August 02, 2019

Mitigating Malicious Firmware by Detecting the Removal of a Storage Device

Vadim Sukhomlinov

Andrey Pronin

Randall Spangler

Mitigating Malicious Firmware by Detecting the Removal of a Storage Device

Abstract:

User equipment (UE), such as smartphones, notebooks, laptops, and the like, require protection from malicious software and firmware. To this end, device manufacturers install security chips on their devices, which are often located on the motherboard of the device. This publication describes hardware designs and methods to detect the removal of a storage device, such as a solid-state drive (SSD), a non-volatile memory (NVM), a non-volatile dual in-line memory module (NVDIMM), an embedded multimedia card (eMMC), and other types of non-volatile memory. After the UE detects the removal of the storage device, the UE sends a signal to a security chip (root of trust (ROT)). The ROT notifies a user that the storage device was removed, later re-installed or replaced, and that a full verification of the firmware of the storage device needs to occur. Full verification of firmware of the storage device has limitations, such as a limited access speed to the storage device. To this end, at times, the UE performs verification of critical OS areas (files). The verification process changes depending on the power state of the UE and the removal detection of the storage device. A "cold boot," or the removal detection of the storage device, triggers a full verification of the storage device, whereas, a "warm boot," without an indication that the storage device was removed, triggers verification of critical OS areas (files).

Keywords:

Firmware, malicious firmware, malicious software, storage device, SSD, NVM, NVDIMM, eMMC, SATA, non-volatile memory, root of trust, RoT, security chip, hardware security, verification, firmware verification.

Background:

User equipment (UE), such as smartphones, notebooks, laptops, and the like, require protection from malicious software and firmware. To this end, device manufacturers install security chips on their devices, which are often located on the motherboard of the device. Among other things, the security chips contain a processor with re-writable (RW) firmware images.

Several UE attempt to achieve security from malicious software or firmware by verifying a pre-determined unique signature using a "verified boot" before releasing control to a next-in-chain component, such as a storage device. This approach is effective for small software components, such as firmware, operating system (OS) kernels, and drivers. Many other software components, however, are large and run on large datasets. Verification of large software components introduces a considerable computing time delay.

When a storage device is temporarily removed or altogether replaced, the firmware of the storage device can be replaced or modified with malicious firmware. In that case, it is important that the UE re-verifies the storage device, which is a lengthy process and can be computationally expensive. Therefore, such re-verification is performed only when there is a clear indication that the storage device was temporarily removed or altogether replaced. As the UE starts the re-verification process, the malicious firmware of the storage device may initially return the pre-determine unique signature to pass the "verified boot." Then, the firmware of the storage device

may gradually introduce code with malicious content. In addition, verifying the firmware of the storage device is challenging to implement in a secure way because the UE does not have direct access to the storage device and accessing the storage device requires the malicious firmware to be running, which can compromise the UE.

Full verification of firmware of the storage device has other limitations, such as a limited access speed to the storage device. For example, for the UE to access a solid-state drive (SSD) through a serial advanced technology attachment (SATA), which is limited at around 500 megabits (MB) per second, a considerable time delay will occur even when reading a few gigabits (GB) of data. To this end, some UE utilize verification of critical OS areas (files) using Merkle trees for hashing. Verification of critical OS files, however, may not detect small changes to the firmware of the storage device, which over time may compromise the security of the UE.

Therefore, it is desirable to have a technological solution that can detect the temporary removal or replacement of the storage device and trigger the UE to take steps to verify the firmware of the storage device.

Description:

This publication describes hardware designs and methods to detect the removal of a storage device, such as a solid-state drive (SSD), a non-volatile memory (NVM), a non-volatile dual in-line memory module (NVDIMM), an embedded multimedia card (eMMC), and other types of non-volatile memory. After a user equipment (UE) detects the removal of the storage device, the UE sends a signal to a security chip (root of trust (RoT)). The RoT notifies a user that the storage device was removed, later re-installed or replaced, and that a full verification of the firmware of

the storage device needs to occur. Figure 1 helps illustrate one embodiment of a removal-detection method of the storage device.

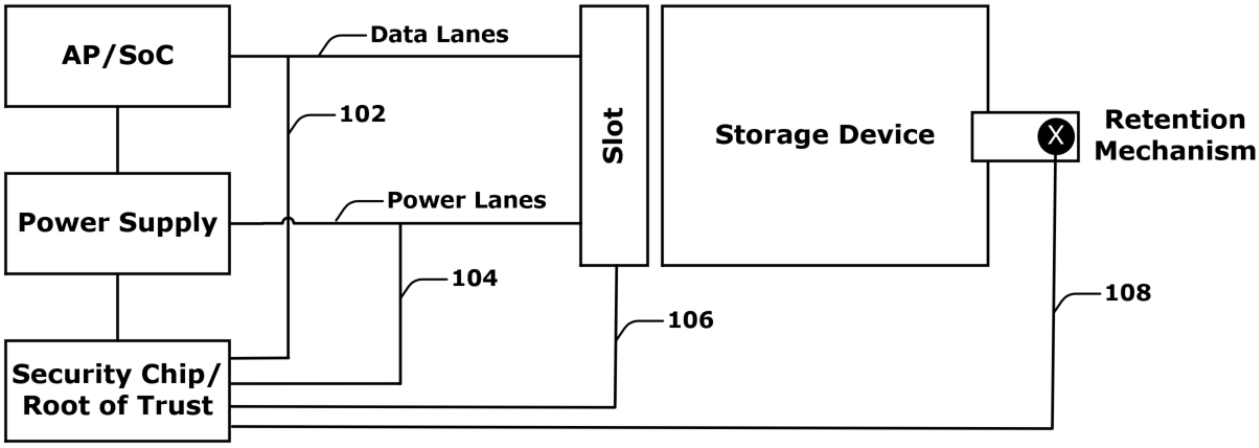

Figure 1

Figure 1 illustrates an interface between the security chip (RoT), an application processor (AP) or a system on chip (SoC), a power supply, a storage-device slot, the storage device, and a storage-retention mechanism. Although the RoT in Figure 1 is illustrated as a separate chip from the AP, the RoT can also be a protected module integrated in the AP. The RoT illustrated in Figure 1 may detect the removal of the storage device by using at least one of the following signals:

- Signal **102** monitors data lanes between the AP and the storage-device slot;
- Signal **104** monitors power lanes between the power supply and the storage-device slot;
- Signal **106** monitors the storage-device slot; or
- Signal **108** monitors the storage-retention mechanism, such as a screw that may be used to physically secure the storage device.

Monitoring the Data Lanes

The RoT may check some parameters of the signal lanes to detect the presence of the storage device when the UE is powered up or down. Assume the UE utilizes a peripheral component interconnect express (PCIe), such as NVM Express (NVMe), which is often used to

interface the UE's motherboard with the storage device, such as the SSD. On the PCIe, the RoT of the UE may detect the presence of an add-in card by monitoring the signals that the add-in card uses to connect the storage-device slot.

In another embodiment, the PCIe may use the AP to assist an operating system (OS) by performing the following actions:

- Check a device link layer link active (DLLLA) bit in a PCIe link status-register of the down-stream ports;
- Read a vendor-specific link status-register of the down-stream ports;
- Read a vendor's identification of the storage device that is connected to the down-stream ports; and
- Determine whether the storage device was removed.

Regardless of the method that the UE uses to detect the removal of the storage device, the RoT does not need to have access or to read the data that are being transferred to and from the AP and the storage device, which helps lower the computing time delay.

Monitoring the Power Lanes

Some power lanes may support hot-swapping (hot-plugging) capabilities that allow the UE to support replacing, removing, or adding components without shutting down the OS. For example, the power lanes may support a slimline SATA connector, which is used in smaller form-factor UEs, such as in notebook optical-drives. A dedicated pin of the slimline power connector may be used to monitor the presence of the storage device, and signal **104** can be coupled from the RoT to the dedicated pin of the slimline power connector that monitors the presence of the storage device.

In another embodiment, the RoT can measure the resistance or the capacitance between the power lanes (*e.g.*, 3.5 Volts, 5.0 Volts) and ground (not explicitly illustrated in Figure 1).

Monitoring the Device-Storage Slot

The receptacle of the device-storage slot can be designed to include a switch to detect the presence of the storage device. This design can be implemented on several interfaces, such as SATA, NVMe, PCIe, or NVDIMM.

Monitoring the Storage-Retention Mechanism

Some storage devices, such as the NVMe, have a dedicated hole that is used to physically secure the storage device using a screw. An original design manufacturer (ODM) can design a UE that enables the RoT to detect the removal of the screw that physically secures the storage device, as is illustrated in Figure 2.

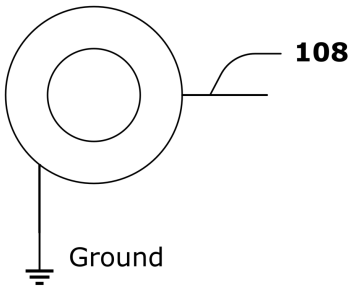

Figure 2

The RoT of the UE may use signal **108** to detect the continuous presence of the screw that is used to physically secure the storage device. The RoT may employ different ways to detect whether the screw was temporarily loosened or altogether removed. In one embodiment, the RoT may use a simple time-domain reflectometer (TDR) to detect an opening at the screw. In another embodiment, the RoT may measure the resistance or the capacitance of the path from the RoT to the grounded screw. If the RoT detects an increase in resistance or a decrease in capacitance in

the path from the RoT to the grounded screw, it is a good indication that the screw was loosened or altogether removed.

Alternatively to the design illustrated in Figure 1 and in Figure 2, the ODM may also design a UE that employs a direct connection from the RoT to the storage device, as is illustrated in Figure 3.

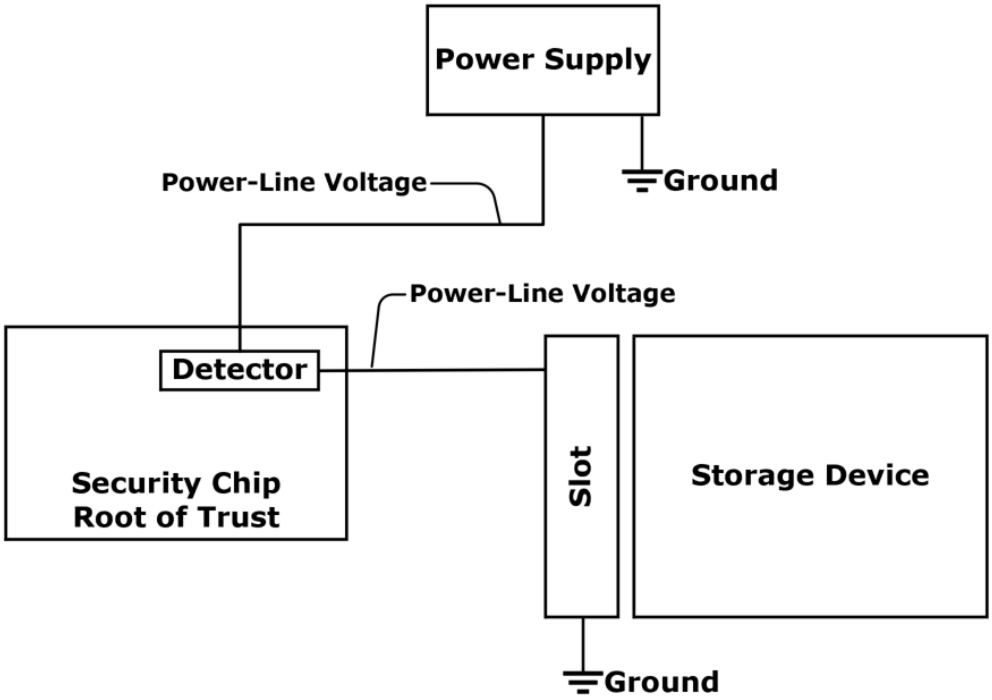

Figure 3

As is illustrated in Figure 2, the power line detection can be implemented such that the power line comes through the security chip (RoT) to the storage-device slot. The ODM can integrate a detector in the RoT of the UE, which can measure the state of the power pins in the storage-device slot. When the storage device is removed, the detector embedded in the RoT senses the loss of power to the storage-device slot.

The example designs illustrated in Figure 1, Figure 2, and Figure 3, help the RoT detect the removal of the storage device, which trigger the UE to take steps to verify the firmware of the storage device, as is illustrated in Figure 4.

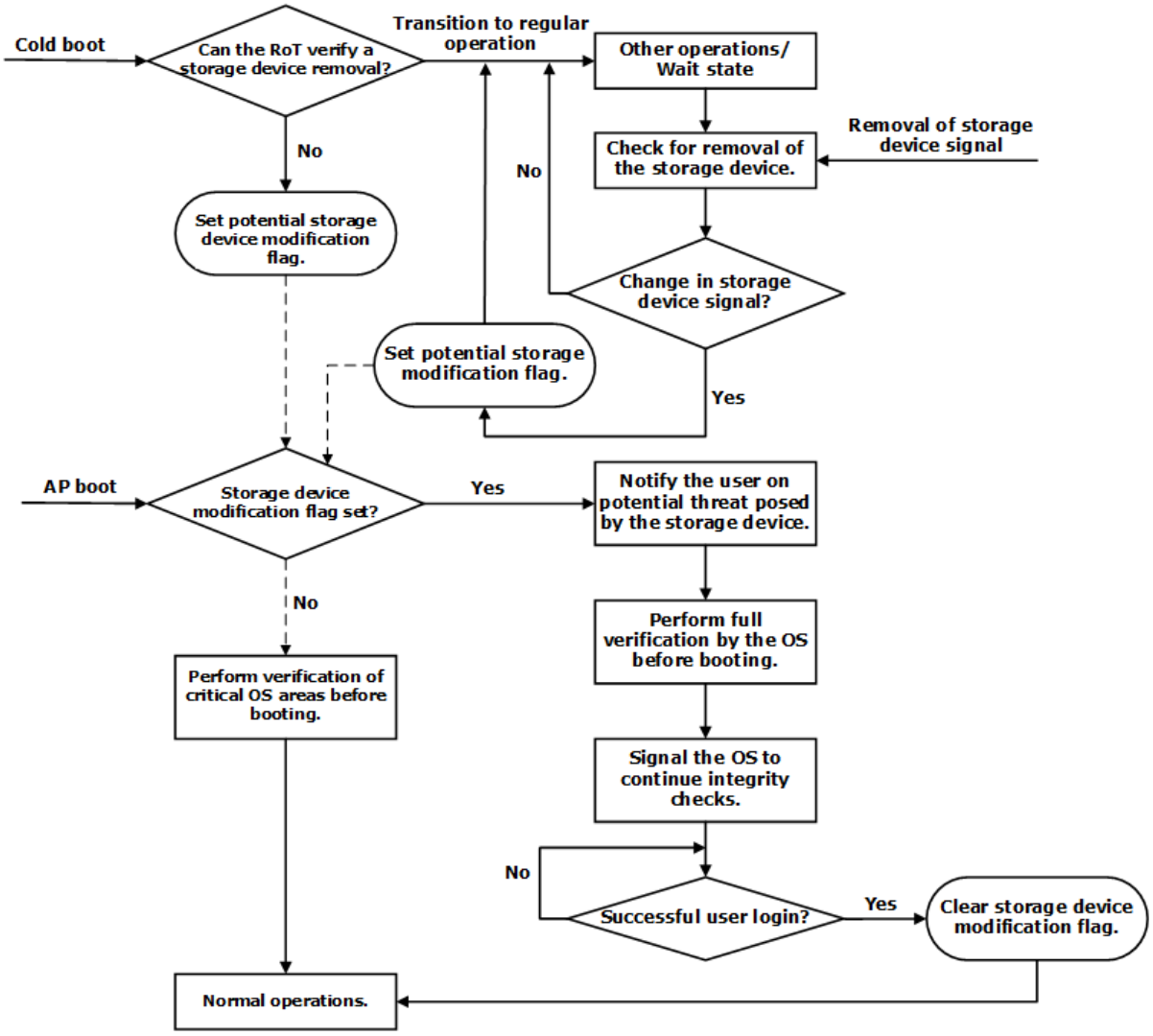

Figure 4

The firmware running on the security chip monitors and records any signal that detects the removal of the storage device. On battery-powered UE, the security chip can be powered up regardless of the power state of the of AP. Therefore, from the perspective of a user, the removal of the storage device can be detected even when the UE is powered off. In addition to powering

down the UE, a full power down requires a removal or a full depletion of the UE's battery. The full power down can limit the ability of the RoT to detect the removal of the device storage. This event, however, is easily recognizable by a "cold boot," which triggers a full verification of the storage device, as is illustrated in Figure 4. As is described herein, a "cold boot" is a boot process in which the UE starts from a powerless state—the UE is turned off and the battery is removed or completely depleted. Figure 4 helps illustrate that the verification process changes depending on the power state of the UE and the removal detection of the storage device by using any of the methods and designs described in Figure 1, Figure 2, and Figure 3. A "cold boot" or a signal that indicates that the storage device was removed, triggers a full verification of the storage device, whereas, an AP boot ("warm boot") without an indication that the storage device was removed, triggers verification of critical OS areas (files).

In conclusion, detecting a temporary removal or replacement of the storage device helps the UE trigger the optimal verification process of the storage device, which increases the security from malicious software and firmware, while managing the computing time delay to perform such verification.

References:

[1] Patent Publication: US20160246968A1. System and method for protecting data stored on a removable data storage device. Filing Date: May 5, 2016.

[2] Patent Publication: US20090321302A1. Protection device for an electronic card. Filing Date: October 2, 2007.