Workgroup: RATS Working Group
Internet-Draft:
draft-ietf-rats-architecture-00
Published: 17 December 2019
Intended Status: Informational
Expires: 19 June 2020
Authors: H. Birkholz
Fraunhofer SIT
D. Thaler
Microsoft
M. Richardson
Sandelman Software Works
N. Smith
Intel

Remote Attestation Procedures Architecture

Abstract

In network protocol exchanges, it is often the case that one entity (a relying party) requires evidence about a remote peer to assess the peer's trustworthiness, and a way to appraise such evidence. The evidence is typically a set of claims about its software and hardware platform. This document describes an architecture for such remote attestation procedures (RATS).

Note to Readers

Discussion of this document takes place on the RATS Working Group mailing list (rats@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/rats/.

Source for this draft and an issue tracker can be found at https://github.com/ietf-rats-wg/architecture.

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 19 June 2020.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction

2. Terminology

The document defines the term "Remote Attestation" as follows: A process by which one entity (the "Attester") provides evidence about its identity and state to another remote entity (the "Relying Party"), which then assesses the Attester's trustworthiness for the Relying Party's own purposes.

This document then uses the following terms:

* Appraisal Policy for Evidence: A set of rules that direct how a verifier evaluates the validity of information about an Attester. Compare /security policy/ in [RFC4949].

* Appraisal Policy for Attestation Result: A set of rules that direct how a Relying Party evaluates the validity of information about an Attester. Compare /security policy/ in [RFC4949].

* Attestation Result: The evaluation results generated by a Verifier, typically including information about an Attester, where the Verifier vouches for the validity of the results.

* Attester: An entity whose attributes must be evaluated in order to determine whether the entity is considered trustworthy, such as when deciding whether the entity is authorized to perform some operation.

* Endorsement: A secure statement that some entity (typically a manufacturer) vouches for the integrity of an Attester's signing capability.

* Endorser: An entity that creates Endorsements that can be used to help evaluate trustworthiness of Attesters.

* Evidence: A set of information about an Attester that is to be evaluated by a Verifier.

* Relying Party: An entity that depends on the validity of information about another entity, typically for purposes of authorization. Compare /relying party/ in [RFC4949].

* Relying Party Owner: An entity, such as an administrator, that is authorized to configure Appraisal Policy for Attestation Results in a Relying Party.

* Verifier: An entity that evaluates the validity of Evidence about an Attester.

*Verifier Owner: An entity, such as an administrator, that is authorized to configure Appraisal Policy for Evidence in a Verifier.

[EDITORIAL NOTE]

The term Attestation and Remote Attestation are not defined in this document, at this time. This document will include pointers to industry uses of the terms, in an attempt to gain consensus around the term, and be consistent with the charter text defining this term.

3. Reference Use Cases

<unclear if the WG wants this section in the arch doc>

4. Architectural Overview

Figure 1 depicts the data that flows between different roles, independent of protocol or use case.

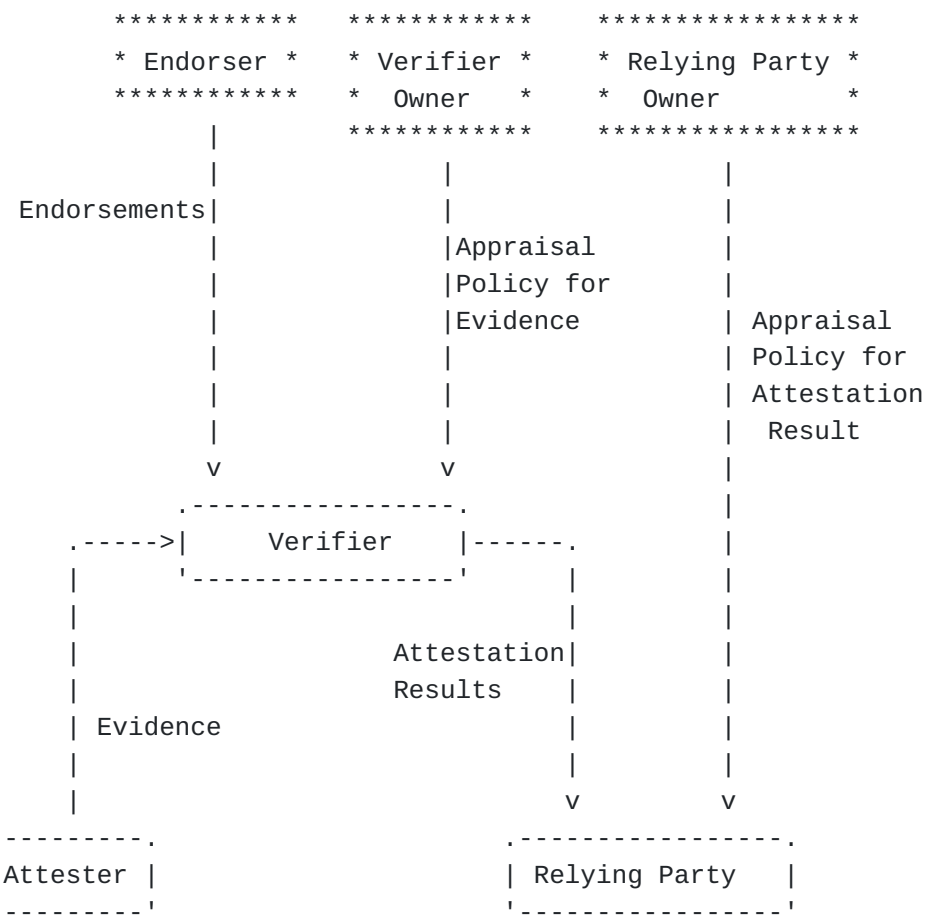

Figure 1: Conceptual Data Flow

An Attester creates Evidence that is conveyed to a Verifier.

The Verifier uses the Evidence, and any Endorsements from Endorsers, by applying an Evidence Appraisal Policy to assess the trustworthiness of the Attester, and generates Attestation Results for use by Relying Parties. The Evidence Appraisal Policy might be obtained from an Endorser along with the Endorsements, or might be obtained via some other mechanism such as being configured in the Verifier by an administrator.

The Relying Party uses Attestation Results by applying its own Appraisal Policy to make application-specific decisions such as authorization decisions. The Attestation Result Appraisal Policy might, for example, be configured in the Relying Party by an administrator.

5. Topological Models

<this section can include Message Flows from draft-birkholz-rats-archite
Architectural Models from draft-thaler-rats-architecture>

6. Two Types of Environments

An Attester consists of at least one Attesting Environment and Attested Environment. In some implementations, the Attesting and Attested Environments might be combined. Other implementations might have multiple Attesting and Attested Environments.

<this section can include Two Types of Environments content from draft-b
but can we find a better name? also this could be a subsection of someth

7. Trust Model

The scope of this document is scenarios for which a Relying Party trusts a Verifier that can evaluate the trustworthiness of information about an Attester. Such trust might come by the Relying Party trusting the Verifier (or its public key) directly, or might come by trusting an entity (e.g., a Certificate Authority) that is in the Verifier's certificate chain. The Relying Party might implicitly trust a Verifier (such as in the Verifying Relying Party combination). Or, for a stronger level of security, the Relying Party might require that the Verifier itself provide information about itself that the Relying Party can use to evaluate the trustworthiness of the Verifier before accepting its Attestation Results.

In solutions following the background-check model, the Attester is assumed to trust the Verifier (again, whether directly or indirectly via a Certificate Authority that it trusts), since the Attester

relies on an Attestation Result it obtains from the Verifier, in order to access resources.

The Verifier trusts (or more specifically, the Verifier's security policy is written in a way that configures the Verifier to trust) a manufacturer, or the manufacturer's hardware, so as to be able to evaluate the trustworthiness of that manufacturer's devices. In solutions with weaker security, a Verifier might be configured to implicitly trust firmware or even software (e.g., a hypervisor). That is, it might evaluate the trustworthiness of an application component, or operating system component or service, under the assumption that information provided about it by the lower-layer hypervisor or firmware is true. A stronger level of security comes when information can be vouched for by hardware or by ROM code, especially if such hardware is physically resistant to hardware tampering. The component that is implicitly trusted is often referred to as a Root of Trust.

8. Conceptual Messages

<this section can include content from Serialization Formats and Concept draft-thaler-rats-architecture, and Role Messages content from draft-bir

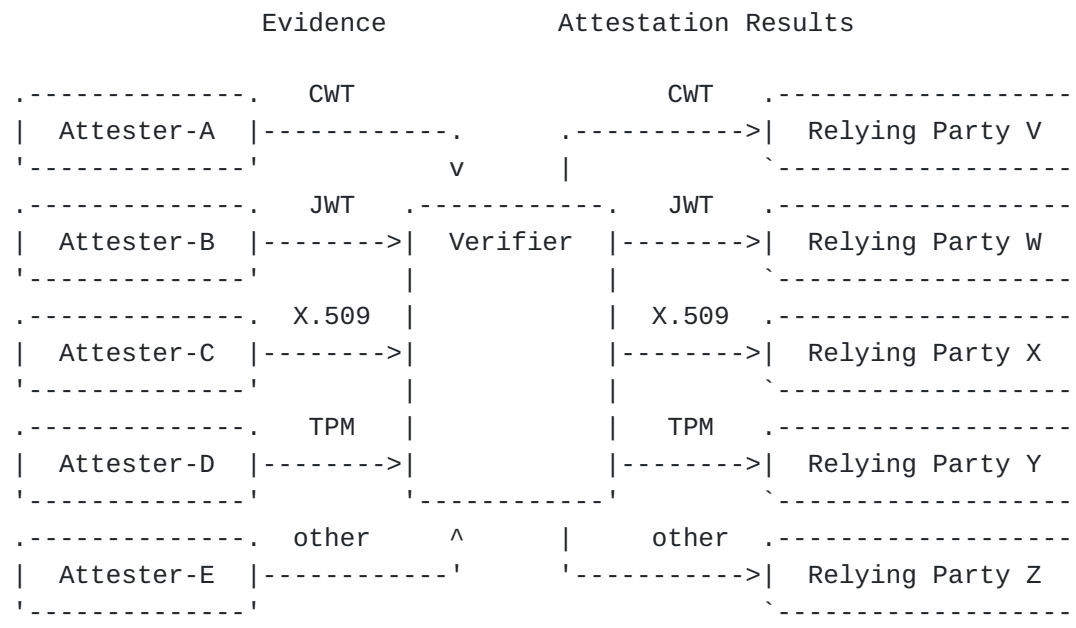

Figure 2: Multiple Attesters and Relying Parties with Different Formats

9. Freshness

<this section can include some high-level content from draft-birkholz-ra

10. Privacy Considerations

The conveyance of Evidence and the resulting Attestation Results reveal a great deal of information about the internal state of a device. In many cases, the whole point of the Attestation process is to provide reliable information about the type of the device and the firmware/software that the device is running. This information is particularly interesting to many attackers. For example, knowing that a device is running a weak version of firmware provides a way to aim attacks better.

Protocols that convey Evidence or Attestation Results are responsible for detailing what kinds of information are disclosed, and to whom they are exposed.

11. Security Considerations

<this section can include Security Considerations from draft-birkholz-ra and draft-thaler-rats-architecture>

12. IANA Considerations

This document does not require any actions by IANA.

13. Acknowledgments

Special thanks go to David Wooten, Joerg Borchert, Hannes Tschofenig, Laurence Lundblade, Diego Lopez, Jessica Fitzgerald-McKay, Frank Xia, and Nancy Cam-Winget.

14. Contributors

Thomas Hardjono created older versions of the terminology section in collaboration with Ned Smith. Eric Voit provided the conceptual separation between Attestation Provision Flows and Attestation Evidence Flows. Monty Wisemen created the content structure of the first three architecture drafts. Carsten Bormann provided many of the motivational building blocks with respect to the Internet Threat Model.

Authors' Addresses

Henk Birkholz
Fraunhofer SIT
Rheinstrasse 75
64295 Darmstadt
Germany

Email: henk.birkholz@sit.fraunhofer.de

Dave Thaler
Microsoft
United States of America

Email: dthaler@microsoft.com

Michael Richardson
Sandelman Software Works
Canada

Email: mcr+ietf@sandelman.ca

Ned Smith
Intel Corporation
United States of America

Email: ned.smith@intel.com