IETF K. Moriarty
Internet-Draft Center for Internet Security (CIS)
Intended status: Standards Track March 8, 2021
Expires: September 9, 2021

Scalable Remote Attestation for Systems, Containers, and Applications
draft-moriarty-attestationsets-00

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

Copyright Notice

Table of Contents

1. Introduction

Attestation from a root of trust (hardware or software), may be accomplished via a number of formats. Some use cases are well defined, including the Root of Trust (RoT) (e.g. Trusted Platfrom Module, OpenTitan) and attestation format as well as the specific policy and measurement expectations at boot. Device identity and measurements can 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. This document describes a method to use existing attestation formats and protocols while allowing for profiles of policies and measurements at defined assurance levels that scale to provide transparency to posture assessment results with remote attestation.

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. 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.

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. 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.

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	Format
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 attestations	

}

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. 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.

5. 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.

6. 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.

7. References

7.1. 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>.

[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>.

[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>.

7.2. Informative References

[I-D.ietf-rats-eat]
Mandyam, G., Lundblade, L., Ballesteros, M., and J. O'Donoghue, "The Entity Attestation Token (EAT)", draft-ietf-rats-eat-06 (work in progress), December 2020.

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.

Author's Address

Kathleen M. Moriarty
Center for Internet Security (CIS)
31 Tech Valley Drive
East Greenbush, NY
US

EMail: Kathleen.Moriarty.ietf@gmail.com