

Network Working Group
Internet-Draft
Intended status: Informational
Expires: March 8, 2019

A. Rein
L. Xia
Huawei
September 04, 2018

The Remote Attestation NFV Use Cases
draft-rein-remote-attestation-nfv-use-cases-01

Abstract

This document proposes the use cases on an architectural level in terms of Remote Attestation for virtualized environments, especially in the context of Network Function Virtualization (NFV).

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 March 8, 2019.

Copyright Notice

Copyright (c) 2018 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
1.1.	Stakeholders	2
1.2.	Major Issue	3
2.	Terminology	4
2.1.	Key Words	4
2.2.	Definition of Terms	4
3.	Remote Attestation Use Cases	4
3.1.	Decentralized Model Use Case	5
3.2.	Centralized Model (in a Single Trust Domain) Use Case	8
4.	IANA Considerations	10
5.	Security Considerations	10
6.	Acknowledgements	10
7.	Normative References	11
	Authors' Addresses	11

[1.](#) Introduction[1.1.](#) Stakeholders

Stakeholders play a major role in NFV and there is a strict hierarchical separation between the stakeholders in terms of responsibility, accessibility and visibility within the the NFV architecture. Although these issues are also relevant for other virtualized environments, for example in private or hybrid clouds, they are most apparent in NFV, especially in multi vendor deployments.

The stakeholders in NFV are:

- o Cloud Service Provider (CSP): The CSP provides the platform, i.e. the hardware and core services, acting as the Virtual Machine Manager (VMM) or hypervisor for the provisioning of Virtual Machines (VM). With regard to this document, the CSP is not responsible for the provisioning itself. The CSP only provides the platform w.r.t. to CSP NFV Infrastructure (CSP:NFI) role. The actual provisioning of specific VMs is carried out by the CSP Management and Orchestration (CSP:MANO) role, whereas both roles may be represented by the same or different organizations. This contribution, however, is not concerned with the internal operations and procedures of the CSP:MANO and therefore does address CSP:MANO neither as a role nor as a functional component.

- o Cloud Service Customer (CSC): The CSC is the actual user of the VMM and requests the provisioning of specific VMs that eventually provide some service. The CSC is also in full control in terms of

which specific VM is actually launched and thus not constrained in this regard.

- o Cloud Service User (CSU): The CSU is an external entity that uses the CSC's provided services. The CSU only has access to public API's provided by the offered service and has neither any responsibilities nor obligations within the NFV internals.

1.2. Major Issue

The most significant issue related to remote attestation is that the stakeholders may be constrained with regards to the information available to them. This means that in a strict model that involves a multi-vendor NFV deployment, access to certain information may only be available to one particular stakeholder. For instance, the CSP may only have direct access to the collected platform information and not to the information of provisioned VMs. Similarly, the CSC may be limited to the information collected on the provisioned VMs and does not have access to the information of the platform. This issue can be resolved by generally allowing the access to the information to all interested entities, w.r.t. a relaxed model, or allowing the access based on the enforcement of access permission policies.

More severe is the information necessary to carry out an appraisal of the measured information, that is the information about the expected configuration of the specific entity.

In principle there are two concerns, either this appraisal information should not be made available to a different entity (a stakeholder from a different organization) or the other entity does not want to carry out the appraisal by itself for any system not under its control. This means, even under the consideration that the collected information is shared between multiple stakeholders, the information necessary for carrying out the appraisal may not be available for different reasons.

To simplify the terminology, this contribution distinguishes between Remote Attestation Information Providers (RAIP) and Remote Attestation Information Consumers (RAIC). In particular:

- o CSP is limited to acting only as a RAIP for all authorized entities
- o CSC is limited to acting as a RAIP for all authorized entities and is a specific RAIC of CSP
- o RATP is limited to acting as a RAIP for all authorized entities and is a specific RAIC of CSP and CSC

Furthermore a new term, the Level of Assurance (LoA) is introduced. The LoA is defined as an hierarchical model that specifies the systems and components to be attested and whether an attestation is carried out on a local or remote basis.

With regards to this document, the overall targeted LoA equivalent to the NFV defined LoA levels 4 and 5 that corresponds to the remote attestation of the VMMs and VMs including the appraisal of load and runtime of applications within the VM's scope.

[2.](#) Terminology

[2.1.](#) Key Words

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [[RFC2119](#)].

[2.2.](#) Definition of Terms

[3.](#) Remote Attestation Use Cases

With regard to the main issue mentioned above, there are two options:

- o Decentralized Model: Each entity carries out the remote attestation only for the particular system under its control. This is referred to as the decentralized remote attestation model and involved multiple remote attestation servers.

- o Centralized Model: A new entity, referred to as a Remote Attestation Trusted Party (RATP), is introduced that has access to all information necessary to carry out a remote attestation on its own. This is referred to as the centralized remote attestation model.

However, the goal of the remote attestation is to convince an internal or external entity that a specific service (a networking function) has been provided by a trusted VM that was executed on a trusted VMM. For case (1.) this implies that the internal or external entity that want to know about the trustworthiness of a service must inherently trust the appraised results of both, the CSP and CSC. For case (2.) this means that the internal or external entity must only trust in the decision made by the RATP.

[3.1.](#) Decentralized Model Use Case

In this case there are multiple independent remote attestation servers controlled and maintained by the CSP or CSC stakeholders.

Assumptions:

- o It is assumed that the model satisfies LoA of 4 and 5

Pre-Conditions:

- o Relevant collected evidence (RA measurement information) is available. Access permissions policies are either defined or enforced, or information is available to all RAICs.
- o Role-specific RA appraisal information is available to the RAIC, but limited to the systems and components directly managed by the corresponding stakeholder.

Use case description:

A deployed NFV system consists of multiple RAIPs and RAICs that are

under the control of stakeholders from different organizations. The RAIPs collect evidence on systems and offer this information, for the purpose of appraising them, to RAICs that are also under the control of stakeholders from the same organization.

For example, any RAIP under the control of stakeholder S1 will only share its collected evidence with RAICs that are also under the control of stakeholder S1.

In addition, the information necessary to carry out an appraisal of the collected evidences (i.e., the RA appraisal information) are limited; RAICs from stakeholder S1 only have access to appraisal information for RAIPs that are under the control of the same stakeholder, i.e. S1. For this reason, a RAIC can only appraise collected evidence from a RAIP operated by the same stakeholder.

For example, there is RAIP1 (i.e. a VMM) and RAIC1 both under the control of CSP. RAIC1 receives the collected evidence from RAIP1, appraises it and makes a statement based on the appraised evidence (i.e. AR1).

```

          VMM
    -----
CSP:  |RAIP 1|  ---> |RAIC 1|  --> |AR1|
    -----

```

Similarly, there is RAIP2 (i.e. a VM instantiated on top of CSP's VMM) and RAIC2 both under the control of CSC. RAIC2 receives the collected evidence from RAIP2, appraises it and makes a statement based on the appraised evidence (i.e. AR2).

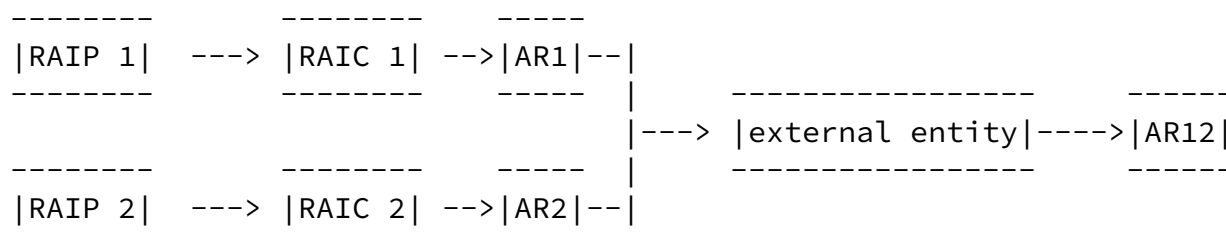
```

          VM
    -----
CSC:  |RAIP 2|  ---> |RAIC 2|  --> |AR2|
    -----

```

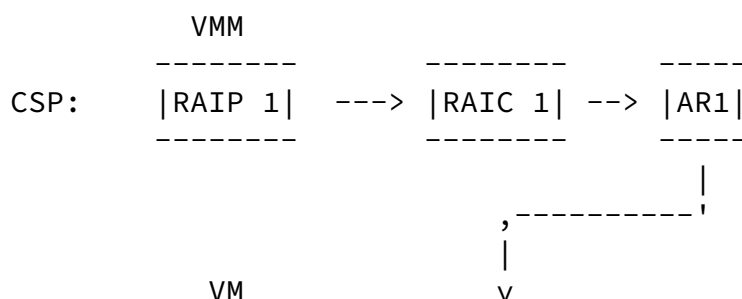
Under the consideration of the requirements defined by LoA 4 and 5 a single RAIC does not have the capability to satisfy these requirements. More specifically this means that at least CSP's and CSC's RAICs must work together to be compliant to LoA 4 and 5 requirements. As a result, RAICs may share appraisal results with

other RAICs or other external entities. This sharing may be constrained by access permission policies. For instance an external entity may request AR1 from RAIC1 and AR2 from RAIC2 and derive AR12 under the assumption it trusts the individual appraised results from either RAIC.



However, the appraisal result generated from any other system but a RAIC (e.g. derived by an arbitrary external entity) is not trusted by any other entity (e.g. CSP, CSC or CSU). This mean that in this case AR12 only has any semantic meaning for the system (i.e. external entity) who derived it.

Alternatively, RAIC2 may use AR1 as an additional input to RAIP2's collected evidence input and derive AR12 accordingly. This is also under the consideration that RAIC2 implicitly trusts the statement made by RAIC1.



```

CSC:  -----
      |RAIP 2|  ---> |RAIC 2| --> |AR12|
      -----

```

In this case, AR12 is derived from CSC's RAIC and therefore other systems do trust this statement because it came from an authorized entity within the system.

See the summary table as below:

	CSP	CSC	CSU	External Entity
Provides RA measurement information	anyone authorized	anyone authorized	-	-
Has RA appraisal information	Only CSP	Only CSC	-	-
Provides RA appraisal results	anyone authorized	anyone authorized	-	-
Has access to RA Appraisal Results	From CSP and, if eligible, CSC	From CSC and, if eligible, CSP	From CSC or CSP (if eligible)	From CSC or CSP (if eligible)

[3.2.](#) Centralized Model (in a Single Trust Domain) Use Case

In this case there are multiple independent remote attestation servers controlled and maintained by the CSP or CSC stakeholders.

Assumptions:

- o It is assumed that the model satisfies LoA of 4 and 5

Pre-Conditions:

- o Relevant collected evidence (RA measurement information) is available to RATP without any restriction.
- o Role-specific RA appraisal information is available to RATP without any restriction.

Use case description:

A deployed NFV system consists of multiple RAIPs and RAICs that are under the control of stakeholders from different organizations and, in addition one RATP that is implicitly trusted by the other entities in the system. The RAIPs collect evidence on systems and offer this information, for the purpose of appraising them, to RAICs that are also under the control of stakeholders from the same organization or to RATP.

For example, any RAIP under the control of stakeholder S1 will only share its collected evidence with RAICs that are also under the control of stakeholder S1 and RATP.

In addition, the information necessary to carry out an appraisal of the collected evidences (i.e., the RA appraisal information) are limited; RAICs from stakeholder S1 only have access to appraisal information for RAIPs that are under the control of the same stakeholder, i.e. S1.

In contrast to this, RATP has access to all appraisal information of any system under evaluation from all stakeholders, i.e. CSP and CSC.

Similar to use-case 1, a RAIC can only appraise collected evidence from a RAIP operated by the same stakeholder, whereas RATP can appraise collected evidence from all stakeholders.

For example, there is RAIP1 (i.e. a VMM) under the control of CSP and RATP. RATP receives the collected evidence from RAIP1, appraises it and makes a statement based on the appraised evidence (i.e. AR1).

```

          VMM
-----
CSP:  |RAIP 1|  ---> |RATP|  --> |AR1|
-----

```

Similarly, there is RAIP2 (i.e. a VM instantiated on top of CSP's VMM) under the control of CSC and RATP. RAIC2 receives the collected evidence from RAIP2, appraises it and makes a statement based on the appraised evidence (i.e. AR2).

```

          VM
-----
CSC:  |RAIP 2|  ---> |RATP|  --> |AR2|
-----

```

Under the consideration of the requirements defined by LoA 4 and 5, RATP satisfies these requirements under the assumption that it received the correlated collected evidences from both VMM and VM. RATP may share its appraisal results with any other entity, however, access permissions policies may constrain access to the information. For instance, considering access permissions allow it, an external entity may request AR12 from RATP.

```

-----
|RAIP 1|  -,
-----  |  -----
          -> |RATP|  ---> |AR12|  -> |external entity|
-----  |  -----
|RAIP 2|  -'
-----

```

Important to note in this case is that the appraisal result provided by RATP is ultimately trusted by all participating systems from any stakeholder and all external entities the request this appraisal result.

See the summary table as below:

Internet-Draft

Remote Attestation NFV Use Cases

September 2018

	CSP	CSC	CSU	RATP	External System
Provides RA measurement information	To RATP or CSP	To RATP or CSC	-	-	
Has RA appraisal information	Only CSP	Only CSC	-	CSP and CSC	
Provides RA appraisal results	-	-	-	For CSP, CSC, CSU, External system (access restrictions may be defined)	
Has access to RA Appraisal results	From RATP (if eligible)	From RATP (if eligible)	From RATP (if eligible)	From RATP (if eligible)	From RATP (if eligible)

4. IANA Considerations

This document makes no request of IANA.

Note to RFC Editor: this section may be removed on publication as an RFC.

5. Security Considerations

To be added.

[6.](#) Acknowledgements

Rein & Xia

Expires March 8, 2019

[Page 10]

Internet-Draft

Remote Attestation NFV Use Cases

September 2018

[7.](#) 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>>.

Authors' Addresses

Andre Rein
Huawei

Email: Andre.Rein@huawei.com

Liang Xia
Huawei

Email: frank.xialiang@huawei.com

