Linux Foundation UEFI Secure Boot System for Open

By James Bottomley - October 10, 2012 - 9:53pm

Guest post from James Bottomley, Linux Foundation Technical Advisory Board

I'm pleased to announce that the Linux Foundation and its Technical Advisory Board have prod
indeed all Open Source based distributions) to continue operating as Secure Boot enabled syst
Foundation will obtain a Microsoft Key and sign a small pre-bootloader which will, in turn, chain
check) a predesignated boot loader which will, in turn, boot Linux (or any other operating syste
a "present user" test to ensure that it cannot be used as a vector for any type of UEFI malware
pre-bootloader can be used either to boot a CD/DVD installer or LiveCD distribution or even bo
secure mode for any distribution that chooses to use it. The process of obtaining a Microsoft si
is complete, the pre-bootloader will be placed on the Linux Foundation website for anyone to d

Philosophy Behind this Announcement

The Linux Foundation is committed to giving users freedom of choice on their platforms. Confc
already published a variety of tools to permit users to take control of their secure boot platform
managing (or replacing) the installed Key Exchange Keys here. However, as one of the enable
Foundation recognizes that not everyone is willing (or able) to do this so it was also necessary
people to continue to try out Linux and other Open Source Operating Systems in spite of the ba
in their way and without requiring that they understand how to take control of their platforms.
technical plan, which is implemented in this pre-bootloader, to allow distributions to continue f
environment.

The current pre-bootloader is designed as an enabler only in that, by breaking the security ver
bootloader, it provides no security enhancements over booting linux with UEFI secure boot turr
Linux to continue to boot on platforms that come by default with secure boot enabled. The Lin
some of the major distributions (e.g. Fedora, SUSE and Ubuntu) to tackle the problem of taking
to enhance platform security and sees the pre-bootloader it is releasing as a stop-gap measure
to come up with plans that take advantage of UEFI secure boot.

Technical Details

The source code for the pre-bootloader is available in

git://git.kernel.org/pub/scm/linux/kernel/git/jejb/efitools.git

As Loader.c

It is designed to be as small as possible, leaving all the work to the real bootloader. The real b
same partition as the pre-bootloader with the known path loader.efi (although the binary may l
The pre-bootloader will attempt to execute this binary and, if that succeeds, the system will bo
load with a security error (because it is unsigned), the pre-bootloader will stop at a splash scre
selecting a menu option, that they wish to continue booting loader.efi. If this confirmation (wh
successful, the pre-bootloader will then execute loader.efi without security verification (if the u
pre-bootloader will signal failure and the UEFI boot sequence will continue on to the next boot
repeat booting (and to make the pre-bootloader useful for booting hard disks as well as USB ke
also check to see if the platform is booting in Setup Mode and if it is, will ask the user for perm
loader.efi into the authorized signatures database. If the user gives permission, the signature
then boot up without any present user tests on all subsequent occasions even after the platfor
mode. The present user test splash screen that appears in secure boot mode asking for permi
direct the user to a Linux Foundation website where we will gather details of how to place platf
user how to do this, either to install the signature of loader.efi or to take full control of the platf
Key Exchange Keys.