Disclaimers

This presentation introduces the new and changed security functionality of z/VM Version 5 Release 4.

References to IBM products, programs, or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM's product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe on any of the intellectual property rights of IBM may be used instead. The evaluation and verification of operation in conjunction with other products, except those expressly designed by IBM, are the responsibility of the user.

The following terms are registered trademarks or trademarks of IBM Corporation in the United States or other countries or both:

IBM IBM logo z/VM RACF

Other company, product, and service names, which may be denoted by double asterisks (**), may be trademarks or service marks of others.

Agenda

- RACF Security Server
- LDAP
- SSL server
- Common Criteria
- DIRMAINT

z/VM RACF Security Server feature

- z/VM 5.3 RACF database mapping error!
  - Unpredictable results if sharing with z/OS or z/VM 5.4
  - Apply APAR VM64383 – Follow the instructions EXACTLY
    - Do NOT upgrade database templates or share the database until this APAR is applied.
- Database has been updated with new templates
  - RACFCONV will fix-up a broken 5.3 database as part of migration, but any 5.3 system that is using it better have VM64383 applied!

z/VM RACF Security Server feature

- IRRUT200 (database copy) instructions updated
  - No serialization, so no sharing
  - Must be run from RACFVM user ID
- IRRUT400 (database copy/split/merge/extend) instructions and examples updated
  - Can be run on active, shared databases

z/VM RACF Security Server feature

- Password change logging for LDAP
  - When password is changed by administrator or user, a PKCS #7 encrypted envelope is created and placed into the RACF database
  - An LDAP change log record is created
  - LDAP client can extract the encrypted field

z/VM RACF Security Server feature

- RACF recognizes current and alternate system operators when RACF server is down
  - Commands are accepted from the current system operator
    - SYSTEM_USERIDS
    - ALTERNATE_OPERATORS
    - SET SYSOPER
  - Allows commands and LOGON, deferring to CP for authorization and password checking

z/VM RACF Security Server feature

- New installs now default to DES password encryption
- Password masking is still available

LDAP Server

- Upgrade to z/OS 1.10 ITDS
- Published back-end APIs to enable usage by other ESMs
- Support for password change logging
  - z/OS uses RACF certificate services
  - z/VM uses System SSL services
- Password phrase can now be used in an ldap bind

SSL Server

- SSL server has been ported to CMS
  - Available December 2008
  - Base does not include any SSL capability
    - Do not migrate to 5.4 immediate if you require SSL
- SSL services provided by System SSL
  - Same as z/OS System SSL
  - Exploits CPACF integrated cryptographic function
  - No exploitation of Cryptographic Coprocessors (cards)
  - APIs are not published or supported for customer use

SSL Server

- Certificate management via gskeyman
  - Introduced in z/VM 5.3 with the LDAP server
  - Data held in BFS
  - Create user certficiates in response to a request
  - Create intermediate CAs and trusted CAs
  - Certificate export, import, renewal
  - Menu driven (linemode, so automation is possible)
- Working on plan to provide private key migration from z/VM 5.2 and 5.3

FTP Clear Command Channel (CCC)

- CCC subcommand recognized by z/VM client and server
- Issued **after** user ID and password are sent
- Control connection switches to clear-text
- File transfer is always encrypted

FTP Clear Command Channel (CCC)

- Enables firewalls to dynamically open and close data ports for file transfer
  - Just like for non-secure FTP
- Enables 3rd-party audit of file transfer
- Eliminates need for PassivePortRange in the server

FTP Clear Command Channel (CCC)

- Partner must support RFC 4217
  - Early drafts of the RFC did not define the behavior of CCC, so it was inferred
- z/OS FTP includes “TLSRFCLEVEL” option in FTP.DATA to control draft vs. RFC. The default is draft.
- No option is provided in z/VM to use the draft version

Common Criteria

- ISO/IEC 15408:2005
  - A set of meaningful security functions
    - Access control
    - Audit
  - Extensive testing of those functions
  - Effective processes
  - Good documentation
- Assurance levels 1 through 7
  - Evaluation by accredited firms
  - Certification by government agencies
  - CommonCriteriaPortal.org

Common Criteria

	Evaluation Assurance Level						
Function	1	2	3	4	5	6	7
function 1	✓	✓	✓	✓	✓	✓	✓
function 2			✓	✓	✓	✓	✓
function 3						✓	✓
strength analysis 1			✓	✓	✓	✓	✓
strength analysis 2					✓	✓	✓
evaluation 1			✓	✓	✓	✓	✓
evaluation 2				✓	✓	✓	✓

Common Criteria

- Higher assurance level does not indicate more or better security
- “Plus” (+) means you can fix a problem in the field
- A **Protection Profile** defines a standardized set of required functions with a minimum EAL

Common Criteria

- Controlled Access Protection Profile (CAPP)
  - Discretionary access controls
  - “I choose to give you access”
  - User- or administrator-controlled access
- Labeled Security Protection Profile (LSPP)
  - Mandatory access controls (MAC)
  - System overrides user
  - Security clearances (if any) and data/user compartmentalization enforced

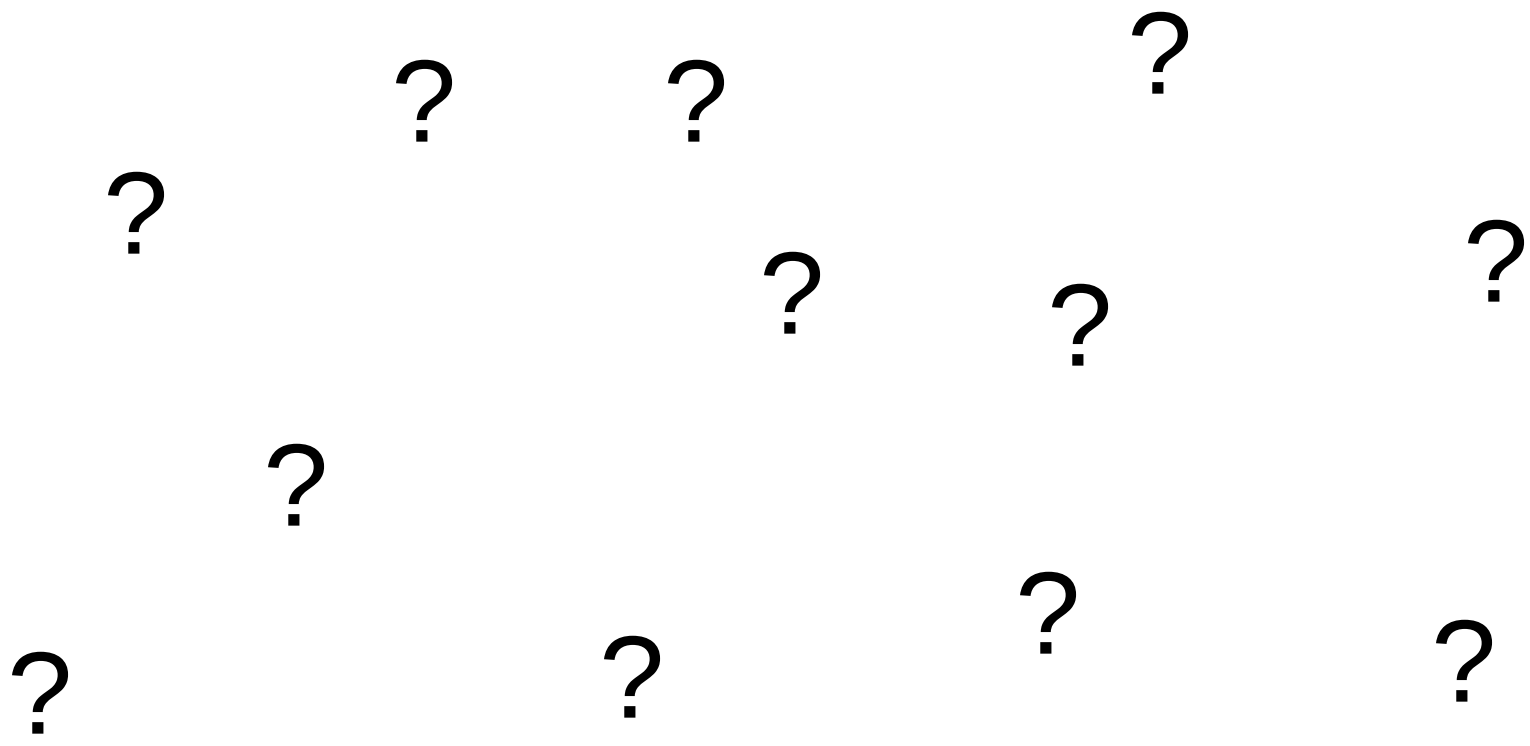
Common Criteria

- z/VM compliance
  - Includes CP, TCP/IP stack with telnet, and RACF
  - **z/VM 5.3** evaluated to CAPP and LSPP at EAL 4+
- z/VM 5.4 will not be evaluated, but we will make z/VM 5.3 available upon request
- LPAR is EAL 5
- z/OS is EAL 4+
- Linux is EAL 4+
- VMware is EAL 4+

DIRMAINT

- Users can authenticate with a password phrase (NEEDPASS YES)
- PW and SETPW can call an ESM to set the password or phrase
- Separation of RACF support from Dirmaint exits
  - Exits can be used in addition to RACF support
- IUCV communication instead of VMCF
  - Use of VMCF was interfering with RACF communications

Questions



Thanks!