Automation at Scale
Remote Attestation Sets

Kathleen M Moriarty
Center for Internet Security

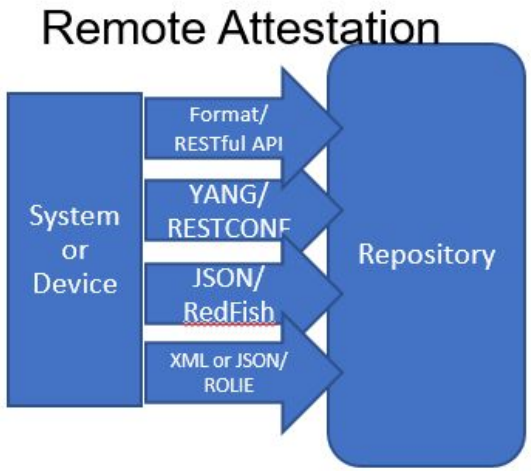
November 2023 (Updated deck from March 2021)

Scaling Assessment

- Current posture assessment requires add-on tools to assess systems against expected policies and measurements. Current methods require expertise at each organization.
    - This requires distributed expertise to customize the current standards-based methods to access and collect assessments (e.g OVAL/XCCDF, SWIMA/NEA)
    - APIs are also used to gather information on software inventory or configuration data
- Existing Work:
    - Trusted boot processes occur using attestation locally against a set of policies and measurements established by the vendor, aligned to both NIST SP 800-193 and TCG's Reference Integrity Measurements
    - Early work proved capability for full stack in NIST NCCOE with RSA, VMware, Intel, and Cisco 10+ years ago
- Proposal
    - What if the local attestations were grouped as a set with log evidence to provide remote reporting?
    - Consistent remote attestations to convey compliance to policy and measurement sets necessary for interoperability
    - Local attestation process may be different between systems and OSes, some may be chained as dependant and others may assume zero trust, thus not necessarily important to standardize by IETF

Attestation Local and Remote

- Attestation is essentially signed evidence from a root of trust (RoT)
- Attestations are verified to ensure the signer is trusted
- Evidence in attestations are matched against expected policies or measurements
- If expectations are not met, remediation occurs
- Zero Trust requires verification, identification, encryption, and logs
- Attestation provides verification to the subsequent processes, applications, modules, etc. before execution is permitted
- Attestation aligned to policy sets and are typically performed on system
- Remote attestation is shared through a RESTful interface



Local attestation data generated from boot and runtime measurements and configuration for all managed systems, how to scale remote?

IETF112 Slides - updated for IETF118

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.

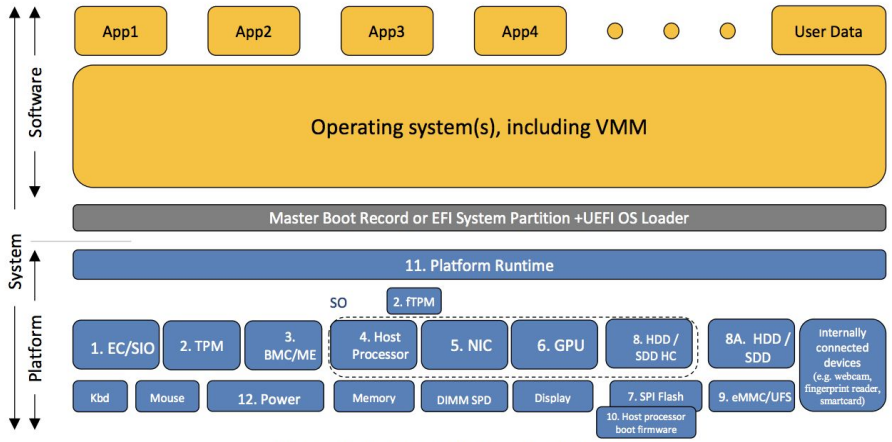
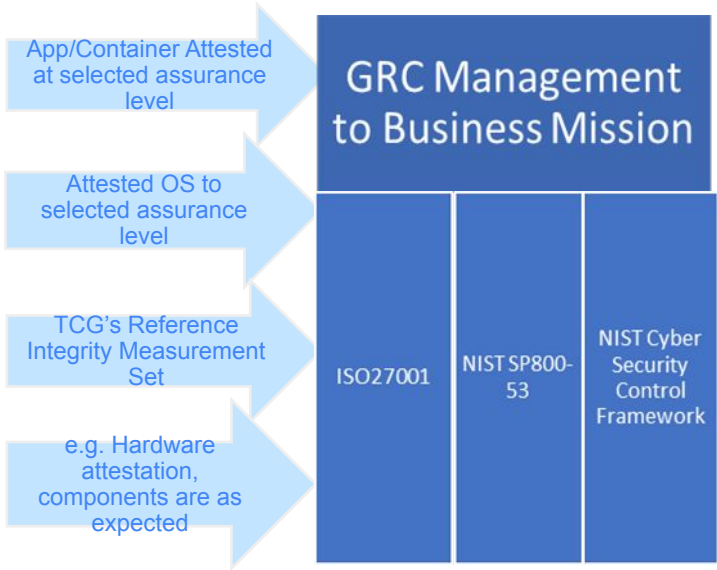


Figure 1: High-Level System Architecture

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 or posture assessment management systems
  - (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 the set names to enable remote attestations in sets
    - Levels may be needed in the case of Benchmark or assurance to hardening guides as decisions may vary for applications.
    - The set may contain the policy **or** measurement values from a standard such as NIST SP 800-193
    - The set may be aligned to all or part of a standard
    - The 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.)

Thank You

Comments welcome and appreciated!

URL: https://www.ietf.org/archive/id/draft-moriarty-attestationsets-03.txt
Status: https://datatracker.ietf.org/doc/draft-moriarty-attestationsets/
Htmlized: https://datatracker.ietf.org/doc/html/draft-moriarty-attestationsets
Htmlized: https://tools.ietf.org/html/draft-moriarty-attestationsets-03