Remote Posture Assessment for Systems, Containers, and Applications at Scale

Was: Remote Attestation Sets

Kathleen M Moriarty
Co-Authors: A.J. Stein, Monty Wiseman

July 2024

Scaling Measured Trust: Attestation Sets

Attestation Sets to specified policy & measurements per component (e.g. NIST, TCG, CIS Benchmarks, etc.), remediated and verified per set on system.

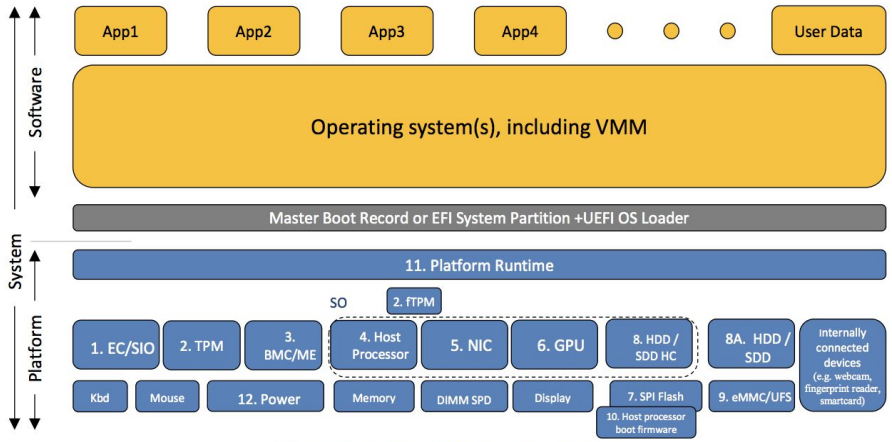
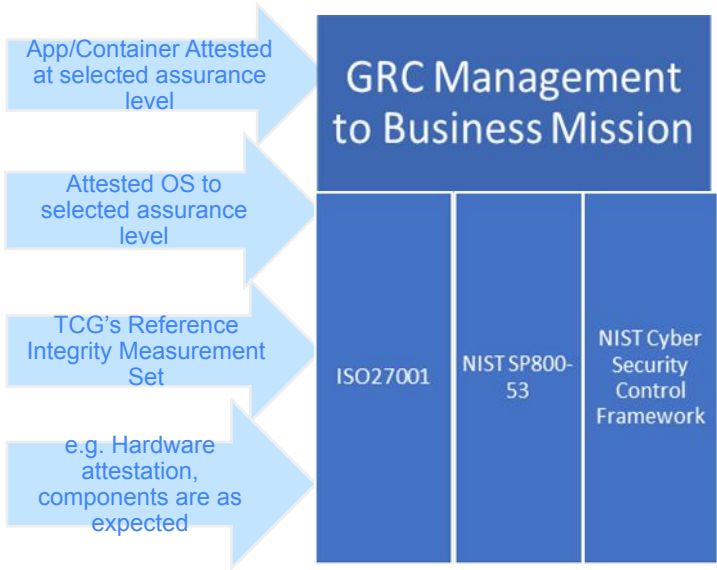


Figure 1: High-Level System Architecture

Image: NIST SP 800-193

Controls and Benchmarks verified locally using known frameworks, controls, or benchmarks (e.g. NIST, CIS Benchmarks, TCG, DISA STIGS, etc.)

Remote Attestation at Scale: **Attestations Aligned** to control frameworks



Attestation on set of locally verified attestations

Mapping to Control Frameworks and Risk Alignment

Attestation Set Draft Establishes a Registry

- Work with WG to determine the appropriate set of claims to enable interoperability for reporting to GRC system or a CSPM
    - (Identifier, Attestation Set Name, Integrity Protected Log of attestation evidence verification for set, timestamp, other useful claims) Signed by Trusted Platform Module or software RoT
    - Establish a registry for appraisal policy definitions to enable reporting in remote attestations
        - Appraisal policy levels may be needed for assurance to hardening guides as decisions may vary for risk appetite.
        - The appraisal policy definition may contain the configuration **or** measurement values from a standard such as NIST SP 800-193
        - The appraisal policy or measurement set may be aligned to all or part of a standard
        - The appraisal policy or measurement set may be complemented by other assessment types, but still having the goal of reducing the distributed assessment criteria and programming - the vendor would be responsible for built-in security and ongoing assurance automation
- Format: Entity Attestation Token (JWT or CWT)
- Protocol: RESTful interface (e.g. RedFish, ROLIE, etc.) or other suitable protocol

Changes from prior version

- Draft name and file name changes from “Attestation Sets” to reflect Posture Assessment focus of the work.
- Language updates to align with RATS terminology
- Multiple Authors added, noted on cover slide
- Review and integration of comments from Henk

Thank You

Comments welcome and appreciated!
https://datatracker.ietf.org/doc/draft-moriarty-rats-posture-assessment/