Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: 26 October 2025

Lu, Ed.
M. Chen
L. Su
China Mobile
24 April 2025

A mechanism of security monitoring and management for service resources in Computing-Aware Traffic Steering (CATS)
draft-lu-cats-smam-security-01

Abstract

This draft proposes a mechanism to realize monitoring and management of service resources.

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 26 October 2025.

Table of Contents

1. Introduction

As described in [I-D.ietf-cats-usecases-requirements], traffic steering that takes into account both the computing resource metric and network metric would improve the QoE of several services, e.g., AR/VR and intelligent transportation. But when executing services, efficiency is not the only factor to consider. Security requirements are important for users, service providers and network providers, such as following security requirements:

1. The services should not be interrupted abnormally, and data of services should not be leaked or unauthorized access;

2. The network should run stably and is not subject to attacks from service resources;

3. The service resources are prevented from being attacked by other resources.

Many resolutions need to be designed and applyed to fully meet security requirements above. But a basic resolution is to monitor and discover corrupted service resources and limit them from providing services and interact with network components as well as other service resources, and more secure service resources should be selected under same conditions. This draft proposes a mechanism to realize monitoring and management of service resources.

2. Problem statement

Service resources face kinds of attacks from inside and outside. Successful attacks may bring security risks for services, such as service unavailable, service data stolen etc, and service resources may become attack tools to interfere activities of other computing resources and functional components in CATS if they are manipulated maliciously. The more vulnerable the resource, the greater the likelihood of being breached. And when service resources have been breached, they will be threats in network.

For protecting service availability, security of services and maintaining network stability, computing resources in CATS should be in security status and services should run on reliable resources. So there should be a mechanism to monitor security status of service resources and discover the resources that are likely to be breached and those that have already been breached in CATS. Then different policies can be applyed for above service resources such as excluding the service resources from CATS or reduce usage of them.

3. Framework and Components

In [I-D.ldbc-cats-framework], a CATS framework for computing-aware traffic steering according to computing metrics of service resources and network metrics is proposed. In this draft, the new functional component C-SeMA is introduced based on the existing CATS framework.

The CATS Security Metric Agent(C-SeMA) is responsible for collecting security information of computing resources that used to carry service instances. Computing resources could be servers, virtual machines or containers. Details of security information are listed in 5.2.

The C-SeMA gathers the security information and decides the security status of the computing resources, then generates security policy according to the security status of computing resources and sends it to C-PS. C-PS could adjust resource selection policy according to the security policy.

4. Workflow

4.1. Overview

Figure 2 shows the main workflow of monitoring and management of computing resources. Two stages are included in the workflow. In stage 1, C-SeMA acquire security information from computing resources or security functions. In stage 2, security policies will be generated according to security information and will be sent to C-PS. In stage 3, C-PS can select service nodes according to the security policies.

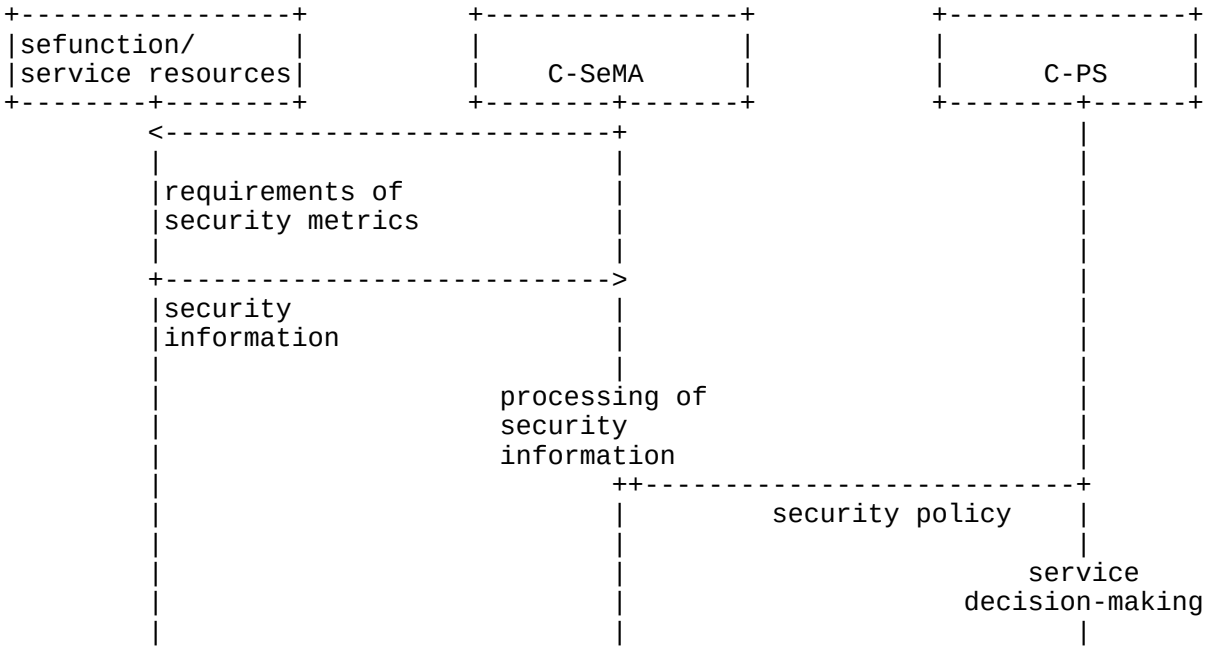

Figure1: overview of workflow

4.2. Collection of security information

C-SeMA need to collect security capability information and security status information of computing resources. Security capability information indicates the security capabilities that are depolyed for protecting computing resources and services running on them from attacks. Security status information including predefined dynamic security metrics of computing resources, such as abnormal traffic, adnormal behaviors, and vulnerability situation etc. C-SeMA need to distribute requirements of security metrics to computing resources or security functions.

C-SeMA collects security information from computing resources or security functions deployed in service sites or network. Different collection methods can be used, such as C-SeMA collects security information periodically or security function push the information when security status changes.

Security information should be associated with a specific computing resource and is associated with service instances by computing resources. Table 1 shows the examples of security information for service resources.

Types of security information	Security metrics	Details
Security capability	Security capabilities of computing resources	Such as X-san , IPS, IDS and confidential computing etc
Security status	Vulnerability information	Current vulnerabilities in computing resources
	Virus information	Current virus in computing resources
	Attack information	Attack events faced by computing resources
	Abnormal behavior information	Abnormal behavior information of service resources such as frequent submission of data, single submission of large amounts of data etc

Table 1: examples of security information

4.3. Processing of security information

C-SeMA sets classification rules for computing resources. The classification rules classify computing resources into different security priority according to security information, such as low, middle, high and disabled. C-SeMA generates initial priority of computing resources when receiving security information for the first time and adjust the priority when security information update.

Two examples of classify rules are as following:

1. Rule 1: define rules of value assignment and weighs of every security metric. Then ass ign values to security metrics of computing resources according to received security info rmation and the rules. And use method of weighting to compute the final security value. S ecurity priority is decided by security value. Security policies will be determined accor ding to the security priority;

2. Rule 2: set classification criteria for every security priority, such as computing res ources are divided into type of disabled if high risk vulnerabilities are found and are d ivided into type of high priority if specific security capabilities are available.

Examples of Initial priority of computing resources are as follows:

Suggests set the security priority of computing resources as low;
Suggests set the security priority of computing resources as middle;
Suggests set the security priority of computing resources as high;
Suggests set the security priority of computing resources as disabled.

C-SeMA processes the updated security information and determines the priority adjustment policy to allocate new priority for computing resources or service instances.

The policies include but not limited to the following types:

Suggests to prohibit using the computing resources(such as high risk vulnerability is found);
Suggests to prohibit using the service instances;
Suggests to reduce the priority of the computing resources;
Suggests to reduce the priority of the service instances;
Suggests to prioritize the computing resources;
Enable the computing resources and assign a security priority;
None.

Specific decision logic is out of the scope of this draft.

4.4. Service decision-making based on security information

C-SeMA submits initial security priority and updated priority policies for specific computing resources or service instances to C-PS. C-PS could take security priority of computing resources as references and adjust selection policies when conducting service decision-making:

If C-SeMA suggests to prohibit specific computing resources/instances, C-PS excludes these computing resources/instances from alternative lists;
If C-SeMA suggests to enable specific computing resources, C-PS puts them into alternative lists;
C-PS selects computing resources/instances of higher security priority to provide service among computing resources/instances with same network and computing conditions.

5. IANA Considerations

This memo includes no request to IANA.

6. Security Considerations

TBD

Authors' Addresses

Li Lu (editor)
China Mobile
BeiJing
China
Email: luli@chinamobile.com

Meiling Chen
China Mobile
BeiJing
China
Email: chenmeiling@chinamobile.com

Li Su
China Mobile
BeiJing
China
Email: suli@chinamobile.com