ORACLE

SBAT revocation mechanism and managing it in Linux distributions

deeper dive into SBAT and how i learned to love it

Aleksandr Burmashev
alexander.burmashev@oracle.com
Oracle Linux and VM Development

Aug, 2024

What is SBAT?

- Why we talk about SBAT right now ?
- UEFI Secure Boot Advanced Targeting
- Developed and introduced by upstream shim development group
- Implemented by both MS and Linux vendors
- Supplements “traditional” UEFI SecureBoot certificate verification but does not replace it
- Ensures less data in UEFI NVRAM storage is needed to store revocation data
- Single affected by any vulnerability signed EFI binary no longer requires certificate rotation

Did someone introduce a new way to “break” boot for Linux systems ?

- Some recent updates by vendors in 2024 caused dual boot failures
- Why MS is in the picture ?
- Who is in fault ? Who is wrong ?
- Should it have been done differently ?
- “Demonizing” SBAT and new features
- coming back to “why it was introduced”

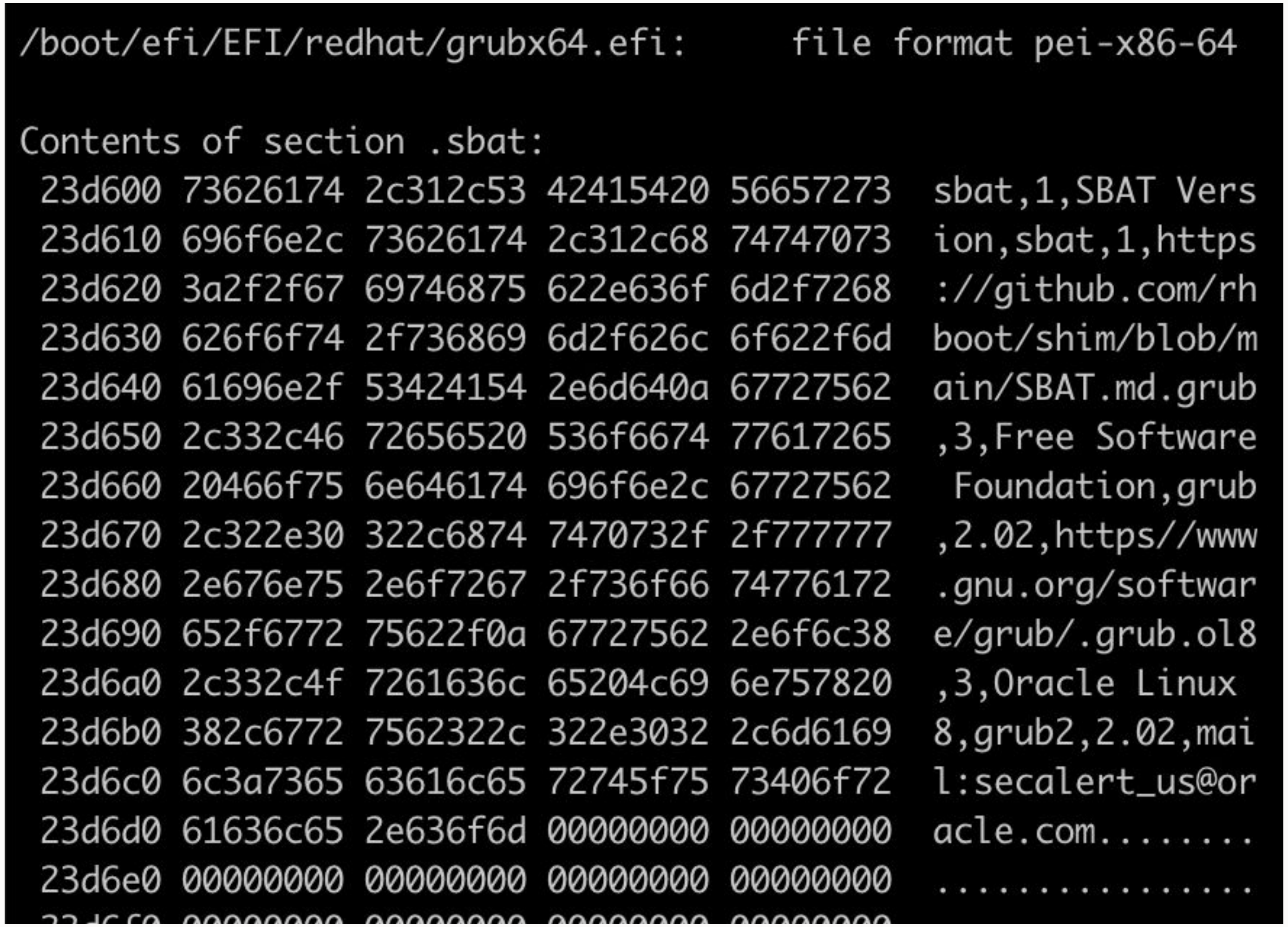
SBAT good practices and how to prevent locking yourself down

- What vendors need to take care of ?
- Integrity of boot stack
- Monitoring upstream development and CVE tracking
- stability/speed vs security
- good old secureboot is often not what we think it is
- userspace tools to work with SBAT
- TESTING(!)

SBAT good practices and how to prevent locking yourself down

- objdump -s -j .sbat <efi binary name> is your friend
- SecureBoot on/off is the ultimate driver for enforcement of SBAT
- mokutil and managing SBAT policies
- monitoring update flow for all distros on a multi-boot system
- embracing the future

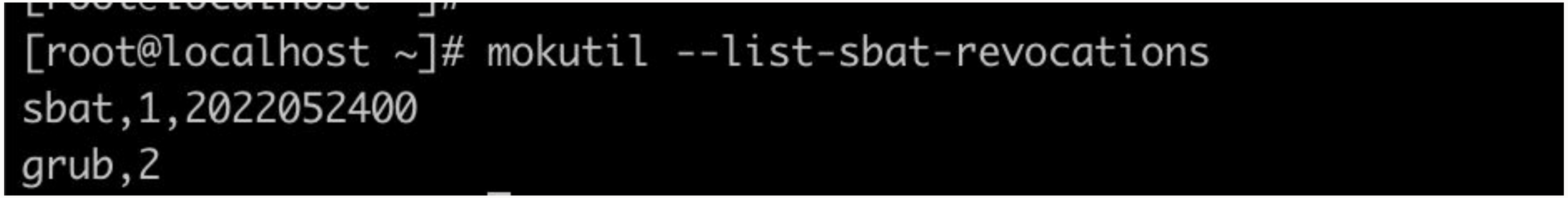
SBAT good practices and how to prevent locking yourself down



```
/boot/efi/EFI/redhat/grubx64.efi:     file format pei-x86-64

Contents of section .sbat:
 23d600 73626174 2c312c53 42415420 56657273  sbat,1,SBAT Vers
 23d610 696f6e2c 73626174 2c312c68 74747073  ion,sbat,1,https
 23d620 3a2f2f67 69746875 622e636f 6d2f7268  ://github.com/rh
 23d630 626f6f74 2f736869 6d2f626c 6f622f6d  boot/shim/blob/m
 23d640 61696e2f 53424154 2e6d640a 67727562  ain/SBAT.md.grub
 23d650 2c332c46 72656520 536f6674 77617265  ,3,Free Software
 23d660 20466f75 6e646174 696f6e2c 67727562   Foundation,grub
 23d670 2c322e30 322c6874 7470732f 2f777777  ,2.02,https//www
 23d680 2e676e75 2e6f7267 2f736f66 74776172  .gnu.org/softwar
 23d690 652f6772 75622f0a 67727562 2e6f6c38  e/grub/.grub.ol8
 23d6a0 2c332c4f 7261636c 65204c69 6e757820  ,3,Oracle Linux
 23d6b0 382c6772 7562322c 322e3032 2c6d6169  8,grub2,2.02,mai
 23d6c0 6c3a7365 63616c65 72745f75 73406f72  l:secalert_us@or
 23d6d0 61636c65 2e636f6d 00000000 00000000  acle.com........
 23d6e0 00000000 00000000 00000000 00000000  ................
```

SBAT good practices and how to prevent locking yourself down



```
[root@localhost ~]#
[root@localhost ~]# mokutil --list-sbat-revocations
sbat,1,2022052400
grub,2
```

Documentation and Useful links

1. Shim github repository
2. Shim SBAT documentation
3. shim review process
4. Mokutil SBAT policy control
5. Shim reference policy commit
6.

Thank you

Aleksandr Burmashev

alexander.burmashev@oracle.com

Oracle Linux and VM development