Contribution ID: **317** Type: **not specified**

Leveraging and managing SBAT revocation mechanism on distribution level

Wednesday 18 September 2024 11:00 (20 minutes)

at first i want to give a brief description of what SBAT is, why it was implemented and what currently supports it (grub2, shim, systemd-boot various EFI tools, like fwupdate and etc).
And also cover that SBAT expects different downstream distros to adopt upstream SBAT values from the code base they consume, so that a proper revocation by SBAT is always ensured.
And explain why SBAT revocation is even needed in the first place instead of revocation by adding a certificate to a DBX.
It is just my experience that SBAT is still a very much grey area for many developers and enterprise users.
Second - i want to cover the scenario of preventing locking yourself down, when you update components de-synced, i.e. new shim is issued with a new grub2, but users decide to install only a new shim, and may end up in locked down system, i want to highlight the fact, that since boot chain is a system critical sub-system, it makes sense to introduce a dependency mechanism that ensures a correct set of packages is being pulled in. In many distros right now it is being ensured simply by "install all updates", but you may end up in a scenario of being unable to boot if you decide to pursue limited package set installation (that happens often if distros are pulling in only packages with "CVE fixes").

Third - i want to cover use case of rolling back to older SBAT "level"in case it is needed in specific production environments. Mainly it will be about how to design your deployment/system so that you do NOT end up locked down, and can prepare in advance for such potential rollback. Instead of just disabling SBAT, in fact a proper design scheme of SBAT levels should be implemented, and trigger events to move from one level to another should be in place.

Fourth - i will be covering scenario of locking yourself down in case of using several distributions on same system due to SBAT update and what is a proper mechanism of getting yourself unlocked and preventing such scenarios.

Primary author: BURMASHEV, Aleksandr (Oracle corporation)

Presenter: BURMASHEV, Aleksandr (Oracle corporation)

Session Classification: System Boot and Security MC

Track Classification: System Boot and Security MC