MVS Security Issues

Steve Wiggin, CISSP
Mutual of Omaha

NEbraskaCERT Conference 2003 Omaha, NE

MVS Security Issues

- A little background
- Not a lot of “techie”
  - Focus is not on RSS’s, but the operating environment
- What’s the problem ?
- Storage protection
- Security related issues

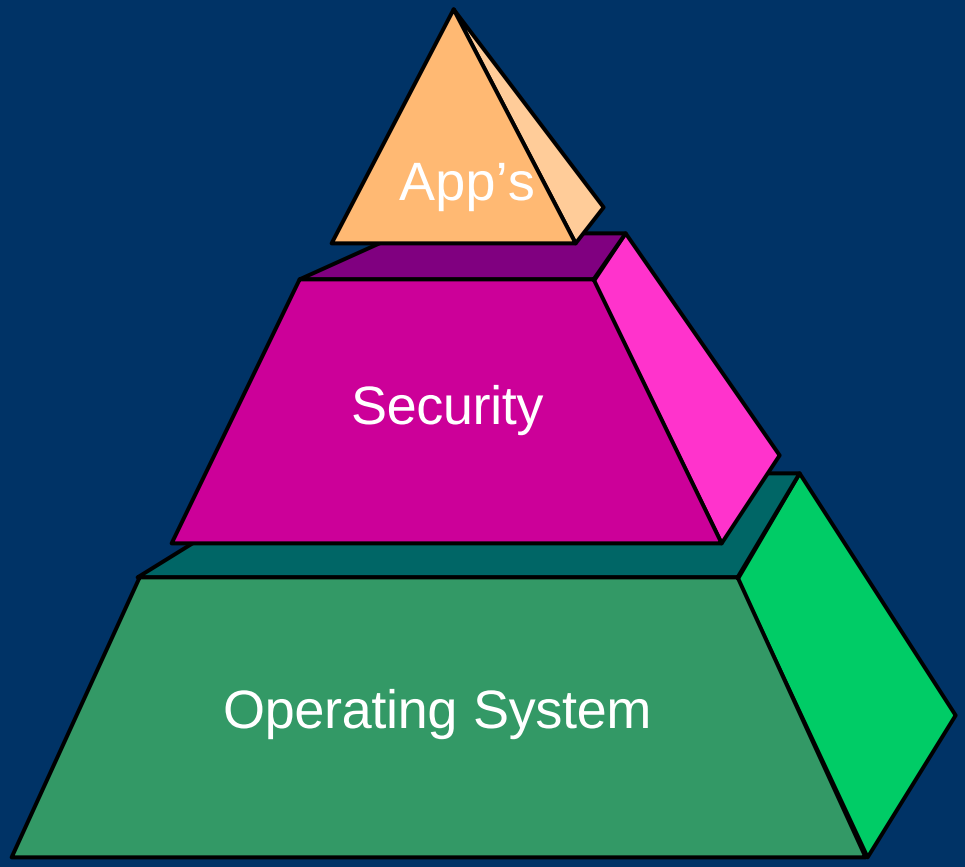
MVS Security Issues
Background

- Predominant operating system for mainframes since the 1960's
- MVS = Multiple Virtual Storage (more on that coming up)
- MVS renamed OS/390; last version of OS/390 is 2.10 before - z/OS
- z/OS versions (so far) are 1.1, 1.2, and bleeding edge 1.3

MVS Security Issues
What's the problem ?

- Perception
  - The mainframe's dead
    - "The report of my death was an exaggeration." Mark Twain, after reading his own obituary, June 2, 1897
  - The mainframe's secure
    - Reliance on the RSS
    - Bank vault analogy
  - This can all lead to a misunderstanding of the issues

MVS Security Issues



MVS Security Issues

~ First, a picture ~

MVS - OS/390 - z/OS

Components:

1. JES
2. DFSMS
3. VTAM
4. TSO
5. Online systems
   (CICS, IMS)

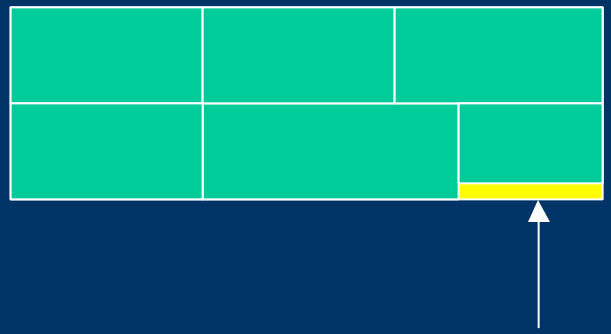
RSS's

CA-ACF2

RACF

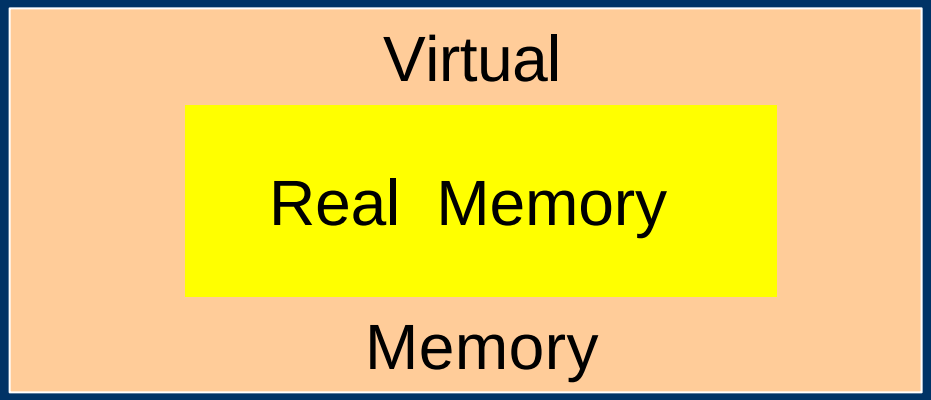
CA-Top Secret

MVS Security Issues



Real Memory

MVS Security Issues



Multiple Virtual Storage

MVS Security Issues
Storage Protection

- Separate Address Space for each user/program
  - their own little chunk of memory (storage)
- RSS's don't control anything in memory
- So how is data in memory protected?

MVS Security Issues
Storage Protection

- Storage protect keys
  - used to prevent unauthorized changes in memory (storage)
  - you need a “key” to change
  - key for every 4k chunk of memory
  - numbered 0 - 15
- What keeps track of all this?
  - The key is in Program Status Word (PSW)

MVS Security Issues
Storage Protection

- Program Status Word (PSW)
  - among other things, indicates the storage protection key held by the instruction
  - indicates the “state” the instruction is running in - more about “states” soon

MVS Security Issues
Storage Protection

- So who can change memory?
  - anyone with an equal key
  - anyone with key 0
- Who can get key 0?
  - many OS programs have key 0
  - macro called MODESET; allows you to change storage protect key in PSW

MVS Security Issues
Storage Protection

- The good news about MODESET is . . .
  - not everyone can use
  - user must have one or more special privileges
    - anyone (or any program) with key 0 (actually, it's probably keys 0 - 7),
    - supervisor (system) state, or
    - Authorized Program Facility (APF)

MVS Security Issues
Storage Protection

- Operating system “states”
  - supervisor (system) state - MVS
    - work done on behalf of the system
  - problem program (user) state
    - work done on behalf of the user
  - system is always in one state or another

MVS Security Issues
Storage Protection

- Authorized Program Facility (APF)
  - not a state, a special characteristic
  - an APF authorized program must reside in an APF-designated library in SYS1.PARMLIB

MVS Security Issues
Storage Protection

- How does a program get APF authorization?
  - a program must be link edited* with AC=1
    - AC = authorization code
  - and an AC=1 load module must reside in an APF-designated library

* Linkage editor - in OS/390 V2 on, and in z/OS, called the program management binder; does essentially the same thing: converts compiled object code into an executable program.

MVS Security Issues
Storage Protection

- Both AC=1 and APF-designated library are required - either alone are meaningless
- APF authorized designation is granted through SYS1.PARMLIB(PROG00)

MVS Security Issues
Storage Protection

Storage Protect Key Assignments

0	MVS-OS/390-z/OS
1	JES
2-4	Reserved by IBM
5	Data management - DFSMS
6	VTAM
7	IMS
8	V=V (virtual) - batch, TSO users
9-15	V=R (real)

MVS Security Issues

Storage Protection

Another key assignment method:

Program Properties Table (PPT)

(SYS1.PARMLIB(SCHEDnn))

Sysview:

SYSVIEW 7.4 CPU1 PROGRAM PROPERTIES TABLE

Entries Available 28, deleted 0

Program	Orig	Ncan	Nswp	Priv	Syst	Ndsi	Npsw	Key	Affn	Sprf	Lprf	Nprf
IEDQTCAM	IBM		NSWP					6	NONE			NPRF
ISTINM01	IBM	NCAN	NSWP		SYST		NPSW	6	NONE			NPRF
IKTCAS00	IBM	NCAN		PRIV	SYST			6	NONE			
AHLGTF	IBM	NCAN	NSWP		SYST			0	NONE			NPRF
HHLGTF	IBM	NCAN	NSWP		SYST			0	NONE			NPRF
IHLGTF	IBM	NCAN	NSWP		SYST			0	NONE			NPRF
IEFIIC	IBM	NCAN		PRIV	SYST			0	NONE			
IEEMB860	IBM	NCAN	NSWP		SYST	NDSI	NPSW	0	NONE			
IEEVMNT2	IBM	NCAN			SYST			0	NONE			
HASJES20	IBM	NCAN	NSWP		SYST	NDSI		1	NONE			
DFSMVRC0	USER	NCAN	NSWP		SYST			7	NONE			

MVS Security Issues
Storage Protection

CA-Examine:

CA-EXAMINE PROGRAM PROPERTIES TABLE ANALYSIS
PPT VERSION ID : 0
THERE ARE 53 PROGRAMS DEFINED IN THE PPT

ENTER S NEXT TO A PROGRAM NAME FOR A SEARCH OF ELIGIBLE APF LIBRARIES.
"*" DENOTES ENTRIES RECOMMENDED FOR REVIEW

PROGRAM NAME	IBM ENTRY	MODULE SOURCE	DATASET INTEGRITY BYPASS	KEY	SECURITY BYPASS	NON-CANCEL	SWAP	SMF TIMING BYPASS	CPU AFFN	PREF STOR FLAG
AHLGTF	YES	IEFSDPPT	NO	0	NO	YES	NO	YES	ALL	001
AKPCSIEP	YES	IEFSDPPT	YES	1	NO	NO	NO	YES	ALL	001
APSPPIEP	YES	IEFSDPPT	YES	1	NO	NO	NO	YES	ALL	001
AVFMNBLD	YES	IEFSDPPT	NO	3	NO	YES	NO	YES	ALL	001
CSVLLCRE	YES	IEFSDPPT	YES	0	YES	NO	NO	YES	ALL	
CSVVFCRE	YES	IEFSDPPT	NO	0	NO	NO	NO	YES	ALL	
DFHSIP	NO	SCHED00	NO	8	YES	NO	NO	NO	ALL	001
DFHSIP	NO	SCHED06	NO	8	YES	NO	NO	NO	ALL	001
DFHSIP	NO	SCHED16	NO	8	YES	NO	NO	NO	ALL	001
DFSMVRCO	YES	IEFSDPPT	NO	7	NO	NO	NO	YES	ALL	
DSNUTILB	YES	IEFSDPPT	NO	7	NO	NO	YES	NO	ALL	
FNMMAIN	NO	SCHED00	NO	6	NO	YES	YES	NO	ALL	
FNMMAIN	NO	SCHED06	NO	6	NO	YES	YES	NO	ALL	
FNMMAIN	NO	SCHED16	NO	6	NO	YES	YES	NO	ALL	
HASJES2A	NO	SCHED00	YES	1	NO	YES	NO	YES	ALL	
HASJES2A	NO	SCHED06	YES	1	NO	YES	NO	YES	ALL	
HASJES2A	NO	SCHED16	YES	1	NO	YES	NO	YES	ALL	
HASJES20	YES	IEFSDPPT	YES	1	YES	YES	NO	YES	ALL	001

MVS Security Issues
Security related issues

Supervisor Calls (SVCs)

- MVS modules that perform supervisor tasks for user programs, e.g., opening datasets (svc0019)
- Get control in Supervisor State & Key 0
- SVC numbers
  - 0 to 199 reserved for IBM
  - 200 - 255 are for installation-written SVCs or third party vendor products

MVS Security Issues
Security related issues

Supervisor Calls (SVCs)

- Installation SVCs are found in SYS1.PARMLIB(IEASVCnn)
- APF(YES) option means the caller of the SVC must:
  - run in supervisor state,
  - run in PSW key 0 - 7, or
  - reside in an APF-authorized library and be linked with AC=1
- Check it out!

MVS Security Issues
Security related issues

Important Dataset: SYS1.NUCLEUS

Use: used at system startup

What's in it: MVS code

Who needs access/what type of access:

CRUD: highly limited to selected MVS systems programmers

Create, read, update, delete

MVS Security Issues
Security related issues

Important Dataset: SYS1.NUCLEUS

- Sometimes referred to as the nucleus initialization program
- SYS1.NUCLEUS(IEANUCnn) is loaded by the IPL program
- May be more than one copy (IEANUC00, IEANUC01, IEANUC08, etc.)
- If more than three, ask your systems programmer why

MVS Security Issues
Security related issues

Important Dataset: SYS1.PARMLIB

Use: MVS system parameters

What's in it: **MOST** MVS controls

Who needs access/what type of access:

CRUD: Highly limited to selected MVS systems programmers

Read: Limited to systems programmers, audit, security

MVS Security Issues
Security related issues

Important Dataset: SYS1.PARMLIB

special member list:

COMMNDnn	Automatic commands issued at IPL
IEASVCnn	User-written SVCs*
IEASYSnn	Index to other control members
IEFSSNnn	Subsystem names
PROGnn	APF authorized libraries*
SCHEDnn	Program Properties Table (PPT)*
SMFPRMnn	SMF parameters

* already discussed

MVS Security Issues
Security related issues

SYS1.PARMLIB(IEASYSnn)

- Index to other control members
  - COMMNDnn is one example
  - default is IEASYS00
- How many does your site have?
- If more than one, why? What are they for?
- Which one is used?
- Can the IEASYS00 member be overridden?
- Who has access/what type

MVS Security Issues
Security related issues

SYS1.PARMLIB(IEFSSNnn)

- Subsystem names - why do we care?
  - Another potential source of integrity bypass
  - Products which run as subsystems are trusted by MVS to run with integrity (do only good things)
  - Subsystems typically bypass all MVS security and controls
- JES, DB2, IMS are examples of products that run as subsystems
- Who has access/what type

MVS Security Issues
Security related issues

SYS1.PARMLIB(SMFPRMnn)

- SMF parameters - what's SMF?
- System Management Facility
  - Record of all MVS activity including security logging
  - The logging activity can be customized in SMFPRMnn; defines which SMF records are recorded or excluded from recording
  - Can indicate which SMF-related exits to use, 3 of which, IEFU83, IEFU84, and IEFU85, can be used to drop or change SMF records. Are you using?
- Who has access/what type

MVS Security Issues
Security related issues

More on SMF

- Logging is captured in SYS1.MANx
- The “x” in MANx is usually 1,2,3 or A,B,C
  - Record of all MVS activity including security logging, performance data, even billing data if you use a charge-back system
- As with SYS1.PARMLIB(SMFPRMnn), it’s important to know who has access/what type

MVS Security Issues
Security related issues

RSS (access control) program protection

- CA-ACF2, CA-Top Secret, IBM RACF
- All have special programs, datasets
  - need to protect the datasets, databases, software libraries and SMF data
  - ensure backups are running
  - periodically test recovery mechanisms
- All have special privileges
- Who has access/what type - should be very limited

MVS Security Issues
Security related issues

RSS Special “Bypass” Privileges

- CA-ACF2
  - NON-CNCL, MAINT, READALL, SECURITY
- CA-Top Secret
  - NODSNCHK, NORESCHK, NOVOLCHK
- RACF
  - AUDITOR, OPERATIONS, SPECIAL

MVS Security Issues
Security related issues

RSS Special “Bypass” Privileges

- CA-ACF2
  - NON-CNCL: full access to all resources
  - MAINT: under certain conditions, full access with no security check or logging
  - READALL: can read all datasets
  - SECURITY: security administrative privileges as well and full access to all resources

MVS Security Issues
Security related issues

RSS Special “Bypass” Privileges

- CA-Top Secret
  - NODSNCHK: full access to all data sets
  - NORESCHK: full access to all resources other than data sets and volumes
  - NOVOLCHK: full access to all volumes

MVS Security Issues
Security related issues

RSS Special “Bypass” Privileges

- RACF
  - AUDITOR: can specify logging options to resources and list any profile, including it’s auditing options
  - OPERATIONS: full access to all data sets
  - SPECIAL: RACF security administration. Note that if a RACF security administrator didn’t also have AUDITOR as a privilege, it wouldn’t allow the user to see if any other IDs had it.