Top 12 Mainframe Security Exposures and Lessons From A Real Mainframe Break-In

Stu Henderson
5702 Newington Road
Bethesda, MD 20816
(301) 229-7187
STU@STUHENDERSON.COM
What You’ll Hear

- One Person’s Experiences
- You May Not Agree with It All
- Just Keep What’s Useful for You
- Real Mainframe Break-In Lessons
- Starting with Stu’s “Top Twelve”
1. MVS Integrity Exposures

- Programs Added to MVS With Privileges and Unsafe

- What “Safe” Means
Mainframe Security Exposures

1. MVS Integrity Exposures

- Privileges Like Supervisor State
- Let a Program Bypass All Security
- Not Covered By IBM’s Integrity Statement for MVS
Mainframe Security Exposures

1. MVS Integrity Exposures

- Common Backdoors: User SVCs, APF-Authorized Programs

- Most Common Example: Authorization SVCs
Mainframe Security Exposures

1. MVS Integrity Exposures
   ~ Simple Solutions ~

- Formal Change Control
- Logging and Review of Updates
- Tools Like New Era’s The Control Editor
Mainframe Security Exposures

1. MVS Integrity Exposures
   ~ Simple Solutions ~

- Stay Current on z/OS Releases and Service (See the IBM Security Portal at http://www.ibm.com/systems/z/advantages/security/integrity.html Click on “Support & download” and Also Browse the Whole Site)
Mainframe Security Exposures

2. Excessive Defaults and Privileges

- RACF: GLOBAL Rules, OPERATIONS, TRUSTED etc.
- ACF2: NON-CNCL, SECURITY, etc.
- TopSecret: ALL Record, NODSNCHK, etc.
2. Excessive Defaults and Privileges

- Started Tasks with Privileges

- “You Don’t Need No Stinkin’ OPERATIONS”
2. Excessive Defaults and Privileges
~ Simple Solutions ~

- An Owner for Each Privilege and Resource Class
- Annual Re-Certification;
- Do the Work to Avoid Needing the Privileges
- Firecall IDs
Mainframe Security Exposures

3. JES Security

- JESSPOOL, SDSF, OPERCMDS Resource Classes
- WRITER, NODES, PROPCNTL Resource Classes
- Spool and Checkpoint Datasets
- Update Access to Proclibs (JCL for Started Tasks with Privileges)
3. JES Security
~ Simple Solutions ~

- Use RACF, ACF2, or TopSecret to Protect The Above
4. Tape Security

- 17 Character DSNAME Problem
- Two Datasets on a Cartridge
- BLP (Bypass Label Processing)
4. Tape Security
   ~ Simple Solutions ~

- DEVSUPxx Member of Parmlib
- Tape Management Software
- SAF (RACF, ACF2, or TopSecret)
5. Residual Data

- (Still There After Dataset Erased)
- Tape and Disk
- PCI (Payment Card Industry) Audits
5. Residual Data
~ Simple Solutions ~

- The Simple Tape Solution
- The Disk Solution (EOS, AUTOERASE)
- (Who Decides, Who Knows, Who Is Responsible?)
Mainframe Security Exposures

6. DB2 Internal Security

- Doesn’t Permit Wildcards
- Originally Didn’t Group Users
- So If 500 Users and Ten Tables, 5000 Commands to Grant Permission
6. DB2 Internal Security
~ Simple Solutions ~

- RACF, ACF2, TopSecret
- DSNR Resource Class
7. Access Production Data

- For Testing?
- For 3 AM Emergencies
- How Often?
7. Access Production Data
~ Simple Solutions ~

- Firecall Userids
Mainframe Security Exposures

8. Windows Sniffer Programs

- Logon to the Mainframe Through a Windows LAN
- Sniffer Program on Any PC Can View All LAN Traffic on the Subnet
- Including Mainframe Userids and Passwords
8. Windows Sniffer Programs
~ Simple Solutions ~

- Kerberos on the Windows Server
Mainframe Security Exposures

9. VTAM Security

- Enterprise Extender and APPN
- Spoofing an Applid
- Little Understood, So Left Alone
9. VTAM Security

~ Simple Solutions ~

- VTAMAPPL, APPCLU Resource Classes
- VTAM Configuration Options
- Net-Q Software
10. Batch Job with Another’s Userid

- Batch Jobs Inherit Submitter’s ID
- Or Some Other ID, But What About the Password?
- Job Scheduling Software
- What If All Production Jobs Have Same Userid?
Mainframe Security Exposures

10. Batch Job with Another’s Userid
~ Simple Solutions ~

- ACF2: JOBFROM Privilege versus RESTRICTED
- TopSecret: NOSUBCHK versus XA ACID=
- All Three: SURROGAT and PROPCNTL
11. Hardware Configuration

- Shared DASD (Disk)
- LPARs and SYSPLEXes
- Multiple Security Software Databases
- HCD (Hardware Configuration Definition) and IODF (Input Output Configuration File)
III. Hardware Configuration
~ Simple Solutions ~

- Formal Change Control
- Learn to Read IODF, HCD
- SAF
- Tools Like New Era’s StepOne
Mainframe Security Exposures

12. Mainframe TCP/IP Connections

- Internet, FTP, TN3270, httpd, Other Daemons
- CICS, MQ Series
12. Mainframe TCP/IP Connections

- DB2, TCPALVER, SQL Injection, Distributed Connections
- Lack of Knowledge
- Weak Communication Between Mainframe and TCP/IP Experts
12. Mainframe TCP/IP Connections ~ Simple Solutions ~

- Basic Steps: Block All the Ports
- Basic Steps: Ensure All Sensitive Data Encrypted, Including Passwords
- PAGENT (Policy Agent) Firewall Like Functions
- Change Control Over Configuration Files, Programs, JCL
Mainframe Security Exposures

SOME COMMON THEMES

All of these weaknesses can be traced to organizational issues:

- Who decides?
- Who approves?
- Who has the knowledge?
- Who is responsible?
- How do we measure?
Example

A Real MAINFRAME BREAK-IN

- This was a deliberate, successful, criminal attack
- On a European service bureau’s mainframes
- Over the Internet.
Example

A Real MAINFRAME BREAK-IN

- Not stealing a tape or tricking out passwords.
- RACF, but applies to ACF2 or TopSecret.
- Discovered from high CPU usage. Shades of “The Cuckoo’s Egg” by Cliff Stoll
Example

A Real MAINFRAME BREAK-IN

- First used FTP to download the RACF database and crack all the userids and passwords.

- People seem to think that because passwords are encrypted, they can’t be read.
Example

A Real MAINFRAME BREAK-IN

- But brute force cracker programs will do the job.

- In a couple of days they cracked the passwords for 30,000 userids.
Example

A Real MAINFRAME BREAK-IN

- “Is this where we process State Police records?” YES

- Hackers broke into front-end distributed computers to get to the mainframes
Hackers installed outbound programs which called out over the Internet, making it easier for the hackers to bypass firewalls and other protections.

All of the holes the hackers used resulted from mis-configuration, not weaknesses in mainframe security or RACF.
A Real Mainframe Break-In

SOME COMMON THEMES

All of these weaknesses can be traced to organizational issues:

- Who decides?
- Who approves?
- Who has the knowledge?
- Who is responsible?
- How do we measure?
A Real Mainframe Break-In

LESSONS LEARNED

- Mainframes are targets now.
- Internet connections make them more vulnerable.
- Most securable platform, but …
- Organizational issues
Top 12 Mainframe Security Exposures and Lessons From A Real Mainframe Break-In

For more information:

- NewEra Software: [www.newera.com](http://www.newera.com)
- The Henderson Group: [www.stuhenderson.com](http://www.stuhenderson.com)
- Net’Q: [www.net-q.com](http://www.net-q.com)