Security Update for z/OS V2R2

Jan Tits
IBM systems
jantits@be.ibm.com

Trademarks

The following are trademarks of the International Business Machines Corporation in the United States and/or other countries.

AIX*	Domino*	Language Environment*	SYSREXX	z10
BladeCenter*	DS6000	MVS	System Storage	z10 BC
BookManager*	DS8000*	Parallel Sysplex*	System x*	z10 EC
CICS*	FICON*	ProductPac*	System z	zEnterprise*
DataPower*	IBM*	RACF*	System z9	zSeries*
DB2*	IBM eServer	Redbooks*	System z10	
DFSMS	IBM logo*	REXX	System z10 Business Class	
DFSMSdss	IMS	RMF	Tivoli*	
DFSMShsm	InfinBand	ServerPac*	WebSphere*	
DFSMSrmm				
DFSORT				

* Registered trademarks of IBM Corporation

The following are trademarks or registered trademarks of other companies.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Windows Server and the Windows logo are trademarks of the Microsoft group of countries.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java and all Java based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

* Other product and service names might be trademarks of IBM or other companies.

Notes:

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

This information provides only general descriptions of the types and portions of workloads that are eligible for execution on Specialty Engines (e.g, zIIPs, zAAPs, and IFLs) ("SEs"). IBM authorizes customers to use IBM SE only to execute the processing of Eligible Workloads of specific Programs expressly authorized by IBM as specified in the “Authorized Use Table for IBM Machines” provided at www.ibm.com/systems/support/machine_warranties/machine_code/aut.html (“AUT”). No other workload processing is authorized for execution on an SE. IBM offers SE at a lower price than General Processors/Central Processors because customers are authorized to use SEs only to process certain types and/or amounts of workloads as specified by IBM in the AUT.

Agenda

- **Digital certificate related Enhancements**
  - RACDCERT granularity
  - PKI multiple approvers
  - Kerberos PKINIT
  - System SSL
- **RACF Enhancements**
  - Read-Only Auditor
  - RRSF Enhancements
  - IRRDBU00 authority change
  - Password Enhancements (In a separate session)
  - Health checks
  - Enhancements for z/OS UNIX
- **ICSF Enhancements**
  - Combined callable service
  - PIN method enhancement
- **SMF Enhancements**
  - Record Signing
  - New record for Callable service
- **Security Portal**

Digital Certificate related Enhancements

RACDCERT Granular Authority

- **RACF RACDCERT functions are used to manage certificates and key rings**
- **Currently, the authority to issue RACDCERT commands is controlled using profiles in the FACILITY class with resources named** `IRR.DIGTCERT.<racdcert function>`
  - READ authority allows you to act on your own certificate or key ring
  - UPDATE allows you to act on the certificate of another user
  - CONTROL allows you to act on a CERTAUTH or SITE resource
- **The control is based on the function performed and the owner, not to the level of individual certificate or key ring**

RACDCERT Granular Authority

- **New model is to provide granular control based on certificate label or key ring name, besides function and owner using the RDATALIB class**
  - `IRR.DIGTCERT.<cert owner>.<cert label>.UPD.<racdcert cert function>`

    Note: LST may be applicable to some functions
  - `<ring owner>.<ring name>.UPD.<racdcert ring function>`
- **Granular control is turned on by the presence of the profile IRR.RACDCERT.GRANULAR in the RDATALIB class, otherwise fall back to original way using the FACILITY class profile**
- **Applies to 13 RACDCERT functions only, including GENCERT, ADD, ADDRING, CONNECT…**
- **Only one level of access – READ**
- **Example: AdminA can generate a certificate for FTPID with label FTPSERVER if he has READ access to**

  `IRR.DIGTCERT.FTPID.FTPSERVER.UPD.GENCERT`

PKI Services: Multiple Administrative Approvals

- **PKI Services provides Certificate Authority functions for enterprises to host their own CA**
- **PKI Services supports both automatic approval mode and administrator approval mode**
- **In the administrator approval mode, only one administrator is required to approve the requests**
- **Some government agencies require all PKI products to have an "NxM" authentication factor**
  - For example, two PKI administrators have to validate a request before issuing the certificate
- **PKI Services will now allow the administrator approval mode to support multiple number of approvers**
- **A configuration option with be provided in the CGI templates file and JSP templates xml file to set the number of administrators required to approve a certificate request**
  - The option will be provided on a per template basis
  - A change of the configured number of approvers will not affect the existing certificate requests, only affect the new requests

PKI Services: OCSP

- Online Certificate Status Protocol (OCSP) is used to get revocation status of certificates. Intended to validate certificates used for SSL and TLS
- OCSP requires server responses to be signed but does not specify a mechanism for selecting the signing algorithm to be used
- Prior to z/OS V2.2, z/OS PKI Services could only use the same signing algorithm used for certificate and Certificate Revocation List (CRL) signing specified in the configuration file to sign the OCSP response
- PKI Services can now sign the OCSP response with the client specified signing algorithm through an extension in the request in the way documented by RFC6227

System SSL: OCSP

- System SSL provides the set of functions for secure communication required by other components running on z/OS
- Certificate validation involves checking of the certificate status. There are two ways. Before V2R2, System SSL only provides the Certificate Revocation List checking mechanism.
- In this release, System SSL retrieves revocation status information for x.509 certificates as described by RFC 2560, RFC 3280 and 5280
- Enable other components like Communications Server, HTTP server, Kerberos applications to check certificate status using SSL/TLS protocol

System SSL: Secure key and interoperability

- Support for the secure key functions available with CEX4 and later crypto features on zEC12 and later processors when configured in EP11 mode
- Supporting secure DSA keys for signing
- To establish the SSL/TLS protocol, both the server and the client need to have a collection of keys and certificates.
  - Examples of this collection are RACF key rings, gskkyman key database, ICSF tokens.
  - In this release System supports PKCS #12 file as a key store database, which is commonly used by Java-based applications
- Allow SSL sessions to be reused across different TCP ports

NAS (Kerberos): PKINIT support and UID 0 removal

- Network Authentication Service is a distributed authentication service that allows user authentication over a physically untrusted network by using tickets issued by a mutually trusted authentication server
- The ticket is encrypted by a secret key which is typically derived from the client's password
- Instead of using password, digital certificate is used to obtain the initial ticket as specified by RFC 4556
- Another enhancement is to lift the requirement of using UID 0 for the Kerberos started task

RACF Enhancements

Read-Only Auditor

- **The read-only auditor (ROAUDIT) user attribute grants the user the ability to perform all of the activities of a user with the AUDITOR attribute except the ability to:**
  - Change profile content (such as AUDIT/GLOBALAUDIT settings)
  - Change system logging options
- **Suitable for use by an external auditor who may need to verify the current security state of a system**
- **Assigned to users with the ADDUSER and ALTUSER commands**
- **If ROAUDIT and AUDITOR are set, AUDITOR attribute takes precedence**

RRSF: Dynamic Main Switching

- **RACF's Remote Sharing Facility (RRSF) allows you to manage remote RACF databases from anywhere in the RRSF network**
- **RRSF system consists of nodes**
  - **Single System Node** – one system, one RACF DB
  - **Multi System Node** – a set of systems sharing one RACF DB
    - **MAIN system –** communicator to the other nodes
    - **Peer systems –** can only communicate to the MAIN system of the other nodes
- **Switching the MAIN system in a multi system node is a challenging "11"-step manual processes that is not feasible for short-term changes**
- **RRSF Dynamic Main Switching allows you to replace this complicated process with a single command**
  - Allows you to avoid even minor outage windows
  - Allows you to move RRSF workload off of a busy system
  - New programming interfaces introduce possibility of automating the switch entirely

RRSF: Unidirectional Connections

- **When two systems are connected using RRSF, it is impossible to prevent a privileged user on one system from escalating his privilege on the other system.**
  - This issue is worsen if one system is a “test” system
- **With Unidirectional RRSF connections, one RRSF node can define another RRSF node such that inbound requests from that node are denied**
  - This can help protect against accidental or malicious damage to your production system
  - You can demonstrate to an auditor your compliance with your security policy, regardless of the configuration established on the remote node

RRSF: Unidirectional Connections

- **The DENYINBOUND keyword on the TARGET command is used to reject commands from the specified node:**

```
TARGET NODE(thatnode) DENYINBOUND
```

- **When the remote node is a multi system node:**

```
TARGET NODE(thatnode) SYSNAME(*) DENYINBOUND
```

- **To change your mind, use ALLOWINBOUND.**
  - This is the default, so you don't need to code it in the parameter library
- **DENYINBOUND is ignored if specified for the LOCAL node**

IRRDBU00: Require only READ Authority

- IRRDBU00 is a utility to unload the RACF database
- Since its inception, IRRDBU00 has required UPDATE authority to the RACF data set(s) which are used as input
- With V2.2, if you specify PARM=NOLOCKINPUT, only READ authority is required

RACF Health Checks related to Password enhancements

- **RACF_ENCRYPTION_ALGORITHM, which raises an exception if "weak" (less 'secure' than DES) encryption is allowed for logon passwords**
  - Having no ICHDEX01 is considered an exception as the absence of ICHDEX01 allows masked passwords
- **RACF_PASSWORD_CONTROLS, which raises an exception if:**
  - Mixed case passwords are not in effect or
  - The maximum number of consecutive failed logon attempts is greater than 3 or
  - A password/password phrase can be valid for more than 90 days

z/OS UNIX: Authority just for Search

- **When opening a file in the z/OS UNIX directory, the user must have READ and SEARCH authority on all directories in the path to the file**
  - Even if the user has an administrative authority such as SUPERUSER.FILESYS.CHANGEPERMS
  - Many installations have just granted those users a higher-than-desired authority such as AUDITOR or SUPERUSER.FILESYS
- **READ authority to the resource SUPERUSER.FILESYS.DIRSRCH in the UNIXPRIV class grants the user read and search permissions on z/OS UNIX directories**
  - Does not grant read, write, or execute permission to ordinary z/OS UNIX files
  - Does not grant write permission to z/OS UNIX directories
  - Generic profiles are supported

z/OS UNIX: File Execution Control

- **Using profiles in the new FSEXEC class, installations can prevent the execution of files within the file system**
  - Profile name must match the FILESYSTEM name (not the MOUNTPOINT) specified on the MOUNT statement
  - Generic profiles are supported
  - Useful for file system that is mounted for temporary directories such as /tmp where any user can write files
  - UPDATE access is required
  - SUPERUSER or AUDITOR does not override FSEXEC denial of access
- **Example:**

```
RDEFINE FSEXEC OMVS.ZFS.ADMIN.** UACC(NONE)
PERMIT OMVS.ZFS.ADMIN.** CLASS(FSEXEC) ID(FRED) ACC(UPDATE)
```

ICSF Enhancements

New ICSF callable services for simplification

- As financial institutions migrate to the use of IC (Integrated Chip) cards, payment system applications are being developed using the EMV (Europay, MasterCard, and Visa) standard
- Although ICSF supports all the encryption primitives necessary for EMV based applications, there is added complexity using native CCA services to implement EMV encryption techniques
- ICSF will provide a new set of callable services tuned to the EMV standard to ease the development and migration of payment systems to the use of IC cards

PIN method improvements

- **Enhancement to provide additional support for the German Banking Industry Committee (Deutsche Kreditwirtschaft (DK)) PIN method**
  - Use AES keys to manage card and account data
  - New callable service to manage PINs, card data and account data
    - CSNBDMP and CSNEDMP
    - generates a PIN and PIN reference value (PRW) for an existing ISO-1 PIN block
  - Provide a service to migrate ISO-1 format PIN blocks to DK PIN block

Misc supports

- Provide support for the TKE workstation to loaded HMAC keys and for ICSF to import them into the CKDS using Operational Key Load
- Provide an option to allow customers to specify the number of digits of the master key verification patterns to display on the Hardware Status panel for auditing purpose
- Provide a new display on the Domain Role panel that shows the access control name and its offset

Console Support (WD#15)

- **Enables customers to perform certain administrative tasks from z/OS operator console rather than using ISPF panels**
- **Two new operator commands: "DISPLAY ICSF" and "SETICSF“**
  - Activate, deactivate, and restart cryptographic devices
  - Enable and disable I/O updates to Key Datasets (KDS)
  - Set and display certain ICSF installation options
  - Display status for ICSF cryptographic devices
  - Display master key status for each cryptographic device
  - Display information related to KDSes
  - List sysplex members who can participate in sysplex-scope commands

SMF Enhancements

Sign SMF Records

- System Management Facility (SMF) provides logging services for z/OS
- SMF records contain critical information about an enterprise and are archived for long durations and they are generally shared among various departments for a number of activities
- There is no built in protection of the SMF data
- Idea is to make SMF a fully-trusted repository of audit data using digital signature
- SMF data is signed on the way to the System Logger
- Calls ICSF PKCS#11 functions to generate key pair
- Enable through the new SMF configuration option RECSIGN

```
RECSIGN(HASH(SHA512),SIGNATURE(RSA),
TOKENNAME(TAMPER#RESISTANT#SMF#TOKEN#NAME1))
```

- The log stream (IFASMFDL) and dataset (IFASMFDP) dump programs are enhanced to handle the signed records

```
SIGVALIDATE(HASH(SHA512),
TOKENNAME(TAMPER#RESISTANT#SMF#TOKEN#NAME1))
```

Create SMF Records for BCPii Callable Service

- Two BPCii callable services HWICMD and HWISET are identified as the services that can affect significant impact on a customers installation
- Need a way to audit any changes to the system through these callable services
- New SMF record type 106 is created with 2 subtypes:
  - Subtype 1 – for HWISET
  - Sybtype 2 – for HWICMD

System z Security Portal

- IBM recommends that you promptly install security and integrity PTFs
- SECINT PTFs are included in RSUs periodically
- The System z Security Portal can help you stay more current with SECINT PTFs by providing SMP/E HOLDDATA you can use to identify these fixes before they are marked RSU
- The System z Security Portal also provides associated Common Vulnerability Scoring System (CVSS) V2 ratings for new APARs*
- To get this information you must register!
  - Because widespread specifics about a vulnerability could increase the likelihood that an attacker could successfully exploit it
  - In response to customer requests to maintain the confidentiality
- IBM recommends that you to register to the System z Security Portal site

Helpful Publications on the enhancements

- SA23-2290 - z/OS Security Server RACF Callable Services
- SA23-2292 - z/OS Security Server RACF Command Language Reference
- SA23-2289 - z/OS Security Server RACF Security Administrator's Guide
- SA23-2286 - z/OS Cryptographic Services PKI Services Guide and Reference
- SC14-7495 - z/OS Cryptographic Services System SSL Programming
- SC23-6786 - z/OS Integrated Security Services Network Authentication Service Administration
- SC23-6787 - z/OS Integrated Security Services Network Authentication Service Programming
- SA23-2231 - z/OS ICSF Writing PKCS #11 Applications
- SC14-7506 - ICSF Administrator's Guide
- SC14-7507 - ICSF System Programmer's Guide
- SC14-7508 - ICSF Application Programmer's Guide
- SA23-6843 - IBM Health Checker for z/OS User's Guide
- SA38-0667 - z/OS MVS System Management Facilities (SMF)