

zD&T

LEARNING WITH A PERSONAL MAINFRAME

Innocent Question

```
17149 22:38:26.28 JACOB3 00000290 D T
17149 22:38:26.33 TSU04462 00000090 IEE345I DISPLAY AUTHORITY INVALID, FAILED BY SECURITY PRODUCT
17149 22:38:26.35 TSU04462 00000281 ICH408I USER(XXXXXX ) GROUP(SYS1 ) NAME(XXXXX XXXXXXXX )
      730 00000281 MVS.DISPLAY.TIMEDATE CL(OPERCMD5)
      730 00000281 INSUFFICIENT ACCESS AUTHORITY
      730 00000281 FROM MVS.* (G)
      730 00000281 ACCESS INTENT(READ ) ACCESS ALLOWED(NONE )
```

Display Time: time is not secret, operator commands are protected.

Shared systems impose restrictions.

This is personal

The image shows a Linux terminal window with the following content:

```
[manager] # define network adapter (OSA) for communication with Linux
name awsosa 0024 --path=A0 --pathtype=OSD --tunnel_intf=QDIO mode
device 400 osa osa
device 401 osa osa
device 402 osa osa

[manager]
name awsctc 300
device E40 3088 3088 ct
device E41 3088 3088 ct

[manager]
name aws3274 0001
terminals
device 0700 3279 3274 m
device 0701 3279 3274 t
device 0702 3279 3274 t
device 0703 3279 3274 t
device 0704 3279 3274 t
device 0705 3279 3274 t
device 0706 3279 3274 t
device 0707 3279 3274 t
device 0708 3279 3274 t
device 0709 3279 3274 t
device 070B 3279 3274 t
device 070C 3279 3274 t
device 070D 3279 3274 t
device 070E 3279 3274 t
device 070F 3279 3274 t
0

[manager]
name awsckd 0002
device 0A80 3390 3390 /
device 0A81 3390 3390 /
device 0A82 3390 3390 /
device 0A83 3390 3390 /
device 0A84 3390 3390 /
device 0A85 3390 3390 /
device 0A86 3390 3390 /
device 0A87 3390 3390 /
device 0A88 3390 3390 /
device 0A89 3390 3390 /
device 0A8A 3390 3390 /
device 0A8B 3390 3390 /
device 0A8C 3390 3390 /
device 0A8D 3390 3390 /

IEE612I CN=L700 DEVNUM=0700 SYS=S0W1
IEE163I MODE= R
```

The terminal also shows the following messages:

```
IBM System z Personal Development Tool (zPDT)
Licensed Materials - Property of IBM
5799-ADE
(C) Copyright IBM Corp. 2007,2013 All Rights Reserved.

z1091, version 1-6.49.23, build date - 10/21/16 for Linux on RedHat 64bit

AWSSTA014I Map file name specified:
AWSSTA204I zPDT started in directory
AWSSTA146I Starting independent 1090
AWSEMI314I CPU 0 zPDTA License Obtain
AWSEMI314I CPU 2 zPDTA License Obtain
AWSEMI005I Waiting for 1090 license
AWSSEMI314I CPU 1 zPDTA License Obtain
OSA code level = 0x4301
AWSDSA010I AWSOSA is ready for chpid
AWSDSA010I AWSOSA is ready for chpid
AWSDDCK006W File name missing on device
AWSDDCK006W File name missing on device
AWSDDCK006W File name missing on device
AWSDDCK006W File name missing on device
Warning: Cannot convert string "-*+
59-1" to type FontStruct
Warning: Missing charsets in String
AWSSTA059I System initialization complete
AWSSTA012I All configured subsystems
[ibmsys1@ztdt-dev1 ~]$
```

The terminal also shows the following messages:

```
IEE136I LOCAL: TIME=17.19.48 DATE=2017.153
TIME=21.19.48 DATE=2017.153
- 17.20.27 /S SMFCLEAR
- 17.20.27 IEE305I /S COMMAND INVALID
- 17.20.59 D U,DASD,ONLINE
- 17.21.16 D T
- 17.21.16 IEE136I LOCAL: TIME=17.21.16 DATE=2017.153
TIME=21.21.16 DATE=2017.153
IEE457I 17.20.59 UNIT STATUS FRAME 1 F E SYS=
UNIT TYPE STATUS VOLSER VOLSTATE SS
device 0A80 3390 S B2RES1 PRIV/RSDNT 0
device 0A81 3390 A B2RES2 PRIV/RSDNT 0
device 0A82 3390 D SARES1 PRIV/RSDNT 0
device 0A83 3390 A B2SYS1 STRG/RSDNT 0
device 0A84 3390 A B2CF61 PRIV/RSDNT 0
device 0A85 3390 A B2USS1 PRIV/RSDNT 0
device 0A86 3390 A B2USS2 PRIV/RSDNT 0
device 0A87 3390 A B2PRD1 PRIV/RSDNT 0
IEE612I CN=L700 DEVNUM=0700 SYS=S0W1
IEE163I MODE= R
```

The terminal also shows the following messages:

```
Session A - [50 x 80]
Menu Utilities Compilers Options Status Help
ISPF Primary Option Menu
Option ==>
0 Settings Terminal and user parameters User ID . : IBMUSER
1 View Display source data or listings Time . . : 16:57
2 Edit Create or change source data Terminal . : 3278
3 Utilities Perform utility functions Screen . . : 1
4 Foreground Interactive language processing Language . : ENGLISH
5 Batch Submit job for language processing Appl ID . : ISR
6 Command Enter TSO or Workstation commands TSO login : ISPFPRDC
7 Dialog Test Perform dialog testing TSO prefix:
9 IBM Products IBM program development products System ID : S0W1
10 SCLM SW Configuration Library Manager MVS acct. : ACCT#
11 Workplace ISPF Object/Action Workplace Release . : ISPF 7.2
M More Additional IBM Products

Enter X to Terminate using log/list defaults
```

The terminal also shows the following messages:

```
Licensed Materials - Property of IBM
5650-Z05 Copyright IBM Corp. 1980, 2015.
US Government Users Restricted Rights -
Use, duplication or disclosure restricted
by GSA ADP Schedule Contract with IBM Corp.
```

zD&T user can

Administer

Modify the system

Examine internal organs

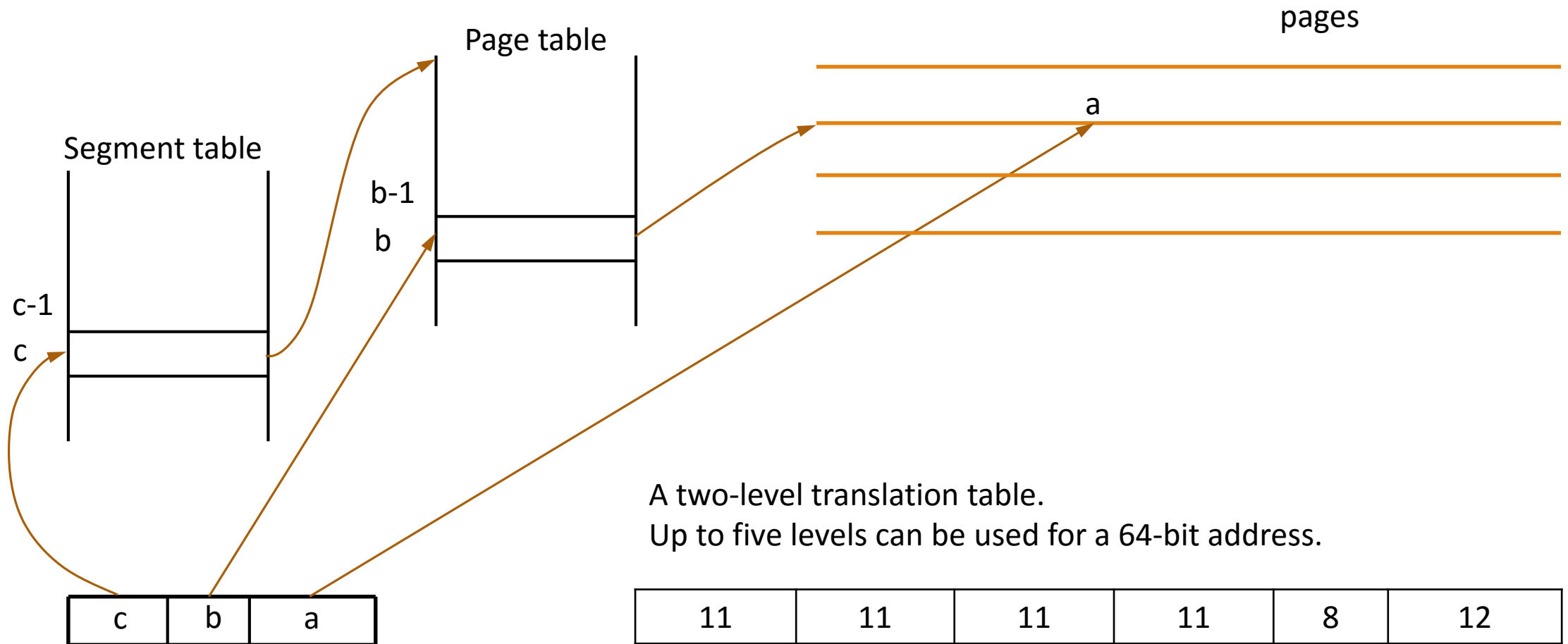
Problem set

Problem 1. A virtual address and a translation table define a name slot in a visitor book located outside your address space. Store your name in this slot.

Problem 2. Intercept SVC 35 (WTO). Write to the system log every time a WTO message arrives.

Problem 3. Define RACF resources for a filtering program that automates the mail work described in the opening pages of *Catch-22*.

Address translation



Visitor Book

```
SYSEVENT TRANSWAP                                Make the book address space non-swappable

STORAGE OBTAIN,LENGTH=4096,LOC=31                Obtain a page and fix it in real storage
ST      1,PAGEADDR
PGSER  R,FIX,(1)

MODESET mode=SUP                                switch to supervisor state
STCTG  1,1,TOKEN                                store ASCE into token
MVC    TOKEN+8(4),=F'0'
MVC    TOKEN+12(4),PAGEADDR                     store 31-bit virtual address

CALL   IEANTCR,(=F'4',
              =CL16'Visitor book',
              TOKEN,
              =F'0',
              RETCODE)
```

```
TOKEN  DS    2AD
```

Translation

ASCE	52-bit number of real storage page for the top-level translation table		T	
------	--	--	---	--

T is the type of the table, tells what level is at the top

```
MODESET MODE=SUP,KEY=ZERO      Arm for privileged code and protected storage
SAM64                           set 64-bit addressing
...
REGION2 DS      0H
      LG      R1,=x'001FFC0000000000'  mask for region-2 index
      NGR     R1,R10                    region index bits
      SRLG    R1,R1,64-22-3            region index times 8
      AGR     R11,R1                    point to table entry
      LURAG   R11,R11                  load the entry
      LHI     R0,32                     1 to validity position
      NR      R0,R11                   is the entry valid?
      JNZ     BADRGN2
      NILL    R11,X'F000'              clear last 12 bits
```

After traversing the tables, R11 contains the real address of the target.

```
LG    R0,=CL8'Visitor'  
STURG R0,R11                make a record
```

For debugging, this code can translate a virtual address in its own address space, where *load real address* (LRA) instruction will show the correct result

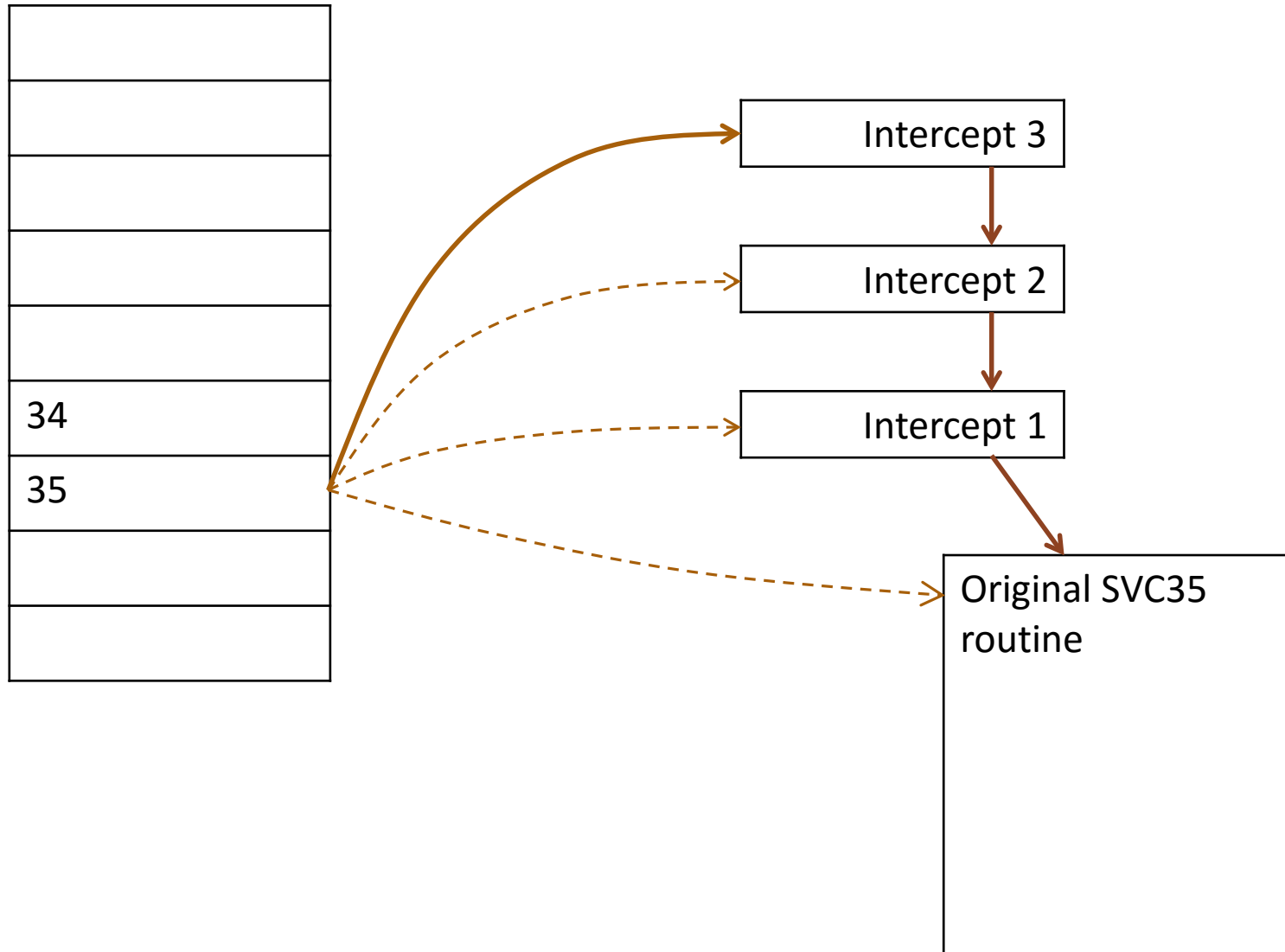
```
LRA   R3,0(,R10)            load real address  
CLGR  R3,R11                compare to my result  
JNE   NOTREAL
```

SVC Routine

SVCSTART	L	R6,ORIGEP-SVCSTART(R6)	original SVC35 entry point
	BAKR	R6,0	save registers
	WTL	'ZDT0001I A message is coming'	write to log
	EREGG	R15,R1	restore some registers
	PR	,	go to real SVC35
ORIGEP	DS	A	

Make a record in syslog and pass control to the original routine.

SVC table



Install

```
STORAGE OBTAIN,LENGTH=SVCLLEN,SP=241,LOC=(31,31)      CSA storage
LR      R2,R1
MODESET KEY=ZERO,MODE=SUP
MVC     0(SVCLLEN,R2),SVCSTART                          copy the code to CSA
OILH   R2,X'8000'                                       amode31 bit
SVCUPDTE 35,REPLACE,TYPE=4,EP=(R2)                     update the table
```

Install a second and a third routine and issue a D T command:

```
ZDT0003I A message is coming
ZDT0002I A message is coming
ZDT0001I A message is coming
IEE136I LOCAL: TIME=10.43.11 DATE=2017.156  UTC: TIME=14.43.11
DATE=2017.156
```

Questions

How to remove an intercept?

Why SVCUPDTE?

Can the interceptor modify the message?

Mail Filter With RACF Rules

Proscribe all but articles.

```
RDEFINE MAILWRD1 *           UACC(NONE)
RDEFINE MAILWRD1 A           UACC(UPDATE)
RDEFINE MAILWRD1 AN          UACC(UPDATE)
RDEFINE MAILWRD1 THE         UACC(UPDATE)
```

Resource class Resource name Default access

RACF is a string-matching engine. With multiple matches, the most specific one wins.

Resource class defines a name space.

Resource class

Class is created as a new resource in the CDT – Class Definition Table

```
RDEFINE CDT MAILWRD1 UACC(NONE)
  CDTINFO(MAXLENGTH(100) FIRST(ALPHA)          alphanumeric strings up to 100 characters
  OTHER(ALPHA,NUMERIC,NATIONAL,SPECIAL) POSIT(22)
```

```
SETROPTS RACLIST(CDT) REFRESH          refresh the table
SETROPTS GENERIC(MAILWRD1)            enable generic matching
SETROPTS CLASSACT(MAILWRD1)          activate the class
```

Filtering Goals

1. Reject every adverb and every adjective
2. Reject articles
3. Allow only the salutation
4. Reject a given city on the mail envelope

Name space needs three dimensions

1. Location in the message (envelope, salutation, signature or body)
2. Part of speech
3. Word

Access Check

The filtering program will have to ask RACF about every word it finds:

```
RACROUTE REQUEST=AUTH,ATTR=UPDATE,           X
          CLASS='MAILWRD1',ENTITYX=RSTRING,    X
          WORKA=WORKAREA,                      X
          RELEASE=77A0
```

```
RSTRING  DC      Y(100,25),CL100'SALUTATION.ADJECTIVE.DEAR'
```

With goal #1, RACF will deny access:

```
ICH408I USER(xxxxxx ) GROUP(xxxx ) NAME(xxxxx )
          SALUTATION.ADJECTIVE.DEAR CL(MAILWRD1)
          INSUFFICIENT ACCESS AUTHORITY
          FROM *.ADJECTIVE.* (G)
          ACCESS INTENT(UPDATE ) ACCESS ALLOWED(NONE )
```

Clean Slate

zD&T can take a snapshot of a disk. The emulator command on Linux to remember the current state of B2SYS1:

```
awsckd -ve z/disks/B2SYS1
```

When experiments are completed, a disk can be restored to the original state:

```
awsckd -vr z/disks/B2SYS1
```