RATS Working Group
Internet-Draft
Intended status: Informational
Expires: December 21, 2019

M. Richardson
Sandelman Software Works

June 19, 2019

Use cases for Remote Attestation common encodings
draft-richardson-rats-usecases-02

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 to describe possible future use cases that would be enabled by common formats.

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 December 21, 2019.

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 for the common RATS technologies 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.

This document will probably not deal with use cases from an end-user point of view, but rather on the technology verticals that wish to use RATS concepts (such as EAT) in their deployments.

End-user use cases that would either directly leverage RATS technology, or would serve to inform technology choices are welcome, however.

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)"

Platform attestions generally come in two categories. This document will attempt to indicate for a particular attestion technology falls into this.

2.1. Static attestions

A static attestion says something about the platform on which the code is running.

2.2. Session attestions

A session attestion says something about how the shared session key was created.

2.3. Statements

The term "statement" is used as the generic term for the semantic content which is being attested to.

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:

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

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

And any additional sources suggested.

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 of a network, if it belongs to the operator, and if it is 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:

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

- o that the firmware is provided by the device manufacturer

- o 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:

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

- o 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:

- o Device Manufacuter
- o Attester ("device under attestation")
- o Verifier (Network Management Station)
- o "Explicit Attestation" is the TCG term for a static (platform) statement.
- o "Implicit Attestation" is the TCG term for a session statement.
- o Reference Integrity Measurements (RIM), which are signed my device manufacturer and integrated into firmware.
- o Quotes: measured values (having been signed), and RIMs
- o Reference Integrity Values (RIV)
- o devices have a Initial Attestion Key (IAK), which is provisioned at the same time as the IDevID.
- o 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.

Android 9 on Pixel 2 and 3 can provided protected confirmation messages. This uses hardware access from the TPM/TEE to display a message directly to the user, and receives confirmation directly from the user. A hash of the contents of the message can provided in an attestation that the device provides.

In addition, the Android Keystore provides attestion information about itself for use by FIDO.

QUOTE: Finally, the Verified Boot state is included in key attestation certificates (provided by Keymaster/Strongbox) in the deviceLocked and verifiedBootState fields, which can be verified by apps as well as passed onto backend services to remotely verify boot integrity [**21]

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

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

- o "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.

A FIDO use case involves a relying party that having a attestion on the biometric system that identifies a human. It is the state of the biometric system that is being attested to, not the identity of the human.

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

According to [fidotechnote] FIDO uses attestion to make claims about the kind of device which is be used to enroll. Keypairs are generated on a per-device _model_ basis, with a certificate having a trust chain that leads back to a well-known root certificate. It is expected that as many as 100,000 devices in a production run would have the same public and private key pair. One assumes that this is stored in a tamper-proof TPM so it is relatively difficult to get this key out. The use of this key attests to the the device type, and the kind of protections for keys that the relying party may assume, not to the identity of the end user.

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

[android_security] Kralevich, R., "The Android Platform Security Model", n.d., <https://arxiv.org/pdf/1904.05572.pdf>.

[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>.

[fidotechnote] FIDO Alliance, ., "FIDO TechNotes: The Truth about Attestation", n.d., <https://fidoalliance.org/fido-technotes-the-truth-about-attestation/>.

[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-01 (work in progress), April 2019.

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

Appendix A. Changes

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

Author's Address

Michael Richardson
Sandelman Software Works

Email: mcr+ietf@sandelman.ca