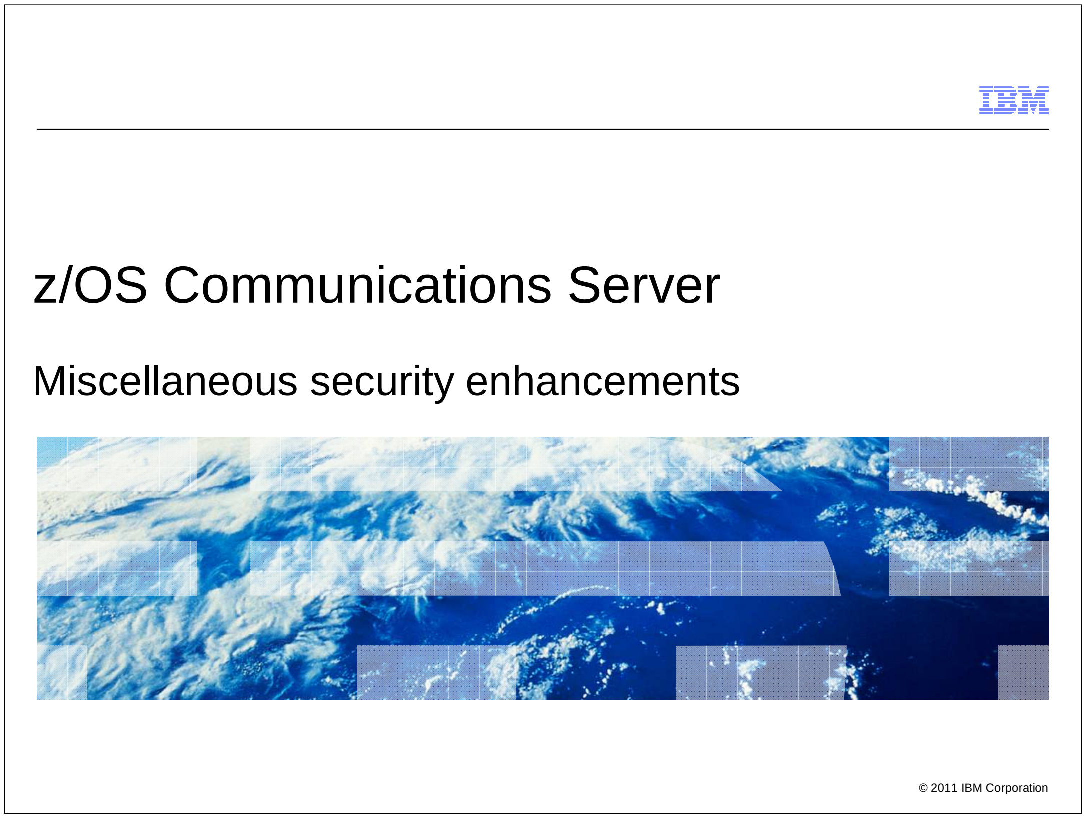
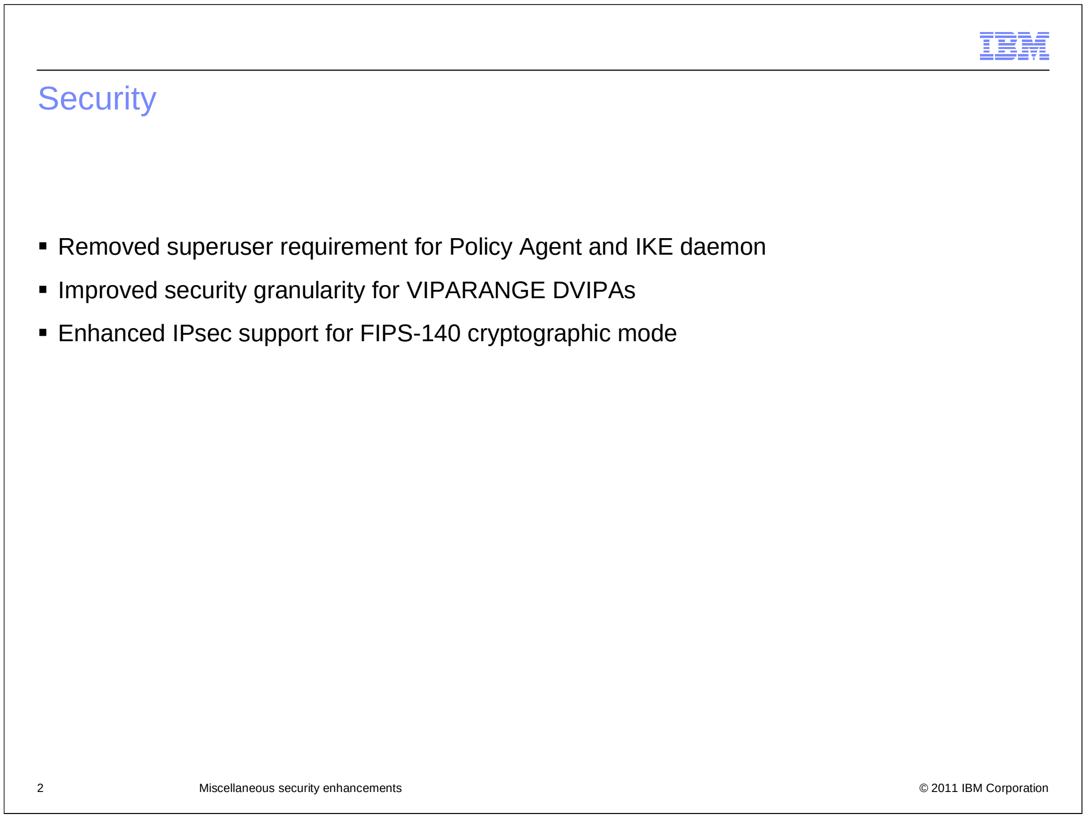


z/OS Communications Server

Miscellaneous security enhancements

This presentation provides an overview of several security enhancements in z/OS® V1R13 Communications Server.



Security

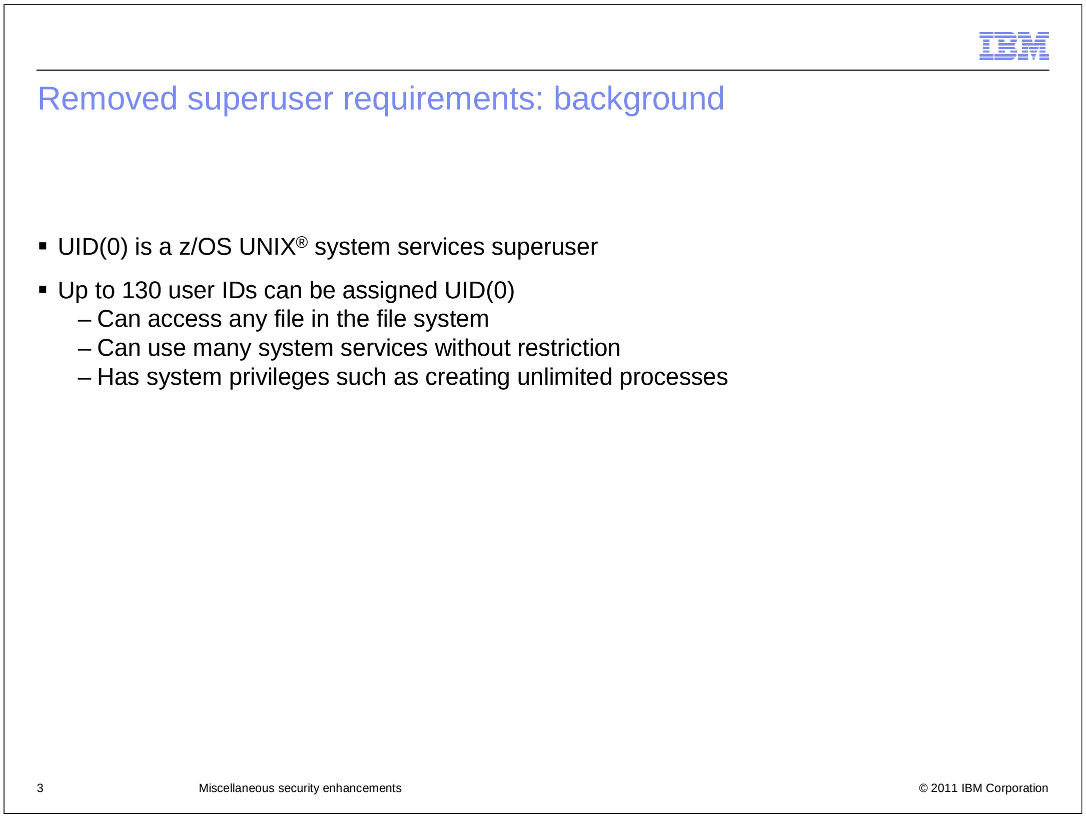
- Removed superuser requirement for Policy Agent and IKE daemon
- Improved security granularity for VIPARANGE DVIPAs
- Enhanced IPsec support for FIPS-140 cryptographic mode

This presentation describes several security enhancements in z/OS V1R13 Communications Server.

The Policy Agent and the Internet Key Exchange (IKE) daemon no longer need to be run as superuser.

Security controls governing the creation of VIPARANGE Dynamic Virtual Internet Protocol Addresses (DVIPAs) are given improved granularity.

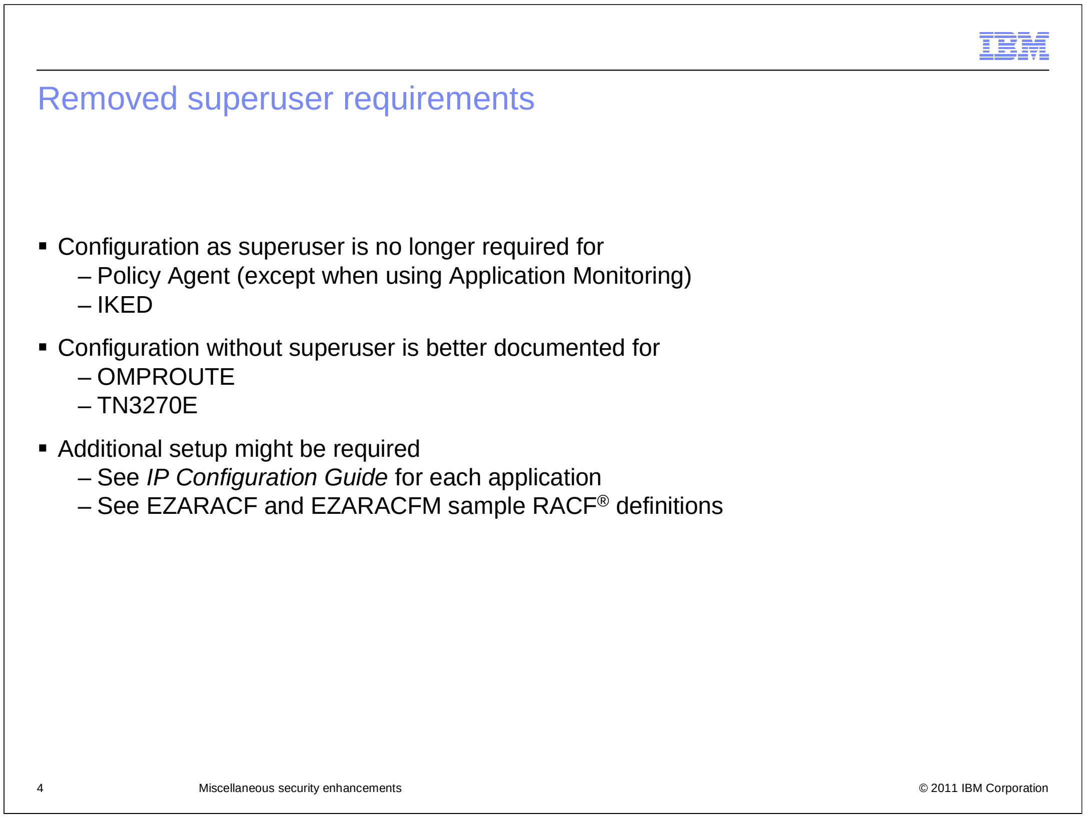
Support for IP security (IPsec) FIPS-140 cryptographic mode is enhanced.



Removed superuser requirements: background

- UID(0) is a z/OS UNIX® system services superuser
- Up to 130 user IDs can be assigned UID(0)
  - Can access any file in the file system
  - Can use many system services without restriction
  - Has system privileges such as creating unlimited processes

As the name superuser implies, it allows users to have special access and privileges in the system. Because superusers have significant authority and are a limited resource, it is wise to limit the number of superuser ids.



IBM

Removed superuser requirements

- Configuration as superuser is no longer required for
  - Policy Agent (except when using Application Monitoring)
  - IKED
- Configuration without superuser is better documented for
  - OMPROUTE
  - TN3270E
- Additional setup might be required
  - See *IP Configuration Guide* for each application
  - See EZARACF and EZARACFM sample RACF® definitions

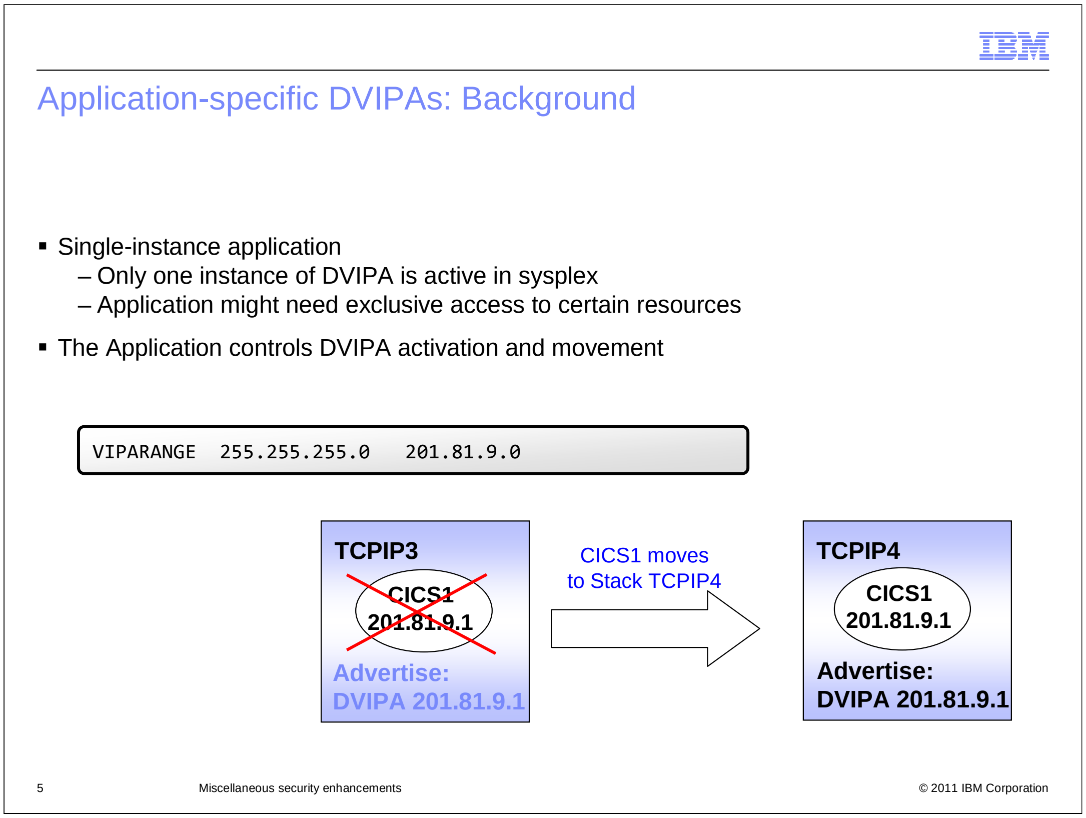
4 Miscellaneous security enhancements © 2011 IBM Corporation

Superuser authority is no longer required when running Policy Agent and the IKE daemon. There is one exception: if you are using Policy Agent to perform Application monitoring it still requires superuser authority.

OMPROUTE and TN3270E are able to run without superuser authority, but the documentation has been corrected to indicate this is the case.

Note that in all cases additional setup might be required when these applications are not running as superuser. For example, they might need to be granted ownership or permission to access configuration and log files. See the configuration instructions for these applications and the sample RACF definitions in EZARACF and EZARACFM.

In any case, you are free to continue to define any of these applications with superuser authority. Removing superuser authority is optional.



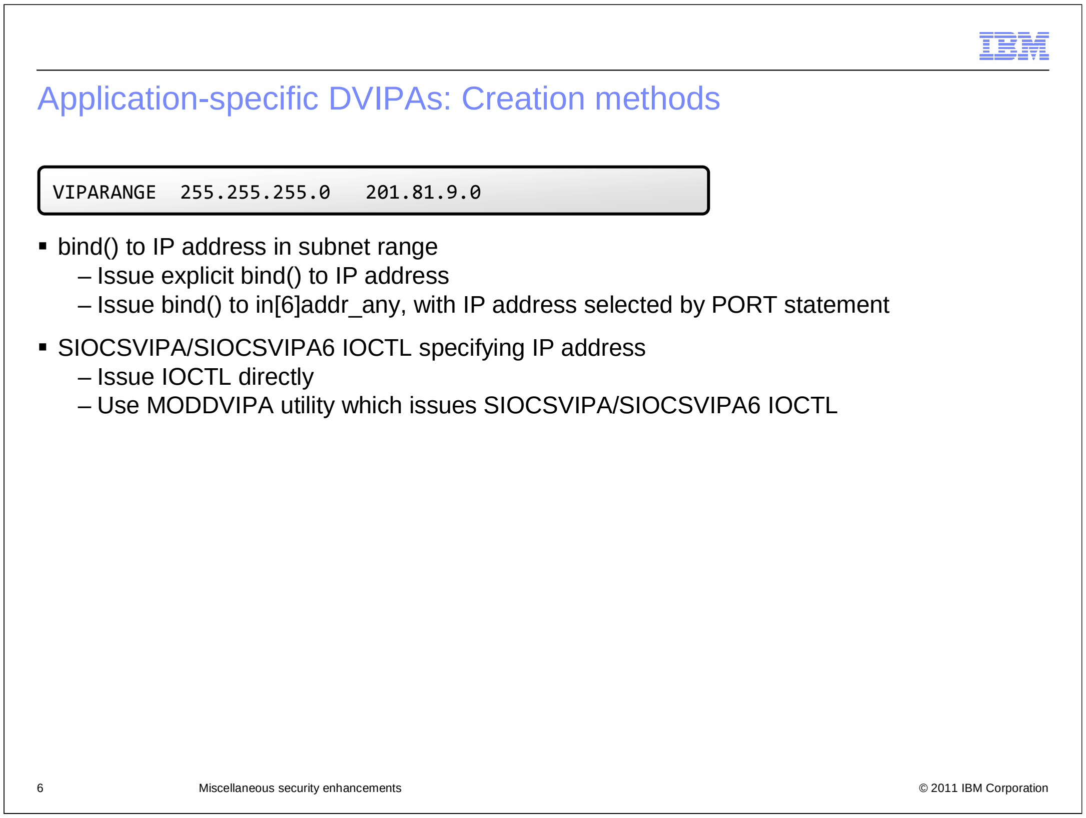
Application-specific DVIPAs: Background

- Single-instance application
  - Only one instance of DVIPA is active in sysplex
  - Application might need exclusive access to certain resources
- The Application controls DVIPA activation and movement

```
VIPARANGE  255.255.255.0   201.81.9.0
```

5 Miscellaneous security enhancements © 2011 IBM Corporation

Application-specific DVIPAs are used when only a single instance of the DVIPA can be active in the sysplex. The application controls the activation and movement of the DVIPA. A VIPARANGE statement defines a subnet range of DVIPAs that can be activated by the application. In the example, as CICS1 moves from TCPIP3 to TCPIP4, the application also causes the DVIPA to move.

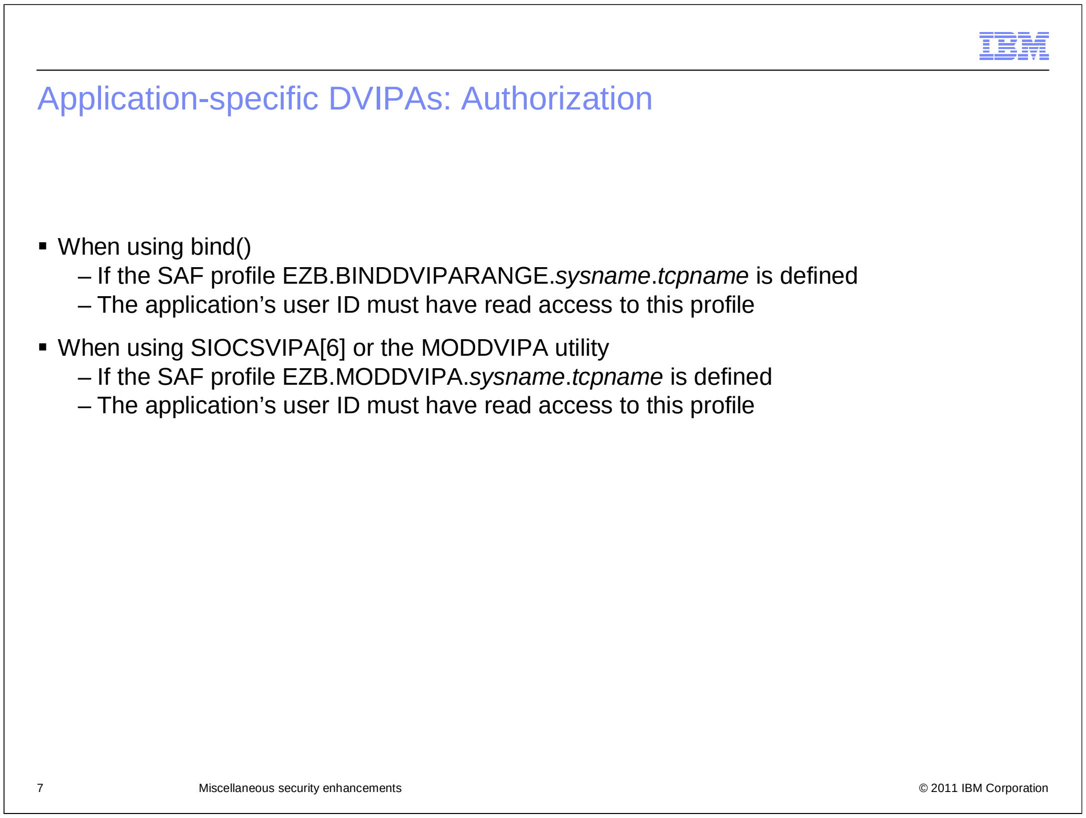


Application-specific DVIPAs: Creation methods

```
VIPARANGE  255.255.255.0   201.81.9.0
```

- bind() to IP address in subnet range
  - Issue explicit bind() to IP address
  - Issue bind() to in[6]addr_any, with IP address selected by PORT statement
- SIOCSVIPA/SIOCSVIPA6 IOCTL specifying IP address
  - Issue IOCTL directly
  - Use MODDVIPA utility which issues SIOCSVIPA/SIOCSVIPA6 IOCTL

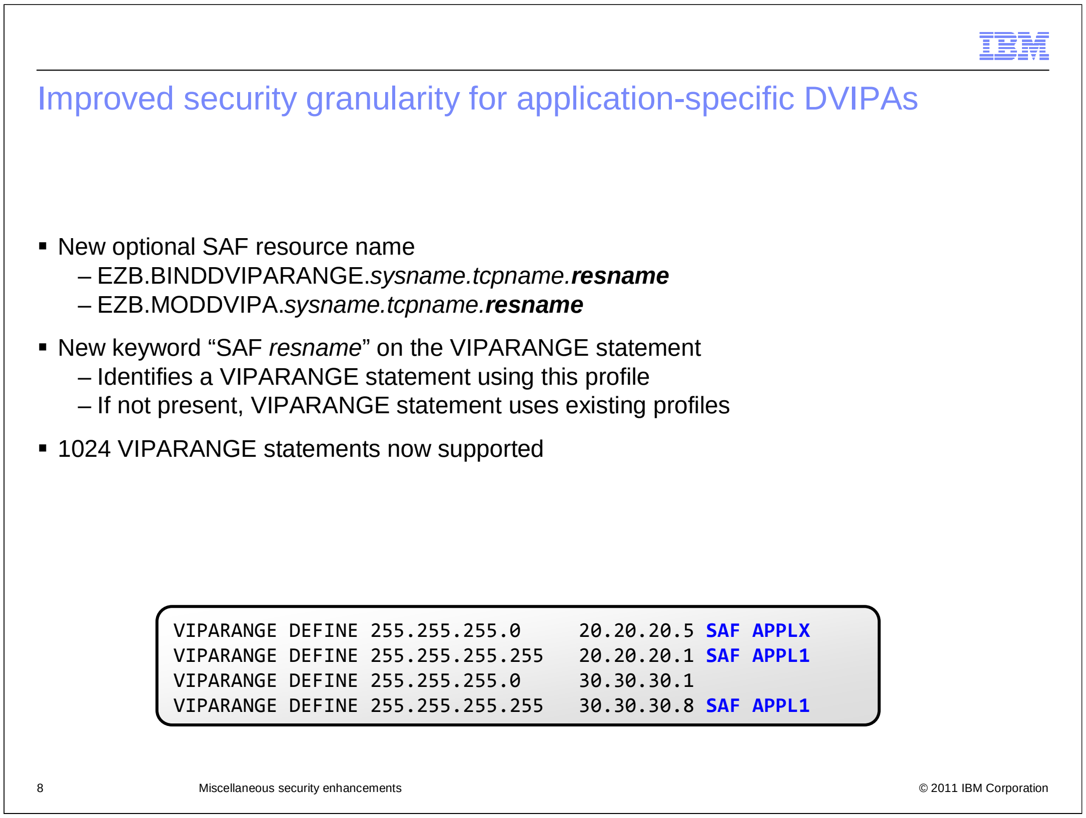
An application can cause a DVIPA to be created by issuing a bind() to the IP address in the VIPARANGE statement’s subnet range. This can be an explicit bind to an IP address or the IP address can be selected by the BIND keyword on a PORT statement. Alternatively, the application can cause the SIOCSVIPA/SIOCSVIPA6 IOCTL to create the IP address; by issuing the IOCTL directly or using the MODDVIPA utility which will issue the IOCTL.



Application-specific DVIPAs: Authorization

- When using bind()
  - If the SAF profile EZB.BINDDVIPARANGE.*sysname*.*tcpname* is defined
  - The application's user ID must have read access to this profile
- When using SIOCSVIPA[6] or the MODDVIPA utility
  - If the SAF profile EZB.MODDVIPA.*sysname*.*tcpname* is defined
  - The application's user ID must have read access to this profile

Before V1R13, z/OS Communications Server provides two SAF profiles for use in authorizing the creation of application-specific DVIPAs. One profile is checked when the DVIPA is created using a bind(), and the other when the DVIPA is created using the SIOCSVIPA or SIOCSVIPA6 IOCTL. If the corresponding profile is defined, the application's user ID must have read access in order for the DVIPA to be created. The disadvantage of this approach is that it is not granular: an application is permitted to create all DVIPAs, or none. This allows applications to interfere with each others' DVIPAs.



Improved security granularity for application-specific DVIPAs

- New optional SAF resource name
  - EZB.BINDDVIPARANGE.*sysname.tcpname.**resname***
  - EZB.MODDVIPA.*sysname.tcpname.**resname***
- New keyword “SAF *resname*” on the VIPARANGE statement
  - Identifies a VIPARANGE statement using this profile
  - If not present, VIPARANGE statement uses existing profiles
- 1024 VIPARANGE statements now supported

```
VIPARANGE DEFINE 255.255.255.0     20.20.20.5 SAF APPLX
VIPARANGE DEFINE 255.255.255.255   20.20.20.1 SAF APPL1
VIPARANGE DEFINE 255.255.255.0     30.30.30.1
VIPARANGE DEFINE 255.255.255.255   30.30.30.8 SAF APPL1
```

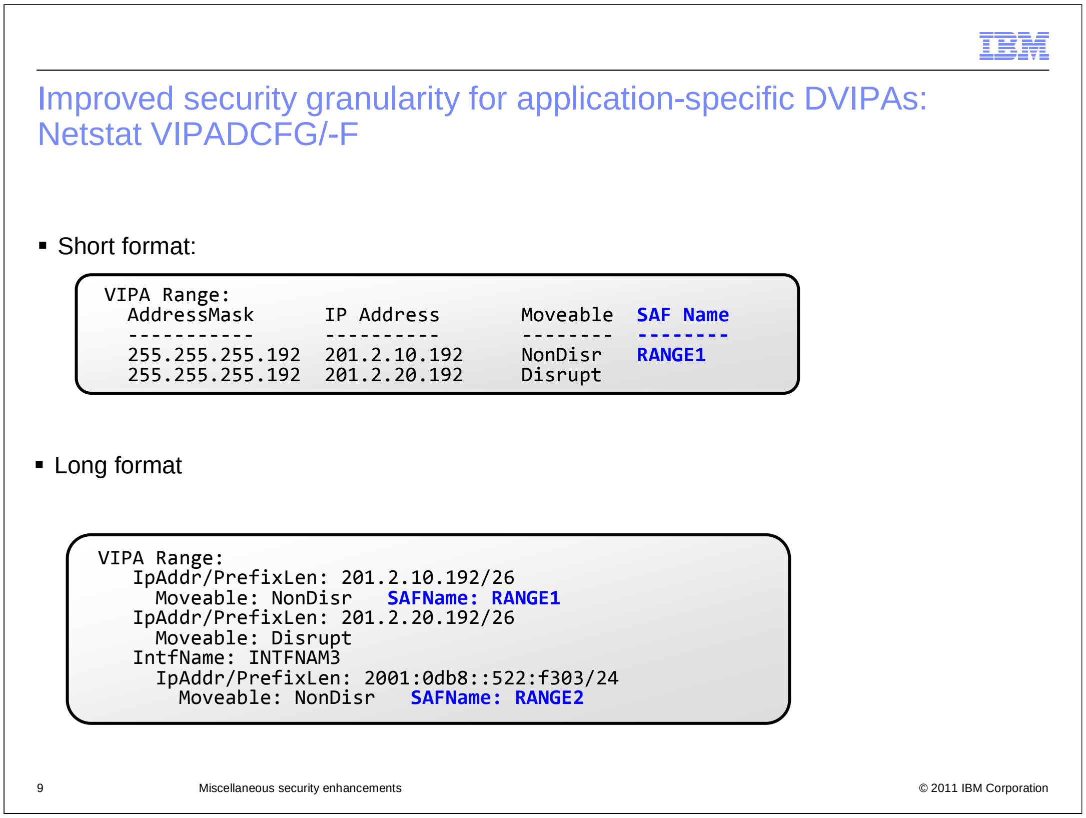
8 Miscellaneous security enhancements © 2011 IBM Corporation

Beginning in V1R13, two new SAF profiles are supported to provide additional granularity for authorization to application-specific DVIPAs. These profiles add an additional qualifier to the existing profile names.

A new optional SAF keyword is supported on the VIPARANGE statement. This keyword indicates that you want to use the more granular profiles, and requires you to specify the resource name (*resname)* qualifier that to use in the profile name. By creating separate profiles for separate VIPARANGE statements, you can now authorize different applications to different DVIPAs. Unlike the existing profiles, if you specify the SAF keyword on the VIPARANGE statement and the profile is not defined to your SAF product, applications are denied access to creating the DVIPA. If you specify the SAF keyword you must both create the profile and grant the appropriate user IDs read access to the profile.

If you do not specify the new SAF keyword, then the existing profile names are used for authorization and all users are permitted to create the DVIPAs if the profile is not defined.

TCP/IP now supports the configuration of up to 1024 VIPARANGE statements for IPv4 and 1024 statements for IPv6. This gives you additional freedom in assigning specific SAF resource names to each DVIPA. There is still a limit of 1024 active IPv4 and IPv6 DVIPAs.



Improved security granularity for application-specific DVIPAs: Netstat VIPADCFG/-F

- Short format:

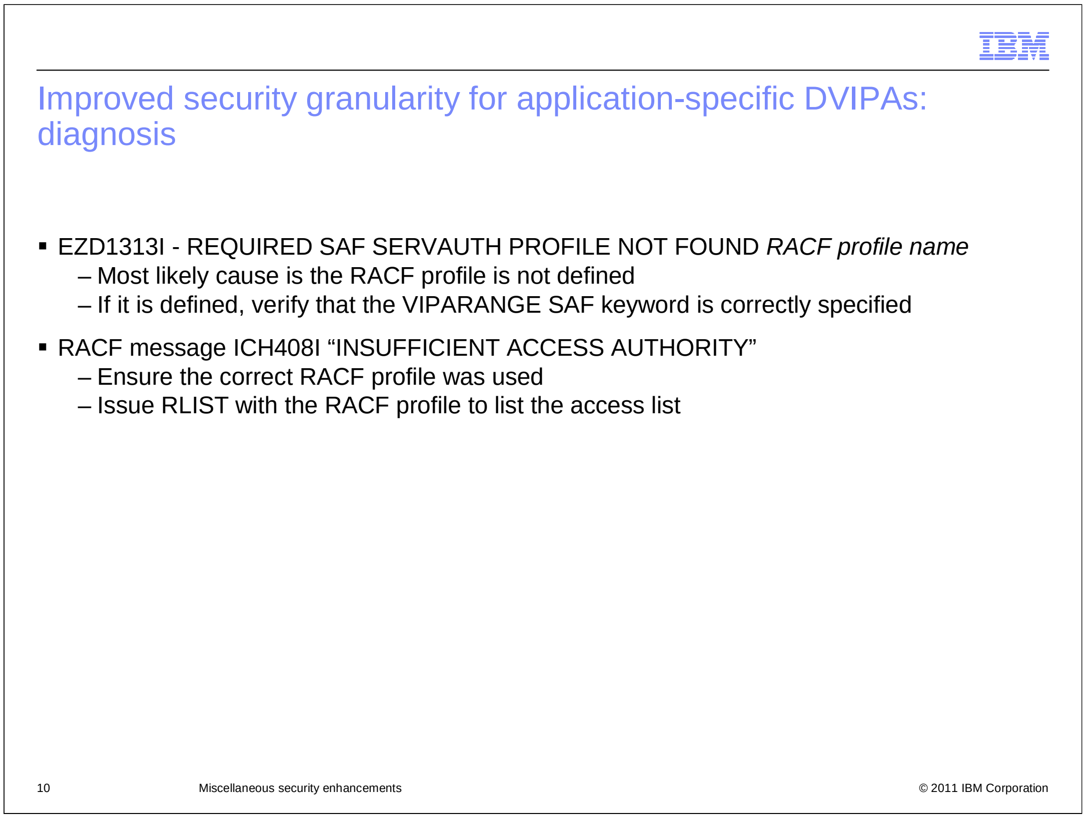
```
VIPA Range:
  AddressMask      IP Address       Moveable  SAF Name
  -----------      ----------       --------  --------
  255.255.255.192  201.2.10.192     NonDisr   RANGE1
  255.255.255.192  201.2.20.192     Disrupt
```

- Long format

```
VIPA Range:
   IpAddr/PrefixLen: 201.2.10.192/26
     Moveable: NonDisr   SAFName: RANGE1
   IpAddr/PrefixLen: 201.2.20.192/26
     Moveable: Disrupt
   IntfName: INTFNAM3
     IpAddr/PrefixLen: 2001:0db8::522:f303/24
       Moveable: NonDisr   SAFName: RANGE2
```

The changes to the short and long format Netstat VIPADCFG/-F display of the VIPARANGE statement are shown.

Corresponding information is provided in DVIPA-related SMF records and in the DVIPA-configuration NMI request, NMTP_DVCFG.



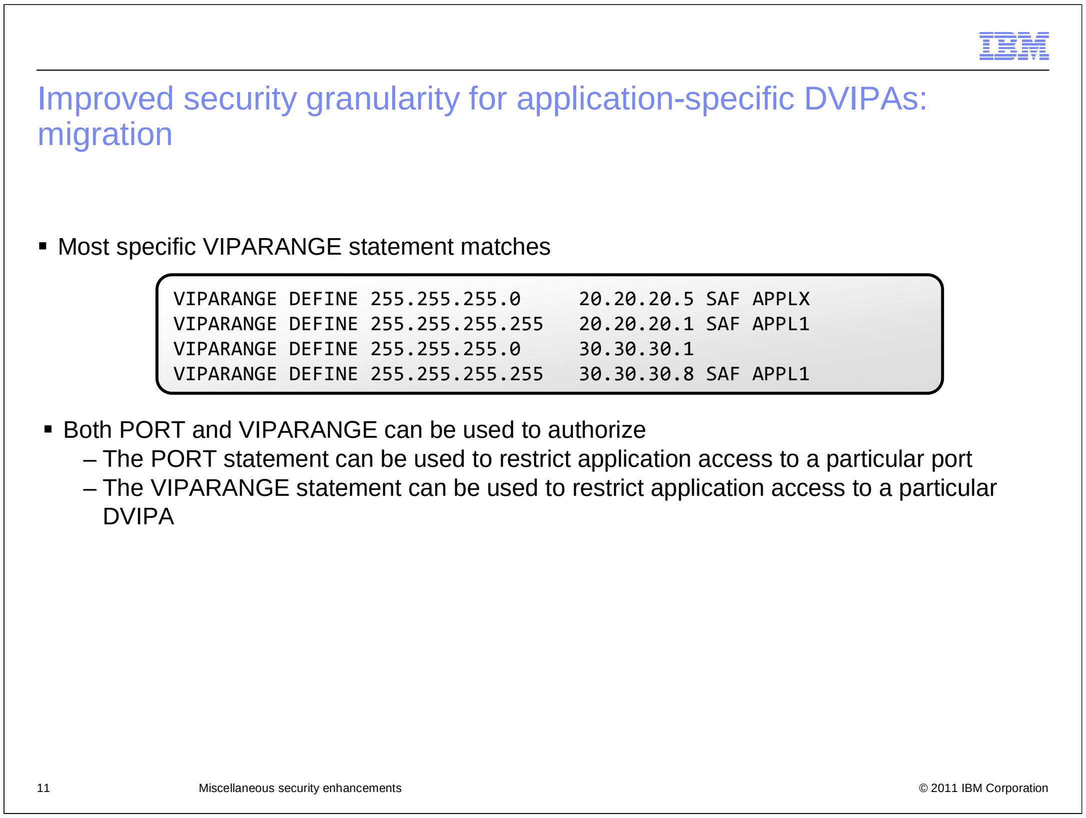
Improved security granularity for application-specific DVIPAs: diagnosis

- EZD1313I - REQUIRED SAF SERVAUTH PROFILE NOT FOUND *RACF profile name*
  - Most likely cause is the RACF profile is not defined
  - If it is defined, verify that the VIPARANGE SAF keyword is correctly specified
- RACF message ICH408I “INSUFFICIENT ACCESS AUTHORITY”
  - Ensure the correct RACF profile was used
  - Issue RLIST with the RACF profile to list the access list

This slide describes what to do if message EZD1313I or ICH408I is displayed.

The most common reason that EZD1313I is displayed is that the RACF profile is not defined. If the profile is defined, verify that the VIPARANGE SAF keyword is specified correctly in the TCP/IP profile.

The most common reason that message ICH408I is displayed is that an incorrect RACF profile was used. Use the RLIST command to show the access list.



Improved security granularity for application-specific DVIPAs: migration

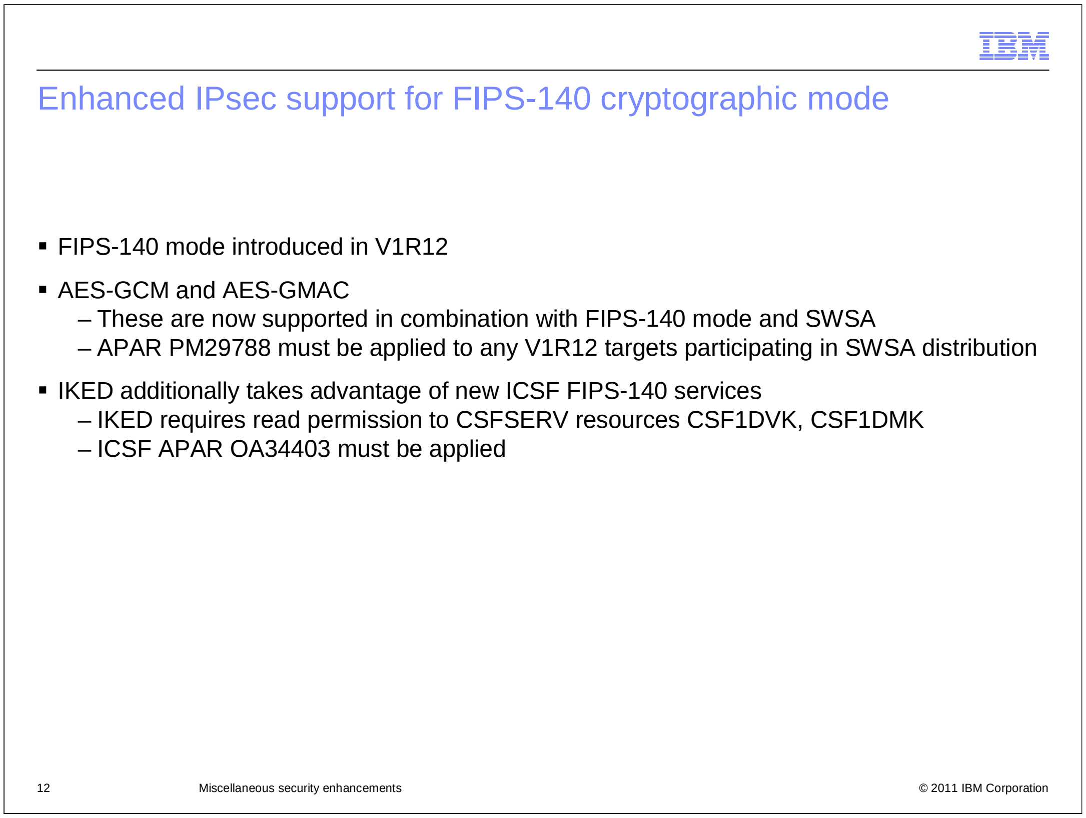
- Most specific VIPARANGE statement matches

```
VIPARANGE DEFINE 255.255.255.0     20.20.20.5 SAF APPLX
VIPARANGE DEFINE 255.255.255.255   20.20.20.1 SAF APPL1
VIPARANGE DEFINE 255.255.255.0     30.30.30.1
VIPARANGE DEFINE 255.255.255.255   30.30.30.8 SAF APPL1
```

- Both PORT and VIPARANGE can be used to authorize
  - The PORT statement can be used to restrict application access to a particular port
  - The VIPARANGE statement can be used to restrict application access to a particular DVIPA

Before V1R13, the first VIPARANGE statement that matched an application request was used to determine the DVIPA’s attributes. Beginning in V1R13, the most specific VIPARANGE that matches an IP address is used to determine the DVIPA’s attributes, including the SAF resource name that is used. In the example on this slide, the second and fourth VIPARANGE statements are more specific than the first and third, and are used for that particular IP address.

The PORT statement can be used to restrict application access to a particular port. The VIPARANGE statement in combination with either the old or new SAF resource names, can be used to restrict application access to a particular DVIPA. Before z/OS V1R13, if an application bind() matched a PORT statement, the EZB.BINDDVIPARANGE SAF profile was not checked. Beginning in z/OS V1R13, even if an application bind() matches a PORT statement, the EZB.BINDDVIPARANGE SAF profile might be checked. This can result in two SAF authorization checks if the PORT statement has the SAF keyword configured.



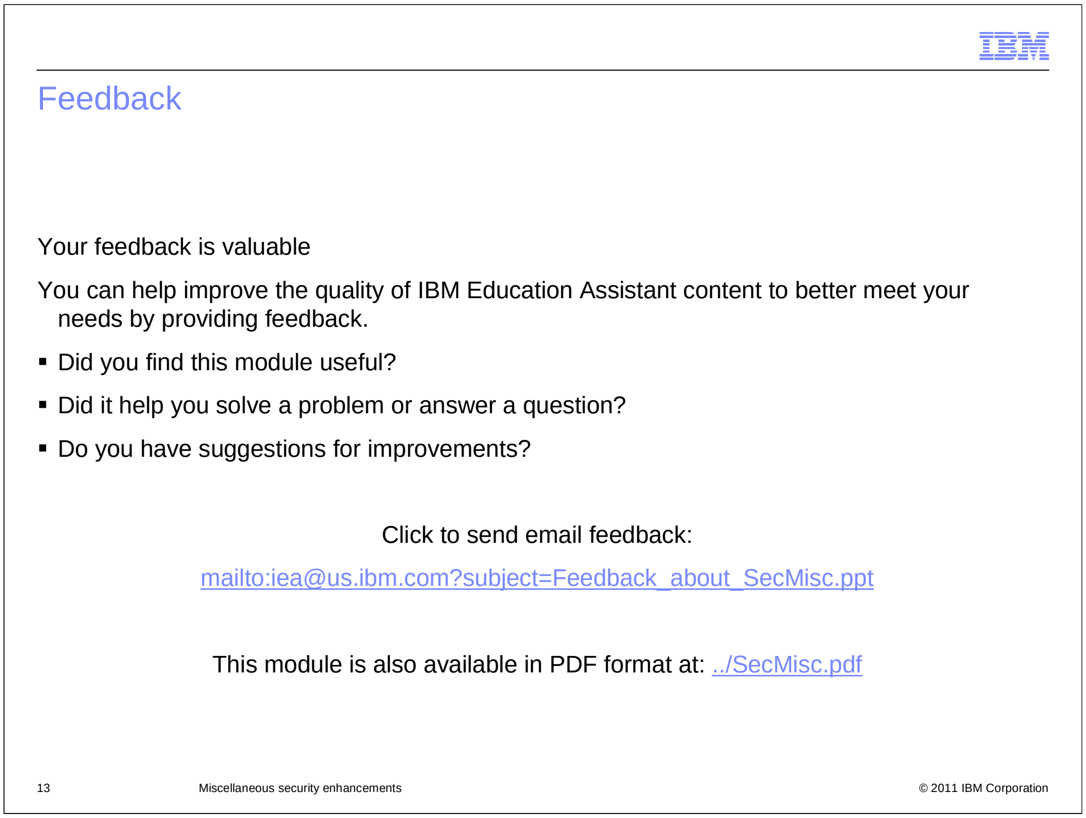
Enhanced IPsec support for FIPS-140 cryptographic mode

- FIPS-140 mode introduced in V1R12
- AES-GCM and AES-GMAC
  - These are now supported in combination with FIPS-140 mode and SWSA
  - APAR PM29788 must be applied to any V1R12 targets participating in SWSA distribution
- IKED additionally takes advantage of new ICSF FIPS-140 services
  - IKED requires read permission to CSFSERV resources CSF1DVK, CSF1DMK
  - ICSF APAR OA34403 must be applied

Beginning in V1R12, z/OS Communications Server supports using ICSF and System SSL in FIPS-140 operational mode for IP security.

Beginning in V1R13, the AES-GCM and AES-GMAC cryptographic algorithms are supported for IPsec tunnels that use both FIPS-140 mode and SWSA. This combination was not supported in prior releases. In order to distribute such tunnels and traffic to V1R12 target systems, you should apply APAR PM29788.

Beginning in V1R13, the IKE daemon takes advantage of additional FIPS-140 cryptographic services provided by ICSF. If the CSFSERV class is active on your system, you should grant IKED read access to the CSF1DVK and CSF1DMK resources. Additionally, ensure that ICSF APAR OA34403 is applied to your system.



Feedback

Your feedback is valuable

You can help improve the quality of IBM Education Assistant content to better meet your needs by providing feedback.

- Did you find this module useful?
- Did it help you solve a problem or answer a question?
- Do you have suggestions for improvements?

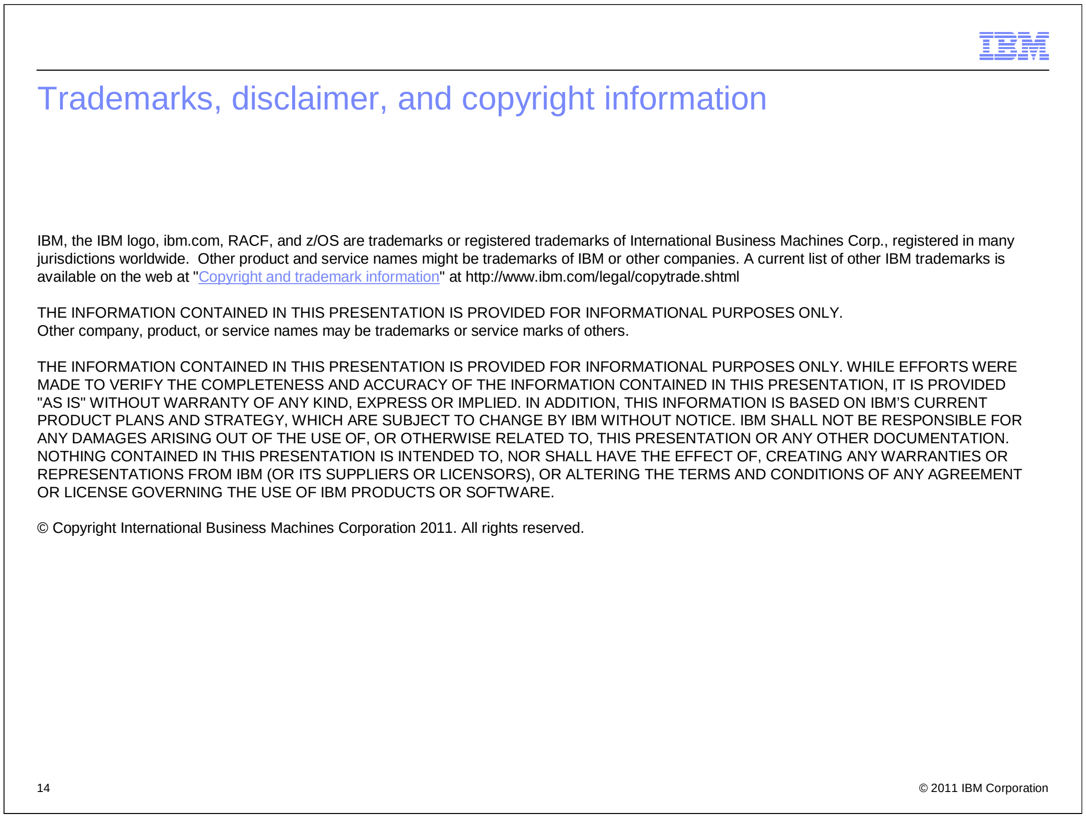
Click to send email feedback:

mailto:iea@us.ibm.com?subject=Feedback_about_SecMisc.ppt

This module is also available in PDF format at: ../SecMisc.pdf

13 Miscellaneous security enhancements

You can help improve the quality of IBM Education Assistant content by providing feedback.



Trademarks, disclaimer, and copyright information

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.