Securing the Computer through a trusted USB device

04.11.2017

AMMANAMANCHI SAI KARTHIK

B150310CS

B BATCH

10

KONGARI SAI MANOJ

B150610CS

B BATCH

35

TANGELLA MAHESH KUMAR

B150588CS

B BATCH

62

Abstract

The boot process of the computer completes only when a usb device with valid key is plugged into the computer and if the key does not match the original we can still insert another usb device and continue trying. If the incorrect usb device is inserted more than 5 attempts or if the correct usb device is not inserted within 100 seconds of kernel boot, the boot does not proceed and the cpu enters a loop.

Compiling and Installing the kernel:

1. make config localmodconfig

2. After you have done this you need to replace the hard coded serial number with the one belonging to your device. This is found in drivers/usb/core/hub.c.

    vim drivers/usb/core/hub.c

Note: some USB devices, like HID devices, won't have a serial number. In these cases serial will be NULL.

3. To compile your kernel using 4 physical cores.

    sudo make -j 4 && sudo make -j 4 modules_install

4. To install your newly created kernel.

    sudo make install

5. sudo update-grub

    Updating the grub to reflect the changes to our kernel in the grub loader.

Functionality:

Allows a user to add an additional layer of authentication. Specifically, it requires that users authenticate themselves using something they have (the USB device) rather than just something they know (a password).

This can easily be extended to accept more than one USB device.

Use Case:

If the user had physically locked down their computer, password protecting the BIOS changing computer's boot sequence to disallow booting from removable media, then this addition to the GNU Linux kernel would indeed add some measure of additional security.If the user had not implemented the aforementioned security measures, this system could easily be overcome by installing a new linux partition and using the computer.