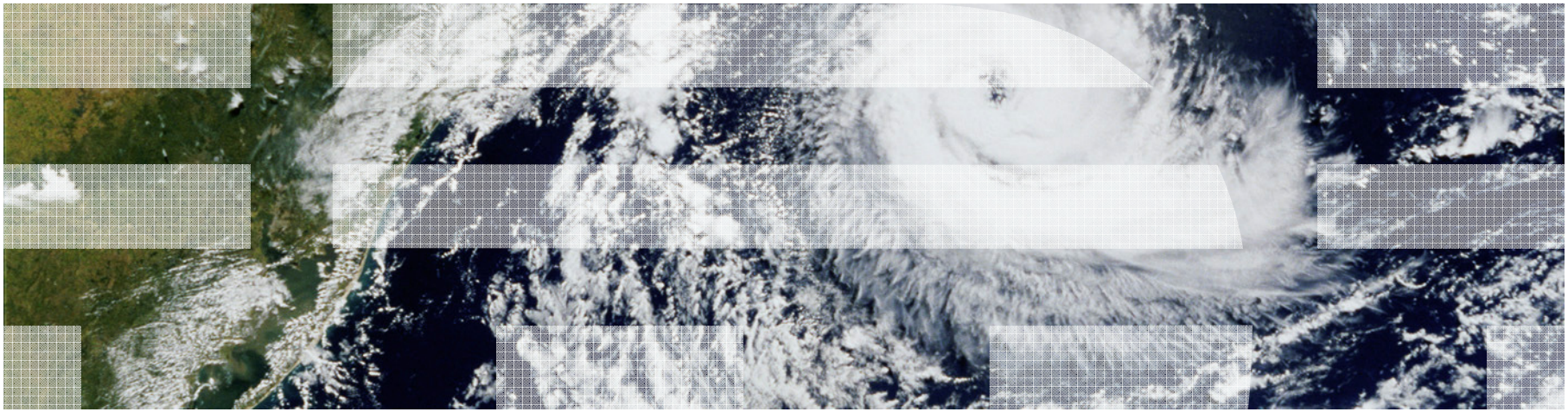
Brian W. Hugenbruch, CISSP
z/VM Security Design and Development
bwhugen@us.ibm.com

IBM

z/VM Security Commands and Features:
Defense in Depth



Trademarks

The following are trademarks of the International Business Machines Corporation in the United States, other countries, or both.

Not all common law marks used by IBM are listed on this page. Failure of a mark to appear does not mean that IBM does not use the mark nor does it mean that the product is not actively marketed or is not significant within its relevant market.

Those trademarks followed by ® are registered trademarks of IBM in the United States; all others are trademarks or common law marks of IBM in the United States.

For a complete list of IBM Trademarks, see www.ibm.com/legal/copytrade.shtml:

*, AS/400®, e business(logo)®, DBE, ESCO, eServer, FICON, IBM®, IBM (logo)®, iSeries®, MVS, OS/390®, pSeries®, RS/6000®, S/30, VM/ESA®, VSE/ESA, WebSphere®, xSeries®, z/OS®, zSeries®, z/VM®, System i, System i5, System p, System p5, System x, System z, System z9®, BladeCenter®

The following are trademarks or registered trademarks of other companies.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.
Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.
Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.
Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
UNIX is a registered trademark of The Open Group in the United States and other countries.
Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.
ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.
IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency, which is now part of the Office of Government Commerce.

* All other products may be trademarks or registered trademarks of their respective companies.

Notes:
Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.
IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.
All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.
This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.
All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.
Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.
Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Disclaimer

The information contained in this document has not been submitted to any formal IBM test and is distributed on an "AS IS" basis without any warranty either express or implied. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer's ability to evaluate and integrate them into the operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

In this document, any references made to an IBM licensed program are not intended to state or imply that only IBM's licensed program may be used; any functionally equivalent program may be used instead.

Any performance data contained in this document was determined in a controlled environment and, therefore, the results which may be obtained in other operating environments may vary significantly. Users of this document should verify the applicable data for their specific environments.

It is possible that this material may contain reference to, or information about, IBM products (machines and programs), programming, or services that are not announced in your country. Such references or information must not be construed to mean that IBM intends to announce such IBM products, programming or services in your country.

Objectives of this Presentation

- To discuss what security means in the z/VM in the context of z/VM
- To discuss the various security options, knobs, dials and widgets available in base z/VM, from the inside out
- To reinforce the idea of layered security
- To discuss (briefly) why an External Security Manager for z/VM is a Good Thing
- **Note**: This presentation does **not** make any claims about Best Practices

Thinking about Security

- **Security** is maintaining the *availability*, *integrity* and *confidentiality* of your information and system services

- A single layer of defense can mean a single point of failure.

- Enforcing security means knowing the capabilities of your virtual machines and your system
  - how CP handles **authentication** of user identity, **authorization** of privileged functions, and the **auditing** of security-relevant data.

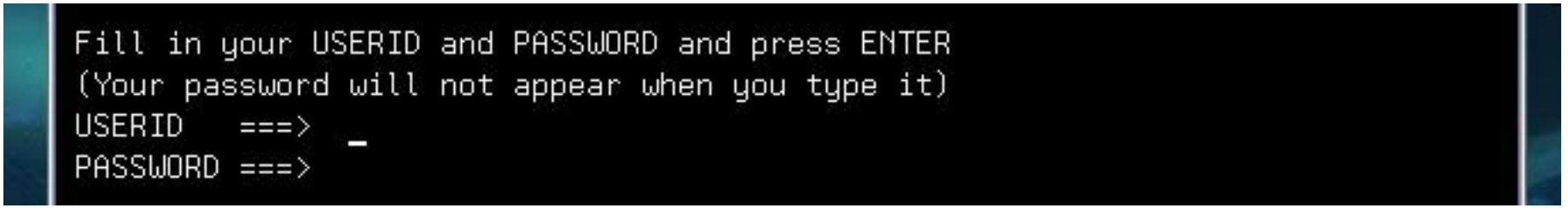
- Knowing where the knobs and dials are allows for the fine-tuning of a system so that it can follow your access model of choice … and meet today's favorite certifications

Thinking about Security … in z/VM terms

- Defending a single virtual machine
- Defending the Control Program
- Protecting data in flight
- Protecting data at rest
- What about adding ESM to your z/VM system?
  - How to reinforce the walls

Defending a Single Virtual Machine

Authentication in z/VM



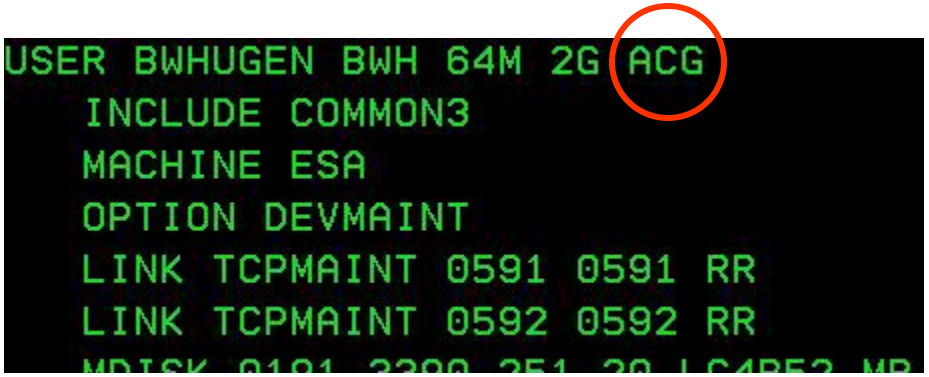
- Each virtual machine has its own userid
  - establishes a unique id to the hypervisor layer
  - forms the foundation of isolation (separation of guests)

- Password-protected
  - up to 8 alphanumeric characters
  - stored in clear text in USER DIRECT
  - obfuscated in the object directory
  - advanced functionality comes from ESMs

Authorization in z/VM

- A user, *once authenticated*, should only have access to system resources which are within scope of responsibility or have been specifically granted
  - This applies to **commands**, **interfaces**, **devices**, and **data**

- The *privilege class* is your first line of protection



- Each user is assigned one or more privilege classes
  - The default for a general user is G

- Defines what commands and DIAGNOSE functions the userid can issue

Defending a Single Virtual Machine

There are seven* IBM-defined Privilege Classes …

A: *System Operators*

B: *System Resource Operators*

C: *System Programmers*

D: *Spooling Operator*

E: *System Analyst*

F: *Service Representative*

G: *General User*

ANY: Commands available to anyone.

… for four kinds of virtual machines:

1. **General user:** Class G authority or less.
2. **Privileged user**: any user with more than Class G authority.
3. **Trusted server**: a virtual machine with high authority which is important to system functionality (e.g., TCPIP). Runs disconnected.
4. **System Operator**: very privileged, but not necessarily trusted!

The capabilities of a virtual machine can therefore be defined based upon the role or roles it is expected to carry out (Role-Based Access Control).

* Class H is also reserved by IBM.

Defending a Single Virtual Machine

But sometimes a Privclass has more power than we want to grant to a single virtual machine.

Class G has over 60 commands, not including the QUERY, DEFINE and SET parameters.

Very few of these are required for the IPL of a Linux guest.
Does a class G user really need QUERY NAMES?
- (See “Less Than Class G”, available on an internet near you.)

Likewise, giving a new Privclass to a user, *especially* for one command, can lead to disastrous consequences.

The FOR and SEND commands are Class C.
But so is the STORE HOST command.

Excess privilege is the root of all evil.

Defending a Single Virtual Machine

So what options are available?

1. Local modification – SET PRIVCLASS (Class ANY and Class C)
   - Remove class authority from inside a virtual machine.
     - `SET PRIVCLASS * -AC`
   - But be careful; the Class C version can exceed directory-granted privilege!

2. Global modification – `MODIFY CMD` and `MODIFY DIAGNOSE` (Class A)
   - Dynamically redefine a command into a different privilege class.
     - `MODIFY COMMAND SHUTDOWN PRIVCLASS S`
     - `MODIFY COM XAUTOLOG IBMCLASS A PRIVCLASS OUX`
     - `MODIFY CMD QUERY SUBCMD NAMES IBMCLASS G PRIVCLASS Z`
     - `MODIFY COMMAND XAUTOLOG RESET`
     - `MODIFY DIAG 94 PRIVCLASS V`

Defending a Single Virtual Machine

Defining new privilege classes … some quick thoughts:

- Can be associated with letters I-Z, and numbers 1-6
- Can contain both IBM commands and locally created commands
- Consider associating the new privclass with certain system roles
  - Helps to coordinate with regulations, certifications and laws
  - While redefining a command to Class Z (for example) can be an easy way to isolate a particular command, one could quickly lose track of what commands belong in which class and why
- User-defined privilege classes won't automatically gain new capabilities in a new release of z/VM

Defending a Single Virtual Machine

Sometimes functionality needs more than a privilege class to define it.

- CSL DMSPASS uses Diagnose x'88' (password / passphrase checking)
- CSL DMSLINK accesses a virtual machine's minidisk or reader queue

We may also only want a command to be issued during virtual machine IPL – assigning it to a new privilege class is overkill, and redefining a privilege class for this may not be worthwhile. (Same goes for PROFILE EXEC updates to SET PRIVCLASS.)

For this, we return to the user directory:

```
OPTION DIAG88
LOGONBY BWHUGEN ALTMARKA WILKINS
COMMAND QUERY VIRTUAL 4567
```

Defending a Single Virtual Machine

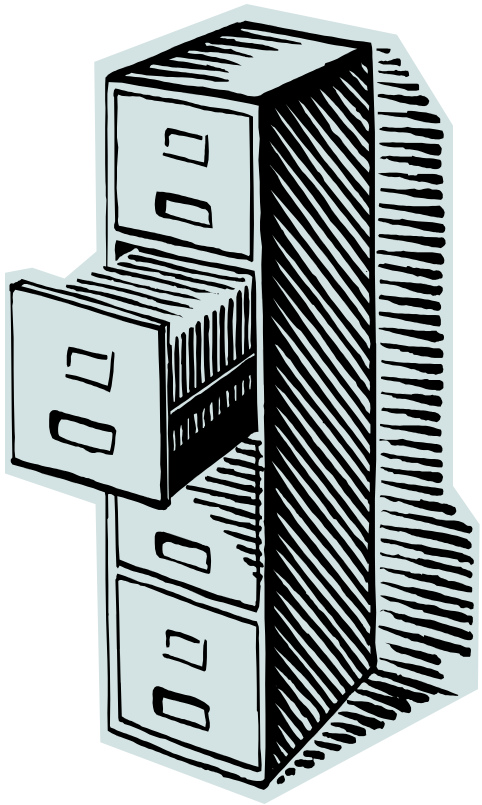
- **OPTION User Directory Statement**

OPTION	Related CMD or Diag	OPTION	Related CMD or Diag	OPTION	Related CMD or Diag	OPTION	Related CMD or Diag
ACCOUNT	DIAG04C	DIAG88	X'88'	LXAPP	X'2C4' (alt: Class B)	QUICKDSP	---
APPLMON	DIAG0DC	DIAG98	X'98'	MAINTCCW	(various)	RMCHINFO	---
CFVM/CFUSER	---	D84NOPAS	X'84'	MAXCONN	---	SETORIG	X'F8'.0
COMSRV	---	IGMAXU	---	MAXVMCFI	---	STGEXEMPT	---
CONCEAL	---	LANG	---	MIH	---	SVC76M	---
CPUID	---	LKFAC	SET LKFACR	NOMEMASSIST	---	SVMSTAT	---
CRYMEASURE	---	LNKEXCLU	LINK ER,EW	NETACCOUNTING	---	TODENABLE	SET VTOD
DEVINFO	X'E4'.0, .1	LNKNOPAS	LINK	NETROUTER	---		
DEVMAINT	X'E4'.0, .1	LNKSTABL	LINK SR,SW	NOKDCFS	---		

  - Enables functionality at the directory level; it doesn't belong to any one job
  - May also be too powerful to allow into a single privilege class
  - Requirements vary by command (DIAG88 vs. LXAPP)

z/VM Auditing Pro-Tip

- `OPTION ACCOUNT / ACCT:`
  - Grants access to Diag x'4C' and allows the user to access the *ACCOUNT system service
  - Allows user to generate accounting records (logon data, minidisk linking, other forms of basic auditing).
  - Normally, accounting records are held by DISKACCT.
  - CP command `RECORDING` (Classes A, B, C, E, or F for various features) can be used to start/stop recording, purge records, or change processing parameters.
  - `RETRIEVE ACCOUNT`
    - gathers pertinent accounting records associated with your virtual machine.



Defending a Single Virtual Machine

- **LOGONBY User Directory Statement**
  - Allows the logging on of a virtual machine with another user's credentials
    - `LOGON OPERATOR by BWHUGEN`
  - BWHUGEN's password is entered instead of OPERATOR's
  - Instead of sharing a single userid/password among multiple administrators, this provides accountability.

To require LOGONBY access for a userid, the USER statement must be modified:

```
>>-User--userid--+-password-+------------------------------>
                 +-NOLOG----+
                 +-NOPASS---+
                 +-AUTOONLY-+
                 '-LBYONLY--'
```

To grant LOGONBY access to other users, the LOGONBY statement must be added:

```
USER OPERATOR LBYONLY
...
LOGONBY BWHUGEN FARMAN JFRANCIS
```

Defending a Single Virtual Machine

- **COMMAND User Directory Statement**
  - Executes a command on the virtual machine after LOGON but before IPL.
  - Useful for connecting to virtual LANs and attaching devices without requiring the full authority of an associated privilege class.

```
>>-+-COMMAND-+--command-------------------------------------><
   '-CMD-----'
```

  - A single command is limited to 220 characters
  - Though, multiple COMMAND directory statements can exist for a virtual machine

```
COMMAND VARY ON 1234
COMMAND ATTACH 1234 TO &USERID AS 4567
```

Defending CP

SYSTEM CONFIG is to z/VM as a user directory entry is to a single virtual machine. It contains multiple statements which can define and enhance security at CP initialization time.

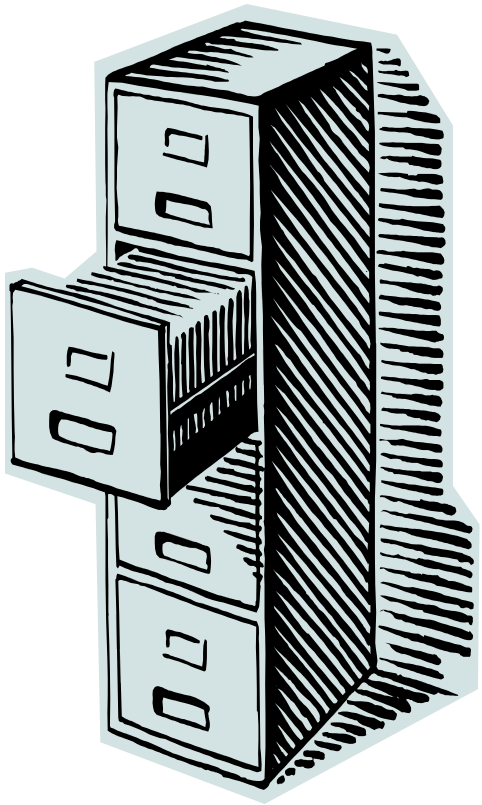
1. `ENABLE / DISABLE / MODIFY COMMAND` or `DIAGNOSE`. The static way to make system-wide privclass-related changes to available functionality.
2. `ALTERNATE OPERATOR`: define specific userids who can become system operator if OPERATOR is shut down.
3. `PRIV_CLASSES` statement: redefine privilege class(es) necessary for certain functions: `IOCP_READ, IOCP_WRITE, OPERATOR, USER_DEFAULT, HW_SERVICE`
4. `FEATURES:`
   - `PASSWORDS_ON_CMDS`
   - `ENABLE/DISABLE CLEAR TDISK`
   - `ENABLE/DISABLE SET_PRIVCLASS`

z/VM Auditing Pro-Tip

- `SYSTEM_USERIDS` Statement: specify certain virtual machines associated with system maintenance functions … including the VM which receives accounting records.

- `JOURNALING` Statement: establishes a more granular form of accounting record generation at system start-up
  - rules for the number of invalid minidisk access / logon attempts before warnings are noted / messages are sent
  - Can also be configured to disable access after `nnn` invalid attempts, or issue a CP-enforced Lockout for `mmm` minutes.
  - This facility is OFF by default

- `QUERY/SET JOURNAL` to understand or adjust settings



Defending CP

Setting Secondary Users and Observers

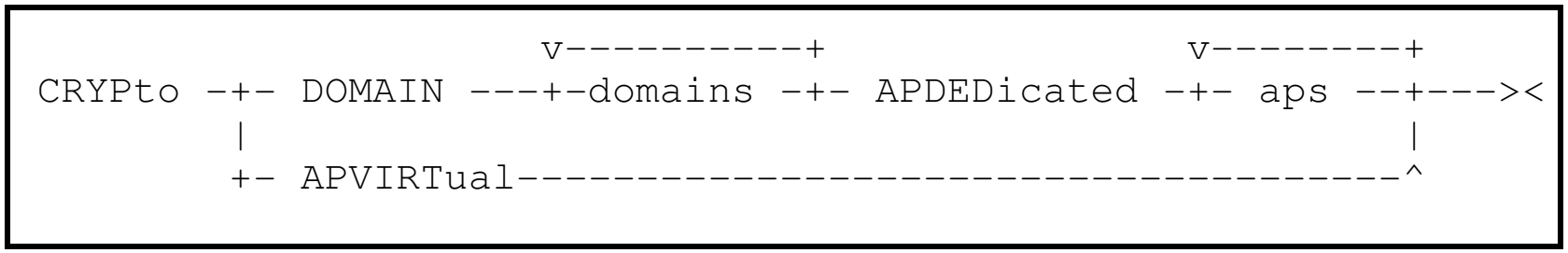
- Rather than logging onto (for example) OPERATOR, one can designate another virtual machine as an **Observer** (view console, but cannot interact) or as a **Secondary User** (sees console, can issue commands on behalf of that virtual machine).
- `QUERY/SET OBSERVER`
- `QUERY/SET SECUSER`
- `CONSOLE` User Directory Statement

Caution: setting someone as a secondary user for another virtual machine can grant unintentionally broad authorities

- **Example**: anyone set as SECUSER for OPERATOR gains Class A authority, whether they have it for themselves or not. This means `CP SHUTDOWN` is now a valid command for them to issue.

Defending CP: Crypto

The CRYPTO User Directory statement grants access to particular domains/APs on available Crypto Express Cards (`CEX2A, CEX2C, CEX3A, CEX3C` ...):



`QUERY CRYPTO`

(Class A, B, C, E) will display which domains/APs are available. Note that this list will be limited to devices available to the LPAR.

`APDED`

Domains granted in the directory are “reserved for dedication”; they are not actually in-use until the virtual machine logs on.

`APVIRT`

Access makes use of shared queues controlled by the system.

Defending CP: The User Directory

- **Without** a Directory Manager:
  - DIRECTXA is the CP utility to update the user directory
  - Requires Class A, B or C authority to issue
  - Lives on the MAINT-controlled disk (away from general users)

- **With** a Directory Manager (using DIRMAINT ***for example purposes only***):
  - The source directory / backups sit on a protected disk
  - The object directory is updated through DIRMAINT operations
  - All DIRMAINT commands and options are authority-controlled
    - Using a separate set of privileges – NOT CP privclasses
    - A, D, G, H, M, O, P, S, Z – each has its own role, and DIRMAINT commands are tied to one of these
    - Separate authorization file inside of DIRMAINT
  - DIRMAINT will also coordinate with RACF

- **Either way:** Be mindful of the default passwords in the User Directory!

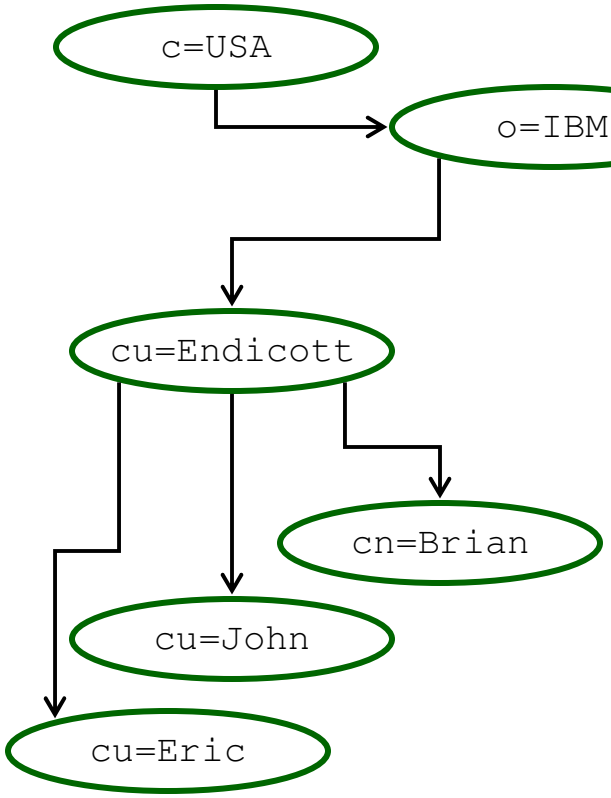
Controlled Logon

- As previously mentioned: LOGONBY, SECUSER, OBSERVER …

- Logon controls also exist for:
  - FTP
  - NFS
  - REXEC

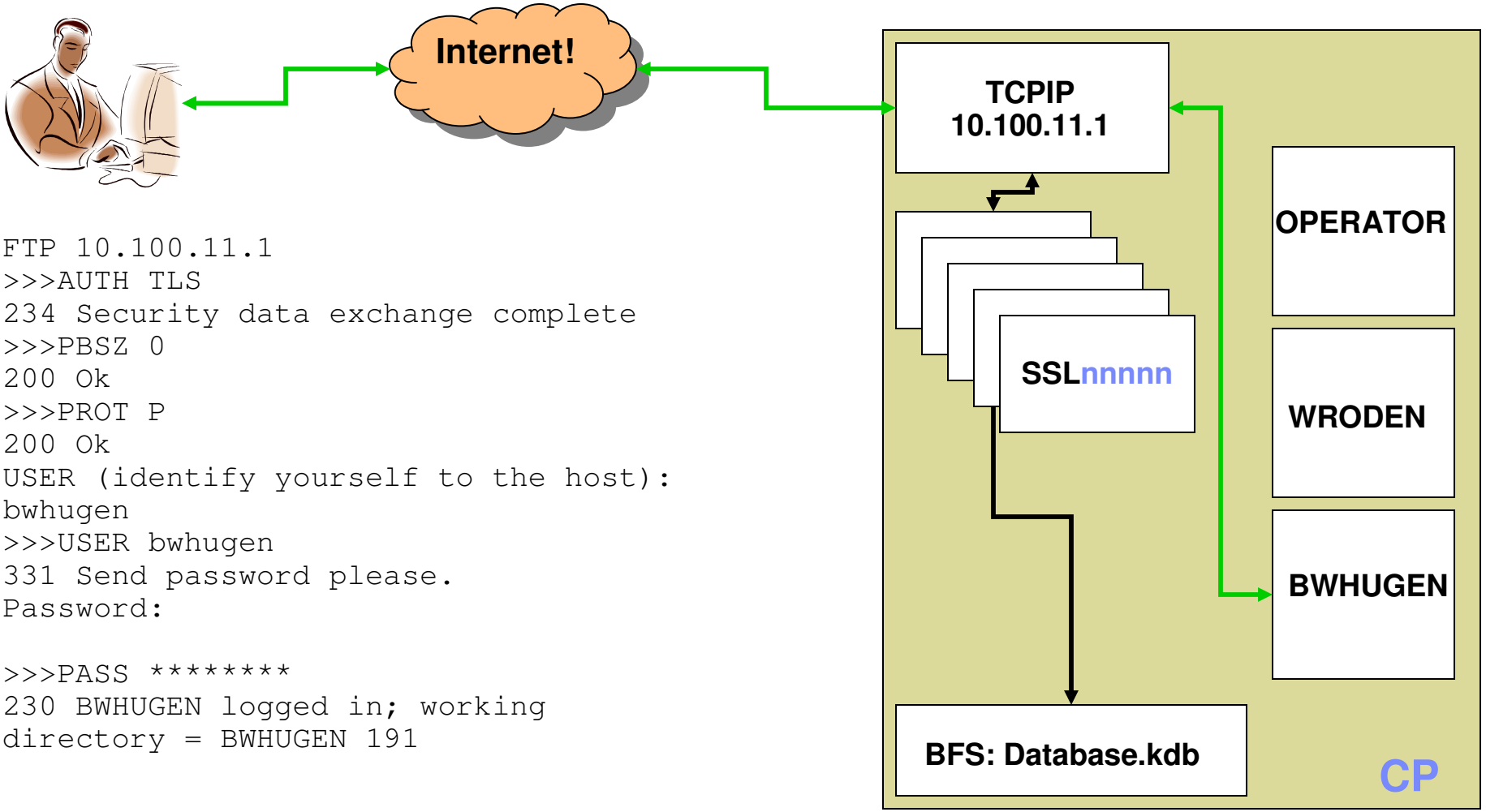
- Logging onto the system is managed through a controlled diagnose instruction – the client session has the capabilities of the logged-on user, instead of the initiating user
  - Adjustable through various configuration files

Identity in Flight: LDAP



- Identity management for z/VM (and its hosted operating systems) can be extended through LDAP
- Based on the z/OS IBM Tivoli Directory Server
- Each server machine can handle a single Directory Information Tree (DIT) with a single schema
  - Object classes, object names, object attributes
- Can support a few different schema types
- Interfaces with various database managers as back-end handlers, including ESMs
  - ESM support for remote audit / authorization
- Both LDAP client and server can use System SSL in z/VM; supports secure connectivity
  - Not necessarily associated with the z/VM SSL Server virtual machine

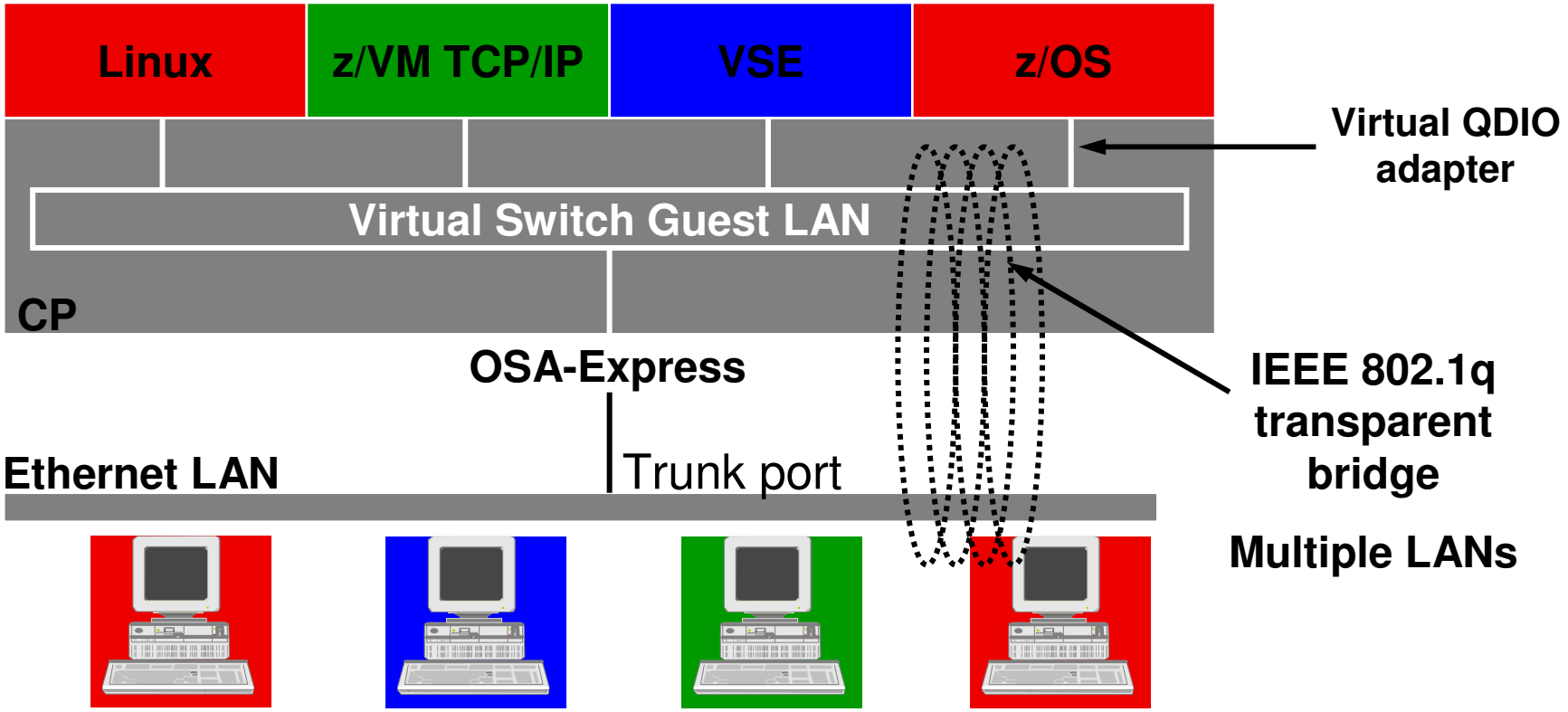
Data In Flight: SSL and TLS



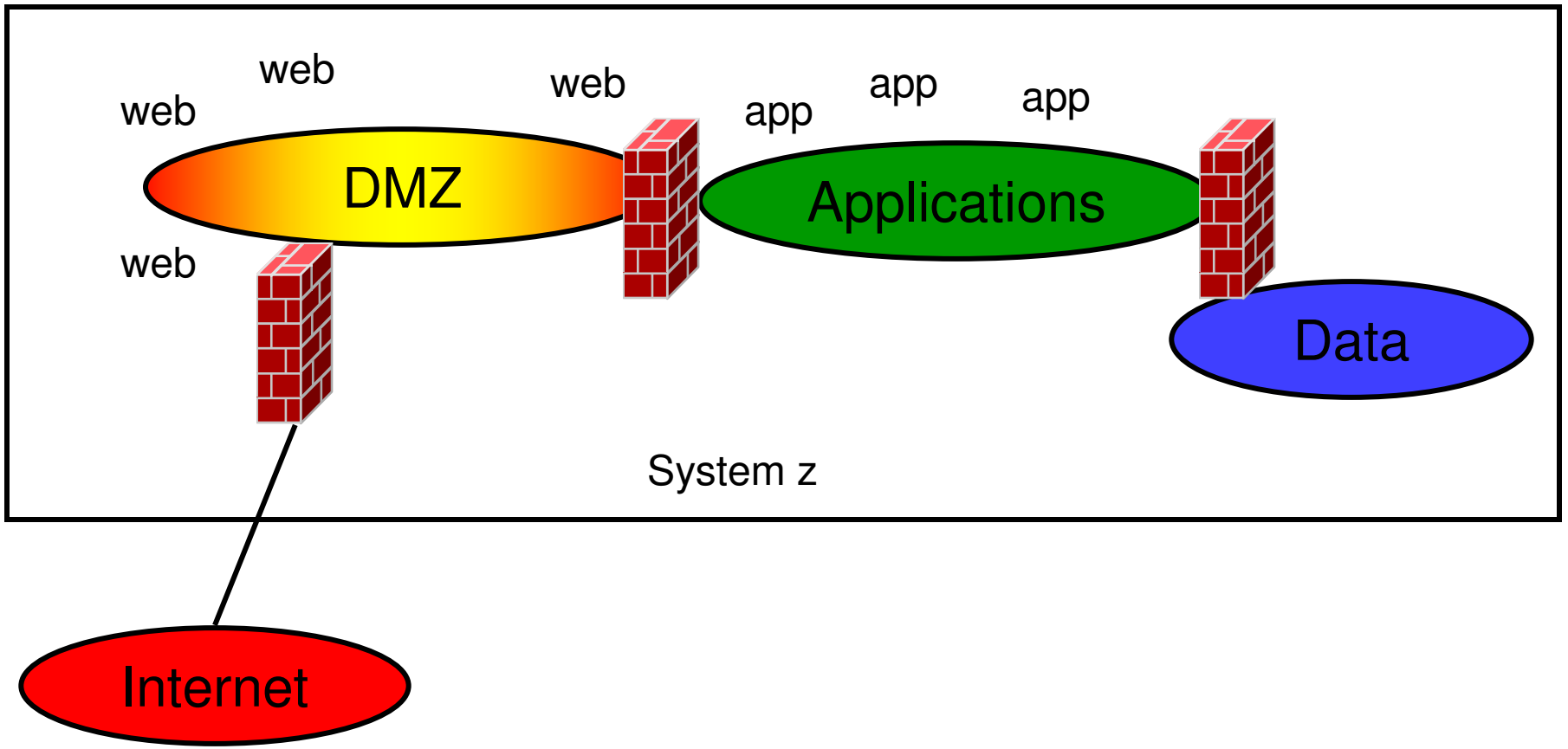

```
FTP 10.100.11.1
>>>AUTH TLS
234 Security data exchange complete
>>>PBSZ 0
200 Ok
>>>PROT P
200 Ok
USER (identify yourself to the host):
bwhugen
>>>USER bwhugen
331 Send password please.
Password:

>>>PASS ********
230 BWHUGEN logged in; working
directory = BWHUGEN 191
```

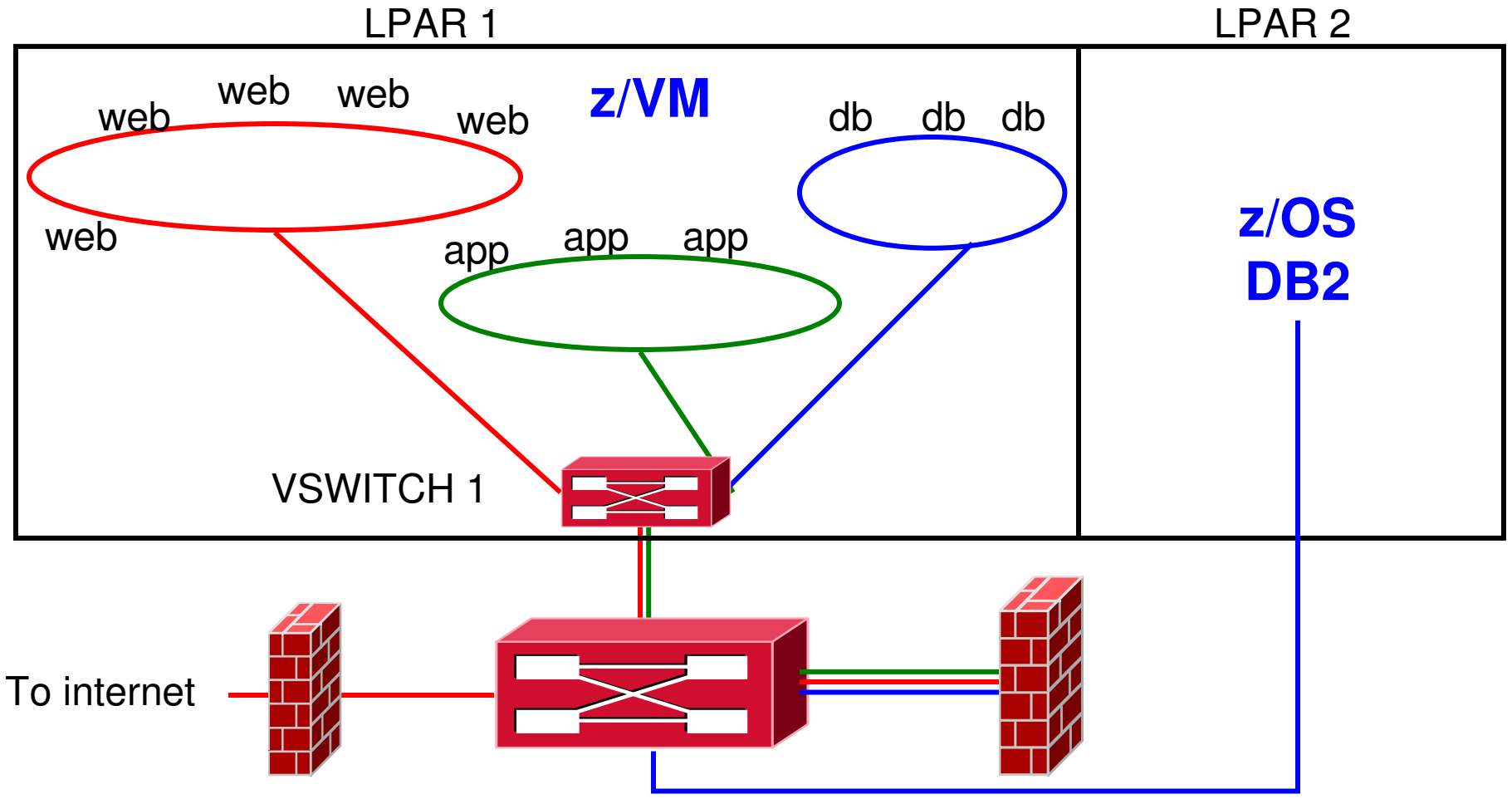
z/VM Virtual Switch – VLAN aware



Multi-zone Network on System z



Protecting Data In Flight: VLANs and VSWITCHes



With 1 VSWITCH, 3 VLANs, and a multi-domain firewall

Protecting Data At Rest

Protecting Data At Rest: File Systems

- Minidisks, as defined in the User Directory, can be guarded by passwords.
- A virtual machine controls access to the minidisks defined as a part of its user directory entry.
- If an MDISK statement has no passwords, then another user cannot link to it dynamically.
  - If the second user has a LINK in its own user directory entry, access can be granted.
- If the MDISK has a password of “ALL,” then no password is required.
  - But who wants free access?
- For certain access modes, an OPTION is required in the User Directory
  - Stable Read/Write, Exclusive Read/Write
- Be mindful of the default passwords in the User Directory!

- An **ESM** may **downgrade** or **reject** a minidisk link request that might otherwise be passed by Native CP.

Protecting Data At Rest: File Systems

- Shared File System (SFS) – a more hierarchical file structure which makes use of available filepools in CMS.
  - Users must first be enrolled into a filepool
  - SFS directories can be accessed at an open filemode, if permissions are granted.
  - `GRANT AUTHORITY <filename> <dirid> TO <user/Public> ( <level>`
  - `<level>: Read, Newread, Write, Newwrite, DIRRead, DIRWrite.`

- Byte-File System (BFS) – an OpenExtensions implementation based on Unix/Linux models. A special subset of filepool operations.
  - Users must be enrolled into the filepool in order to gain access. Posix membership must also be entered in the User Directory.
  - Access can be granted by owners to directories or files through use of `chmod` or `openvm permit`

- File Systems and ESMs:
  - An External Security manager may maintain a greater list of access controls, either on a general basis (profiles) or as a discrete list (DAC checking).

Protecting Data At Rest: Storage

- z/VM supports Encrypted-Read and Encrypted-Write of data to/from the 3592 Model E05 tape drives (and C06 Control Unit)
- Guests don't need to be aware of encryption taking place – operations can be transparent after configuration (if using default keys)
- Requires use of an "out of band" Encryption Key Manager (EKM)

Reinforcing the Walls: ACI and ESMs

So we start to lock all the doors …

- No user-defined Guest LANs
  - VMLAN LIMIT TRANSIENT 0
- No virtual CTC
  - MODIFY COMMAND DEFINE IBMCLASS G PRIVCLASS M
- No VMCF
  - MODIFY DIAGNOSE DIAG068 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 SECUSER IBMCLASS G PRIV M

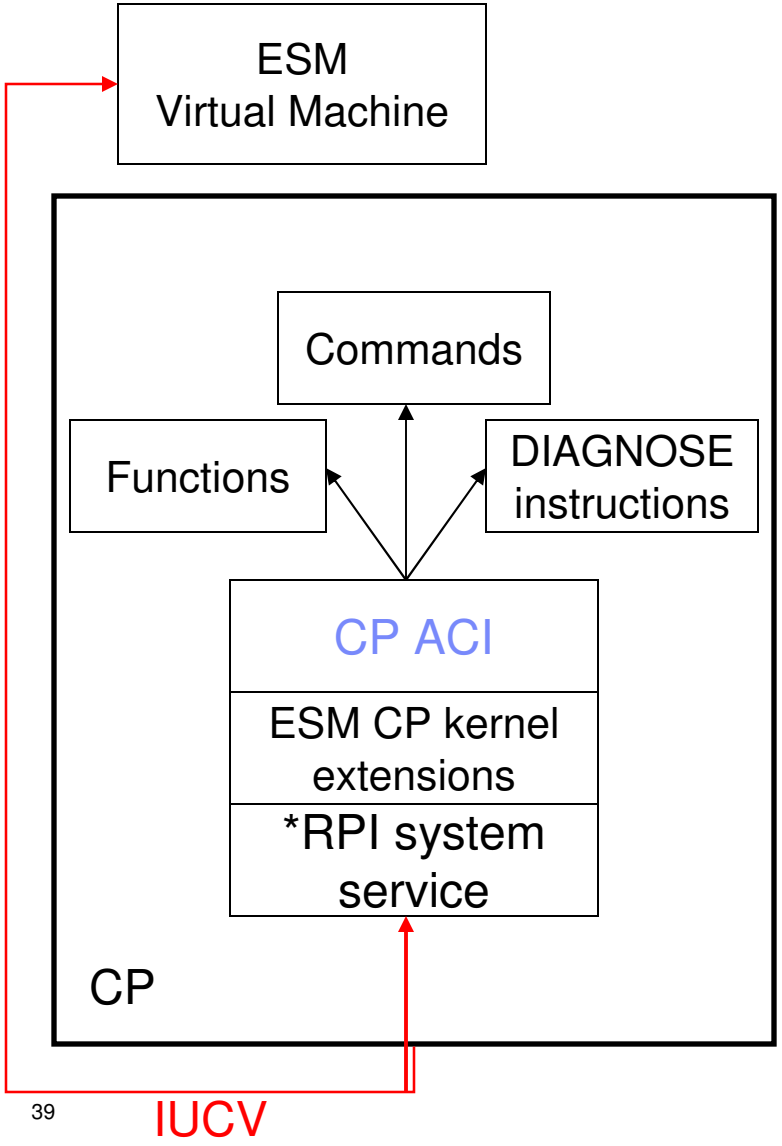
But what else might there be?

… but the more we try to hold on …

- ESA/XC mode address space sharing
- DCSS controls
- “Less than Class G” considerations
- And new interfaces may be added in an APAR

- **Where do we draw the line?**

Reinforcing the Walls: ACI and ESMs



The ACI (Access Control Interface) is the control block CP uses to interact with a given external security manager. Installing an ESM replaces CP stub files with modifications that the ESM can understand.

It is through this interface that CP can validate the activity being processed with the rules, roles and labels programmed into the security manager in use.

When the ACI is accessed in order to confirm authority, the ESM can return one of three possible answers:

- "Authorization granted."
- "Defer security decision to Native CP."
- "Authorization denied."

Reinforcing the Walls: ACI and ESMs

So what does an ESM provide, that Native CP does not?

- Enhanced control of certain commands (STORE HOST, FOR …)
- Control of system resources (VLANs, VSWITCHes, Minidisks, NSSes, shared memory …)
- Configurable overrides for Native CP security commands
- Stronger and more flexible password management (and password phrases)
  - Obfuscated and encrypted
  - 100 characters for password phrases, plus special characters
- DAC and MAC controls (a little more on this in a moment)
- Auditing – lots of auditing.

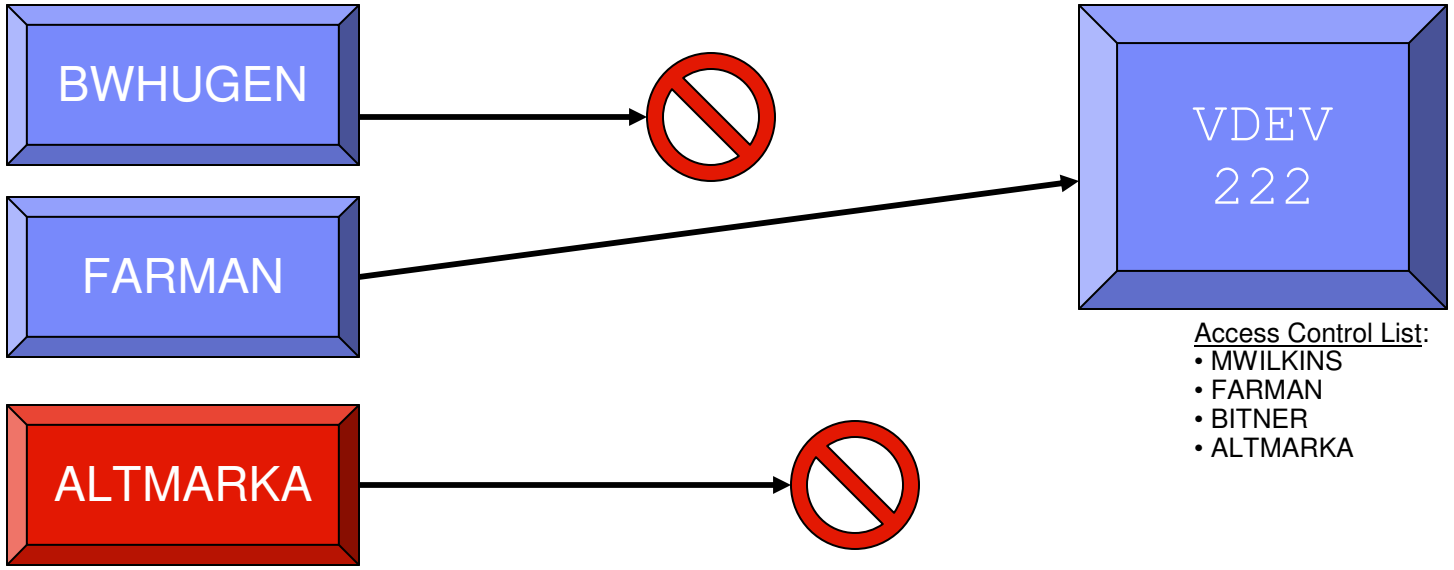
An ESM provides both a finer granularity of control and the ability to enact more complete isolation of guests and projects … in a consolidated interface.

Multi-Zoning with RACF

- **Discretionary Access Controls** (DAC) are set by an end user
  - an Access Control List for a minidisk, for example

- **Mandatory Access Controls** (MAC) are system "rules" that 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
    - **Can always change a "yes" to a "no"; never a "no" to a "yes."**

Discretionary and Mandatory Access Controls



- ALTMARKA (SECLABEL RED) attempts to access 222 and automatically fails (since 222 has SECLABEL BLUE).
- BWHUGEN (SECLABEL BLUE) passes the MAC check, but is still not on the DAC access control list.
- FARMAN (SECLABEL BLUE) can safely access the data.

Multi-Zoning with RACF

Create security levels and data partitions
(using some special RACF commands)

```
RDEFINE SECDATA SECLEVEL ADDMEM(DEFAULT/100)
RDEFINE SECDATA CATEGORY
   ADDMEM(INTERNET DMZ APPS DATA COMMON)
RDEFINE SECLABEL PUBLIC SECLEVEL(DEFAULT)
   ADDCATEGORY(COMMON) UACC(NONE)
RDEFINE SECLABEL RED SECLEVEL(DEFAULT) ADDCATEGORY(DMZ COMMON)
   UACC(NONE)
RDEFINE SECLABEL GREEN SECLEVEL(DEFAULT) ADDCATEGORY(APPS COMMON)
   UACC(NONE)
RDEFINE SECLABEL BLUE SECLEVEL(DEFAULT) ADDCATEGORY(DATA COMMON)
   UACC(NONE)
```

Assign virtual machines their SECLABELs

```
PERMIT RED CLASS(SECLABEL)
   ID(ALTMARKA) ACCESS(READ)
ALTUSER ALTMARKA SECLABEL(RED)

PERMIT GREEN CLASS(SECLABEL)
   ID(BWHUGEN) ACCESS(READ)
ALTUSER BWHUGEN SECLABEL(GREEN)
```

Multi-Zoning with RACF

- **But sometimes a server serves the Greater Good, one must provide services to all users**

- **Exempt server from label checking**

- **Assign system servers label SYSNONE**

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

Multi-Zoning with RACF

Assign labels to resources

- VMMDISK – Minidisk
- VMLAN – Guest LANs and Virtual Switches

```
RALTER VMMDISK LXHTTP01.201 SECLABEL(RED)
RALTER VMLAN SYSTEM.NET1 SECLABEL(RED)
RALTER VMLAN SYSTEM.NET2.0307 SECLABEL(GREEN)
RALTER VMLAN SYSTEM.NET2.0410 SECLABEL(BLUE)
```

If you intend to activate TERMINAL or VMSEGMT classes, those resources all need SECLABELs

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.
This is easier!

Or

```
SETROPTS MLACTIVE(FAILURES)
```

If resource doesn't have a seclabel, command fails.
This is more secure!

Conclusion

- z/VM has layers of security options and features to offer
  - even before an ESM is considered.

- An ESM provides a finer means of control and stricter rules in a consolidated interface
  - But it works best when one understands the features it enhances and protects

- Depending upon configurations, administrators can exploit Role-Based Access, Mandatory Access and/or Discretionary Access control models.

- Select the options that are right for you – and for your company security policy
  - Protect system capabilities
  - Protect data in flight
  - Protect data at rest
  - … and do the auditing to prove that system has been secured.

For more information …

- **Speaker**: Brian W. Hugenbruch, CISSP
  - Web: http://www.vm.ibm.com/devpages/hugenbru
  - Mail: bwhugen at us dot ibm dot com

On the web:

- z/VM Security resources: http://www.VM.ibm.com/security
- z/VM Secure Configuration Guide: http://publibz.boulder.ibm.com/epubs/pdf/hcss0b30.pdf
- System z Security: http://www.ibm.com/systems/z/advantages/security/
- Redbook: z/VM Security, SG24-7471