z/VM Security Update
S71

Alan Altmark
z/VM Development
Endicott, NY

IBM System z Expo
September 17-21, 2007
San Antonio, TX

Disclaimers

This presentation introduces the new and changed security functionality of z/VM Version 5 Release 3.

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 FL530**
- **Password phrases and mixed-case passwords**
- **SSL server**
- **LDAP**
- **Common Criteria**

Virtualization security risks being overlooked, Gartner warns

Gartner raises warning on virtualization and security.

Companies in a rush to deploy virtualization technologies for server consolidation efforts could wind up overlooking many security issues and exposing themselves to risks, warns research firm Gartner.

“Virtualization, as with any emerging technology, will be the target of new security threats,” said Neil MacDonald, a vice president at Gartner, in a published statement.

Network World
April 6, 2007

z/VM RACF Security Server feature

- Name change consistent with z/OS
- Specific to each level of CP: FL530
- Service roll-up
- New books with unrelated z/OS information removed
- RACF/VM Version 1 Release 10 was withdrawn from marketing in March 2007
  - Service until April 2009 (z/VM 5.2 EOS)

Password phrases

- CP supports a maximum of 200 characters with an ESM
  - Limited by ESM
  - Longer than 8 characters
- RACF FL530 adds the PHRASE option
  - ADDUSER, ALTUSER, and PASSWORD commands
  - Maximum of 100 characters
- Any character, including blanks
- In addition to, or instead of, a traditional password
  - Phrases can be used on LOGON, FTP, REXECD, IMAP

Password phrases

- Single quotes required when password start or end is ambiguous
  - logon alan ‘this is my password’ noipl
  - logon alan ThisIsMyPassword noipl
- Double single quotes when present in phrase
  - logon alan ‘alan’’s password’
- Recommendations:
  - No leading or trailing blanks, single quotes, or line editing characters

Mixed-case passwords with RACF

- SETROPTS PASSWORD(MIXEDCASE | NOMIXEDCASE)
- Setting is remembered when a password is defined or changed
- NOMIXEDCASE does not convert mixed-case passwords to uppercase
  - Password reset will be required
- Evaluate applications carefully before engaging

Integrated Password Security API

- Enable ESM to integrate password verification into a single CP interface
- Diagnose 0x88 subcode 8
- No more RPIVAL!
- DMSPASS CSL routine
  - Calls Diag 0x88 subcode 8
  - Calls DMSPWCHK automatically, if required

Miscellaneous RACF Updates

- Unload the SMF audit trail in XML format
  - View in a browser
- ALTUSER …. PASSWORD(xxxxxxx) NOEXPIRED
  - Enables service machines to more easily change the password and have it not immediately expire
- Password phrase installation exit
  - Password RULES do not apply

SSL/TLS enhancements

- Updated support for SLES9 and RHEL4 service packs
- Encryption suites classified as low, medium, and high
  - Simplified exclude mechanism
- FTP, Telnet, and SMTP now support RFC-based in-band change from clear-text to secure both z/VM server *and* clients
  - FTP: RFC 4217
  - SMTP: RFC 3207
  - Telnet: TLS-based telnet security draft #6

SSL/TLS enhancements

- Eliminates need for pre-defined SECURE port
  - Port 990 for ftps
  - Port 992 for telnets
  - Still supported
- Uses new Pascal APIs
- Configured in application instead of PROFILE
  - Required, Preferred, Allowed, Never
  - Specify label name

© IBM Corporation 2007
2007 System z Technical Conference

LDAP server and utilities

- Enables remote hosts or applications to securely authenticate users against the RACF database on z/VM
- Central management of Linux passwords and POSIX identity information
- IBM Tivoli Directory Server (ITDS)
  - Equivalent to z/OS 1.8 ITDS
  - SDBM – RACF for password verification
  - LDBM – BFS directory structure to hold identity data

LDAP server and utilities

- Avoid defining users & groups in Linux
  - /etc/passwd
  - /etc/shadow
  - /etc/group
- User defined exactly once in LDAP
  - Change password once!
- **Session S73:** Securing Linux with RACF on z/VM

LDAP server and utilities

- **CMS client utilities**
  - **ldapadd add**
  - **ldapsrch search**
  - **ldapmdfy modify**
  - **ldapmrdn modify rdn**
  - **ldapdlet delete**

LDAP Security

- **SSL/TLS certificate management does not use SSL server**
- **Certificates and keys managed by** gskkyman
  - **Manage X.509 certificates**
  - **Generate public/private key pairs**
  - **Files kept in BFS**
  - **Used by clients and servers**

Common Criteria

- An ISO standard that ensures
  - A set of meaningful security functions
    - Identification
    - Access control
    - Audit
  - Extensive testing of those functions
  - Effective processes
  - Good user and administrator documentation
- Assurance levels 1 through 7
  - Evaluation by accredited firms
  - Certification by government agencies
  - CommonCriteriaPortal.org

Common Criteria

- z/VM Version 5.1 completed evaluation
  - October 2005
  - Includes CP, TCP/IP stack with telnet, and RACF/VM
  - z/VM Secure Configuration Guide
- Labeled Security Protection Profile (LSPP)
  - Mandatory access controls
  - Security clearances and compartmentalization enforced
- Controlled Access Protection Profile (CAPP)
  - Discretionary access controls
  - User- or administrator-controlled access
- Evaluation Assurance Level (EAL) 3+

Common Criteria

- **z/VM Version 5.3**
  - **Currently in evaluation for CAPP/LSPP EAL 4+**
  - **YE 2007**
- **z/VM Version 5.2**
  - **Will not be certified**
  - **Statement of Direction modified by z/VM V5.3 announcement**
- **z/VM Version 5.1**
  - **Withdrawn from service September 2007**

Thanks!