July 2021

SECURE BOOT AND EVENT-TRIGGERED VERIFICATION ON DOCKS

HP INC

Secure Boot and Event-Triggered Verification on Docks

Abstract: A universal docking station ensures the integrity of the dock firmware by implementing a secure boot process and re-executing it when a host device is disconnected from the dock.

This disclosure relates to the field of portable computers.

A technique is disclosed that adapts secure boot technology to the architecture of a universal docking station to guarantee that the firmware running on the dock has not been compromised by a malicious third party.

Universal docking stations for portable computers, such as for example laptop and notebook computers, are becoming available. These docks provide the most convenient way for the computers to connect to monitors and peripheral devices. With this ease of usability, however, security becomes a concern for the end user; in particular, ensuring that the firmware running on the dock has not been compromised.

According to the present disclosure, the dock includes a secure boot mechanism to implement an event-triggered code verification.

The dock management controller (DMC) is denoted as the critical boot device for the dock. As such, the critical boot device implements the security measures for the dock.

The first security measure is Secure Boot: the boot loader and credentials are stored within a write-protected flash. Upon boot, the DMC firmware image is validated before it is allowed to execute.

The second security measure is Validation on Disconnect Event: Upon the event of a disconnect from the host, the DMC forces a recycle and re-performs a secure boot, in order to verify the integrity of the DMC firmware. To expedite short disconnect/connect events, the DMC implements a certain delay after disconnect before forcing the validation. This is a fairly short process, so if the host is reconnected during this time, there is negligible disruption perceived by the user.

The Secure Boot feature advantageously ensures that the code is validated before being loaded for execution. The Validation check on Disconnect event advantageously ensures that the runtime integrity of the dock is validated periodically.

Disclosed by Roger D. Benson and Syed Abbas, HP Inc.