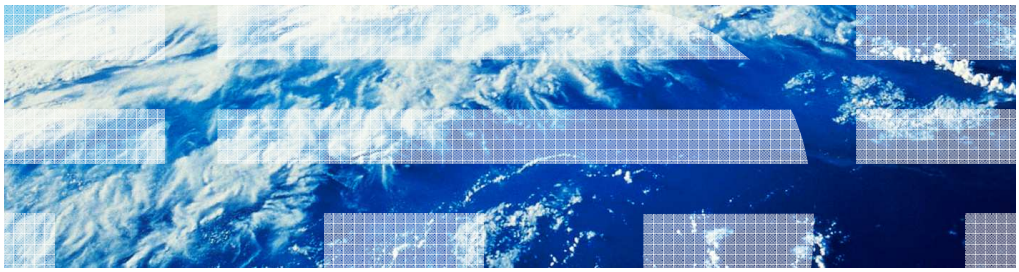
z/OS V1R13

RACF: ID Propagation 2



Session objectives

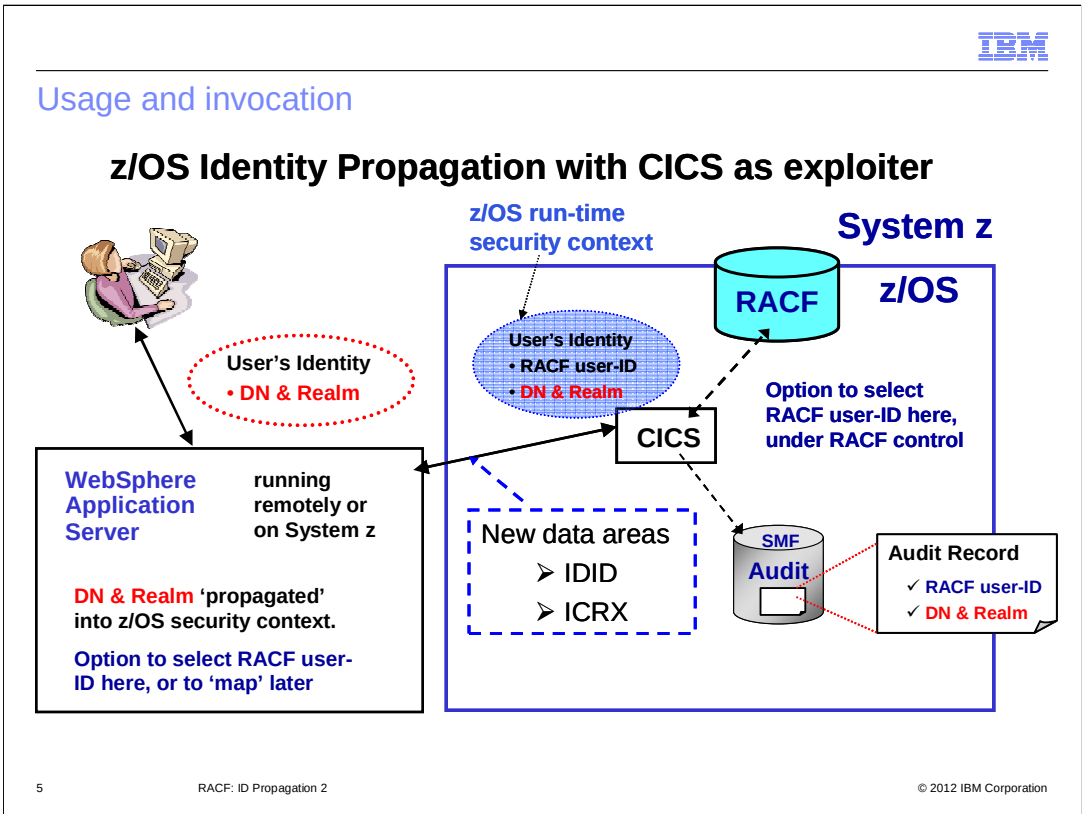
- Describe function and value of new support - ID Propagation 2.
- Describe how this function is implemented and how to exploit it.
- List considerations when implementing support.

Overview (1 of 2)

- Problem Statement / Need Addressed
  - In z/OS V1R11 RACF introduced a new function, z/OS Identity Propagation, to address the lack of end-to-end security identity consistency and auditing by our primary Internet business products. The objective of that function was to provide "*consistent end-to-end auditing of z/OS transactions that originate from the Internet by maintaining the user's distributed identity information, without impacting the performance characteristics of transaction providers.*"
- Solution
  - This line item extends this support by implementing enhancements that are needed/required by exploiters of the RACF support for z/OS Identity Propagation.
- Benefit / Value
  - End-to-end security identity consistency and auditing.

Overview (2 of 2)

- The enhancements implemented as follow-on to the z/OS Identity Propagation function introduced in z/OS V1R11 are the following:
  - Modified the R_usermap callable service to provide a query service invoked via the callable interface which will take a Distinguished Name (DN) and a Registry/Realm Name and return the matching RACF user ID.
  - Modified the RACMAP command to provide a query function for the which will use the UserDIDfilter Name and Registry Name to return the matching RACF user ID.
  - Modified the RACLIST function, for the IDIDMAP class, to RACLIST the DIDLIST1 repeat group and eliminate the need to go to the RACF DB to extract Registry information when a user has more than one registry (when the same User's Distinguished Name is defined for more than one registry).
  - Modified the Branch-entry RACXTRT function to allow extracting the DIDLIST1 repeat group
  - Modified the R_cacheserv callable service to
    - Provide a service to validate an ICRX containing an IDID with section 1 completed.
    - Allow reusable ICRX objects.
  - Normalize the Distributed Identity Filter Name if it is in X.500 format.



RACF z/OS Identity Propagation with CICS as exploiter

At a concept level, z/OS Identity Propagation can be summarized as supporting the notion of making the identity of the end-user available – securely - to the back-end business logic program and transaction processing z/OS subsystems, at the application and security domain level.

The terms “Realm and Registry Name” and “Distinguished Name and Distributed Identity” are used interchangeably:

Usage and invocation

- Enhancements to the following existing interfaces:
  - The **RACMAP** command has been enhanced to provide a **query** function which will use the **UserDIDfilter Name** and **Registry Name** to return the matching RACF user ID.
- Syntax:

RACMAP
QUERY
USERDIDFILTER(NAME(*'distributed-identity-user-name'*))
REGISTRY(NAME(*'distributed-identity-registry-name'*))

RACMAP QUERY example:

Suppose you had used the **RACMAP MAP** function to create the distributed identity filter:

RACMAP ID(INET1ID) MAP
USERDIDFILTER(NAME('OU=Internet Demo,O=O''Dooley''s Mart,L=Internet'))
REGISTRY(NAME('ldaps//us.odooleysmart.com'))
WITHLABEL('General Internet ID Map')

If you remember the RACF user ID that this filter was associated with, you can use the **RACMAP LISTMAP** function to list the information:

RACMAP ID(INET1ID) LISTMAP

If no errors are encountered, the **RACMAP LISTMAP** output will look like this:

Mapping information for user INET1ID:
Label: General Internet ID Map
Distributed Identity User Name Filter:
>OU=Internet Demo,O=O'Dooley's Mart,L=Internet<
Registry Name:
>ldaps//us.odooleysmart.com<

If you do not remember the RACF user ID that the filter is associated with, you cannot use the **RACMAP LISTMAP** function to get the information you want.

You can now use the new **RACMAP QUERY** function to get the information:

RACMAP QUERY
USERDIDFILTER(NAME('OU=Internet Demo,O=O''Dooley''s Mart,L=Internet'))
REGISTRY(NAME('ldaps//us.odooleysmart.com'))

If no errors are encountered, the **RACMAP QUERY** output will look like this:

RACMAP QUERY result. RACF user ID: INET1ID

Usage and invocation

- Enhancements to the following existing interfaces:
  - **R_cacheserv** has been enhanced with two new option codes for **Function Code 7** (manage an extended read/write cache).
    - **Option Code 4**
      - » Store and return a **reusable ICRX**
    - **Option Code 5**
      - » Validate a **user-built ICRX** (a.k.a. **"pseudo" ICRX**)

Usage and invocation

- Enhancements to the following existing interfaces:
  - **R_usermap** has been enhanced with
    - A new **Function Code** (**8**) and
    - Two new parameters:
      - » **Distinguished_Name**
      - » **Registry Name**

CALL IRRSIM00 (Work_area,
ALET, SAF_return_code,
RACF_return_code,
RACF_reason_code,
Option_word,
Certificate,
Distinguished_Name,
)

ALET,
ALET,
ALET, Function_code,
RACF_userid,
Application_userid,
Registry_Name

Usage and invocation

- Enhancements to the following existing interfaces:
  - **RACF CVT**
    - The **RCVT** has a new programming interface field to indicate that Identity Propagation 2 services are available on the system. This value is set at IPL during RACF Initialization.

Offset	Data Type	Data Length	Field Name	Field Description
376 (x'178')	**Unsigned Integer**	**1**	**RCVTIDPV**	**A value of 1 indicates that Identity Propagation 2 services are available on the system.**

Usage and invocation - New and changed messages

- The following are new RACMAP command messages:
  - **IRRW214I The** *KeyWord-Name* **keyword is ignored when specified with the** *Function-Name* **function.**
  - **IRRW215I No user ID found associated with the specified USERDIDFILTER and REGISTRY name.**
  - **IRRW216I Unexpected** *Callable-Service-Name* **callable service error encountered during command processing. SAF RC = x'***RetCode***', RACF RC = x'***RetCode***', RACF RSN = x'***RsnCode***'.**

Interactions and dependencies

- Hardware Dependencies
  - None
- Software Dependencies
  - None
- Exploiters
  - None

Migration and coexistence considerations

- For those customers that have started exploiting the z/OS Identity Propagation function:
  - Since we are now normalizing the User's Distinguished Name specified in
    - The RACMAP command as USERDIDFILTER(NAME(...))
    - The R_usermap Callable Service with the Distinguished_Name parameter
    - In the IDID when it is passed in with
      - » initACEE and
      - » RACROUTE REQUEST=VERIFY
- The customers will have to:
    - Delete the old filters, that were defined in the IDIDMAP class as profiles, and re-define them using the updated RACMAP command.
    - Disable RACGLIST for the IDIDMAP class until the APAR's have been applied to all the systems in the sysplex.
  - A sysplex-wide IPL is not necessary, a rolling IPL should suffice.

Installation

- APARs OA34258 (RACF parts) and OA34259 (RACF SAF parts)
- After the APARs have been applied, the installation MUST re-IPL all systems before trying to exercise the Identity Propagation function(s). In addition, if the installation had Distributed Identity Filter Names defined prior to this APAR, the installation should:
  - Generate a DB Unload report
  - Customize and run the sample utility that is provided. This utility will use the DB Unload report, to generate the appropriate RACF commands to delete and redefine the Distributed Identity Filter Names.

Session summary

- Describe function and value of new support - ID Propagation 2.
- Describe how this function is implemented and how to exploit it.
- List considerations when implementing support.

Appendix (1 of 2)

- New return and reason codes for R_cacheserv

SAF return code	RACF return code	RACF reason code	Explanation
8	100	Offset to the ICRX field in error.	This return/reason code is issued when R_cacheserv is invoked to validate an ICRX. It indicates non-valid data in the ICRX portion of ICRX. The offsets are calculated from the beginning of the ICRX.
8	104	Offset to the IDID field in error.	This return/reason code is issued when R_cacheserv is invoked to validate an ICRX. It indicates non-valid data in the IDID portion of ICRX. The offsets are calculated from the beginning of the IDID.
8	108	Offset to the IDID Section 1 field in error.	This return/reason code is issued when R_cacheserv is invoked to validate an ICRX. It indicates non-valid data in Section 1 of the IDID portion of ICRX. The offsets are calculated from the beginning of Section 1 of the IDID.
8	112	Offset to the User's Distinguished Name field in error.	This return/reason code is issued when R_cacheserv is invoked to validate an ICRX. It indicates non-valid data in the User's Distinguished Name Data Section in Section 1 of the IDID portion of ICRX. The offsets are calculated from the beginning of the User's Distinguished Name Data Section.
8	116	Offset to the Registry Name field in error.	This return/reason code is issued when R_cacheserv is invoked to validate an ICRX. It indicates non-valid data in the Registry Name Data Section in Section 1 of the IDID portion of ICRX. The offsets are calculated from the beginning of the Registry Name Data Section.

Appendix (2 of 2)

- New return and reason codes for R_usermap

SAF return code	RACF return code	RACF reason code	Explanation
8	8	36	High order bit was not set to indicate last parameter.
8	8	40	The Distinguished Name length is not valid, or the Distinguished Name string is entirely blank (x'20' in UTF-8) and/or null (x'00').
8	8	44	The Registry Name length is not valid, or the Registry Name string is entirely blank (x'20' in UTF-8) and/or null (x'00').
8	8	48	There is no distributed identity filter mapping the supplied distributed identity to a RACF user ID, or The IDIDMAP RACF general resource class is not active or not RACLISTed

Appendix - References

- Publications affected
  - SA22-7691 - z/OS Security Server RACF Callable Services
  - SA22-7687 - z/OS Security Server RACF Command Language Reference
  - GA22-7680 - z/OS Security Server RACF Data Areas
  - SA22-7682 - z/OS Security Server RACF Macros and Interfaces
  - SA22-7686 - z/OS Security Server RACF Messages and Codes
  - SA22-7683 - z/OS Security Server RACF Security Administrator's Guide
  - SA22-7692 - z/OS Security Server RACROUTE Macro Reference

Trademarks, disclaimer, and copyright information

IBM, the IBM logo, ibm.com, CICS, RACF, and z/OS are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of other IBM trademarks is available on the web at "Copyright and trademark information" at http://www.ibm.com/legal/copytrade.shtml

THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY.
THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. WHILE EFFORTS WERE MADE TO VERIFY THE COMPLETENESS AND ACCURACY OF THE INFORMATION CONTAINED IN THIS PRESENTATION, IT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. IN ADDITION, THIS INFORMATION IS BASED ON IBM'S CURRENT PRODUCT PLANS AND STRATEGY, WHICH ARE SUBJECT TO CHANGE BY IBM WITHOUT NOTICE. IBM SHALL NOT BE RESPONSIBLE FOR ANY DAMAGES ARISING OUT OF THE USE OF, OR OTHERWISE RELATED TO, THIS PRESENTATION OR ANY OTHER DOCUMENTATION. NOTHING CONTAINED IN THIS PRESENTATION IS INTENDED TO, NOR SHALL HAVE THE EFFECT OF, CREATING ANY WARRANTIES OR REPRESENTATIONS FROM IBM (OR ITS SUPPLIERS OR LICENSORS), OR ALTERING THE TERMS AND CONDITIONS OF ANY AGREEMENT OR LICENSE GOVERNING THE USE OF IBM PRODUCTS OR SOFTWARE.