 System SSL Enhancements**



Selected OS/390 V2R10 Functions

Program Control Usability

- **New diagnostic messages when functions requiring "clean" environment (PADS, execute-control, UNIX server / daemon) fail**
  - Messages will state that failure occurred because of "dirty" environment
  - Messages will give the reason environment became dirty
    - module name, library name, etc.
  - Example: ICH420I PROGRAM PAYROL5 FROM LIBRARY SYS2.PAYLIB CAUSED THE ENVIRONMENT TO BECOME UNCONTROLLED.
- **New RACROUTE REQUEST=AUTH reason code to inform ICHRCX02 that the request would have worked except for dirty environment**
- **Should greatly reduce the need for GTF tracing for Program Control and PADS problems.**

Mixed-Case Profile Name Support

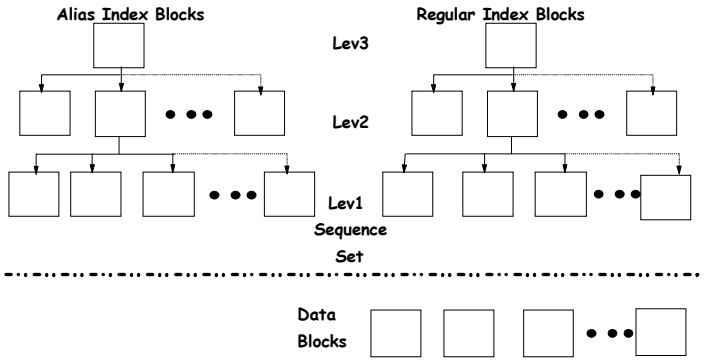
- **Supports Enterprise Java Beans in WebSphere via new classes EJBROLE, GEJBROLE**
- **New CDT option CASE=** UPPER | ASIS allowed for customer-defined classes
- No existing IBM resource classes changed
  - helps ensure compatibility and avoid administrative surprises
- For mixed-case classes, RACF commands and ISPF panels will use profile names as specified by the user
  - RDEFINE EJBROLE (xyz XYZ xYz)
    - defines 3 different profiles
- Also available on OS/390 V2R8 and V2R10 via SPE APAR OW46859
- Full documentation in SYS1.SAMPLIB(IRR46859) or in z/OS books

Application Identity Mapping

- **Eliminates need for some kinds of "mapping" profiles:**
  - UNIXMAP -- UNIX UID / GID to user ID or group name
  - NDSLINK -- Novell Directory Services UNAME to user ID
  - NOTELINK -- Lotus Notes (Domino) SNAME to user ID
- **Should:**
  - reduce size of RACF database by eliminating the profiles
  - provide better data integrity in the database
  - provide consistent mapping for shared UIDs or GIDs
- **Uses new "alias" index structure in RACF data base**

Alias Index Structure...

- Alias IX blocks, are similar to regular IX blocks at upper levels. In the Sequence Set, instead of pointers to data profiles, Alias IX entries contain base profile info.



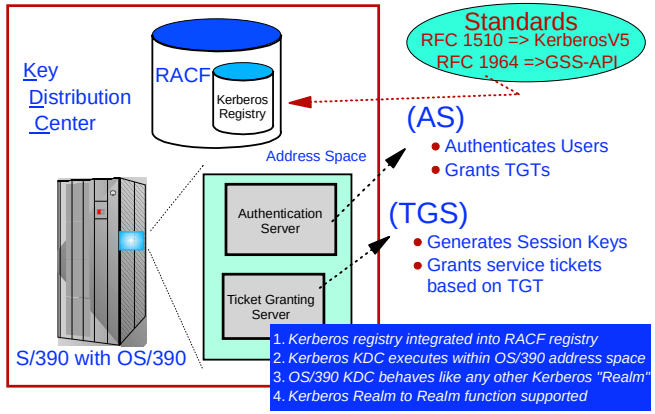
Network Authentication Service

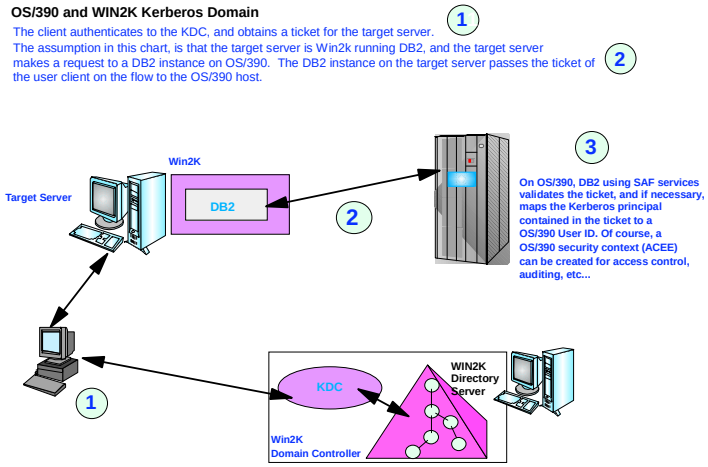
- **New Security Server component**
  - licensed with OS/390 base, for all OS/390 customers, like the LDAP server
  - requires RACF support or compatible other security product
- **OS/390 implementation of MIT's Kerberos Version 5**
- **Provides services for:**
  - USER AUTHENTICATION
  - DELEGATION
  - DATA CONFIDENTIALITY
- **Interoperates with other industry Kerberos Version 5 implementations**
- **Can provide consistent user authentication for Kerberos-aware applications spanning a network including, e.g. OS/390, Windows 2000, UNIX, AS/400**

Network Authentication Service...

- **RACF provides support for the server:**
  - definition of local Kerberos principals (users)
    - KERB segment
  - definition of the local Kerberos realm& foreign realms
    - REALM class
  - definition of foreign Kerberos principals with a local identity
    - KERBLINK profiles
  - Basically, the RACF database ***IS*** the Kerberos registry for OS/390
  - RACF password ***IS*** the user's Kerberos password
- **Server uses SAF callable services to interact with RACF: parse Kerberos tickets to obtain principal names; map from principal to RACF user and vice versa**
  - Enhanced R_usermap service
  - new R_kerbinfo service
  - new R_ticketserv service

Network Authentication Service...





Network Security and Usability

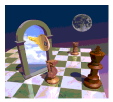
- **Functions provided by IBM Communications Server for OS/390**
- **TN3270E Server SSL enhancements**
  - Implements SSL negotiation based on enterprise security policy
  - Can force use of SSL based on IP address, hostname, or link
  - Allows use of same port for SSL and non-SSL, simplifying server and client configuration
- **TCP/IP protection of network resources**
  - Controls OS/390 users' access to
    - TCP/IP stack
    - TCP or UDP port
    - Network
  - Uses profiles in the SERVAUTH class
  - Allows grouping of network IP addresses into a "security zone" that you can protect as a RACF resource.

Network Security and Usability ...

- **Virtual Private Network "On-Demand" Tunnels**
  - Tunnel: An encrypted data pipe from one system to another
  - Before OS/390 V2R8: configured manually by the administrator
  - With OS/390 V2R8: dynamic configuration (key exchange) possible
    - clients could request creation of tunnel for data sent to OS/390
    - or administrator could manually create one for data sent from OS/390
  - New support: Policy can cause automatic creation of tunnels for data sent from OS/390, too.

z/OS R2 RACF Enhancements

UNIVERSAL Groups



- **Goal: You want to connect many (say, 10K) users to a group**
- **Problem: RACF limits you to 5957 users per group**
- **z/OS R2 solution: ADDGROUP xyz UNIVERSAL**
  - Can have an unlimited number of regular users (USE authority)
  - Limit of 5957 still applies to users with more privilege:
    - users with CREATE, CONNECT, or JOIN in the group
    - users with group-SPECIAL, group-OPERATIONS, or group-AUDITOR
  - Available only for ADDGROUP, not ALTGROUP

UNIVERSAL Groups...

- **CONNECT user1 GROUP(xyz) AUTH(use)**
  - updates user1 USER profile to show a connection to xyz.
  - does not update xyz GROUP profile.
- **LISTGRP xyz will not show the regular users**
  - they are not actually present in the GROUP profile
  - listing would be difficult to use given its size, anyway
  - for reporting, use IRRDBU00 output
- **LISTUSER user1 will show xyz as one of the user's groups**
- **RACROUTE REQUEST=VERIFY will include xyz in the ACEE**
  - access lists with xyz in them will work as you expect

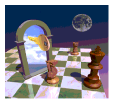
SAF Trace

- Provides tracing of RACROUTE, SAF callable service, and ICHEINTY requests to aid problem diagnosis
- Enabled via RACF subsystem SET TRACE command
- Can specify which requests to trace and which address spaces to trace
  - Example: SET TRACE(JOBNAME(xyz) RACROUTE(TYPE(1)))
    - will trace all RACROUTE REQUEST=AUTH from job xyz
  - SET TRACE(ASID(25) DATABASE(ALTER))
    - will trace all ICHEINTY ALTER, ADD, DELETE, RENAME from address space 25
- Trace goes to GTF, like other RACF SET TRACE output
- Use IPCS to read the trace, with the GTF USR command

Cross-System VLF Enhancement

- IRRACEE class in VLF helps improve performance by caching ACEEs for later reuse
- Problem: If system A and system B share the RACF database, a USER profile change from system A will purge all the cached ACEEs on system B
- Solution: Use XCF to communicate between z/OS R2 systems:
  - System A can tell system B exactly which ACEE changed
  - System B can purge just the changed ACEEs, not all of them
  - Requires RACF sysplex communications
- Does not help in all cases:
  - Group changes or port-of-entry changes could still cause purging
  - However: most purging comes from user profile changes

Coupling Facility Error Enhancement



- RACF Data Sharing mode uses Coupling Facility (CF) in a sysplex as a large data buffer
- Improves performance
- Problem: CF errors treated as RACF database I/O errors
  - Can cause ABENDs
  - Has caused problems like IMS subsystem failures
- Solution: In z/OS R2, if CF failure occurs, RACF will attempt to wait for a CF REBUILD operation to fix the problem, and retry the CF operation

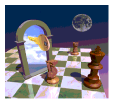
Other z/OS R2 Security Server Enhancements

z/OS R2 Network Authentication Service Enhancements

- **Supports three Kerberos encryption methods:**
  - DES (previously supported in R10)
  - Triple DES
  - DES with derivation keys
- **Supplies kpasswd and kadmin client commands to run on z/OS**
  - allows administration of foreign Kerberos realms.
- **Additional exploiters:**
  - LDAP server and client
  - FTP, TELNET, RSH

z/OS R2 LDAP Server Enhancements

- **Ability to manage USER->GROUP connections**
  - i.e. CONNECT command support
- **Support for LNOTES, NDS, and KERB segments for USER profiles**
- **Ability to search for a**
  - USER via UID
  - GROUP via GID
- **Support for authentication via Kerberos V5**

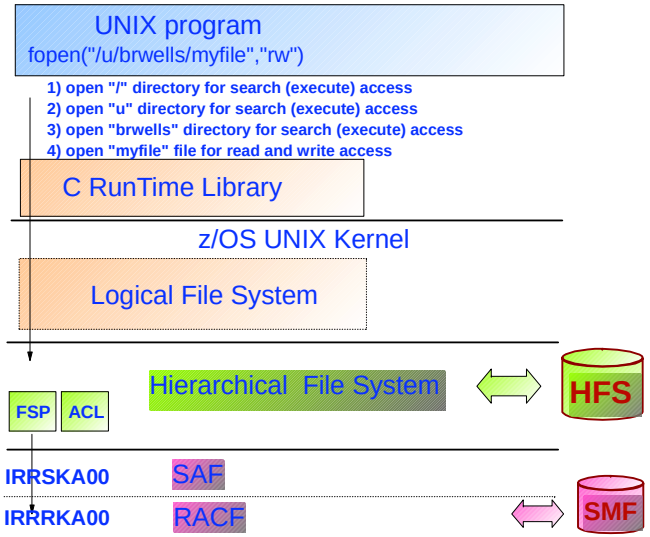


z/OS R3 RACF/SAF Enhancements: UNIX File Security Enhancements

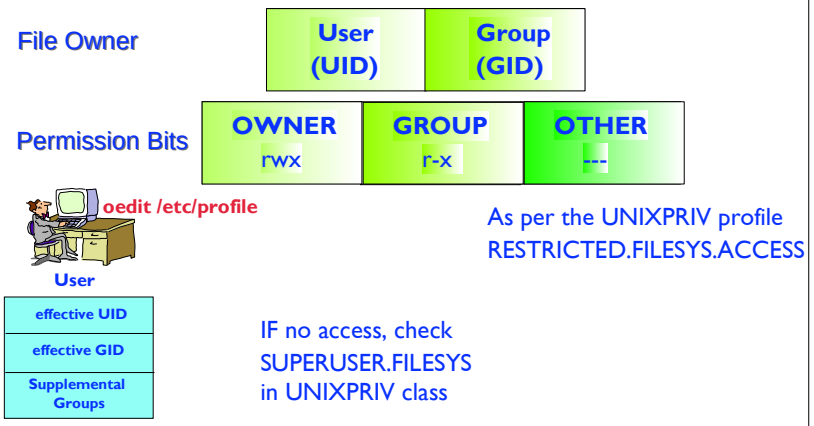
UNIX File Security

- **UNIX invokes RACF through SAF services**
- **No profiles in RACF database**
- **Access control by permission bits and (NEW) access control lists (ACLs)**
  - read, write, execute permissions (non-hierarchical)
  - POSIX-compliant 'owner', 'group', 'other' classes
  - ACL entries for individual users and groups
- **File security info stored with file in file system**
  - owning UID and GID
  - permission bits and ACLs
  - audit settings
  - extended attributes (APF, program-controlled, etc)

Access Checking Architecture

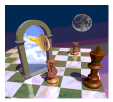


File Access Control with Permission Bits



See z/OS V1R3 Security Administrator's Guide Appendix F for detailed list of steps

Making the RESTRICTED attribute applicable to UNIX files



- **UNIX 'OTHER' bits analogous to RACF profile UACC**
  - but RESTRICTED attribute does not apply by default
- **Define RESTRICTED.FILESYS.ACCESS in the UNIXPRIV class with UACC(NONE)**
  - RESTRICTED applies to 'OTHER' bits system-wide
- **For exceptions, permit RESTRICTED user with READ access**
  - This does **not** grant access to the file (that's what an ACL is for), it just allows the 'OTHER' bits to be checked

Access Control Lists (ACLs)

- **Loosely based on the POSIX draft (never adopted)**
  - similar to the Solaris implementation
- **Contained within the file system**
  - file security is portable
- **Enabled with SETROPTS CLASSACT(FSSEC)**
  - Can be defined prior to activating FSSEC
- **Deleted automatically with file**
  - even on downlevel systems

Access Control Lists (ACLs) ...

- **Are displayed with the getfacl UNIX command and created, modified, and deleted with the setfacl UNIX command**
  - Must be UID(0), file owner, or have READ access to UNIXPRIV profile SUPERUSER.FILESYS.CHANGEPERMS
- **Can contain a maximum of 1024 entries**
  - an entry consists of a type (user or group) and identifier (UID or GID) and permissions (read, write, and execute)
- **Support inheritance**

File Access Control with Permission Bits and ACLs

Permission Bits

	OWNER rwx	GROUP rwx	OTHER rwx
ACL consistsol	User1 rwx	Group1 rwx	
	User2 rwx	Group2 rwx	
	Usern rwx	Groupn rwx	

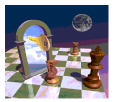
As per UNIXPRIV profile RESTRICTED.FILESYS.ACCESS

IF no access, check SUPERUSER.FILESYS or SUPERUSER.FILESYS.ACLOVERRIDE

IF FSSEC class active

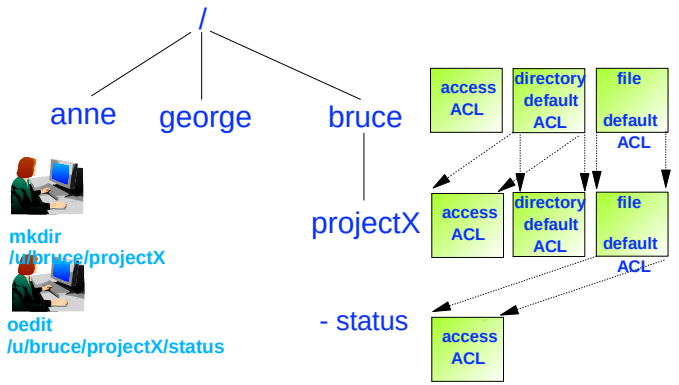
See z/OS V1R3 Security Administrator's Guide Appendix F for detailed list of steps

ACL Inheritance



- Can establish default (or 'model') ACLs on a directory
- Get automatically applied to new files/directories created within the directory
- Separate default used for files and subdirectories
- Reduces administrative overhead

ACL Inheritance ...

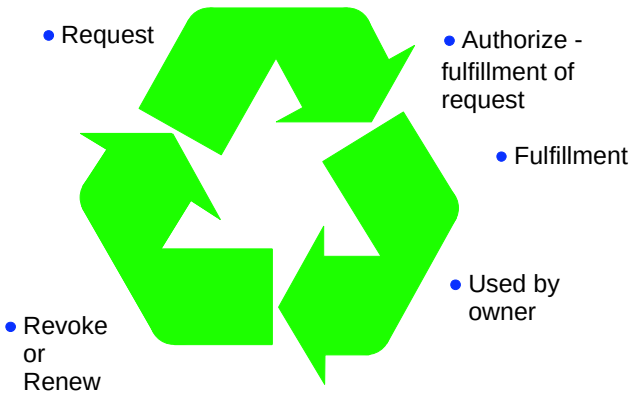


z/OS R3 PKI Services

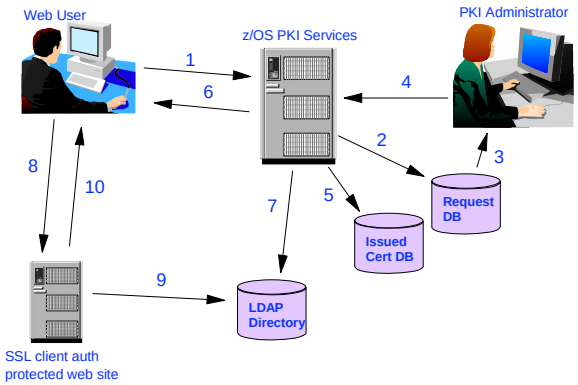
Introduction

- **What is PKI Services?**
  - New component of the z/OS Security Server
    - Always enabled but closely tied to RACF
  - Complete Certificate Authority (CA) package
    - Full certificate life cycle management
      - ✓User request driven via customizable web pages
    - Browser or server certificates
      - ✓Automatic or administrator approval process
    - Administered using same web interface
      - ✓End user / administrator revocation process
  - Manual - "z/OS Security Server PKI Services Guide and Reference"

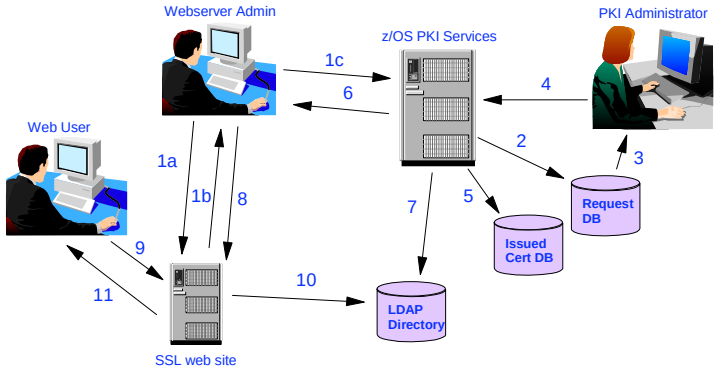
Certificate Life Cycle



Browser Certificates



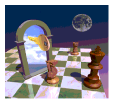
Server Certificates



z/OS PKI Services Architecture

- **HTTP Server**
  - Provides browser/CGI interface for end-users and administrators
    - Web page logic defined in certificate templates file
    - CGIs - Read template file, control flow
      - ✓Optional customer provided exit - pkiexit
      - ✓Invoke z/OS PKI Services through SAF interface R_PKIServ
- **R_PKIServ - SAF callable service backed by RACF (or other)**
  - End-user functions - Request, retrieve, verify, revoke, or renew a certificate
  - Administrator functions - Query, approve, modify, or reject certificate requests, query and revoke issued certificates
  - Interface to call PKI Services
  - SMF auditing
- **PKI Services Daemon**
  - Services threads for incoming requests
  - Background threads for certificate/certificate revocation list (CRL) issuance
  - VSAM DBs for requests (ObjectStore) and issued certificate list (ICL)

z/OS PKI Services Architecture...

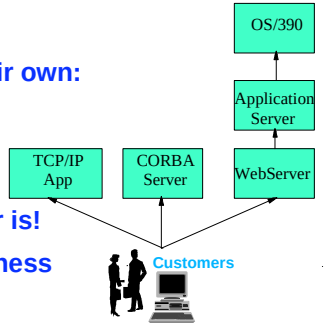


- **Open Cryptographic Services Facility (OCSF) and Open Cryptographic Enhanced Plug-ins (OCEP)**
  - Provided the crypto facilities for PKI Services
    - OCEP - Access to CA certificate and private key in RACF
    - OCSF - BSAFE or ICSF (Hardware) crypto engines
- **LDAP Directory**
  - Publication of issued certificates and CRLs

z/OS R3 RACF/SAF Enhancements: Support for Policy Director Authorization Services for z/OS and OS/390

Tivoli Access Manager for e-business

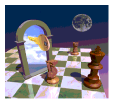
- **Distributed applications have their own:**
  - Security administration tools
  - Authentication models
  - Authorization policies
- **Do not agree on who a given user is!**
- **Tivoli Access Manager for e-business (formerly Policy Director)**
  - Unites core technologies around common security policies
  - Addresses inability to implement security policies across multiple distributed platforms



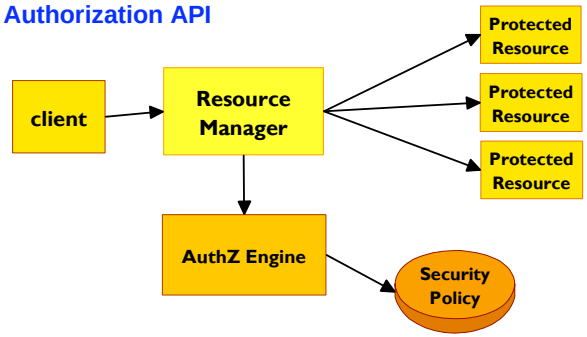
What does Tivoli Access Manager do?

- **Maintains a central user registry**
  - Users and groups (LDAP)
  - Authentication information
- **Maintains a model of the Protected Objectspace**
  - Hierarchically organized
- **Defines permitted actions on objects**
  - Uses Access Control List templates
  - ACL represents relationship between user or group of users and some resource
  - ACLs are attached to entries in objectspace
- **Provides an API for making authorization queries**
  - And provides exploiting applications (NetSEAL, WebSEAL, PD for MQ Series)

Application Structure



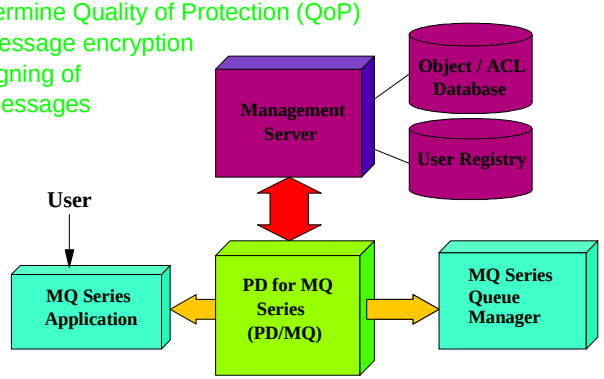
- **The Authorization API**



For example...

Security policy can be used to

- Control access to queues
- Determine Quality of Protection (QoP)
  - message encryption
  - signing of messages



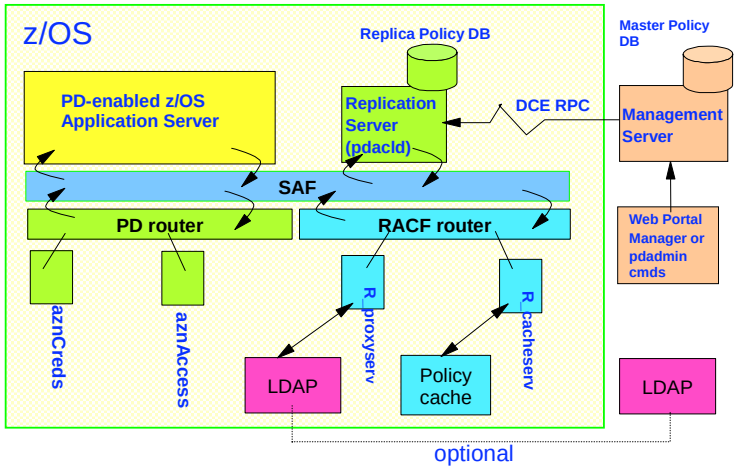
Tivoli Access Manager Summary

- A distributed e-business security solution
- Provides a mechanism for defining common security policy
- Provides a standardized interface for applications to determine user authorization rights to resources
- Supports many different operating system platforms
- Has an extendable model
- Also provides out-of-the-box solutions (WebSEAL, NetSEAL, PD for MQ Series ...)

IBM Policy Director Authorization Services for z/OS and OS/390

- Provides support for use of Tivoli Access Manager by applications on z/OS and OS/390
  - Runs on OS/390 V2R10 and z/OS V1R1 or later
  - Independent product, free to current licensees of z/OS and OS/390
- Allows z/OS and OS/390 to plug-and-play in an existing Tivoli Access Manager secure domain
- Provides local replica of policy data
- PD applications invoke new SAF services for authorization decisions

Components



RACF Enhancements for PDAS

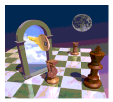
- Support for OS/390 V2R10 and z/OS V1R2 provided by APAR OW49959/OW49960
  - R_cacheserv for management of the local policy cache
  - R_proxyserv for extract of User registry information from LDAP
- The RACF database can be used for harden and restore of the Policy Director Authorization Services local policy cache
- The RACF SMF Unload utility will unload Policy Director Authorization Services SMF audit records
- SAF trace support includes not only R_cacheserv and R_proxyserv, but also aznCreds and aznAccess

z/OS R4 Security Server Enhancements

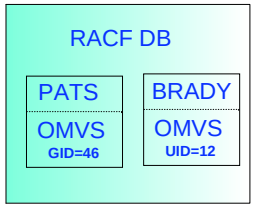
Prevention of shared UID/GID

- New SHARED.IDS profile in the UNIXPRIV class
- Acts as a system-wide switch to prevent assignment of an ID which is already in use
- No generic characters allowed in name: discrete profile name must be used
- Requires AIM stage 2 or 3
- Does not affect pre-existing shared IDs
  - Customer must clean those up separately, if desired
    - Not a pre-req for using the new support
  - Can use IRRICE report to find shared UIDs
    - Can modify this report to find shared GIDs

Prevention of shared IDs ... Example



- RDEFINE UNIXPRIV SHARED.IDS UACC(NONE)
- SETROPTS RACLIST(UNIXPRIV) REFRESH
- ADDUSER MARCY OMVS(UID(12))
- ADDGROUP ADK OMVS(GID(46))



IRR52174I Incorrect UID 12. This value is already in use by BRADY.

IRR52174I Incorrect GID 46. This value is already in use by PATS.

Prevention of shared IDs ... SHARED keyword

- There are valid reasons to assign a non-unique UID/GID
  - E.G. Assigning UID(0) to started task user IDS
- Do so using the new SHARED keyword in the OMVS segment of the ADDUSER, ALTUSER, ADDGROUP, and ALTGROUP commands
- SHARED requires SPECIAL, or at least READ authority to SHARED.IDS
  - Profile level audit settings can be used to log successes and failures to SHARED.IDS

SEARCH enhancement to map UIDs and GIDs

- SEARCH CLASS(USER) UID(0)
  - OMVSKERN
  - BPXOINIT
  - SUPERGUY
- SEARCH CLASS(GROUP) GID(99)
  - RACFDEV
- SEARCH CLASS(USER) UID(1234567)

ICH31005I NO ENTRIES MEET SEARCH CRITERIA

Automatic UID/GID Assignment

- New AUTOUID keyword in the OMVS segment of the ADDUSER and ALTUSER commands
- New AUTOGID keyword in the OMVS segment of the ADDGROUP and ALTGROUP commands
- Derived values are guaranteed to be unique

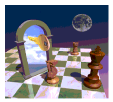
ADDUSER MELVILLE OMVS(AUTOUID)

IRR52177I User MELVILLE was assigned an OMVS UID value of 4646.

ADDGROUP WHALES OMVS(AUTOGID)

IRR52177I Group WHALES was assigned an OMVS GID value of 105.

Automatic UID/GID Assignment ... BPX.NEXT.USER



- Uses APPLDATA of new BPX.NEXT.USER profile in the FACILITY class to derive candidate UID/GID values
- APPLDATA consists of 2 qualifiers separated by a forward slash ('/')
  - left qualifier specifies starting UID value, or range of UID values
  - right qualifier specifies starting GID value, or range of GID values
  - qualifiers can be null, or specified as 'NOAUTO', to prevent automatic assignment of UIDs or GIDs

Obtaining this new function

- All of this new function is available on OS/390 V2R10 through z/OS V1R3 via APAR OW52135
  - PTF UW89970 (OS/390 V2R10, z/OS R1)
  - PTF UW89971 (z/OS R2)
  - PTF UW89972 (z/OS R3)
- RACF ISPF Panels **NOT** updated via these PTFs
- Full function (including panels) available in z/OS R4
- For more information:
  - RACF Home Page What's New section
    - http://www.ibm.com/servers/eserver/zseries/zos/racf/whatsnew.html
  - z/OS R4 books

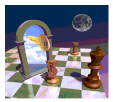
z/OS R4 UNIX File Group-Ownership

- **UNIX Files have an owner (UID) and an owning group (GID)**
- **Previously owning group inherited from directory**
- **Can now choose:**
  - Assign from owning group of directory, as before
  - Assign from effective GID of user creating the file
- **RDEFINE UNIXPRIV FILE.GROUPOWNER.SETGID**
  - Directory set-gid on: assign from directory
  - Directory set-gid off: assign from user

z/OS R4 Basic PADS Usability / Security

- **PADS Usability & Security Improvement**
- **Suppose:**
  - User runs program ABC
  - You want to allow READ to ABC.DATA from program ABC
  - However, ABC invokes ABC2, and ABC2 does the OPEN
- **Previously:**
  - RDEFINE PROGRAM ABC* ADDMEM('ABC.LINKLIB'//NOPADCHK)
  - PERMIT ABC.DATA ID(*) ACCESS(READ) WHEN(PROGRAM(ABC2))

z/OS R4 Basic PADS Usability / Security...



- **New alternative:**
  - RDEFINE PROGRAM ABC* ADDMEM('ABC.LINKLIB'//NOPADCHK)
  - PERMIT 'ABC.DATA' ID(*) ACCESS(READ) WHEN(PROGRAM(ABC))
- **Better Usability**
  - Administrator needs less knowledge about application structure
  - Less chance for error
- **Better security**
  - PERMIT 'SYS1.LINKLIB' ID(SYSPROG) ACCESS(UPDATE) WHEN(PROGRAM(GIMSMP))

z/OS R4 Program Security Modes

- **Two modes of operation**
  - BASIC (original/default)
  - ENHANCED (better security)
    - PADS and EXECUTE work only from programs defined as MAIN
- **RDEFINE FACILITY IRR.PGMSECURITY**
  - APPLDATA('BASIC') --> BASIC mode
  - APPLDATA('ENHANCED') --> ENHANCED mode
  - Other values --> ENHANCED-WARNING mode
- **Three types of programs**
  - MAIN RDEF PROGRAM xyz ... APPLDATA('MAIN')
  - BASIC RDEF PROGRAM xyz ... APPLDATA('BASIC')
  - normal RDEF PROGRAM xyz ...
- **You still need to keep environment clean!**

z/OS R4 Program Security Modes...

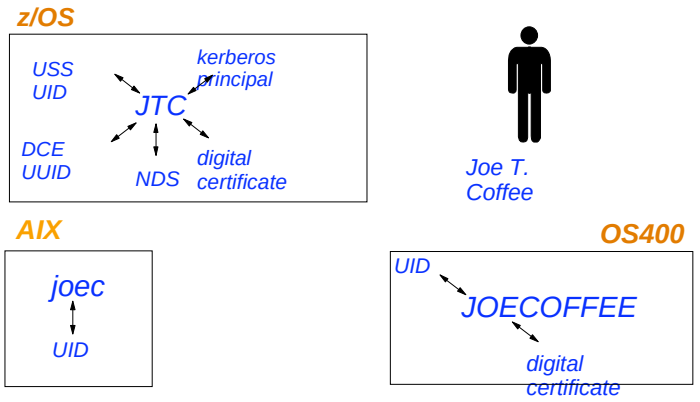
- **Consider: // EXEC PGM=AAA**
  TSOEXEC AAA
  - AAA then OPENs AAA.DATA, and you want to use PADS to allow this access;
    or
  - AAA calls AAA2, and AAA2 OPENs AAA.DATA and you want to use PADS
- **If running in ENHANCED mode, this will work only if**
  - you define AAA as MAIN:
    - RDEFINE PROGRAM AAA ADDMEM('library.name'//NOPADCHK) APPLDATA('MAIN')
      or
  - you define AAA or AAA2 as BASIC:
    - RDEFINE PROGRAM AAA ADDMEM('library.name'//NOPADCHK) APPLDATA('BASIC')
- **Provides better security and safety from malicious users**

z/OS R4 Program Security Modes...

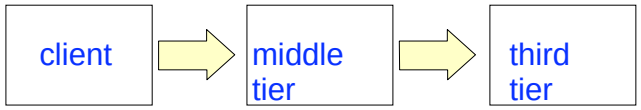
- **Consider: TSO command AAA, invoked at READY or within ISPF, or via TSO/E CALL command**
  - AAA then OPENs AAA.DATA, and you want to use PADS to allow this access;
- **If running in ENHANCED mode, this will work only if**
  - you define AAA as BASIC:
    - RDEFINE PROGRAM AAA ADDMEM('library.name'//NOPADCHK) APPLDATA('BASIC')
      or
  - AAA runs APF-authorized or via TSOEXEC and you define it as either BASIC or MAIN (preferred)

z/OS R4 Enterprise Identity Mapping (EIM) Support

Enterprise User Problems



Enterprise User Problems



jcoffee/admin@k390.ibm.com

The Enterprise User Problems

- **Many userids represent an enterprise user**
  - operating systems with different registries
  - application specific user identification schemes
  - distributed technologies for user identification
- **System/application specific authorization mechanisms**
- **Managing the enterprise user**
  - creating / changing / deleting
  - auditing a user's activity

z/OS R4 Enterprise Identity Mapping (EIM) Support

- **New eServer cross-platform initiative**
- **Infrastructure component**
  - New services and API (C/C++)
  - LDAP extensions
- **Allows development of servers and administrative applications to**
  - Transform user IDs as work flows across systems
  - Administer multi-system, cross-platform ID mappings
- **EIM provides a foundation to solve the Enterprise User problems**
- **RACF support in z/OS R4: new EIM segment, new LDAPBIND class**

z/OS R4 Network Authentication Service (Kerberos) Extensions

- Support for IPV6 Network Addressing
- NDBM Support
  - Supports KDC database in UNIX file system instead of RACF database
  - Better interoperability with other platforms
    - remote administration via kadmin
    - database propagation
  - However:
    - May not scale as well as RACF database configuration for large numbers of users
    - SYSPLEX support not as robust
    - May require administering users in both RACF and NDBM

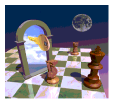
z/OS R4 PKISERV Enhancements

- **email Notification For**
  - Completed Certificate Requests
  - Certificate Expiration Warnings
- **MAIL, STREET, POSTALCODE qualifiers for DNs**
- **Support for PKCS#7 Certificate Chains**
- **Use PCI Crypto Coprocessor to generate key pairs**

z/OS R4 LDAP Server Enhancements

- **New authentication methods:**
  - CRAM-MD5
  - DIGEST-MD5
- **SSL V3 and TLS V1 support**
  - including support for conversations that start unprotected and then switch to SSL/TLS protection
- **TDBM ACL enhancements**
  - attribute-level access control
  - ability to explicitly deny access to information
- **TDBM Modify DN support, including subtree relocation**
- **Server Activity Logging**
- **Removal of RDBM; only TDBM and SDBM supported**

z/OS R4 Firewall Technologies Enhancements



- **SYSPLEX support for Dynamic VIPA**
  - DVIPA a.b.c.d on System A
  - a.b.c.d moved to System B
  - Firewall ISAKMP server will recognize this and
  - Move Security Association (SA) from A to B and
  - Renegotiate tunnel with remote server

z/OS R4 System SSL

- **Added AES cipher support for SSL V3 and TLS V1**
- **IPV6 Network Address Support**
- **CRL Caching in storage for improved performance**
- **SYSPLEX SSL/TLS Session Cache**
  - **allows session takeover on another system**
- **RACF keyring enhancements**
  - **private key storage in ICSF**
  - **applications can be allowed to use other user's keyrings**
- **New APIs**
  - **Build/manage key database (like gskkyman does)**
  - **use kdb or keyring certificates for non-SSL purposes**
  - **build/process PKCS#7 messages for application communication**
  - **gskkyman ehancements for**
    - **export/import of PKCS#12 V3 and PKCS#7 certificates**
    - **creation of Digital Signature Standard certificates (FIPS 186-1)**
    - **modification of certificate labels**

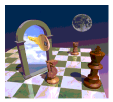
Reminder!

Additional Information

Reminder: Service End Dates

- **Already out of service:**
  - All OS/390 Releases below V2R9
- **March 31, 2003:**
  - OS/390 V2R9

IBM Manuals



- **On the web, in either PDF or Book Manager formats:**
  - Security Server for OS/390 V2R10:
    - http://publibz.boulder.ibm.com/cgi-bin/bookmgr_OS390/Shelves/ICH1K132
  - Security Server for z/OS R3:
    - http://publibz.boulder.ibm.com/cgi-bin/bookmgr_OS390/Shelves/ICHZBK20
  - OS/390 library:
    http://www.ibm.com/servers/s390/os390/bkserv/index.html
  - z/OS library: http://www.ibm.com/servers/eserver/zseries/zos/bkserv/
  - General Site:
    http://publibfp.boulder.ibm.com/cgi-bin/bookmgr/LIBRARY
- **Redbooks:**
  - http://www.ibm.com/redbooks

RACF Home Page

- **http://www.ibm.com/servers/eserver/zseries/zos/racf/**
  - Latest release information on RACF
  - Links to announcement letters
  - Sample code
  - Frequently Asked Questions
  - RACF user group information
  - RACF-L information
  - Presentations on RACF-related topics

OS/390 Security Home Page

- **http://www.ibm.com/servers/eserver/zseries/zos/security**
  - Overview of security concepts, including animations
  - Overview of S/390, zSeries, OS/390, and z/OS security functions
  - Links to related web sites for OS/390 and z/OS components