Workgroup: IETF
Internet-Draft:
draft-moriarty-attestationsets-04
Published: 10 December 2021
Intended Status: Standards Track
Expires: 13 June 2022
K. Moriarty
Center for Internet
Security (CIS)
A. Fontes
Dell Technologies

Scalable Remote Attestation for Systems, Containers, and Applications

Abstract

This document establishes an architectural pattern whereby a remote attestation could be issued for a complete set of benchmarks or controls that are defined and grouped by an external entity, preventing the need to send over individual attestations for each item within a benchmark or control framework. This document establishes a pattern to list sets of benchmarks and controls within CWT and JWT formats for use as an Entity Attestation Token (EAT).

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 13 June 2022.

Table of Contents

1. Introduction

Posture assessment has long been desired, but has been difficult to achieve due to complexities of customization requirements at each organization. By using policy and measurement sets that may be offered at various assurance levels, automating posture assessment through attestation becomes achievable for organizations of all sizes. The measurement and policy groupings may be provided by the vendor or by a neutral third party to enable ease of use and consistent implementations. This provides simpler options to enable posture assessment at selected levels by organizations without the need to have in-house expertise. The measurement and policy sets may also be customized, but not necessary to achieve posture assessment to predefined options. This document describes a method to use existing attestation formats and protocols while allowing for profiles of policies, benchmarks, and measurements at defined assurance levels that scale to provide transparency to posture assessment results with remote attestation.

By way of example, the Center for Internet Security (CIS) hosts recommended configuration settings to secure operating systems, applications, and devices in CIS Benchmarks developed with industry experts. Attestations aligned to the CIS Benchmarks or other configuration guide such as a DISA STIG could be used to assert the configuration meets expectations. This has already been done for multiple platforms to demonstrate assurance for firmware according to NIST SP 800-193, Firmware Resiliency Guidelines. In order to scale remote attestation, a single attestation for a set of Benchmarks or policies being met may be sent to the remote atteststaion management system.

On traditional servers, assurance to NIST SP 800-193 is provable through attestation from a root of trust (RoT), using the Trusted Computing Group (TCG) Trusted Platform Module (TPM) chip and attestation formats. At boot, policy and measurement expectations are verified against a set of "golden policies" from collected and attested evidence. Device identity and measurements can also be attestated at runtime. The attestations on evidence (e.g. hash of boot element) and verification of attestations are typically contained within a system and are limited to the control plane for

management. The policy and measurement sets for comparison are protected to assure the result in the attestation verification process for boot element. Event logs and PCR values may be exposed to provide transparency into the verified attestations. Remote attestation on systems is intended to provide an assessment of posture for all managed systems and across various layers in each of these systems in an environment.

There is a balance of exposure and evidence needed to assess posture when providing assurance of controls and system state. Currently, logs and TPM PCR values may be passed to provide assurance of verification of attestation evidence meeting set requirements. Providing the assurance can be accomplished with a remote attestation format such as the Entity Attestation Token (EAT) [I-D.ietf-rats-eat] and a RESTful interface such as ROLIE or RedFish. Policy definition blocks may be scoped to control measurement sets, where the EAT asserts compliance to the policy or measurement block specified and may include claims with the log and PCR value evidence. Measurement and Policy sets may be published and maintained by separate entities (e.g. CIS Benchmarks, DISA STIGs). The policy and measurement sets should be maintained separately even if associated with the same benchmark or control set. This avoids the need to transition the verifying entity to a remote system for individual policy and measurements which are performed locally for more immediate remediation as well as other functions.

Examples of measurement and policy sets include, but are not limited to:

- *Hardware attribute certificates
- *Hardware Attribute Certificate Comparison Results
- *Reference Integrity Measurements for firmware
- *Operating system benchmarks at Specified Assurance Levels
- *Application hardening Benchmarks at Specified Assurance Levels
- *Container security benchmarks at Specified Assurance Levels

Scale, ease of use, full automation, and consistency for customer consumption of a remote attestation function or service are essential toward the goal of consistently securing systems against known threats and vulnerabilities. Mitigations may be baked into policy. Measurement verification sets and the attestation that the sets meet expected policies and measurements are conveyed in an Entity Attestation Token made available to a RESTful interface in aggregate for the systems managed.

2. Policy and Measurement Set Definitions

This document defines EAT claims in the JWT [RFC7519] and CWT [RFC8392] registries to provide attestation to a set of verified claims within a defined grouping. The trustworthiness will be conveyed on original verified evidence as well as the attestation on the grouping.

{

Claim	Long Name	Description
MPS	Measurement or Policy Set	Name for the MPS
LEM	Log Evidence of MPS	Log File or URI
PCR	TPM PCR Values	
FMA	Format of MPS Attestations	Format of included attestat
HSH	Hash Value/Message Digest	Hash va,ue of configuration

}

3. Supportability and Re-Attestation

The remote attestation framework shall include provisions within the system and attestation authority to allow for Product modification.

Over its lifecycle, the Product may experience modification due to: maintenance, failures, upgrades, expansion, moves, etc..

The customer can chose to:

*Run remote attestation after product modification, or

*Not take action and remain un-protected

In the case of Re-Attestation:

*framework needs to invalidate previous TPM PCR values and tokens,

*framework needs to collect new measurements,

*framework needs to maintain history or allow for history to be logged to enable change traceability attestation, and

*framework needs to notify that the previous attestation has been invalidated

4. Configuration Sets

In some cases, it may be difficult to attest to configuration settings for the initial or subsequent attestation and verification processes. The use of an expected hash value for configuration settings can be used to compare the attested configuration set. In this case, the creator of the attestation verification measurements would define a set of values for which a message digest would be created and then signed by the attestor. The expected measurements would include the expected hash value for comparison. The configuration set could be the full attestation set to a Benchmark or a defined subset.

5. Remediation

If policy and configration settings or measurements attestated do not meet expected values, remediation is desireable. Automated remediation performed with alignment to zero trust architecture principles would require that the remeidation be performed prior to

any relying component executing. The relying component would verifiy before continuing in a zero trust architecture.

Ideally, remediation would occur on system as part of the process to attest to a set of attestations, similar to how attestation is performed for firmware in the boot process. If automated remediation is not possible, an alert should be generated to allow for notification of the variance from expected values.

6. Security Considerations

This document establishes a pattern to list sets of benchmarks and controls within CWT and JWT formats. The contents of the benchmarks and controls are out of scope for this document. This establishes an architectural pattern whereby a remote attestation could be issued for a complete set of benchmarks or controls as defined and grouped by external entities, preventing the need to send over individual attestations for each item within a benchmark or control framework. This document does not add security consideration over what has been described in the EAT, JWT, or CWT specifications.

7. IANA Considerations

This memo includes no request to IANA, yet. This will list the initial registration sets to the JWT and CWT registries if adopted.

8. Contributors

Thank you to reviewers and contributors who helped to improve this document. Thank you to Nick Grobelney, Dell Technologies, for your review and contribution to separate out the policy and measurement sets. Thank you, Samant Kakarla and Huijun Xie from Dell Technologies, for your detailed review and corrections on boot process details. Section 3 has been contributed by Rudy Bauer from Dell as well and an author will be added on the next reveision.

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8392] Jones, M., Wahlstroem, E., Erdtman, S., and H. Tschofenig, "CBOR Web Token (CWT)", RFC 8392, DOI 10.17487/RFC8392, May 2018, <https://www.rfc-editor.org/info/rfc8392>.

[RFC7519] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Token (JWT)", RFC 7519, DOI 10.17487/RFC7519, May 2015, <https://www.rfc-editor.org/info/rfc7519>.

9.2. Informative References

[I-D.ietf-rats-eat] Lundblade, L., Mandyam, G., and J. O'Donoghue, "The Entity Attestation Token (EAT)", Work in Progress,

Internet-Draft, draft-ietf-rats-eat-11, 24 October 2021, <https://www.ietf.org/archive/id/draft-ietf-rats-eat-11.txt>.

Appendix A. Change Log

Note to RFC Editor: if this document does not obsolete an existing RFC, please remove this appendix before publication as an RFC.

Appendix B. Open Issues

Note to RFC Editor: please remove this appendix before publication as an RFC.

Authors' Addresses

Kathleen M. Moriarty
Center for Internet Security (CIS)
31 Tech Valley Drive
East Greenbush, NY,
United States of America

Email: Kathleen.Moriarty.ietf@gmail.com

Antonio Fontes
Dell Technologies
176 South Street
Hopkinton, MA,
United States of America

Email: Antonio.Fontes@dell.com