November 2019

# Verifying Read-Only Firmware For Open-Box Returns

Randall Spangler



# Verifying Read-Only Firmware For Open-Box Returns

ABSTRACT

A customer who returns a laptop or other electronic device to a retailer may, for benign or malign reasons, have changed its firmware. The retailer typically certifies the laptop for resale as refurbished equipment by sending it to the factory to verify its firmware. This is a time-consuming and expensive process. The techniques of this disclosure leverage an on-board security chip to verify the firmware at the location of the retailer itself. Shipping of the electronic device from retailer to factory is obviated, saving time and cost.

KEYWORDS

- Electronics retail
- Return merchandise authorization (RMA)
- RMA verification
- Security chip
- Read-only firmware
- In-store return
- Cryptographic hash
- Open-box returns

## BACKGROUND

The firmware of a laptop (or other electronic device) that is returned by a customer to a retailer may have changed from the original factory shipped product. The retailer typically certifies the laptop for resale as refurbished equipment by sending it to a factory to verify its firmware. This is a time-consuming and expensive process.

A challenge in the return process is verifying that the normally read-only firmware on the application processor (AP-RO) or embedded controller (EC-RO) has not been altered. For example, firmware alterations may be performed in order to run other operating systems in an attempt to achieve shorter boot delay. A malicious user may modify firmware to install malware, either directly in the firmware or by changing the signing keys/update path for a device, such it delivers an OS payload from an unofficial source.

Whether the RO firmware is altered for benign or malign reasons, to make sales of refurbished devices to customers, there is a need to ensure that the device is running official firmware and receiving official updates.

## DESCRIPTION

Per the techniques of this disclosure, a security chip within the returned electronic device runs protected, e.g., unalterable, firmware that can compute an encrypted, e.g., signed, hash of the read-only firmware and operating system of the electronic device. In principle, the security chip itself can verify if the device firmware has been altered, e.g., by comparing the computed hash with the known hash of the unaltered firmware and operating system. However, displaying the results of the verification on the device itself is subject to security risks. For example, the operating system of the device may have been altered such that the verification result from the security chip is falsely displayed on the screen. An altered read-only firmware can either falsify the output of the security chip, or it can patch later stages of the boot, e.g., rewritable firmware, recovery image, etc. such that they falsify the output of the security chip.

This disclosure describes techniques to verify the returned electronic device, e.g., securely obtain the true results of the verification procedure performed by the security chip.

*Verifying a returned electronic device using a trusted device*

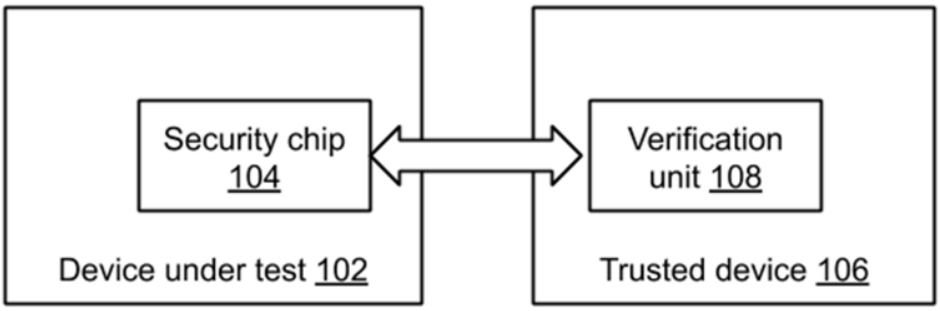


**Fig. 1: Verifying a returned electronic device using a trusted device**

Fig. 1 illustrates the verification of a returned electronic device using a trusted device. As mentioned before, the returned electronic device, also referred to as device under test (DUT) (102), includes a security chip (104) that can securely compute an encrypted, e.g., signed, hash of the read-only firmware and operating system of the DUT.

A trusted device (106) which can for example, be a laptop or mobile device owned by the retail outlet, connects to the DUT, e.g., using a USB cable. The trusted device includes a verification unit (108) that receives the encrypted hash computed by the security chip. The verification unit detects if the read-only firmware, e.g., AP-RO, EC-RO, etc., and/or operating system of the DUT has been altered by receiving the encrypted hash, decrypting it, and comparing it with the known hash of the unaltered firmware and operating system of the DUT. If the received hash has been tampered with during its transmission from the DUT to the trusted device, then such tampering is detected using cryptographic methods.

*Verifying a returned electronic device using a server and a trusted device*

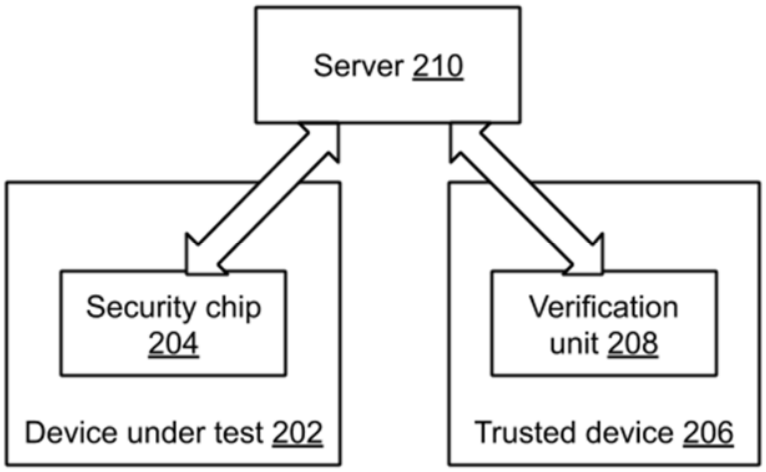


**Fig. 2: Verifying a returned electronic device using a server and a trusted device**

Fig. 2 illustrates verification of a returned electronic device using a server and a trusted device. As mentioned before, the DUT (202) includes a security chip (204) that can securely compute an encrypted, e.g., signed, hash of the read-only firmware and operating system of the DUT. Per the techniques, the DUT sends the computed hash over the Internet to a server (210).

A trusted device (206), which can, for example, be a laptop or mobile device owned by the retail outlet, connects to the server. The trusted device includes a verification unit (208) that requests and receives from the server the encrypted hash. The verification unit detects if the read-only firmware, e.g., AP-RO, EC-RO, etc., and/or operating system of the DUT has been altered by receiving the encrypted hash, decrypting it, and comparing it with the known hash of the unaltered firmware and operating system of the DUT. If the received hash has been tampered with during its transmission from the DUT to the server and onwards to the trusted device, then such tampering is detected using cryptographic methods. Alternately, the verification unit can be

on the server, such that the retail outlet receives from the server a binary (pass/fail) response as to whether the returned electronic device has altered firmware.

In either case, the server uses device attestation to verify that it is communicating to a genuine security chip as follows. The server generates a temporary public-private key pair and sends the public key (signed with the device's endorsement key), which the security chip uses to sign the report. That key is regenerated at each attempt to prevent replay attacks, e.g., where a compromised OS tries to resend a response from a good system. The server report includes the date and time the DUT last sent a report, such that the retail outlet knows that the report is from the current test and not from a previous test.

*Verifying a returned electronic device using an on-device indicator such as an LED*

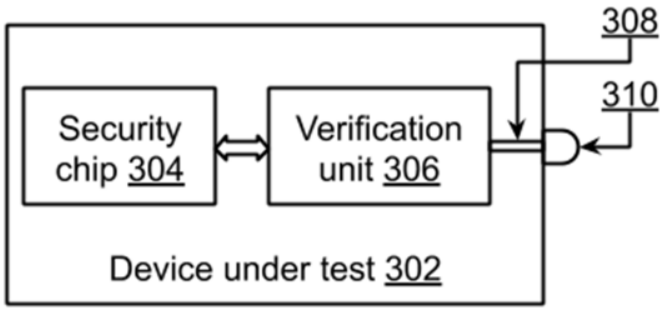


**Fig. 3: Verifying a returned electronic device using an on-device indicator such as an LED**

Fig. 3 illustrates verification of a returned electronic device using an on-device indicator such as an LED. As mentioned before, the DUT (302) includes a security chip (304) that can securely compute an encrypted, e.g., signed, hash of the read-only firmware and operating system of the DUT.

The DUT also includes a secure verification unit (306) that can compare a hash computed by the security chip with the known hash of the unaltered firmware and operating system of the

DUT. The verification unit is connected via a trusted channel (308) to an external indicator such as an LED (310). The trusted channel is such that the device firmware and operating system has no control over it.

The security chip computes a hash of the read-only firmware, e.g., e.g., AP-RO, EC-RO, etc., and/or operating system of the DUT. The verification unit compares the computed hash with the known hash of the unaltered firmware and operating system of the DUT, and lights up the LED based on the result of the comparison. For example, if the hashes match, the LED can turn green, or turn on and off in a particular pattern; if the hashes don't match, the LED can turn red, or turn on and off in another distinct pattern.

*Verifying a returned electronic device using a secure self-test and a trusted device*

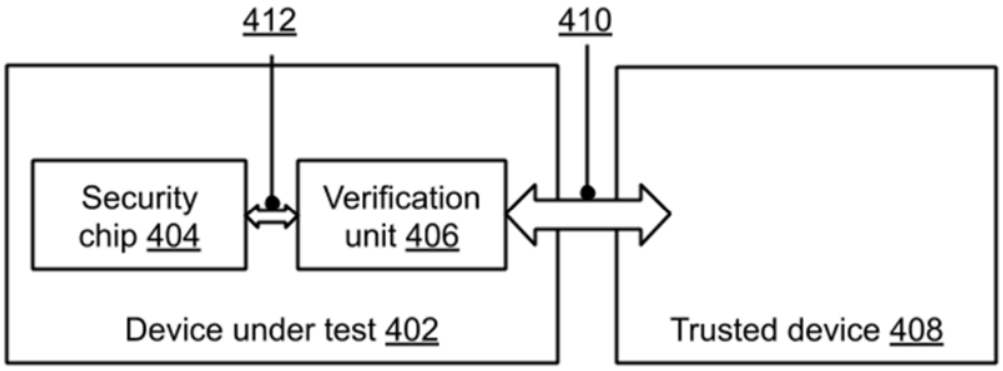


**Fig. 4: Verifying a returned electronic device using a secure self-test and a trusted device**

Fig. 4 illustrates verification of a returned electronic device using a secure self-test and a trusted device. As mentioned before, the DUT (402) includes a security chip (404) that can securely compute an encrypted, e.g., signed, hash of the read-only firmware and operating system of the DUT. The DUT also includes a secure verification unit (406) that can compare a hash computed by the security chip with the known hash of the unaltered firmware and operating system of the DUT. The verification unit has a trusted connection (412) to the security chip.

A trusted device (408), which can, for example, be a laptop or mobile device owned by the retail outlet, connects to the DUT using a trusted channel (410). The verification unit detects if the read-only firmware, e.g., AP-RO, EC-RO, etc., and/or operating system of the DUT has been altered by receiving from the security chip the encrypted hash, decrypting the hash, and comparing it with the known hash of the unaltered firmware and operating system of the DUT. By incorporating the security chip and the verification unit within the DUT, the DUT in effect performs a self-test of its firmware and operating system. The trusted device (408) is used by an operator to read the results of the self-test.

A device that passes the check based on the techniques herein can be qualified at the retail outlet itself as a refurbished unit. A device that fails the check can be sent through a full return merchandise authorization (RMA) procedure. While the techniques verify the read-only firmware, the other components on the device, e.g., WiFi modem, disk, keyboard, video out, touchpad, etc. are tested via normal test procedures, e.g. using a stripped-down factory image. Some components may have their own firmware, which are independently verified and/or updated.

The described techniques herein do not detect a hardware attack, e.g., modifying device hardware by adding a microcontroller in between the SPI bus and the SPI flash chip, piggybacking a keyboard logger onto the keyboard flex, etc. These can be tested for by opening the returned electronic device and looking for evidence of rework.

## CONCLUSION

The techniques of this disclosure use a security chip on board an electronic device to verify the firmware and operating system of the device when the device is returned by a

customer to a retail outlet. Shipping of the returned electronic device from retailer to factory is obviated, saving time and cost.