Session 17520

Virtual Security Zones on z/VM

Alan Altmark
Senior Managing z/VM Consultant
IBM Systems Lab Services
Agenda

- Introduction
- Securing System z hardware
- A multi-zone network
- VLANs and traffic separation
- Enforcing the rules
The Myth of Mainframe Security
The Reality of Mainframe Security
Securing the Hardware
z/VM Security begins with System z security

- Protect the HMC
  - Don’t share user IDs
  - …but don’t be afraid to connect it to your internal network
  - Limit span of control as appropriate; add roles

- Protect the I/O configuration
  - Create a separate LPAR that is authorized to modify the I/O configuration
  - Give partitions access only to devices they require
<table>
<thead>
<tr>
<th>LPAR 1</th>
<th>LPAR 2</th>
<th>LPAR 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>z/VM production</td>
<td>z/OS production</td>
<td>Dynamic I/O configuration management authority</td>
</tr>
<tr>
<td>Minimal z/OS or z/VM</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**PR/SM**

I/O device access is controlled by PR/SM

- Ethernet
- HiperSockets

**SHARE in Orlando 2015**

Complete your session evaluations online at [www.SHARE.org/Orlando-Eval](http://www.SHARE.org/Orlando-Eval)

© 2008, 2014 IBM Corporation
Warning: Shared Open Systems Adapters

A shared OSA creates a “short circuit” between LPARs unless QDIO data connection isolation is used.

Complete your session evaluations online at www.SHARE.org/Orlando-Eval

© 2008, 2014 IBM Corporation
A HiperSocket is a LAN segment.

Treat is like one.
Multi-zone Networks
A DMZ (demilitarized zone) is the name given to the subnet that insulates critical network components (servers) from a public network.
Firewalls

“Where, oh, where has my firewall gone?”
Inboard (internal) firewalls
Outboard (external) firewalls
Guest LANs with HiperSockets

LPAR 1

web
web
web
web

app
app
app

z/VM

LPAR 2

z/OS
DB2

HiperSockets

PR/SM

Internet

= Firewall Router

Complete your Session evaluations online at www.SHARE.org/2015/Eval
© 2008, 2014 IBM Corporation
HiperSockets & z/OS packet filters

LPAR 1

web
web
web
web

web

web

web

app
app
app
app

app

app

app

HiperSockets

Internet

PR/SM

LPAR 2

z/VM

z/OS
DB2

Comms
Server
packet
filter

= Firewall Router

Complete your session evaluations online at www.SHARE.org/Orlando-Eval

© 2008, 2014 IBM Corporation
VLAN Separation
VLAN-unaware VSWITCH

SET VSWITCH FLOOR2
GRANT LINUXn

← Virtual access port

← Physical access port on VLAN 10

© 2008, 2014 IBM Corporation

Complete your session evaluations online at www.SHARE.org/Orlando-Eval
© 2008, 2014 IBM Corporation
VLAN-aware VSWITCH

SET VSWITCH FLOOR1
GRANT ROUTER
PORTTYPE TRUNK
VLAN 10 20

SET VSWITCH FLOOR1
GRANT LINUX3
PORTTYPE ACCESS
VLAN 20

Virtual trunk port ➔

Virtual access port

Physical trunk port

Complete your session evaluations online at www.SHARE.org/Orlando-Eval

© 2008, 2014 IBM Corporation
Access vs. Trunk

Access port and Trunk port

When used on a trunk port, the switch will associate it with the native VLAN ID (VID)

Tagged Ethernet Type II Frame (discarded by access port)

Trunk port
Network with VSWITCH (fully shared)

With 1 VSWITCH, 3 VLANs, and a multi-domain firewall
Multi-zone Network with VSWITCH (red zone physical isolation)

With 2 VSWITCHes, 3 VLANs, and a multi-domain firewall

Complete your session evaluations online at www.SHARE.org/Orlando-Eval

© 2008, 2014 IBM Corporation
Enforcing the Separation
Turn off backchannel communications

- No user-defined Guest LANs
  - VMLAN LIMIT TRANSIENT 0
- No virtual CTC
  - MODIFY COMMAND DEFINE IBMCLASS G PRIVCLASS M
- No IUCV
  - Use explicit IUCV authorization in the directory, not IUCV ALLOW or IUCV ANY
- No secondary consoles
  - MODIFY COMMAND SET SUBCMD SECUSER IBMCLASS G PRIVCLASS M
- But what else might there be?
Turn off backchannel communications

- VMCF
  - MODIFY DIAGNOSE DIAG068 IBMCLASS G PRIVCLASS M
- ESA/XC mode address space sharing
- DCSS
- New interfaces added by APAR or new releases
- Google “less than class g” by Rob van der Heij
- Too hard for some folks

- Consider RACF Mandatory Access Controls instead
  - SELinux provide the same capabilities for Linux
Multi-Zoning with RACF

• Mandatory access controls override end user controls
  – Users are assigned to one or more named projects
  – Minidisks, guest LANs, VSWITCHes, and VLAN IDs, NSSes, DCSSes, spool files
    • all represent data in those same projects
  – Users can only access data in their assigned projects
  – Overrides user- or admin-given permissions
Multi-Zoning with RACF

• A Security Label combines the concepts of
  – Security clearance (secret, top secret, eyes only)
  – Information zones

• Information zones apply to any place data may exist
  – disks, networks, and other users

• Security clearance
  – Ensures servers cannot see extra-sensitive data in their information zone
  – Prevents copying of data to medium that is readable by servers with lower security clearance ("No write down")
  – Not prevalent since there is no equivalent in distributed networking solutions

• Label “dominance” is established based on intersection of zones and security clearance
  – Not just a simple string comparison
Multi-zone z/VM LPAR with RACF Security Label Enforcement
Multi-Zoning with RACF

- Create security levels and data partitions

RDEFINE SECDATA SECLEVEL ADDMEM(DEFAULT/100)
RDEFINE SECDATA CATEGORY ADDMEM(DMZ APSS DATA)

RDEFINE SECLABEL RED  SECLEVEL(DEFAULT) ADDCATEGORY(DMZ)  UACC(NONE)
RDEFINE SECLABEL GREEN SECLEVEL(DEFAULT) ADDCATEGORY(APPS)  UACC(NONE)
RDEFINE SECLABEL BLUE  SECLEVEL(DEFAULT) ADDCATEGORY(DATA)  UACC(NONE)
Multi-Zoning with RACF

- Assign virtual machines their SECLABELs
  - PERMIT BLUE CLASS(SECLABEL) ID(LINUX1) ACCESS(READ)
  - ALTUSER LINUX1 SECLABEL(BLUE)
  - PERMIT RED CLASS(SECLABEL) ID(LINUX2) ACCESS(READ)
  - ALTUSER LINUX2 SECLABEL(RED)
Multi-Zoning with RACF

• But sometimes a server serves the Greater Good, providing services to all users

• Exempt server from label checking

• Assign predefined label SYSNONE

PERMIT SYSNONE CLASS(SECLABEL) ID(TCPIP) ACCESS(READ)

ALTUSER TCPIP SECLABEL(SYSNONE)
Multi-Zoning with RACF

• Example: Assign labels to resources
  – VMMDISK: Minidisk
  – VMLAN: Guest LANs and Virtual Switches

  – RALTER VMMDISK LXHTTP01.191 SECLABEL(RED)
  – RALTER VMMDISK LXHTTP01.201 SECLABEL(RED)

  – RALTER VMLAN SYSTEM.INTERNET SECLABEL(RED)

  – RALTER VMLAN SYSTEM.APPDATA SECLABEL(SYSNONE)
  – RALTER VMLAN SYSTEM.APPDATA.0010 SECLABEL(BLUE)
  – RALTER VMLAN SYSTEM.APPDATA.0020 SECLABEL(RED)

  – PERMIT SYSTEM.APPDATA.0010 CL(VMLAN) ID(LINUX1) ACC(UPDATE)
  – PERMIT SYSTEM.APPDATA.0020 CL(VMLAN) ID(LINUX2) ACC(UPDATE)
Multi-Zoning with RACF

• Activate RACF protection
  – SETROPTS CLASSACT(SECLABEL VMMDISK VMLAN)
  – SETROPTS RACLIST(SECLABEL)
  – SETROPTS MLACTIVE(WARNINGS)
    • If resource doesn’t have a seclabel, message is issued and seclabels are ignored.
  – Or
  – SETROPTS MLACTIVE(FAILURES)
    • If resource doesn’t have a seclabel, command fails.
      – This is more secure!
Summary

• Check network design with network architect

• Place firewalls where the network security team wants them to go

• Use common sense
  – Protect the hardware
  – Protect your data
  – Protect your servers
  – Protect your company
  – Protect yourself!!
Reference Information

• This presentation

• z/VM Security resources

• z/VM Secure Configuration Guide

• System z Security

• z/VM Home Page
Contact Information

Alan C. Altmark
Senior Managing z/VM Consultant
z Systems Delivery Practice
IBM Systems Lab Services

IBM
1701 North Street
Endicott, NY 13760

Mobile 607 321 7556
Fax 607 429 3323
Email: alan_altmark@us.ibm.com

Mailing lists: IBMTCP-L@vm.marist.edu
IBMVM@listserv.uark.edu
LINUX-390@vm.marist.edu