OPEN POSSIBILITIES.

What's in the OCP 2021 security checklist and why?

NOVEMBER 9-10, 2021

What's in the OCP 2021 security checklist and why?

Yigal Edery
Senior Director of Products, NVIDIA

Bryan Kelly
Principal Firmware Engineer, Azure – Cloud Server Infrastructure, Microsoft

Elaine Palmer
Senior Technical Staff Member, IBM Research

Agenda

SECURITY

Intro to OCP-Security Project

Checklists for OCP Product Contributions

Security Checklist for 2021

- Motivation and checklist overview
- Drill thru into specific requirements

Future Thinking and Feedback Gathering

Call to action

OPEN POSSIBILITIES.

OCP GLOBAL SUMMIT

NOVEMBER 9-10, 2021

OCP Security Project Goals

SECURITY

NIST 800-193 compliance (Firmware resiliency)

- Protect, Detect, Recover

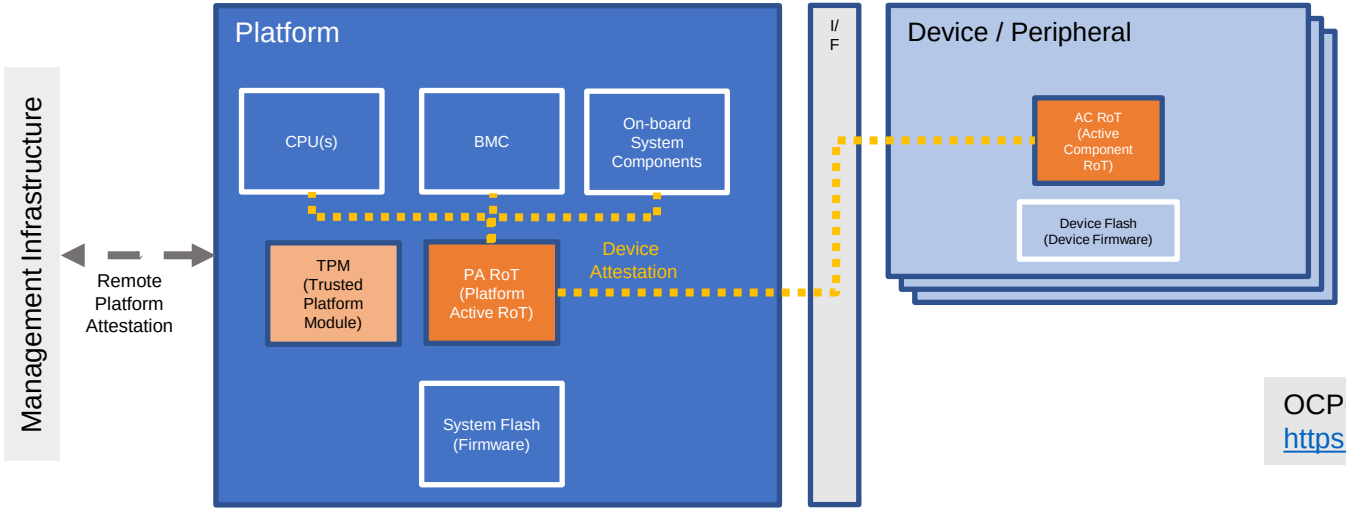
Focused on data centers and cloud providers

- Servers, Devices (Cards), Switches, Racks, Data Center Environments, etc.

Push the industry forward

- Establish a common bar for what “secure HW” means

The OCP-Security Model & Requirements Documents



Specs:

- Platform Security Overview (WIP)
- Common Threats
- Secure Boot
- Attestation
- Recovery (WIP)
- Ownership Transfers (WIP)
- Backlog

OCP-Security Wiki
https://www.opencompute.org/wiki/Security

OPEN POSSIBILITIES.

OCP GLOBAL SUMMIT
NOVEMBER 9-10, 2021

2021 Checklists for OCP Product Contributions

SECURITY

As part of product submissions, suppliers are required to fill in a “suppliers' checklist” for OCP-Accepted™ and OCP-Inspired™

- Supplier & Product information
- Open System Firmware
- Security
- Hardware Management
- BMC

	A	B	C	D	E	F
1	EFFECTIVE JULY 7th, 2021					
2	All Suppliers seeking OCP Product Recognition are required to fill out this form.					
3						
4	1) Name this file as follows:		YEAR Supplier Name PRODUCT (INSP or ACPT)			
5	2) Fill out the sheet depending on which Product Recognition you are seeking. See table below.					
6	3) Fill out Appendix B of the Base Spec on which the product is based. Add this link to this spreadsheet in the tal					
7	4) Complete the requirements for OCP Product Recognition: OCP Solution Provider Agreement, OCP Certificati					
8	5) Contact OCP with any questions					
9						
10						
11	**For OCP Inspired™**	**All Products**	**Notes**			
12	Supplier Details	X				
13	Open System Firmware					
14	Security (No Badge Level)	X	Needed for main board or any cards. For Additional Security Badges (Bronze/Silver/Gold), member can fill out the detailed Security Profile Requirements for that level.			
15	Hardware Management	X				
16	BMC					
17						
18	**For OCP Accepted™**	**All Products**	**Notes**			
19	Supplier Details	X				
20	Open System Firmware	X	Initialization Firmware			
21	Security (No Badge Level)	X	Needed for main board or any cards. For Additional Security Badges (Bronze/Silver/Gold), member can fill out the detailed Security Profile Requirements for that level.			
22	Hardware Management	X				
23	BMC	X	Source Code + Binary Blobs			

https://www.opencompute.org/contributions/agreements

OPEN POSSIBILITIES.

OCP GLOBAL SUMMIT
NOVEMBER 9-10, 2021

Motivation for the security checklist

SECURITY

Goals

- Compliance to a common set of security expectations that meets the customer demands
- Keep the bar updated as security threat landscape evolves
- Enable customers to make informed purchase choices

2021

- Information gathering
- Optional Badge

Future

- Yeah, we're working on that and welcome your feedback

OPEN POSSIBILITIES.

OCP GLOBAL SUMMIT
NOVEMBER 9-10, 2021

The 2021 Checklist

SECURITY

A set of required “disclosures” to help customers understand the security profile of OCP-Accepted™ and OCP-Inspired™ devices

Part of the OCP supplier-requirements checklist.
Badge level (Bronze, Silver, Gold) reflects “completeness, richness and openness of security offering”
Self-assessment (not a formal certification program).

Divided into sections (to be discussed in next slides):

- ❑ Cryptography
- ❑ Secure Provisioning
- ❑ Secure Boot
- ❑ Attestation
- ❑ Firmware Updates
- ❑ Recovery
- ❑ Threat Assessment
- ❑ Access to firmware source code

2021 Badge levels:

- ❑ Bronze: secure boot + attestation support ("must" requirements)
- ❑ Silver: Bronze level + "should" requirements + secure update + secure recovery + threat assessment document + semi-open (e.g., source code available to customers under NDA)
- ❑ Gold Silver + full feature set (including support for "may" requirements), publicly open security code, and FIPS certification.

OPEN POSSIBILITIES.

Do I have to do this?

Yes!

The supplier's checklist 2021 process is required for any new product being submitted to OCP-Accepted™ or OCP-Inspired™ programs.

For the security part – fill out the questionnaire, with the answers you're willing to share.

- If you comply with one of the badge levels, ask for it (optional).
- If not, you can still get OCP-Accepted/Inspired badges. Just no "Security Badge".

Crypto & Secure Provisioning

Self-Assessment Form			
1. Badge Level			
a. What is being certified? ***System*** *= a motherboard, or the main board of a system.* ***Card*** *= a peripheral device, such as NIC, HBA, Disk, etc.*	**System**		
b. What level of security badge are you applying for?	**No Badge**		
2. Cryptograpy and Randomness	**Self-Assessment**	**Badge Level**	**Additional Explanation (if needed)**
a. Does all the cryptography used in product follow the recommendations in relevant NIST Special Publications? (e.g. NIST CNSA suite)	**[Yes/No]**	Bronze	
b. Are cryptographic implementations validated under the NIST Cryptographic Algorithm Validation Program (CAVP)??	**[Yes/No]**	Silver	
c. Are cryptographic modules validated at overall level 2 or higher under FIPS 140-2 or FIPS 140-3?	**[Yes/No]**	Gold	
3. Secure Provisioning	**Self-Assessment**	**Badge Level**	**Additional Explanation (if needed)**
a. Are initial provisioning operations carried out in a trusted facility?	**[Yes/No]**	Bronze	
b. Does the product have a unique and immutable device ID key, an attestation key, and a key identifying the authority over updates?	**[Yes/No]**	Bronze	
c. Does the product support authenticated ownership transfer?	**[Yes/No]**	Gold	

Secure Boot

SECURITY

*Secure Boot is the mechanism that **verifies the integrity** of every code being loaded, **before it's allowed to execute**.*

*This includes, for example, checking code for **proper signature by an approved signer.***

Secure Boot is considered successful if the integrity check and signature verification passes, and fails if it does not.

Secure Boot - Why it's important

SECURITY

Prevents unauthorized code from booting the device.

Defends against malicious code booting the device and attacking other mechanisms; measurement, ransomware, cryptography

Measured boot is very valuable, “better to know what was booted than assume device booted security”.

Measured boot and secure boot are complementary, and solve different challenges

Secure Boot Checklist

4. Secure Boot support	Self-Assessment	Badge Level	Additional Explanation (if needed)
a. Does secure boot start from an immutable source?	[Yes/No]	Bronze	
b. On each reset of a device, are secure boot public keys used to authenticate the first stage mutable code or manifest?	[Yes/No]	Bronze	
c. Is an anti-rollback mechanism provided?	[Yes/No]	Bronze	
d. Is error detection of critical security parameters implemented?	[Yes/No]	Bronze	
e. Is secure boot failure notification provided?	[Yes/No]	Bronze	
f. Is a secure boot key revocation mechanism provided?	[Yes/No]	Silver	
g. Does the device support multiple secure boot root keys or root key digests?	[Yes/No]	Silver	

Attestation

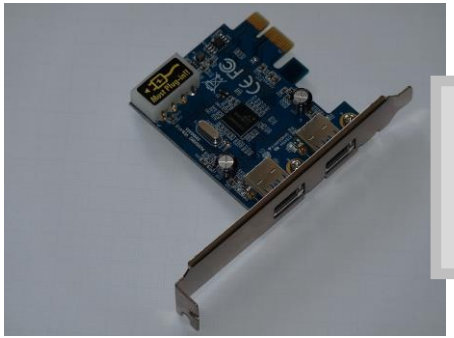
SECURITY

*An **attester** is a collection of hardware, software, firmware, and a root of trust (RoT) with the ability to provide **reliable evidence of trustworthiness** (i.e. measurements) to the **verifier.***

Source: “Attestation of System Components v1.0”, OCP Security Workgroup, Elaine Palmer, editor, 2020

Attestation Evidence

Device reports its measurements to platform



PCIe card with two USB_3.0 ports, 2013,
photo courtesy of Dmitry G under public domain

This is what I am.
This is who made me.
This is the firmware I'm running.
Can I come in?

Photo licensed under CC1.0

Attestation

5. Attestation support	Self-Assessment	Badge Level	Additional Explanation (if needed)
5.1 Measurement and Attestation *(only needed if certifying a component device)*			
a. Does the device support the OCP Attestation protocol, as an attester device?	[Yes/No]	Bronze	
b. Is the first measurement taken by an immutable root of trust?	[Yes/No]	Bronze	
c. Must the device be reset in order to clear the measurements?	[Yes/No]	Bronze	
d. Is the measurement storage integrity protected (e.g., in a TPM)?	[Yes/No]	Bronze	
e. Are dynamic changes in configuration or firmware measured?	[Yes/No]	Silver	
f. Does the vendor provide a list of what is measured (code and configuration)?	[Yes/No]	Silver	
g. Does the vendor provide expected measurement values?	[Yes/No]	Gold	
h. Does the device offer a structured log of measurements?	[Yes/No]	Gold	
5.2 Verification Support *(only needed if certifying a platform)*			
a. Does the platform support the OCP Attestation protocol, as a verifier?	[Yes/No]	Bronze	
b. Does the platform support comparing the inventory to a manifest containing expected devices and their configurations?	[Yes/No]	Gold	

FW Updates & Recovery

6. Secure Firmware Update support	Self-Assessment	Badge Level	Additional Explanation (if needed)
a. Does the product support secure firmware updates (i.e. validate firmware signatures upon update)	[Yes/No]	Silver	
b. If yes, please provide link to relevant feature documentation:	[Link]	Silver	
c. Are dynamic updates authenticated and / or measured?	[Yes/No]	Silver	

7. Recovery support	Self-Assessment	Badge Level	Additional Explanation (if needed)
a. Does the product support automatic recovery in case of firmware corruption?	[Yes/No]	Silver	
b. If yes, please provide link to relevant feature documentation:	[Link]	Silver	

Threats Assessment & Openness

8. Threats Assessment	Self-Assessment	Badge Level	Additional Explanation (if needed)
a. Are there any known **unfixed** CVE's in the product or one of its components, as-of the date of release? *(If yes, please provide explanation on how the security risk is mitigated)*	**[Yes/No]**	Bronze	
b. What is the mechanism available for getting future firmware patches? (e.g. provide a link to a documented security response process, or free form explanation)	**[Freeform text, or Link to documentation]**	Bronze	
c. Please provide a link to a threat model document for the product. *(For an example template for a threat model document, please refer to appendix A of the common security threats document)*	**[Link]**	Silver	
d. Was the product developed following any documented SDL (Security Development Lifecycle) ?	**[Yes/No]**	Silver	
e. If Yes, and the SDL is available publicly, please provide a link to it.	**[Link]**	Silver	

9. Access to firmware source code	Self-Assessment	Badge Level	Addtional Explanation (if needed)
a. Is the source code for security-relevant features available for review (e.g. code available under NDA, or via a trusted 3rd party audit report)?	**[Yes/No]**	Silver	
b. Is the source code and build environment for all security features available in a public repository?	**[Yes/No]**	Gold	
c. If Yes, please provide the link to the source code:	**[Link]**	Gold	

Recap – Yes, you have to do this!

The supplier's checklist 2021 process is required for any new product being submitted to OCP-Accepted™ or OCP-Inspired™ programs.

For the security part – fill out the questionnaire, with the answers you're willing to share.

- If you comply with one of the badge levels, ask for it (optional).
- If not, you can still get OCP-Accepted/Inspired badges. Just no "Security Badge".

What’s beyond 2021?

Feedback on current security checklist

SECURITY

1. ”We don’t need no stinkin’ badges!” Everyone wants gold.
2. We are *not* going to reveal our vulnerabilities!
3. Nothing in our 2-3 year pipeline can meet these requirements. Hard requirements are needed to change or commit development plans.
4. While we *can* and will meet some of these, we can’t meet the strength of crypto now.
5. What is the scoring algorithm across categories?
6. No one checklist fits all {customers, devices, environments, threats}
7. The checklist doesn’t take international requirements into account, (e.g., algorithm suite, certifications).
8. Is the checklist a compliance document, or is it simply informative to customers?
9. We should distinguish security r*equirements* from security *features.*

OPEN POSSIBILITIES.

OCP GLOBAL SUMMIT

NOVEMBER 9-10, 2021

Working draft of next Security Checklist

Self-Assessment Form			
What is being certified? *System = a motherboard, or the main board of a system.* *Card = a peripheral device, such as NIC, HBA, Disk*	System		
		Suggested or required?	
1. Cryptograpy	**Current Availability**	**Required Availability**	**Additional Explanation (if needed)**
a. Does cryptography in the product follow national or international standard algorithms? If so, which ones? If not, please explain.	[Yes,No,N/A]	2022	
b. Is cryptography in the product quantum safe?	[Yes,No,N/A]	2024+	
2. Certifications	**Current Availability**	**Required Availability**	**Additional Explanation (if needed)**
a. Are cryptographic implementations validated under the NIST Cryptographic Algorithm Validation Program (CAVP) or ISO/IEC 18033(?)?	[Yes,No,N/A]	2023	
b. Are cryptographic modules validated at overall level 2 or higher under FIPS 140-3 or ISO/IEC 19790?	[Yes,No,N/A]	2024+	
3. Secure Provisioning	**Current Availability**	**Required Availability**	**Additional Explanation (if needed)**
a. Are initial provisioning operations carried out in a trusted facility?	[Yes,No,N/A]	2022	
b. Does the product have a unique and immutable device ID key?	[Yes,No,N/A]	2022	attestation and update keys separated out
c. Does the product have an attestation key, and a key identifying the authority over updates?	[Yes,No,N/A]	2023	
d. Does the product support authenticated ownership transfer?	[Yes,No,N/A]	2024+	

Revised sections

1. Cryptography
2. Certifications
3. Secure Provisioning

(not shown)

4. Secure Boot support
5. Attestation support
6. Secure Firmware Update support
7. Recovery support
8. Threat Assessment
9. Access to firmware source code

OPEN POSSIBILITIES.

OCP GLOBAL SUMMIT
NOVEMBER 9-10, 2021

Call to Action

How to get involved in the OCP Security Project Community

- Join our mailing list
- Join our project calls every Tuesday at 11:30 am ET (details are on the project wiki)
- Share your use cases, pain points, and successes
- Edit or contribute a relevant white paper

If you're in another OCP project, talk to us about your security needs!

Where to find additional information on the Security Project

- Project Wiki with latest documents : https://www.opencompute.org/wiki/Security
- Project mailing list: https://ocp-all.groups.io/g/OCP-Security

OPEN POSSIBILITIES.

OCP GLOBAL SUMMIT
NOVEMBER 9-10, 2021

Open Discussion