ACEECHK Yourself Before You Wreck Yourself

(Tom Conley)

ACEECHK Yourself

- ACEE is RACF control block defining user and their privileges
- OA53441, OA55163 added support for a new RACF class ACEECHK
- ACEECHK detects changes to ACEE that raise privilege
- Prevents "magic SVC" or other authorized code from gaining system privileges to circumvent security controls
- New message IRR421I is issued when privilege escalation detected

```
IRR421I ACEE modification detected
for user TSOUSR8 in address space ID 0x00000026 running under user
TSOUSR8 and job name TSOUSR8 while program ADDUSER is running. The
RACF function detecting the modification is IRRENV00.
Rsn=0x60000000. (ACEEPRIV is ON) (ACEESPEC is ON). Occurrences 1.
Command=ADDUSER. Call chain: ADDUSER <- IKJEFT02 <- IKJEFT01
```

- Unfortunately for IBM, fortunately for us, this uncovered some dirty laundry

Before You Wreck Yourself

- IBM products were found to be hacking the ACEE
- Before enabling ACEECHK class, apply the following maintenance
- Multiple PTF's were issued for DFSMShsm
  - OA54740 - ALLOW HSM TO RUN AS A TRUSTED STARTED PROCEDURE
  - OA55295 - AE FIX CONTINUATION OF OA54740
- OA55295 also contained many doc updates for DFSMShsm
  - Define DFSMShsm started task id with SPECIAL and OPERATIONS
  - Create STARTED class profile and ICHRIN03 entry to make HSM TRUSTED
- OA57418 - ACEECHK RACF CLASS SUPPORT IN RMM
- OA57421 - RACF IDENTITY TOKEN SUPPORT

Before You Wreck Yourself

- Many ISV products were also affected
- BMC Mainview for DB2
  - Add BMC Mainview DB2 to ACEECHK Exclude List
  - Technical Bulletin for BMC DB2 Products
- FDR/ABR
  - ABR Users of z/OS 2.4 who activate the ACEECHK class in RACF, and users of earlier releases who install PTFs to support ACEE modification detection and who activate the ACEECHK class in RACF, require V 5.4/89 spin 2, or V 5.4/89 with ZAP P-54.8922.
- CA-Disk (Broadcom Knowledge Base Article)
  - If you have elected to enable ACEE protection using RACF's ACEECHK, you also need to add CA Disk to the exclusion list. The ACEE is modified for System Administration mode and other Auto-Restore functions.

Ohhh No!! Linux Won't Boot on my PC, CLONEZILLA!!

(Tom Conley)

Converting my Linux Platform from HDD to SSD

- I run ZD&T (z/OS on a PC) under Linux on a PC at home
- I/O on ZD&T is slow, so I thought, "Why not convert to SSD?"
- Clonezilla is a Unix-live image you can boot off CD
- I use it primarily for backups, but it can also clone images
- I installed SanDisk SSD in my PC
- I booted Clonezilla and selected option to clone HDD to SSD
- Clonezilla said it would update all the files so the system would boot
- Key was to reinstall GRUB2, a popular Linux bootloader
- Clonezilla said it would reinstall GRUB2 (spoiler alert, it lied)
- After the clone, I tried to boot from the SSD, it wouldn't boot
- I got messages saying it couldn't find the Linux image files
- Gave me an option to enter command line recovery mode as root

The Internet to the Rescue (Not Really)

- Best thing about Linux is copious help available on Internet
- Worst thing about Linux is copious help available on Internet
- You'll get multiple fixes for your issues, many of which won't work
- Try to find help for your specific Linux distro and release
- Linux likes to mix things up, so /etc/rc might be /etc/rc.d
- I wasn't able to access filesystems on the SSD
- I found articles for /etc/fstab, the Linux filesystem mount table
- Armed with some info, I rebooted
- I selected option for command line recovery mode as root

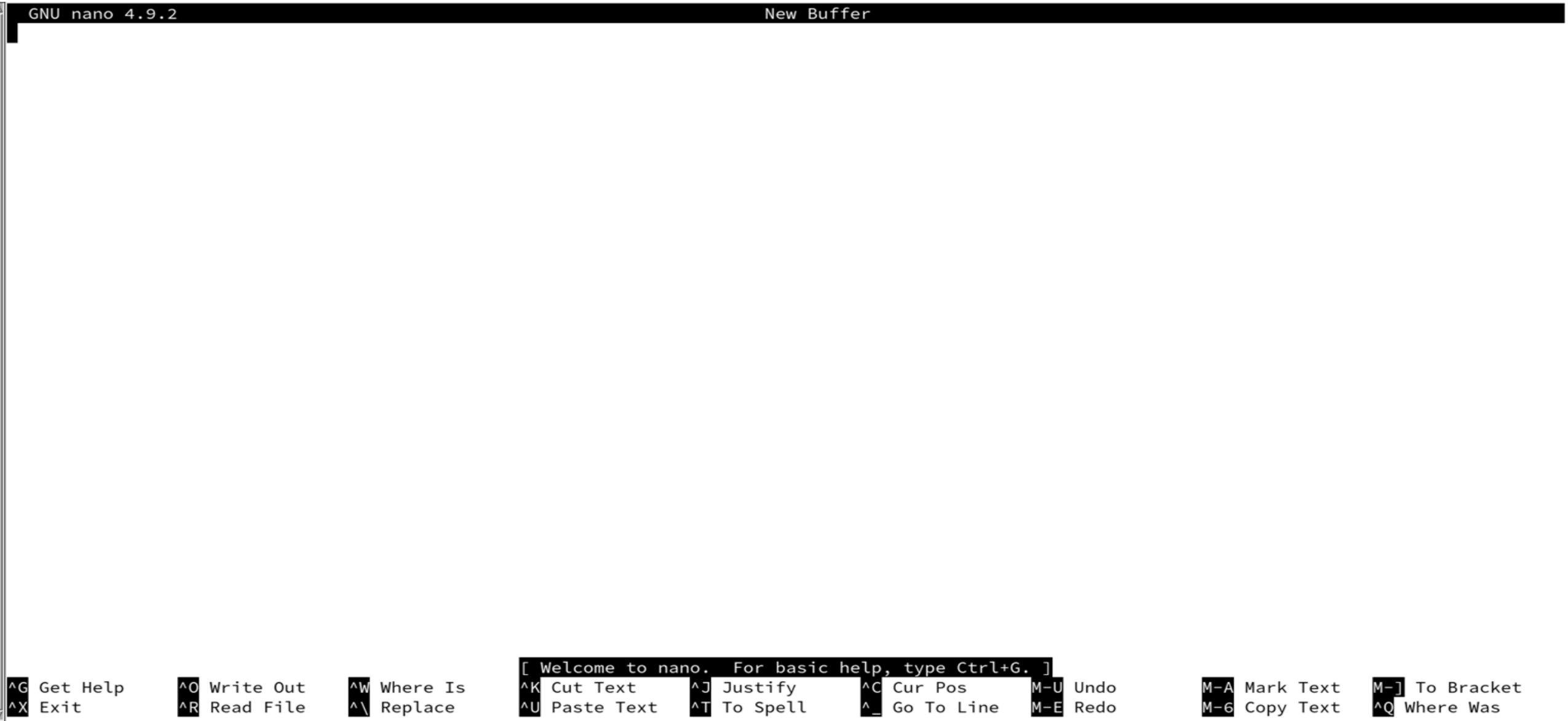
/etc/fstab

- I issued Unix command "cat /etc/fstab":

```
/dev/disk/by-id/scsi-1ATA_ST2000DM001-1CH164_Z340P11C-part1 swap       swap defaults        0 0
/dev/disk/by-id/scsi-1ATA_ST2000DM001-1CH164_Z340P11C-part2 /          ext4 acl,user_xattr 1 1
/dev/disk/by-id/scsi-1ATA_ST2000DM001-1CH164_Z340P11C-part3 /z         ext4 acl,user_xattr 1 2
```

- My /etc/fstab was still referencing Seagate HD, not SanDisk SSD
- Clonezilla did not update /etc/fstab for the new SSD drive
- I got cold chill, thinking I would have to use dreaded "vi" editor
- Luckily, I discovered nano, a fullscreen editor with easy commands
- Help is a keystroke away, and common commands listed on bottom

nano


GNU nano 4.9.2
New Buffer
[Welcome to nano. For basic help, type Ctrl+G.]
^G Get Help
^X Exit
^O Write Out
^R Read File
^W Where Is
^\ Replace
^K Cut Text
^U Paste Text
^J Justify
^T To Spell
^C Cur Pos
^_ Go To Line
M-U Undo
M-E Redo
M-A Mark Text
M-6 Copy Text
M-] To Bracket
^Q Where Was

/etc/fstab

- Using nano, updating /etc/fstab was easy:

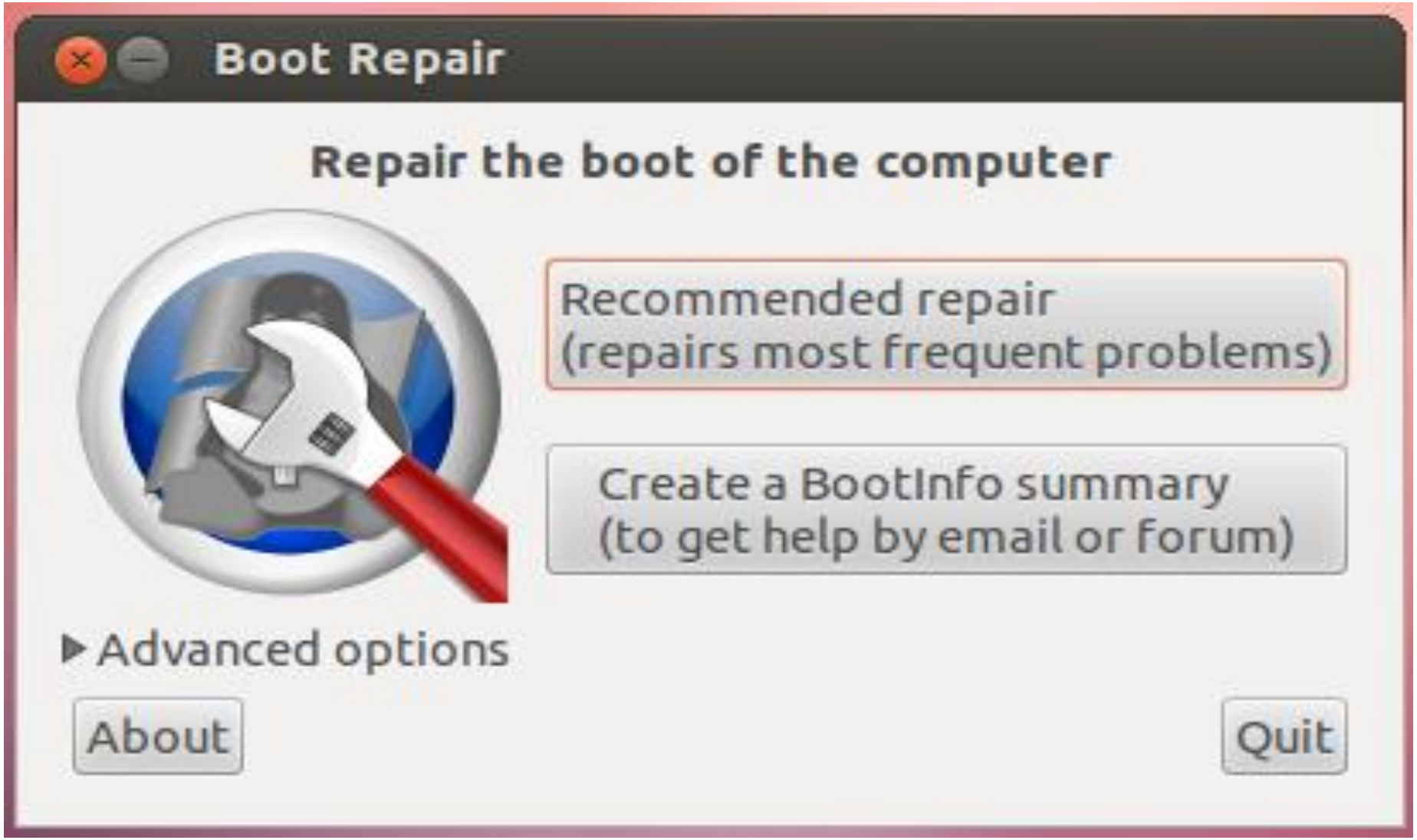
```
/dev/disk/by-id/ata-SanDisk_SDSSDH3_2T00_19431D801620-part1 swap       swap defaults        0 0
/dev/disk/by-id/ata-SanDisk_SDSSDH3_2T00_19431D801620-part2 /          ext4 acl,user_xattr 1 1
/dev/disk/by-id/ata-SanDisk_SDSSDH3_2T00_19431D801620-part3 /z         ext4 acl,user_xattr 1 2
/dev/disk/by-id/scsi-1ATA_ST2000DM001-1CH164_Z340P11C-part1 /hddstore ext4 defaults        1 3
```

- First three lines were for the cloned partitions
- Line 4 added after successful reboot and reformat of Seagate HD
- Created mountpoint /hddstore for hard drive
- I use hard drive as repository for software and inactive data

BootRepair

- Even after fixing /etc/fstab, Linux still wouldn't boot
- I finally found a freebie called BootRepair
- BootRepair is a Linux Live .iso that you burn onto a CD and boot
- I selected the Recommended Repair option
- From BootRepair log, I could tell that it correctly installed GRUB2
- The log also showed that it pointed at the correct Linux image
- I rebooted and VIOLA! I had my OpenSUSE Leap 15.1 back
- BootRepair succeeded where Clonezilla failed in reinstalling GRUB2

BootRepair


Boot Repair
Repair the boot of the computer
Recommended repair
(repairs most frequent problems)
Create a BootInfo summary
(to get help by email or forum)
Advanced options
About
Quit

Acknowledgements (Knowing and Unknowing)

- Mark Nelson, IBM
- Joel Tilton
- Bruce Wells,IBM
- Glenn Wilcock, IBM