September 16, 2019

USB TYPE-C PORT SYSTEM POWER ON SECURITY KEY

HP INC

USB Type-C port system power on security key

As computing device technology advances, system security has become increasingly challenging in protecting physical system hacking. With advent of new hardware equipment and software tools, even an unskilled person can gain access the system and instrument a setup to tap in critical buses and capture password for login one's account to steal sensitive data. Systems at public place, shared workspace and lost unit are particularly vulnerable as they could fall under wrong hand. Defending physical attacks in firmware and software is very difficult as the data can be plucked directly from hardware signals on system board of the computing device with the right equipment.

This innovation is an invention to change the fundamental way which a system is power on by using a physical security key in system USB type-C port to replace the power button. When system is powered and starts executing, all subsystems and buses enter active state with data transmitting on system board allowing it to be captured with external equipment.

The described design and implementation herein are specific to the use of USB type-C alternative-mode to communicate with system Embedded Controller (EC) and provide credential matching and power on the system. The same methodology may be designed to use other types of I/O ports, e.g. USB-A, SD, Smartcard, using mux to add the interface for communication between physical key in the I/O port and EC.

In the USB type-C design and implementation, the communication will be supported with a vendor specific USB type-C alt-mode protocol, i.e. HP alt-mode, from the Power Delivery (PD) controller for the port to the physical USB key plugged in the USB type-C port via CC signal (Figure1). The credential data in this case will be read and transferred to the EC through interface between PD and EC, e.g. I2C bus.

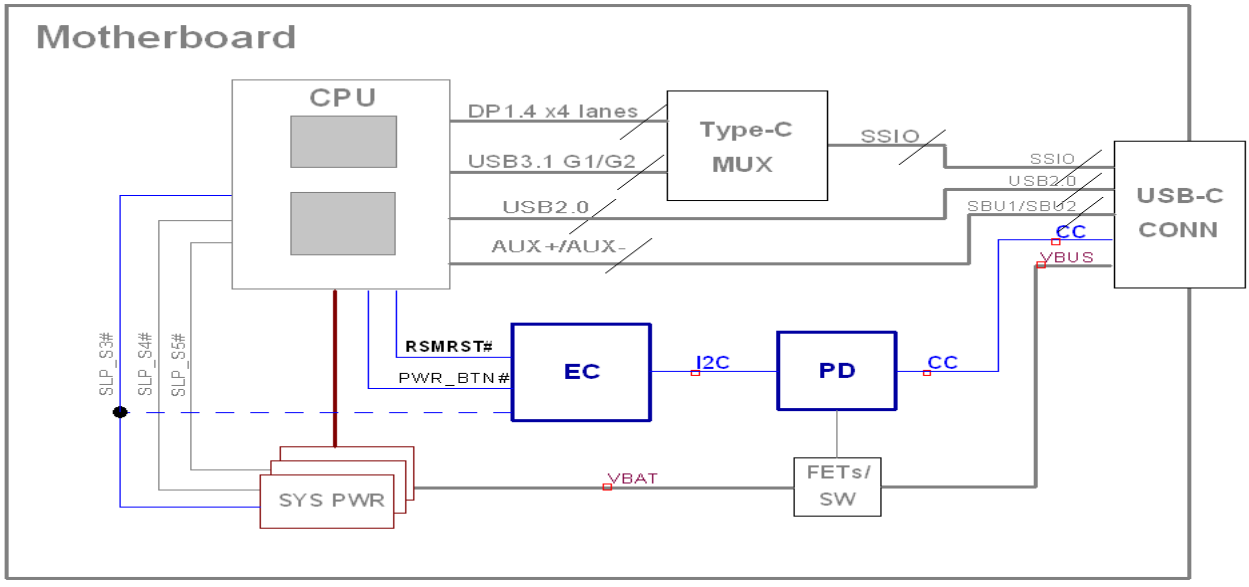

Figure1: Topology supporting USB type-C Vendor Defined Message (VDM) alt-mode from PD to EC via I2C.

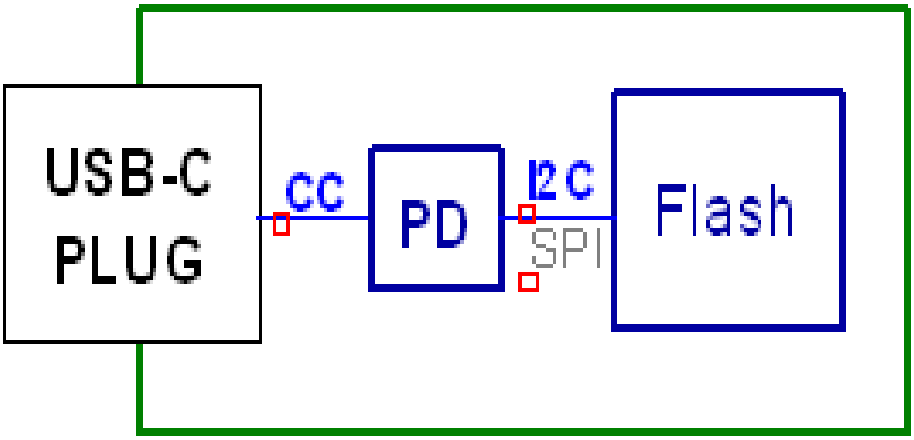

Figure2: Passive physical system power key with PD to support VDM alt-mode communication to EC in host system. Encrypted credential stored in local flash ROM

A direct connect method connecting physical USB key plugged in the type-C port and EC with a dedicated type-C alt-mode utilizing the type-C SBU1, and SBU2 pins as I2C will be the most efficient way to establish a trusted link to receive authentication status.

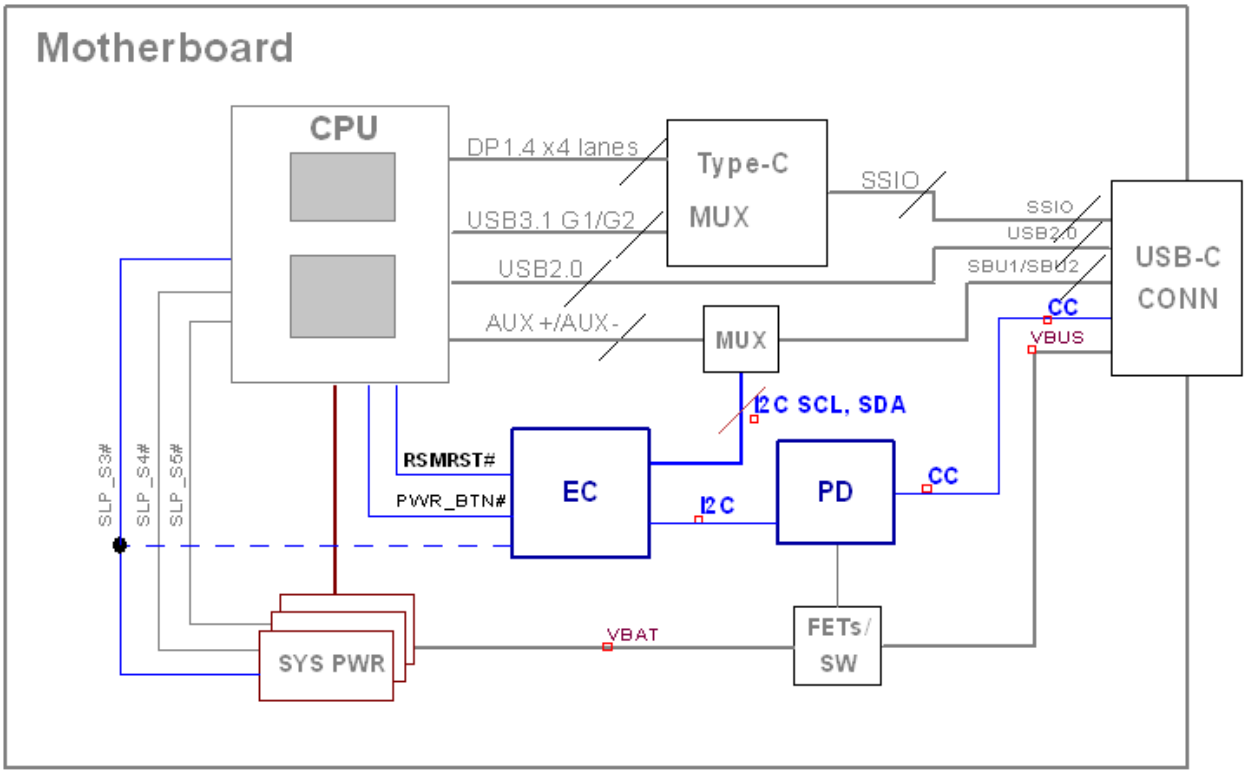

Figure3: Topology supporting direct EC connection to USB physic key via I2C multiplexed on SBU1 and SBU2 as SCL and SDA

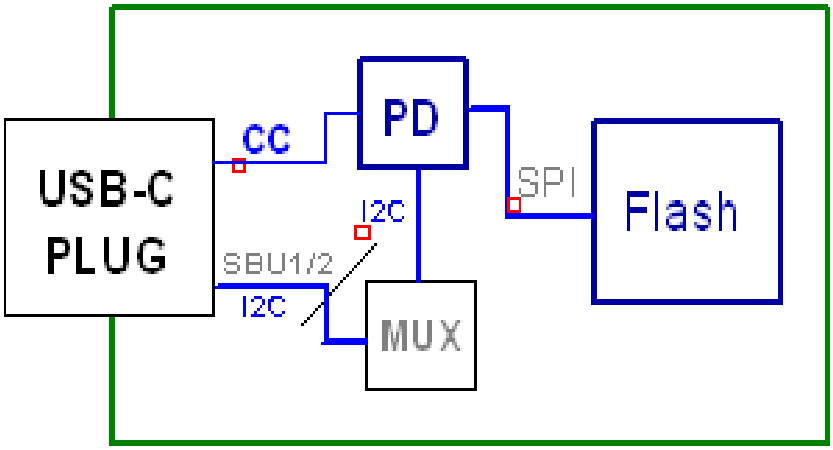

Figure4: Passive physical system power key with I2C on PD connected to SBU1, and SBU2 through multiplexer for direct communication. Encrypted credential stored in local flash ROM.

The USB2.0 interface in type-C connection may also be used and can be connected to the EC through mux if it supports an integrated USB2.0 controller.

The physical USB system power key may be passive, Figure2 and Figure4, with encrypted credential, e.g.

A TPM generated private software key, downloaded and stored in its local static memory. The physical USB system power on key can be an active key, Figure5, integrating an active authentication device such as FPR or camera to identify user to allow power on the system, providing additional layer of security to further hardening overall system security.

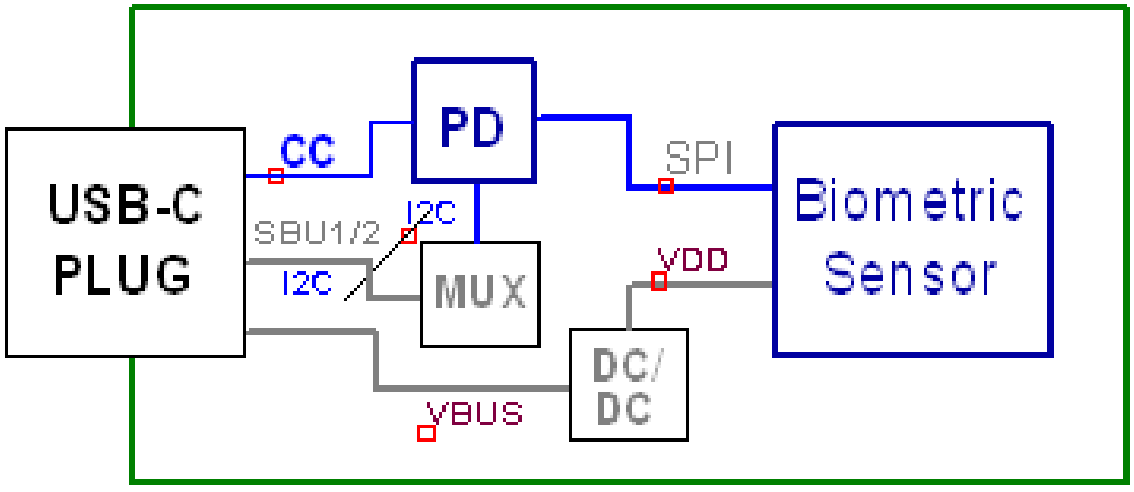

Figure5: Active USB physical system power-on key with biometric sensor for authentication.

Referencing figure 1 or figure 3, EC uses authentication from either stored credential on passive USB physical system power-on key or biometric sensor on active physical system power-on key to determine

authorization to power on the system. From system power states S4 and S5 (hibernation and off respectively).

EC uses the RSMRST# to control the release of chipset power signals (SLP_Sn#) that enable system power rails. From S3 standby or Modern Standby Connected (MSC) suspend states, EC also monitors the SLP_Sn# signals as well as resume command from system BIOS to allow power on from wake events as well as physical USB system power-on key. EC may block power on from suspend state by overriding it low with signals from its GPIOs as shown in figure1 and figure3 or by gating SLP_Sn# in design that pass the signals through GPIOs.

In situation where the system cannot be powered on by USB power-on key due to credential data corruption, physical USB key damage or loss of physical USB key, several recover methods may be implemented. A spare physical USB key is the simplest backup solution. Another can be requesting IT to provide credential to recover the corrupted key or create a new USB physical key.

Advantages:

Computing devices using a physical USB-C secure power-on key to power on will not be able to power on without the correct credential that attacks such as trying to replace system flash BOM, access live RAM, modify TPM module data and snoop critical buses will all be averted.

The physical USB-C power-on key may also be used as power on mechanism to system support Single Sign-On feature allowing user to power on and login Windows in one step, replacing password and Windows Hello.

Disclosed by Richard Lin, Fangyong Dai, Baosheng Zhang and Sean Ma, HP Inc.