OCP-Security Documents Backlog

Documents list in the works, and future work to be delivered from OCP-Security workgroup.

#	Document	Prio	Purpose & Content	Link	Status & ETA for release	Owner
** Done **						
1	**Secure Boot**	0	Requirements for Secure Boot (for devices)	Link	Done, Published	Bryan
2	**Attestation**	0	Requirements for attestation of peripherals. (Does not cover attestation of platforms)	Link	Done, Published	Elain
3	**Common Threats Scope + Draft checklist.**	0	Map the threat model into the relevant specs and documents, ensure no gaps in the story. Call out what's in/out of scope.	Link	Done, Published	Yigal
4	**FW Best Practices**	0	Guidelines on how to develop secure firmware.	Link	Done, Published	CSIS

5	**Threats Checklist for vendor compliance**	0	A template for vendor to fill in, as part of requirements for a badge (Appendix to Threats scope doc)	Link	Done, Published	Yigal Elaine
6	**Requirements checklist for badge of 2021**	0	Suppliers security checklist for badge for 2021	Link	Done, Published	Yigal, Elaine
7	**Secure Recovery**	1	Requirements for secure firmware updates and recovery (Note: Old docs here and here) (Updates is current out of this rel)	Link	Done, publishing TBD	Eric Spada
**** Next Set of Work Items ****						
8	**Port remediation**		Guidance and protocols for mitigating against datacenter machine port risks			Thomas Koh
9	**Ownership transfer**		A protocol for implementing ownership transfer in devices	Link		Chris Hillier
10	**Streaming boot / secure firmware update**		Hyperscalar requirements for flashful / flashless boot/update			Varun, Bryan

			Boot protocol for flashless devices (supports buses that OCP Recovery does not)			
11	**Security requirements for BMCs → Common Criteria profile**					Elaine
12	**Cryptography**		Minimum cryptographic requirements to meet OCP specifications Should add effective-as-of date		In Progress	Eric Hibbard
13	**Supply Chain Transparency**	Med	What are the gaps, device/system BOM, firmware provenance, etc.. (how to mitigate the SolarWinds case…) Maybe this ends up folding into the FW/HW best practices (SDL). Meeting every 2 weeks, reporting in to the main body as appropriate		Not Started	Eric Eilertson / Þórður Björnsson
14	**Secure Platform Overview & Platform Requirements**	2	An overview of what we're trying to accomplish and the model of OCP-Security, and which specs cover what. Topics to cover:	Link	Draft In Progress ETA: 202XQY	(Jeff)

			- Overview - Badge - Admissible architecture - Extend requirements to platform level. - PA RoT requirements, and synergy with the BMC and/or main CPU - Attestation of a platform, role of all RoTs and TPMs Old docs of high level requirements draft doc here and here			
**** Prioritized Backlog (for later work) ****						
	Certificate management for platforms and devices		Trust anchor provisioning / distribution flows CA best practices (e.g. how many levels) Formats			Alberto
	Sealing and Roots of Trust		Behaviors and interfaces required for roots of trust			

	Attestation V1.1	Med	List of requirements around tamper resistance from a RoT on devices (draft here) Focus on device-level - expand attestation spec as needed. System level attestation of complex systems? Disaggregated + non-disruptive update flows General guidance on attestation for current + journey FIPS 140-2 Level 2+ or 3? Do we require tamper evident/resistant/responding? RoT for Measurement		Not Started	Elaine / Eric Eilertson
14	**Physical Interfaces**		which physical interface to use for attestation, update, recovery, etc. Maybe as appendix for types of cards (e.g. PCIe cards). Should we just “endorse” MCTP bindings (I2C and I3C bindings are done already)? Work with the OCP Management group?			Bryan
15	**Reference information for attestation**	High	How to know “what’s good measurements”? What do we expect from vendors?			Piotr Kwidzinski (AMD)

			A manifest of expected reference values. Mechanism to deliver it. (TCG is active on that front. Engage.)			
17	**Example Threat Models**	Low	Canned threat models (implementations of #6) for specific applications: Co-lo, datacenter, tellco Maybe examples are the way to get the checklist easier to fill? Maybe do a practical approach - attempt to fill the checklist by some org. Ben willing to help.		Not Started	Prabhu
19	**Secure Facilities Requirements**	Low	- Chip provisioning flow / secure facility assumptions		Not Started	
~~**20**~~	~~**Platform Level Tamper Resistance**~~	~~Low~~	~~Probably will be different per use-case.~~ **11/29/22 - merge with port remediation**		~~Not Started~~	
~~**21**~~	~~**HW Best Practices / Physical Security**~~	~~Low~~	~~How to design secure hardware. It was suggested in the threats doc that we need one…~~ ~~Requirements for debug headers, pads, and ports~~		~~Not Started~~	~~Rob?~~

			11/29/22 - merge with port remediation			
22	**Improve interaction with other OCP projects**	Med	Not a document but spend time with other groups, cross-pollinate, get more use cases, etc.			
23	**Security in other types of devices (e.g. switches/routers/network devices) and data center equipment**	Med	We currently don't differentiate them from platforms. Should we? Verify if we missed anything.			
25	**Reference Implementations**		Open source reference implementations for attestation (attestor and attestee), sealing, etc.			
***** Administrative & housekeeping work *****						
26	**Issues Log**	TBD	Every time we discuss some topic/issue, we should document the resolution and point to recordings from the relevant session.		Not Started	Bryan
27	**Notes Log**	TBD	Transcription of meetings (can it be automated?) Maybe OCP tried it with some other group?		Not Started	Bryan / Project Secretary ?

- Future ideas (09/06/22, 11/15/22)
    - TPM+attestation - how does the host's measurements tie together with AC-RoT measurements
        - OCP-endorsed subset of TPM functionality
        - Discrete vs firmware TPM
        - Whither RTMs? (e.g. Caliptra)
    - Attestation+repairs - how to fix machines that fail attestation
    - SBOMs
        - Attestation verification story
        - Measurement of code *and* config
        - OCP can endorse something else, such as TCG's RIM/CoRIM
        - Unified Hardware Model
    - Secure fw updates
        - DMTF has PLDM, OCP can endorse that and say the payload needs to be signed
    - Checklists? (cc Elaine)
    - Work with other projects, such as storage & server
        - Make sure they're not defining their own security
        - Present to those projects, get them to throw rocks
            - Both the why and what
    - Post-quantum crypto
    - Streaming boot protocol (support for flashless devices)
        - Need a suitable connector (SPI, I3C)
        - Existing recovery spec is tied to SMBUS
        - File I/O vs packetized network interface
        - **Owners: Bryan, Varun**