RATS Architecture Design Team Status and Walkthrough

WHO:

- Henk Birholz(*)
- Thomas Fossati
- Andrew Guinn
- Thomas Hardjono
- Sarah C. Helble
- Xinxin Fan IoTeX
- Eliot Lear
- Peter Loscocco
- Laurence Lundblade
- Nicolae PALADI
- Wei (William) Pan(*-new)
- Michael Richardson(*)
- Paul Rowe
- Ned Smith(*)
- Dave Thaler(*)
- Akura Tsukamoto
- Eric Voit
- Monty Wiseman
- Ling (Frank) Xia

WHEN: Tuesdays 10am EST.
(+ a few Fridays/adhoc)

eight meetings since IETF108

ISSUES: 159 total

2 issues open, 1 wontfix

Pull requests:

104 pull requests closed

(*)-listed author

DONE? DONE? DONE?

Major changes in -07

Reference Values

a
signing

ements

be
ion data,

n the
f
/relying

Endorsement: A secure statement that an Endorser vouches for the integrity of an Attester's various capabilities such as Claims collection and Evidence signing

Endorser: An entity (typically a manufacturer) whose Endorsements help Verifiers appraise the authenticity of Evidence

Evidence: A set of information about an Attester that is to be appraised by a Verifier. Evidence may include configuration data, measurements, telemetry, or inferences.

Reference Value Provider: An entity (typically a manufacturer) whose Reference Values help Verifiers appraise the authenticity of Evidence.

Reference Values: A set of values against which values
be compared as part of applying an Appraisal Policy
Reference Values are sometimes referred to in other
known-good values, golden measurements, or nominal va
although those terms typically assume comparison for
whereas here Reference Values might be more general
any sort of comparison.

Relying Party: A role performed by an entity that depe
validity of information about an Attester, for purpos
reliably applying application specific actions. Comp

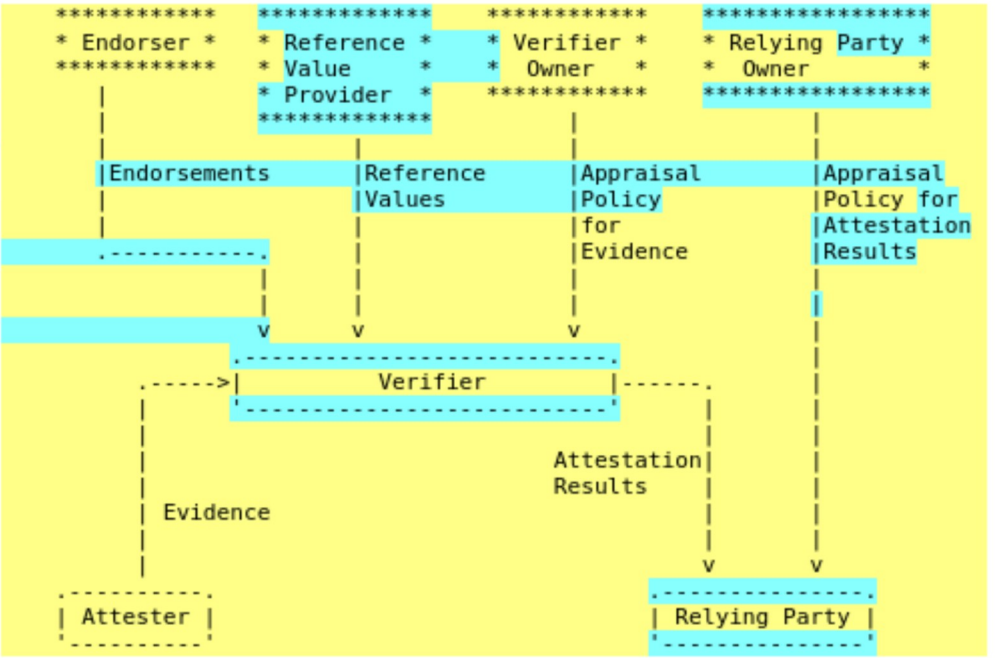

Figure 1: Conceptual Data Flow

About the Verifier

7.4. Verifier

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 appraise the trustworthiness of that manufacturer's devices. In a typical solution, a Verifier comes to trust an Attester indirectly by having an Endorser (such as a manufacturer) vouch for the Attester's ability to securely generate Evidence.

In some solutions, a Verifier might be configured to directly trust an Attester by having the Verifier have the Attester's key material (rather than the Endorser's) in its trust anchor store.

Such direct trust must first be established at the time of trust anchor store configuration either by checking with an Endorser at that time, or by conducting a security analysis of the specific device. Having the Attester directly in the trust anchor store narrows the Verifier's trust to only specific devices rather than all devices the Endorser might vouch for, such as all devices manufactured by the same manufacturer in the case that the Endorser is a manufacturer.

Such narrowing is often important since physical possession of a device can also be used to conduct a number of attacks, and so a device in a physically secure environment (such as one's own premises) may be considered trusted whereas devices owned by others would not be. This often results in a desire to either have the owner run their own Endorser that would only Endorse devices one owns, or to use Attesters directly in the trust anchor store. When there are many Attesters owned, the use of an Endorser becomes more scalable.

That is, it might appraise the trustworthiness of an application component, operating system component, or service under the assumption that information provided about it by the lower-layer firmware or software is true. A stronger level of assurance 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. In most cases, components that have to be vouched for via Endorsements because no Evidence is generated about them are referred to as roots of trust.

The manufacturer of the Attester arranges for its Attesting Environment to be provisioned with key material. The key material is typically in the form of an asymmetric key pair (e.g., an RSA or ECDSA private key and a manufacturer-signed IDevID certificate) secured in the Attester.

The Verifier is provided with an appropriate trust anchor, or provided with a database of public keys (rather than certificates), or even carefully secured lists of symmetric keys. The nature of how the Verifier manages to validate the signatures produced by the Attester is critical to the secure operation an Attestation system, but is not the subject of standardization within this architecture.

A conveyance protocol that provides authentication and integrity protection can be used to convey unprotected Evidence, assuming the following properties exists:

Freshness and other edits

https://www.ietf.org/rfcdiff?url1=draft-ietf-rats-architecture-06&url2=draft-ietf-rats-architecture-07

Questions
Discussion