Network Working Group
Internet-Draft
Intended status: Informational
Expires: January 5, 2018

H. Birkholz
Fraunhofer SIT
M. Wiseman
GE Global Research
H. Tschofenig
ARM Ltd.

July 04, 2017

Reference Terminology for Attestation Procedures
draft-birkholz-attestation-terminology-00

Abstract

This document is intended to illustrate and remediate the impedance mismatch of terms related to attestation procedures used in different domains today. New terms defined by this document provide a consolidated basis to support future work on attestation procedures in the IETF and beyond.

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 http://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 January 5, 2018.

Copyright Notice

Copyright (c) 2017 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 (http://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

Over the years, the term attestation has been used in multiple contexts and multiple scopes and therefore accumulated various connotations with slightly different semantic meaning.

In order to better understand and grasp the intend and meaning of specific attestation procedures in the security area - including the requirements that are addressed by them - this document provides an overview of existing work, its background, and common terminology. As the contribution, from that state-of-the-art a set of terms that provides a stable basis for future work on attestation procedures in the IETF is derived.

The primary application of attestation procedures is to increase the trust and confidence in the integrity of the characteristics and properties of an entity that intends to provide data to other entities remotely. How an objects's characteristics are attested and which characteristics are actually chosen to be attested varies with

the requirements of the use case, or--in essence--depends on the risk that is intended to be mitigated via an attestation procedure. It is important to note that the activity of attestation itself in principle only provides the evidence that proves integrity as a basis for further activities. The resulting attestation procedure defines the greater semantic context about how the evidence is used and what an attestation procedures actually accomplishes; and what it cannot accomplish, correspondingly. Hence, this document is also intended to provide a map of terms, concepts and applications that illustrate the ecosystem of current applications of attestation procedures.

Before an adequate set of terms and definitions for the domain of attestation procedures can be defined, a general understanding and the global definitions of the "what" and the "how" have to be established. In consequence, [enter final structure here].

Please note that the time before the I-D deadline did not suffice to fill in all the references. Most references are therefore still under construction. The majority of definitions is still only originating from IETF work. Future iterations will pull in more complementary definitions from other SDO (e.g. Global Platform, TCG, etc.) and a general structure template to highlight semantic relationships and capable of resolving potential discrepancies will be introduced. A section of context awareness will provide further insight on how attestation procedures are vital to ongoing work in the IETF (e.g. I2NSF & tokbind). The definitions in the section about Remote Attestation are basically self-describing in this version. Additional explanatory text will be added to provide more context and coherence.

1.1. Requirements notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119, BCP 14 [RFC2119].

2. Basic Attestation Roles

The use of the term remote attestation always implies the involvement of at least two parties that each take on a specific role in corresponding procedures - the attestee role and the verifier role. Depending on the characteristics attested and the nature of the parties, information is exchanged via specific types of interconnects between them. The type of interconnect ranges from GIO pins, to a bus, to the Internet, or from a direct physical connection, to a wireless association, to a world wide mesh of peers. In other words, virtually every kind communication path can be used by the two roles.

In fact, a single party can take on both roles at the same time, but there is only a limited use to this architecture.

Attestee: The role that designates the subject of the attestation. The provider of evidence.

Verfifier: The role that designates the appraiser of the attestee's attestation. The consumer of evidence.

Interconnect: A channel of communication between attestee and verifier that enables the appraisal of evidence created by the attestee.

3. Computing Context

This section introduces the term computing context in order to simplify the definition of attestation terminology.

The number of approaches and solutions to create things that provide the same capabilities as a "simple physical device" continuously increases. Examples include but are not limited to: the compartmentalization of physical resources, the separation of software instances with different dependencies in dedicated containers, and the nesting of virtual components via hardware-based and software-based solutions.

In essence, every physical or logical system is a composite. Every component in that composite is a potential computing context capable of taking on the roles of attestee or verifier. The scope and

application of these roles can range from continuous mutual attestation procedure, in which every component in a hierarchically structured composite that constitutes a single distinguishable endpoint on the management plane, to sporadic attestation of the integrity of an experiment in earth orbit.

Analogously, the increasing number of features and functions start to blur the lines that are required to categorize each solution and approach precisely. To address that increasingly difficult categorization, the term computing context defines the characteristics of the entities that can take on the role of an attestee - and in consequence the role of a verifier. This approach is intended to provide a stable basis of definitions for future solutions that continuous to remain viable long-term.

Computing context : An umbrella term that combines the scope of the definitions of endpoint [ref NEA], device [ref 1ar], and thing [ref t2trg], including hardware-based and software-based sub-contexts that constitute independent and distinguishable slices of

a computing context created by compartmentalization mechanisms, such as trusted execution environments or virtual network security function contexts.

3.1. Formal Semantic Relationships

The formal semantic relationship of a computing context and the definitions provided by RFC 4949 is a as follows.

The scope of the term computing context encompasses

- an information system,
- an object and in consequence a system component or a composite of system sub-components, and
- a system entity or a composite of system entities.

Analogously, a sub-context is a subsystem and as with system components, computing contexts can be nested and therefore be physical system components or logical ("virtual") system (sub-)components.

The formal semantic relationship is based on the following definitions from RFC 4949.

(Information) System: An organized assembly of computing and communication resources and procedures - i.e., equipment and services, together with their supporting infrastructure, facilities, and personnel - that create, collect, record, process, store, transport, retrieve, display, disseminate, control, or dispose of information to accomplish a specified set of functions.

Object: A system component that contains or receives information.

Subsystem: A collection of related system components that together perform a system function or deliver a system service.

System Component: A collection of system resources that (a) forms a physical or logical part of the system, (b) has specified functions and interfaces, and (c) is treated (e.g., by policies or specifications) as existing independently of other parts of the system. (See: subsystem.)

An identifiable and self-contained part of a Target of Evaluation.

System Entity: An active part of a system - [...] (see: subsystem) - that has a specific set of capabilities.

3.2. Characteristics of a computing context

While the semantic relationships highlighted above constitute the fundamental basis to define the context of computing context, the following list of characteristics is intended to improve the intuitive understanding of the term and provide a better understanding of its meaning:

A computing context:

- creates its own independent environment in regard to executing and running software,
- creates its own separate control plane state (by potentially interacting with other computing contexts) and can provide a

dedicated management interface by which control plane behavior can be effected,

- can be identified uniquely and therefore reliably differentiated in a given scope, and

- does not necessarily has to include a network interface with associated network addresses (as required, e.g. by the definition of an endpoint) - although it is very likely to have (access to) one.

In contrast, a docker [ref docker, find a more general term here] context is not a distinguishable slice of a computing system and therefore is not an independent computing context.

Examples include: a smart phone, a nested virtual machine, a virtualized firewall function running distributed on a cluster of physical and virtual nodes, or a trust-zone.

4. Computing Context Identity

The identity of a computing context provides a basis for data origin authentication. Confidence in the identity assurance level [NIST SP-800-63-3] or the assurance levels for identity authentication [RFC4949] impacts the confidence in the evidence an attestee provides.

If a secret key is used to sign a public key

5. Attestation Workflow

This section introduces terms and definitions that are required to illustrate the scope and the granularity of attestation workflows in the context of security automation. Terms defined in the following sections will be based on this workflow-related definitions.

In general, attestation is an iterative procedure that is conducted

over and over again in a computing context under specific conditions. It is neither a generic set of actions nor simply a task, because the actual actions to be undertaken in order to conduct an attestation procedure can vary significantly depending on the protocols employed and types of computing contexts involved.

Activity: The condition in which things are happening or being done. In the scope of attestation, an activity is a sequence of actions that is intended to produce a specifically defined result. The actual composition of actions can vary, depending on the characteristics of the computing context they are conducted by/in and the protocols used. A single activity provides a only a minimal required amount of semantic context, e.g. by the activity's requirements imposed on the computing context, or via set of actions it is composed of. Example: The conveyance of cryptographic evidence or the acquisition of an trusted time stamp token are activities.

Task: A piece of work to be done or undertaken. In the scope of attestation, a task is a procedure to be conducted. Example: A Verifier can be tasked with the appraisal of evidence originating from a specific type of computing contexts.

Action: The accomplishment of a thing usually over a period of time, in stages, or with the possibility of repetition. In the scope of attestation, an action is the execution of an operation or function in the scope of an activity conducted by a single computing context. A single action provides no semantic context by itself, although it can limit potential semantic contexts of attestation procedures to a smaller subset. Example: Signing an existing public key via a specific openssl library, transmitting data, or receiving data are actions.

Procedure: A series of actions that are done in a certain way or order. In the scope of attestation, a procedure is a composition of activities (sequences of actions) that is intended to create a well specified result with a well established semantic context. Example: The activities of attestation, conveyance and verification compose a remote attestation procedure.

6. Reference Use Cases

This document provides NNN prominent examples of use cases attestation procedures are intended to address:

- Verification of the source integrity of a computing context via data integrity proofing of installed software instances that are executed, and

- Verification of the identity proofing of a computing context.

These use case summary highlighted above is based in the following terms defined in RFC4949 and complementary sources of terminology:

Assurance: An attribute of an information system that provides grounds for having confidence that the system operates such that the system's security policy is enforced [RFC4949] (see Trusted System below).

In common criteria, assurance is the basis for the metric level of assurance, which represents the "confidence that a system's principal security features are reliably implemented".

The NIST Handbook [get ref from 4949] notes that the levels of assurance defined in Common Criteria represent "a degree of confidence, not a true measure of how secure the system actually is. This distinction is necessary because it is extremely difficult-and in many cases, virtually impossible-to know exactly how secure a system is."

Historically, assurance was well-defined in the Orange Book [http://csrc.nist.gov/publications/history/dod85.pdf] as "guaranteeing or providing confidence that the security policy has been implemented correctly and that the protection-relevant elements of the system do, indeed, accurately mediate and enforce the intent of that policy. By extension, assurance must include a guarantee that the trusted portion of the system works only as intended."

Confidence: The definition of correctness integrity in [RFC4949] notes that "source integrity refers to confidence in data values". Hence, confidence in an attestation procedure is referring to the degree of trustworthiness of an attestation activity that produces evidence (attestee), of an conveyance activity that transfers evidence (interconnect), and of a verification activity that appraises evidence (verifier), in respect to correctness integrity.

Identity: [pull relevant rfc4949 parts here]

Identity Proofing: A process that vets and verifies the information that is used to establish the identity of a system entity.

Source Integrity: The property that data is trustworthy (i.e., worthy of reliance or trust), based on the trustworthiness of its sources and the trustworthiness of any procedures used for handling data in the system.

Data Integrity: (a) The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner. (See: data integrity service. Compare: correctness integrity, source integrity.)

(b) The property that information has not been modified or destroyed in an unauthorized manner.

Correctness: The property of a system that is guaranteed as the result of formal verification activities.

Correctness integrity: The property that the information represented by data is accurate and consistent.

Verification: (a) The process of examining information to establish the truth of a claimed fact or value.

(b) The process of comparing two levels of system specification for proper correspondence, such as comparing a security model with a top-level specification, a top-level specification with source code, or source code with object code.

6.1. The Lying Endpoint Problem

A very prominent goal of attestation procedures - and therefore a suitable example used as reference in this document - is to address the "lying endpoint problem".

Information created, relayed, or, in essence, emitted by a computing context does not have to be correct. There can be multiple reasons why that is the case and the "lying endpoint problem" represents a scenario, in which the reason is the compromization of computing contexts with malicious intend. A compromised computing context could try to "pretend" to be integer, while actually feeding manipulated information into a security domain, therefore compromising the effectiveness of automated security functions.

Attestation - and remote attestation procedures specifically - is an

approach intended to identify compromised software instances in computing contexts.

Per definition, a "lying endpoint" cannot be "trusted system".

Trusted System: A system that operates as expected, according to design and policy, doing what is required - despite environmental disruption, human user and operator errors, and attacks by hostile parties - and not doing other things.

Remote attestation procedures are intended to enable the consumer of information emitted by an computing context to assess the validity and integrity of the information transferred. The approach is based on the assumption that if evidence can be provided in order to prove the integrity of every software instance installed involved in the activity of creating the emitted information in question, the emitted information can be considered valid and integer.

In contrast, such evidence has to be impossible to create if the software instances used in a computing context are compromised. Attestation activities that are intended to create this evidence therefore also to also provide guarantees about the validity of the evidence they can create.

6.2. Who am I a talking to?

[working title, write up use case here, ref teep requirements]

7. Trustworthiness

A "lying endpoint" is not trustworthy.

Trusted System: A system that operates as expected, according to design and policy, doing what is required - despite environmental disruption, human user and operator errors, and attacks by hostile parties - and not doing other things.

Trustworthy: pull in text here

8. Remote Attestation

Attestation: An object integrity authentication facilitated via the creation of a claim about the properties of an attestee, such that the claim can be used as evidence.

Conveyance: The transfer of evidence from the attestee to the verifier.

Verification: The appraisal of evidence by evaluating it against declarative guidance.

Remote Attestation: A procedure composed of the activities attestation, conveyance and verification.

8.1. Building Block Terms

[working title, pulled from various sources, vital]

Attestation Identity Key (AIK): A special purpose signature (therefore asymmetric) key that supports identity related operations. The private portion of the key pair is maintained confidential to the computing context via appropriate measures (that have a direct impact on the level of confidence). The public portion of the key pair may be included in AIK credentials that provide a claim about the computing context.

Claim: A piece of information asserted about a subject. A claim is represented as a name/value pair consisting of a Claim Name and a Claim Value [RFC7519]

In the context of SACM, a claim is also specialized as an attribute/value pair that is intended to be related to a statement [I-D.ietf-sacm-terminology].

Computing Context Characteristics: The composition, configuration and state of a computing context.

Evidence: A trustworthy set of claims about an computing context's characteristics.

Identity: A set of claims that is intended to be related to an entity. [merge with RFC4949 defintion above]

Integrity Measurements: Metrics of computing context characteristics (i.e. composition, configuration and state) that affect the confidence in the trustworthiness of a computing context. Digests of integrity measurements can be stored in shielded locations (e.g. a PCR of a TPM).

Reference Integrity Measurements: Signed measurements about a computing context's characteristics that are provided by a vendor or manufacturer and are intended to be used as declarative guidannce [I-D.ietf-sacm-terminology] (e.g. a signed CoSWID).

Trustworthiness: The qualities of computing context characteristics that guarantee a specific behavior specified by declarative

guidance. Trustworthiness is not an absolute property but defined with respect to a computing context, corresponding declarative guidance, and has a scope of confidence. A trusted system is trustworthy. [refactor defintion with RFC4949 terms]

Trustworthy Computing Context: a computing context that guarantees trustworthy behavior and/or composition (with respect to certain declarative guidance and a scope of confideence). A trustworthy computing context is a trusted system.

Trustworthy Statement: evidence that trustworthy conveyed by a computing context that is not necessarily trustworthy. [update with tamper related terms]

9. IANA considerations

This document will include requests to IANA:

- first item
- second item

10. Security Considerations

There are always some.

11. Acknowledgements

Maybe.

12. Change Log

No changes yet.

13. References

13.1. 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, <http://www.rfc-editor.org/info/rfc2119>.

[RFC4949] Shirey, R., "Internet Security Glossary, Version 2", FYI 36, RFC 4949, DOI 10.17487/RFC4949, August 2007, <http://www.rfc-editor.org/info/rfc4949>.

13.2. Informative References

[I-D.ietf-sacm-terminology] Birkholz, H., Lu, J., Strassner, J., and N. Cam-Winget, "Security Automation and Continuous Monitoring (SACM) Terminology", draft-ietf-sacm-terminology-12 (work in progress), March 2017.

[RFC7519] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Token (JWT)", RFC 7519, DOI 10.17487/RFC7519, May 2015, <http://www.rfc-editor.org/info/rfc7519>.

Authors' Addresses

Henk Birkholz
Fraunhofer SIT
Rheinstrasse 75
Darmstadt 64295

Germany

Email: henk.birkholz@sit.fraunhofer.de

Monty Wiseman
GE Global Research
USA

Email: monty.wiseman@ge.com

Hannes Tschofenig
ARM Ltd.
110 Fulbourn Rd
Cambridge CB1 9NJ
UK

Email: hannes.tschofenig@gmx.net