RATS Working Group
Internet-Draft
Intended status: Informational
Expires: September 29, 2019

M. Richardson
Sandelman Software Works
March 28, 2019

Use cases for Remote Attestation common encodings
draft-richardson-rats-usecases-01

Abstract

This document details mechanisms created for performing Remote Attestation that have been used in a number of industries. The document intially focuses on existing industry verticals, mapping terminology used in those specifications to the more abstract terminology used by RATS.

The document (aspires) goes on to go on to describe possible future use cases that would be enabled by common formats.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

The recently chartered IETF RATS WG intends to create a system of attestations that can be shared across a multitude of different users.

This document exists as place to collect use cases in support of the IETF RATS charter point 1. This document is not expected to be published as an RFC, but remain open as a working document. It could become an appendix to provide motivation for a protocol standards document.

2. Terminology

Critical to dealing with and constrasting different technologies is to collect terms with are compatible, to distinguish those terms which are similar but used in different ways.

This section will grow to include forward and external references to terms which have been seen. When terms need to be disambiguated they will be prefixed with their source, such as "TCG(claim)" or "FIDO(relying party)"

3. Requirements Language

This document is not a standards track document and does not make any normative protocol requirements using terminology described in [RFC2119].

4. Overview of Sources of Use Cases

The following specifications have been convered in this document:

- The Trusted Computing Group "Network Attestation System" (private document)

- Android Keystore

- Fast Identity Online (FIDO) Alliance attestation,

This document will be expanded to include summaries from:

- Trusted Computing Group (TCG) Trusted Platform Module (TPM)/Trusted Software Stack (TSS)

- ARM "Platform Security Architecture" [I-D.tschofenig-rats-psa-token]

5. Use case summaries

5.1. Trusted Computing Group (TCG)

The TCG is trying to solve the problem of knowing if a networking device should be part a network. If it belongs to the operator, and if it running approriate software.

This proposal is a work-in-progress, and is available to TCG members only. The goal is to be multi-vendor, scalable and extensible. The proposal intentionally limits itself to:

- "non-privacy-preserving applications (i.e., networking, Industrial IoT)",

- that the firmware is provided by the device manufacturer

- that there is a manufacturer installed hardware root of trust (such as a TPM and boot room)

Service providers and enterprises deploy hundreds of routers, many of them in remote locations where they're difficult to access or secure. The point of remote attestation is to:

- identify a remote box in a way that's hard to spoof

- report the inventory of software was launched on the box in a way that can not be spoofed

The use case described is to be able to monitor the authenticity of software versions and configurations running on each device. This allows owners and auditors to detect deviation from approved software and firmware versions and configurations, potentially identifying infected devices.

Attestation may be performed by network management systems. Networking Equipment is often highly interconnected, so it's also possible that attestation could be performed by neighboring devices.

Specifically listed to be out of scope includes: Linux processes, assemblies of hardware/software created by end-customers, and equipment that is sleepy (check term).

The TCG Attestion leverages the TPM to make a series of measurements during the boot process, and to have the TPM sign those measurements. The resulting "PCG" hashes are then available to an external verifier.

The TCG uses the following terminology:

- Device Manufacuter

- Attester ("device under attestation")

- Verifier (Network Management Station)

- Reference Integrity Measurements (RIM), which are signed my device manufacturer and integrated into firmware.

- Quotes: measured values (having been signed), and RIMs

- Reference Integrity Values (RIV)

- devices have a Initial Attestion Key (IAK), which is provisioned at the same time as the IDevID.

- PCR - Platform Configuration Registry (deals with hash chains)

The TCG document builds upon a number of IETF technologies: SNMP (Attestion MIB), YANG, XML, JSON, CBOR, NETCONF, RESTCONF, CoAP, TLS and SSH. The TCG document leverages the 802.1AR IDevID and LDevID processes.

5.2. Android Keystore system

[keystore] describes a system used in smart phones that run the Android operation system. The system is primarily a software container to contain and control access to cryptographic keys, and therefore provides many of the same functions that a hardware Trusted Platform Module might provide.

On hardware which is supported, the Android Keystore will make use of whatever trusted hardware is available, including use of Trusted Execution Environment (TEE) or Secure Element (SE)). The Keystore therefore abstracts the hardware, and guarantees to applications that the same APIs can be used on both more and less capable devices.

A great deal of focus from the Android Keystore seems to be on providing fine-grained authorization of what keys can be used by which applications.

XXX - clearly there must be additional (intended?) use cases that provide some kind of attestion.

5.3. Fast IDentity Online (FIDO) Alliance

The FIDO Alliance [fido] has a number of specifications aimed primarily at eliminating the need for passwords for authentication to online services. The goal is to leverage asymmetric cryptographic operations in common browser and smart-phone platforms so that users can easily authentication.

FIDO specifications extend to various hardware second factor authentication devices.

Terminology includes:

- "relying party" validates a claim

- "relying party application" makes FIDO Authn calls

- "browser" provides Web Authentication JS API

- "platform" is the base system

- "internal authenticator" is some credential built-in to the device

- "external authenticator" may be connected by USB, bluetooth, wifi, and may be an stand-alone device, USB connected key, phone or watch.

FIDO2 had a Key Attestion Format [fidoattestation], and a Signature Format [fidosignature], but these have been combined into the W3C document [fido_w3c] specification.

The FIDO use case involves a relying party that wants to have the HW/SW implementation does a biometric check on the human to be strongly attested.

FIDO does provides a transport in the form of the WebAuthn and FIDO CTAP protocols.

6. Privacy Considerations.

TBD

7. Security Considerations

TBD.

8. IANA Considerations

TBD.

9. Acknowledgements

10. References

10.1. 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>.

10.2. Informative References

[fido] FIDO Alliance, ., "FIDO Specification Overview", n.d., <https://fidoalliance.org/specifications/>.

[fido_w3c] W3C, ., "Web Authentication: An API for accessing Public Key Credentials Level 1", n.d., <https://www.w3.org/TR/webauthn-1/>.

[fidoattestation] FIDO Alliance, ., "FIDO 2.0: Key Attestation", n.d., <https://fidoalliance.org/specs/fido-v2.0-ps-20150904/fido-key-attestation-v2.0-ps-20150904.html>.

[fidosignature]
FIDO Alliance, ., "FIDO 2.0: Signature Format", n.d., <https://fidoalliance.org/specs/fido-v2.0-ps-20150904/fido-signature-format-v2.0-ps-20150904.html>.

[I-D.tschofenig-rats-psa-token]
Tschofenig, H., Frost, S., Brossard, M., and A. Shaw, "Arm's Platform Security Architecture (PSA) Attestation Token", draft-tschofenig-rats-psa-token-00 (work in progress), March 2019.

[keystore]
Google, ., "Android Keystore System", n.d., <https://developer.android.com/training/articles/keystore>.

Appendix A. Changes

- added comments from Guy, Jessica, Henk and Ned on TCG description.

Author's Address

Michael Richardson
Sandelman Software Works

Email: mcr+ietf@sandelman.ca