Remote Attestation NFV Use Cases

draft-rein-remote-attestation-nfv-use-cases-00

Liang Xia Huawei

Andre Rein Huawei

IETF-101, London
March 22, 2018

Agenda

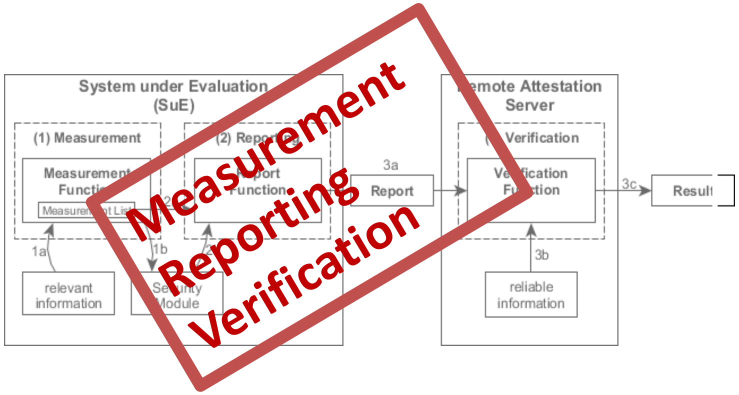
- Introduction
- Motivation
- Draft Overview
- Two Models
- Next Steps, Plans and Questions

Introduction: Remote Attestation – System State Evaluation

System integrity attestation is to make a statement whether the state of a system is considered to be good (trustworthy) or malicious (untrustworthy).

But there is no common procedure that specifies how the information is exchanged from a system A (to be attested) to a system B (the attesting system).

<u>This results in incompatibility, which is one of the major reasons why RA has not been widely used to this day!</u>



Furthermore, RA specification for architectures utilizing virtualization, e.g. NFV, have not been considered. Scalability issues have not yet been addressed either.

Motivation in Short

- Remote Attestation (RA) lacks a proper protocol specification
  - Without a protocol RA will not be used
  - Proprietary protocols will lead to incompatibility
- Modern architecture requirements
  - Virtualization, multi-vendor deployments and stakeholders must be considered during design
- Scalability
  - Will become an issue in bigger deployments

RA Characteristics in NFV Network

- NFV is build upon a modern architecture (NFV) with the following characteristics:
  - Different stakeholders (Cloud Service Provider, Cloud Service Customer) are responsible for specific parts within the architecture
  - Other stakeholders only use a service (Cloud Service User)
  - Multi-vendor deployments are very common
- Holistic view of multiple related components is necessary
  - To determine a state of a virtualized system, the hypervisor must also be attested
- Constrained access to information
  - Stakeholders, especially in multi-vendor deployments, may be restricted in terms of access to necessary information
  - Example 1: A stakeholder may access a provisioned virtual machine, but not the hypervisor not under his control
  - Example 2: A stakeholder may lack the information to carry out an appraisal

Two Models: Decentralized vs Centralized

Architectural Models of Operations

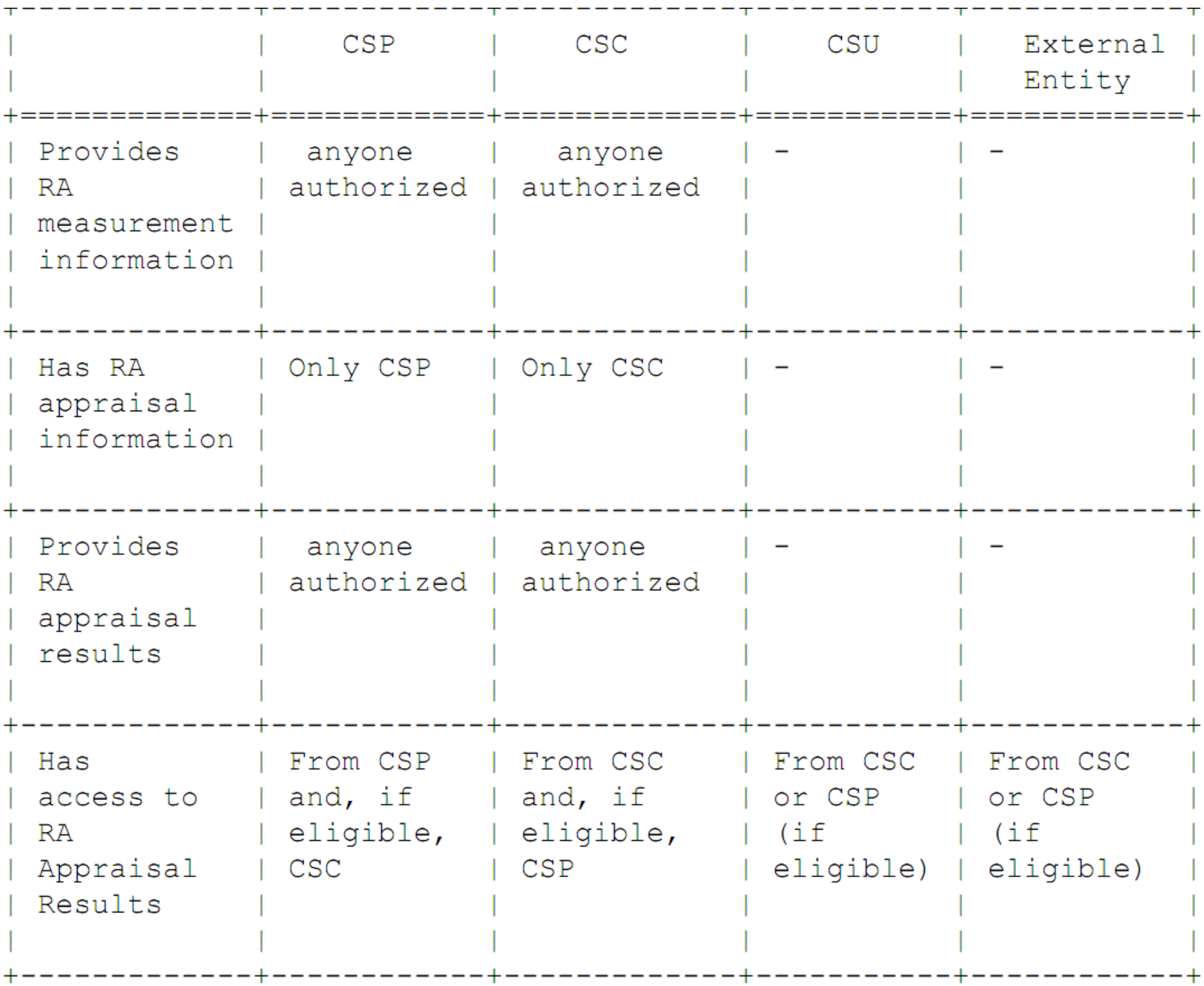
Decentralized Model

- Carry out independent attestation of accessible systems under direct control
- Make the determined attestation result statements available to other stakeholders
- Establish a relation between individual attestation statements
- Enforcement of more complex access permission policies necessary

Centralized Model

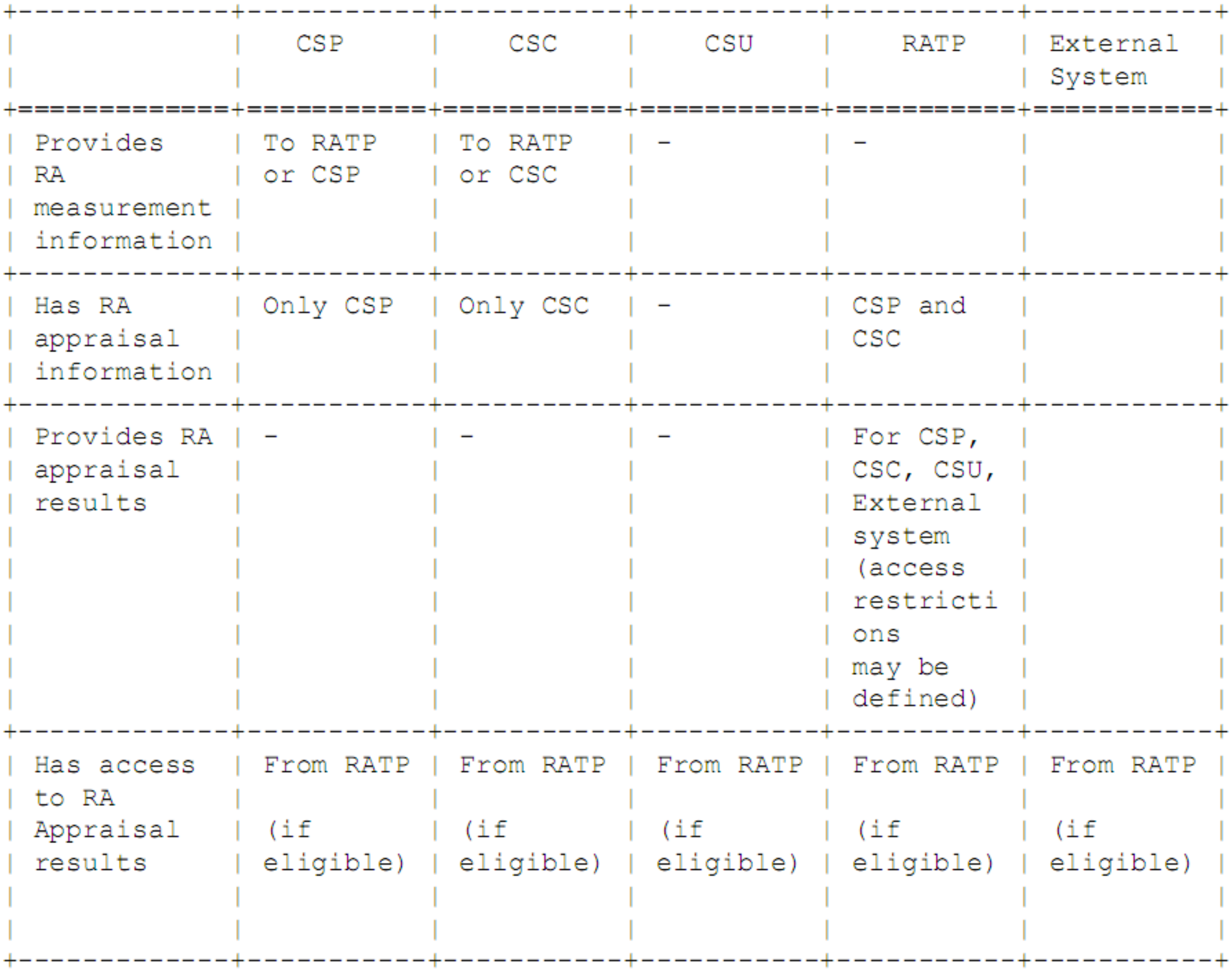
- Attestation is carried out by one central Trusted Third Party (TTP)
- TTP has access to all systems and information necessary
- TTP establishes the relation of systems implicitly
- TTP offers attestation results to eligible other stakeholders
- Enforcement of simple access permissions

Decentralized Model



	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)

Centralized Model



	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)

Next Steps and Plans

- Refine the current draft
  - Add more details
  - Add scenario use-cases and examples (contribution from Ericsson in draft-1)
  - Possibly incorporate non-NFV related use-cases
- Welcome comments and further co-authors

Thanks!

Liang Xia (Frank)