June 2023

Telemetry to Securely Track the Extended Life of a Personal Computer System by Measuring CSME Health and PSR Data Integrity Counters Records

HP INC

Title

Telemetry to Securely Track the Extended Life of a Personal Computer System by Measuring CSME Health and PSR Data Integrity Counters Records

Abstract

Current chipsets of notebooks and laptops do not have the capability to track refurbishment or remanufacturing status of the notebook under the operating system, i.e., at the silicon chip layer. PC manufacturers can design a notebook PC to be refurbished and/or remanufactured to extend the life the PC and/or resell the PC as a second life device (or with follow-on refurbishment services, as a 3rd, 4th, etc. life device) with specific tracking information to determine if and when the PC had been refurbished, if any incidents have occurred to the PC, and to track if any components within the PC had been replaced or repaired.

The PC can be designed with a refurbishment counter and unique id, e.g., Unique Platform ID (UPID) record embedded and starting at time of manufacture and securely update the counter whenever a certified refurbishment service has occurred subsequently. This innovation allows for the PC manufacture to create and maintain a permanent "VIN-like" record (an identifier associated and unique to the specific PC) secured at the silicon chip layer in the PC. This innovation also allows for the creation and maintenance of a "CarFax-like" record of certain incidents, thresholds exceeded, and repaired/replaced components have been performed during the lifetime of the PC.

The telemetry recorded includes data such as a refurb counter (e.g., the times the PC has been refurbished or remanufactured), intrusion detection (e.g., the times a PC has been opened for repair or upgrading), shock incidents (e.g., the times a PC has been dropped), thermal incidents (e.g., exceeding specified temperature thresholds) and similar telemetry. The telemetry stored and maintained below the operating system layer, at the silicon chip layer, provides a more secure, persistent, permanent and reliable record as opposed to storing the telemetry at or above the operating system and software layer which can be altered, deleted or lost by reimaging the storage device of the PC.

Article

Introduction

This disclosure relates to the field of personal computers and the telemetry data that is entered, stored, retrieved, and managed from and at the silicon chip layer, i.e., below (and without the necessity of) the operating system and/or above the operating system, and leveraging the telemetry data to enable information technology management and services in a secure and efficient manner.

At time of manufacture, a personal computer can be programmed with a tool to set certain information into secure, non-volatile memory at the silicon chip layer (below the operating system). This information can include data elements defined from a Platform Service Record (PSR), a Unique Platform Identification (UPID), and data specified by the personal computer OEM. This information can also be augmented with additional telemetry data from hardware sensors, integrated circuits, embedded controllers, and related firmware implemented by the personal computer OEM; for example, thermal/power events tracked and logged by the OEM-supplied sensors or the firmware update/recovery events which relies on OEM's design.

PSR data elements can include (but not limited to):

- Basic PC system information
- PC system runtime events and counters
- OEM-defined metadata
- BIOS or firmware update
- Firmware recovery mechanism
- Abnormal reboot, hang-up, shutdown or power loss
- Hardware component detection (display, memory, etc.)

The personal computer is associated with a Unique Platform ID which is a unique and persistent identity data record to identify a personal computer throughout its lifetime and does not change during its lifetime.

The personal computer OEM can also augment the PSR and UPID telemetry with additional OEM-developed telemetry from sensors, integrated circuits, embedded controllers and related OEM firmware, and combine it with the PSR/UPID information as a persistent log of metadata and telemetry that remains persistent with the personal computer.

The UPID is analogous to the VIN number which uniquely identifies an automobile.

The combined PSR and OEM-specific telemetry is analogous to "CarFax" information uniquely associated with an automobile.

During the lifetime of the personal computer, these data elements (telemetry) can be logged and securely retrieved from the system and can be leveraged for information technology management services, to validate refurbishment/remanufacturing status, to maintain a persistent log of critical events that have occurred to the personal computer over its lifetime, to confirm the personal computer has not be adversely tampered with, and other information services.

The telemetry stored on the endpoint is routinely and securely transmitted to a cloud-based (or on-prem based) data lake via a PC OEM collector agent operating below-the-OS at the silicon chip layer (or optionally via an above-the-OS software agent) to be catalogued, de-duplicated and data cleansed, and leveraged for machine learning, artificial intelligence algorithms and generative AI functions for discovery, diagnostic, predictive and prescriptive analytics. The resulting analytics can be used for refurbishment/remanufacturing services, information

technology management services, predictive insights services, warranty/repair customer support services, and other useful IT management functions.

Refurbishment Service Use Case

One specific use case and resulting technique has been developed to design a personal computer to be refurbished and/or remanufactured to extend the life the PC and/or resell the PC as a second life device and potentially for follow-on refurbishment services as a 3rd, 4th, etc. life device. A technique has been designed to log specific telemetry persistently on the personal computer to determine if and when the PC had been refurbished, if any critical events or incidents have occurred to the PC, and to track if any components within the PC had been replaced or repaired since the original manufacturing date.

At time of manufacture, the PC is given a UPID data record logged and embedded into the hardware of the PC at the silicon chip layer. This UPID record is globally unique and stays persistent through the lifetime of the PC embedded with the silicon chip and non-volatile memory components of the PC which are typically soldered (or remain permanent) to the main system board. Also at time of manufacture, an initial PSR record is logged and embedded to the PC with the initial PSR metadata and all counters set to original values.

At any time post-manufacturing and when the PC is used by end users, the various counters, events, sensor activities, etc. when triggered, are securely logged at the silicon layer to the PC and remain persistent with the PC during its lifetime. When a PC is serviced for refurbishment or remanufacturing, a tool designed and authorized for use by the personal computer OEM is used to securely read and update the PC telemetry (UPID, PSR, OEM specific metadata).

For example, after a PC has been successfully serviced during a refurbishment or remanufacturing exercise, a PSR refurbishment counter record would be updated and logged by the OEM tool by an increment, e.g., from “1” (the original manufacture count) to “2” (the first refurbishment service count) to indicate that the PC has undergone a certified refurbishment/remanufacturing event since time of original manufacture. The event date/time and any sub-event details would also be logged associated with the updated counter. And subsequent refurbishment or remanufacturing exercises would continue the increment logging.

The OEM tool would also read any of the UPID, PSR and OEM-specific telemetry to make determinations of the current and past state/events associated with the personal computer and its past usage. For example, the information retrieved from the personal computer via the OEM tool could provide metadata that has been updated, e.g., if OEM source data adversely changed or erased, power or thermal events and when they occurred, excessive shock events (the times a PC has been dropped), chassis intrusion events (the times a PC chassis has been opened up for repair or upgrades), OEM sensor threshold events (e.g., the total amount of power used to-date by all the components of the PC or thermal thresholds exceeded by specific components of the PC), firmware update/recovery events, abnormal system power transition events or any hardware component broken detections, etc. All of these telemetry elements

are logged with descriptors of the event, the date/time of the event, and any detailed data associated with the event.

In addition, any changes to the internal components of the personal computer could be validated from time of manufacture and during the lifetime of the personal computer could be tracked. For example, if a memory module or storage module was replaced, the module replacement could be recorded into an event record with descriptive details noting the original module and the subsequent replaced module into the metadata record.

The telemetry stored on the endpoint in the above example is routinely and securely transmitted to a cloud-based (or on-prem based) data lake via a PC OEM collector agent operating below-the-OS at the silicon chip layer (or optionally via an above-the-OS software agent) to be catalogued, de-duplicated and data cleansed, and leveraged for machine learning, artificial intelligence algorithms and generative AI functions for discovery, diagnostic, predictive and prescriptive analytics.

Technique Workflow Details

At time of manufacture of the PC, a technique has been developed in the factory by the personal computer OEM to use the Intel Firmware Programming Tool (FPT) to log and embed the initial telemetry elements to the PC and associated silicon chip layer. For example, the originating/initial values at time of manufacture would be logged to the PC with:

- Genesis date (date/time of manufacture)
- OEM name, OEM make of PC, OEM model of PC, country of manufacture
- OEM-specific data
- Counters set to original values (e.g., “0” or “1”): S0 runtime odometer, Power On counters, Sx state counters, platform erase/sanitization counter, excessive shock counter, excessive temperature counter
- Intel CSME health and PSR integrity initial counters
- Initial event data (event date/time, event type, sub-event details)
- OEM-specific sensor initial data, e.g., power, thermal, keyboard, display, memory, dock, etc.

Also at time of manufacture, the PC OEM would read the UPID information and securely log it into the PC OEM BIOS of the personal computer endpoint. The PC OEM would securely log the personal computer UPID, PSR records and OEM-specific data telemetry to the PC OEM cloud-based data lake for record keeping and machine learning/artificial intelligence analytics.

During the lifetime of the PC, if a refurbishment or remanufacturing exercise is performed on the PC, a certified PC OEM tool would be used via the PC OEM BIOS to securely increment the UPID refurbish counter in CSME via BIOS HECI commands that are available only pre-EOP (End of Post) and when SPI is in refurbish state. The refurbish counter is subsequently stored in the PC OEM ME firmware. At any subsequent time, a BIOS HECI command (e.g., HeciGetUpidRefurbishCounter) can be exercised for the PC OEM BIOS to securely retrieve the

record and counter information. Other BIOS HECI commands can also be enabled to retrieve other UPID, PSR and OEM-specific data telemetry records.

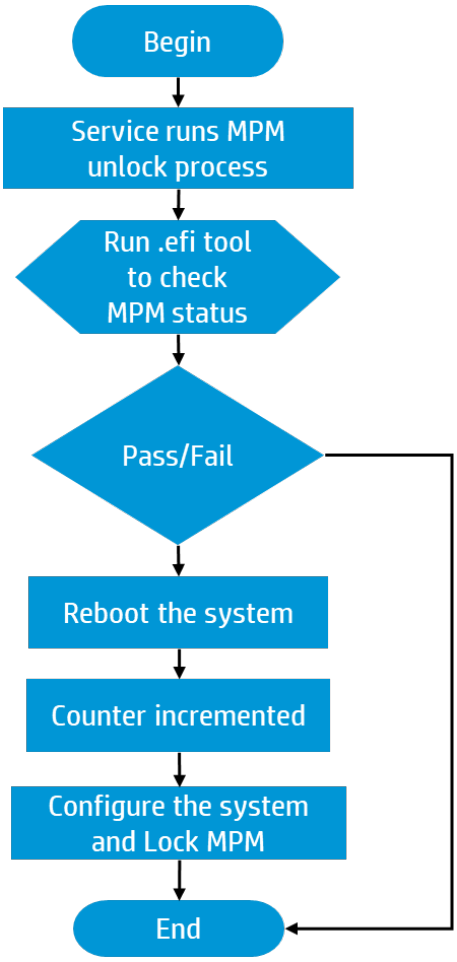

Figure 1. Refurbishment Counter Implementation Flow Chart

Value Proposition

The telemetry stored and maintained below the operating system layer, at the silicon chip layer, provides a more secure, persistent, permanent and reliable record as opposed to storing the telemetry at or above the operating system. Telemetry stored at or above the software layer is subject to be altered, deleted and lost by reimaging the storage device of the PC or manipulating the data with a software application. This is avoided by securely capturing and managing telemetry below the operating system at the silicon layer.

This innovation allows for several services that can benefit information technology management and services. It allows for:

- the PC manufacture to create and maintain a permanent “VIN-like” record (an identifier associated and unique to the specific PC) secured at the silicon chip layer in the PC.
- the creation and maintenance of a “CarFax-like” record of specific incidents, thresholds exceeded, and if repaired/replaced components have been performed during the lifetime of the PC and secured at the silicon chip layer in the PC.
- the accurate validation if a PC has undergone a refurbishment or remanufacturing exercise and introduces a “CPO-like” (certified pre-owned) assurance of the quality of the PC to the end user.
- Ensuring that a PC system hasn’t been tampered with (chassis intrusion), confirm all the original manufactured components are intact and not replaced, determine if any excessive shocks (PC dropped) or thermal activities (PC overheating) have occurred, and similar assurances.
- designing future services and offerings that leverage secure telemetry that can be processed with machine learning, artificial intelligence and generative AI from personal computer hardware via below-the-OS data collection and monitoring.

Disclosed Fred Sung, Ray Hsu, Baraneedharan Anbazhagan, Martin Schwarz, Abu Baker, HP Inc.