OCP Data Center-Secure Control Module/Host Processor Module (DC-SCM/HPM) Architecture Security Considerations

Background:

1. With the DC-MHS modular server architecture, security and control logic is centralized on the DC-SCM module (Secure Control Module), which plugs into a main board called a Host Processor/Memory Module (HPM).
2. The bus/signal interfaces between DC-SCM and HPM traverse the Secure Control Interface (DC-SCI)
3. DC-SCM contains: BMC, Platform Root-of-trust (PRoT), BMC and BIOS Flash, DC-SCM CPLD, and TPM.
4. HPM contains: Processors, Memory, HPM FPGA, FRU, any HW authentication logic, power elements and numerous interfaces to peripheral subsystems
5. The DC-SCM is NOT intended to be hot-pluggable.
6. The HPM is intended to be stateless, meaning that any firmware or configuration state stored on the HPM can be measured and updated under control of the DC-SCM. However, there are stateful elements in the HPM (mutable firmware of FPGA, mutable firmware of power elements, FRU contents, CPU fuses and PIROM, and authenticator configuration if used).

New Physical Attack Threats:

1. Since 1) the DC-SCM is a standard form-factor and 2) connects to the HPM via a standard DC-SCI connector, and 3) the DC-HPM is a standard form-factor with standard interfaces to other chassis components (cooling, power-supplies, storage and I/O subsystems, etc.), the modular architecture makes it easier (relative to monolithic motherboard designs) for an adversary to apply a Drive-By Physical Attack by inserting a clone DC-SCM or clone HPM into a server during shipping, installation, or service.

   Such a clone DC-SCM could have firmware that mimics an authentic DC-SCM but is capable of eavesdropping or implementing zero-day attacks. Likewise, a clone HPM could have additional devices added for eavesdropping or DOS attacks.

2. Decoupling several control lines across a standardized connector, facilitates a persistent interposer attack threat by low-skilled adversaries. An adversary can insert some level of interposer between the DC-SCM and HPM.
   a. By interposing on SPI, the adversary may take effective control of the HPM via boot code, silently circumventing the DC-SCM PRoT
   b. SPI interposition is a well-known form of attack against TPMs
   c. By interposing on JTAG (if the HPM design supports remote CPU debug via DC-SCM), the adversary may take effective control of the HPM during runtime, gaining debug-level access to data in process via register and microarchitecture scans

Deployments that use strong remote attestation frameworks may have different minimum mitigation requirements for detecting these attacks than other common enterprise data center deployments, but all DC-MHS designs need to address the new attack threats.

Base-Specification Mitigation Requirements:

- DC-HPM designs shall prevent hot-plug of DC-SCM. The removal of a serviceable DC-SCM therefore shall force the DC-HPM to disable to pre-standby mode (no mutable code execution) or be powered-off.
- Even though the horizontal DC-SCM form factor offers a variant with external thumb screws, like the OCP NIC 3.0, designs should require internal chassis access to decouple the DC-SCM from the HPM. This method increases the replacement effort. Depending on the intrusion detection implementation may provide forensics of the intrusion and/or decoupling event.
- DC-HPM designs should comply with OCP guidelines for attestation and secure boot, including the measurement and/or verification of all HPM state and pluggable components like add-in cards.
- Designs may implement mutual attestation and verification between DC-SCM and HPM as soon as functionally possible after power-on, and before any of the host domain firmware is fetched.
- Designs may implement mutual securing (via encryption, authentication or other method) between DC-SCM and DC-HPM of control lines whose integrity impacts confidentiality of user data – including but not limited to SPI and JTAG.

- While the HPM may contain battery backed registers and CMOS RAM holding state, the DC-SCM physical model does not change the platforms choices on supporting host domain read/write or clearing via local physical switch/jumper, system BIOS domain or via BMC remote access.
- The HPM FRU (SEEPROM) used for discovery by the DC-SCM (to identify HPM type/version) shall be write protected (or writable only after mutual attestation and verification between DC-SCM and DC-HPM).

Special cases:

- On multi-node systems, the 2nd TPM (or possibly both TPMs) may be placed on the DC-HPM due to lack of buses on the DC-SCI. A future DC-SCM/SCI/HPM specification can address potential concerns regarding the added statefulness of the DC-HPM in this case.