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

Operating System

Security

App’s
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

Virtual Memory

Real Memory

Memory

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
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

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>MVS-OS/390-z/OS</td>
</tr>
<tr>
<td>1</td>
<td>JES</td>
</tr>
<tr>
<td>2-4</td>
<td>Reserved by IBM</td>
</tr>
<tr>
<td>5</td>
<td>Data management - DFSMS</td>
</tr>
<tr>
<td>6</td>
<td>VTAM</td>
</tr>
<tr>
<td>7</td>
<td>IMS</td>
</tr>
<tr>
<td>8</td>
<td>V=V (virtual) - batch, TSO users</td>
</tr>
<tr>
<td>9-15</td>
<td>V=R (real)</td>
</tr>
</tbody>
</table>
Another key assignment method: Program Properties Table (PPT) (SYS1.PARMLIB(SCHEDnn))

### Sysview:

```
SYSVIEW 7.4  CPU1

Entries Available  28, deleted  0

<table>
<thead>
<tr>
<th>Program</th>
<th>Orig</th>
<th>Ncan</th>
<th>Nswp</th>
<th>Priv</th>
<th>Syst</th>
<th>Ndsi</th>
<th>Npsw</th>
<th>Key</th>
<th>Affn</th>
<th>Sprf</th>
<th>Lprf</th>
<th>Nprf</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEDQTCAM</td>
<td>IBM</td>
<td>NCAN</td>
<td>NSWP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>6</td>
<td>NONE</td>
<td>NPRF</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISTINM01</td>
<td>IBM</td>
<td>NCAN</td>
<td>NSWP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>6</td>
<td>NONE</td>
<td>NPRF</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IKTCAS00</td>
<td>IBM</td>
<td>NCAN</td>
<td>NSWP</td>
<td>PRIV</td>
<td>SYST</td>
<td>NPSW</td>
<td>6</td>
<td>NONE</td>
<td>NPRF</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AHLGTF</td>
<td>IBM</td>
<td>NCAN</td>
<td>NSWP</td>
<td></td>
<td>SYST</td>
<td>NPSW</td>
<td>6</td>
<td>NONE</td>
<td>NPRF</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HHLGTF</td>
<td>IBM</td>
<td>NCAN</td>
<td>NSWP</td>
<td></td>
<td>SYST</td>
<td>NPSW</td>
<td>6</td>
<td>NONE</td>
<td>NPRF</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IHLGTF</td>
<td>IBM</td>
<td>NCAN</td>
<td>NSWP</td>
<td></td>
<td>SYST</td>
<td>NPSW</td>
<td>6</td>
<td>NONE</td>
<td>NPRF</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IEFIIIC</td>
<td>IBM</td>
<td>NCAN</td>
<td>NSWP</td>
<td>PRIV</td>
<td>SYST</td>
<td>NPSW</td>
<td>6</td>
<td>NONE</td>
<td>NPRF</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IEEMB860</td>
<td>IBM</td>
<td>NCAN</td>
<td>NSWP</td>
<td></td>
<td>SYST</td>
<td>NDSI</td>
<td>NPSW</td>
<td>6</td>
<td>NONE</td>
<td>NPRF</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IEEVMNT2</td>
<td>IBM</td>
<td>NCAN</td>
<td>NSWP</td>
<td></td>
<td>SYST</td>
<td>NPSW</td>
<td>6</td>
<td>NONE</td>
<td>NPRF</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HASJES20</td>
<td>IBM</td>
<td>NCAN</td>
<td>NSWP</td>
<td></td>
<td>SYST</td>
<td>NDSI</td>
<td>1</td>
<td>NONE</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DFSMVRC0</td>
<td>USER</td>
<td>NCAN</td>
<td>NSWP</td>
<td></td>
<td>SYST</td>
<td>NDSI</td>
<td>1</td>
<td>NONE</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```
## 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**

<table>
<thead>
<tr>
<th>PROGRAM NAME</th>
<th>IBM ENTRY</th>
<th>MODULE SOURCE</th>
<th>DATASET INTEGRITY</th>
<th>SECURITY KEY</th>
<th>NON-CANCEL SWAP</th>
<th>SMF TIMING BYPASS</th>
<th>CPU AFFN FLAG</th>
</tr>
</thead>
<tbody>
<tr>
<td>AHLCGF</td>
<td>YES</td>
<td>IEFSDPPT</td>
<td>NO</td>
<td>0</td>
<td>YES</td>
<td>NO</td>
<td>YES</td>
</tr>
<tr>
<td>AKPCSIEP</td>
<td>YES</td>
<td>IEFSDPPT</td>
<td>YES</td>
<td>1</td>
<td>NO</td>
<td>NO</td>
<td>YES</td>
</tr>
<tr>
<td>APSSPIEP</td>
<td>YES</td>
<td>IEFSDPPT</td>
<td>YES</td>
<td>1</td>
<td>NO</td>
<td>NO</td>
<td>YES</td>
</tr>
<tr>
<td>AVFMMBLO</td>
<td>YES</td>
<td>IEFSDPPT</td>
<td>NO</td>
<td>3</td>
<td>NO</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td>CSVLLCRE</td>
<td>YES</td>
<td>IEFSDPPT</td>
<td>YES</td>
<td>0</td>
<td>YES</td>
<td>NO</td>
<td>YES</td>
</tr>
<tr>
<td>CSVVFCCRE</td>
<td>YES</td>
<td>IEFSDPPT</td>
<td>NO</td>
<td>0</td>
<td>NO</td>
<td>NO</td>
<td>YES</td>
</tr>
<tr>
<td>DFHISIP</td>
<td>NO</td>
<td>SCHED00</td>
<td>NO</td>
<td>8</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>DFHSIP</td>
<td>NO</td>
<td>SCHED06</td>
<td>NO</td>
<td>8</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>DFHISIP</td>
<td>NO</td>
<td>SCHED16</td>
<td>NO</td>
<td>8</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>DFSMVRCO</td>
<td>YES</td>
<td>IEFSDPPT</td>
<td>NO</td>
<td>7</td>
<td>NO</td>
<td>NO</td>
<td>YES</td>
</tr>
<tr>
<td>DSNUTILB</td>
<td>YES</td>
<td>IEFSDPPT</td>
<td>NO</td>
<td>7</td>
<td>NO</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td>FNMMAIN</td>
<td>NO</td>
<td>SCHED00</td>
<td>NO</td>
<td>6</td>
<td>NO</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>FNMMAIN</td>
<td>NO</td>
<td>SCHED06</td>
<td>NO</td>
<td>6</td>
<td>NO</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>FNMMAIN</td>
<td>NO</td>
<td>SCHED16</td>
<td>NO</td>
<td>6</td>
<td>NO</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>HASJES2A</td>
<td>NO</td>
<td>SCHED00</td>
<td>YES</td>
<td>1</td>
<td>NO</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td>HASJES2A</td>
<td>NO</td>
<td>SCHED06</td>
<td>YES</td>
<td>1</td>
<td>NO</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td>HASJES2A</td>
<td>NO</td>
<td>SCHED16</td>
<td>YES</td>
<td>1</td>
<td>NO</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td>HASJES20</td>
<td>YES</td>
<td>IEFSDPPT</td>
<td>YES</td>
<td>1</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
</tr>
</tbody>
</table>

---

Used by permission of Eberhard Klemens Co.  
Copyright 2002 EKC Inc.
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(IEASVCCnn)

• 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
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(IEASYSYSnn)

- Index to other control members
  - COMMNDnn is one example
  - default is IEASYSYS00
- How many does your site have?
- If more than one, why? What are they for?
- Which one is used?
- Can the IEASYSYS00 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
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.