SACM
Internet-Draft
Intended status: Informational
Expires: March 12, 2015

N. Cam-Winget
Cisco Systems
L. Lorenzin
Juniper Networks

September 8, 2014

# Secure Automation and Continuous Monitoring (SACM) Requirements
# draft-ietf-sacm-requirements-00

Abstract

This document defines the scope and set of requirements for the Secure Automation and Continuous Monitoring working group. The requirements and scope are based on the agreed upon use cases.

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 March 12, 2015.

Table of Contents



## 1. Introduction

Today's challenges of evolving threats and improved analytics highlight a need to automate the securing of both information and the systems that store, process and transmit the information that can and is being leveraged to improve on both threats and analytics to detect such threats. SACM's charter focuses on addressing some of these challenges in a narrower scope by bounding the task to address use cases that pertain to the posture assessment of endpoints.

This document focuses on describing the requirements for facilitating the exchange of posture assessment information, in particular, for the use cases as exemplified in [I-D.ietf-sacm-use-cases].Also, this document uses terminology defined in [I-D.ietf-sacm-terminology].

## 2. Requirements

This document defines requirements based on the SACM use cases defined in [I-D.ietf-sacm-use-cases]. This section describes the requirements used by SACM to assess and compare candidate information models and protocols to suit the architecture. These requirements express characteristics or features that a candidate protocol or data model must be capable of offering so as to ensure security and interoperability.

### 2.1. General SACM requirements

The use cases defined in [I-D.ietf-sacm-use-cases] apply to many deployment scenarios. To ensure interoperability, scalability and flexibility in any of these deployments, the following requirements are defined for all use cases:

G-001 Extensibility: the data models, protocols and transports defined by SACM must be extensible to allow support for non-standard and future extensions. The transport protocol must support easily adding new operations while maintaining backwards compatibility. The query language must allow general inquiries as well as expression of specific paths to follow; retrieval of specific information based on an event, as well as on a continuous basis; and the ability to retrieve specific pieces of information, specific classes of information, and/or the entirety of available information. The information model must accommodate the addition of new data types and/or schemas in a backwards compatible fashion.

G-002 Interoperability: The data models, protocols and transports must be specified with enough details and state machine to ensure interoperability.

G-003 Scalability: The data models, protocols and transports must be scalable. SACM must support a broad set of deployment scenarios. As such, it is possible that the size or posture assessment information can vary from a single assessment that is small in (record or datagram) size to a very large datagram or a very large set of assessments and must be addressed by the SACM specifications defined.

G-004 Agility: The agility requirement is to ensure that the data model, protocols, transports and its implementations are suitable to fit in different deployment models and scenarios. Considerations for the lightweight implementations of data models and transports is required. Use cases, especially in the vulnerability assessment and threat defense applications require time criticality in both obtaining the information as well as consuming (e.g. parsing) the data.

G-005 Transport variability: Different transports must be supported to address different deployment and time constraints. Supporting transports at the Layer 2, Layer 3 and higher application layers.

G-006 Extensibility: a method for expressing both standard and non-standard (implementer-specific) data attributes while avoiding collisions should be defined. For interoperability and scope boundary, an explicit set of data attributes as mandatory to implement should be defined and focused on Posture Assessment should be described to allow for interoprability too.

G-007 Data Integrity: A method for ensuring data integrity must be provided. This method is required to be available (i.e. all data-handling components must support it), but is not required to be used in all cases.

G-008 Data Protection: Transport protocols must ensure data protection for data in transit by encryption and robustness against protocol-based attacks (such as reputation or store-and-forward attacks). Protection for data at rest is not in scope for SACM. Data protection may be used for both privacy and non-privacy scenarios.

G-009 Topology Flexibility: Both centralized and decentralized (peer-to-peer) information exchange must be supported. Centralized data exchange enables use of a common data format to bridge together data exchange between diverse systems, and can leverage a virtual data store that centralizes and offloads all data access, storage, and maintenance to a dedicated resource. Decentralized data exchange enables simplicity of sharing data between relatively uniform systems, and between small numbers of systems, especially within a single enterprise domain; systems can utilize an already established mutually agreed upon native data format, which may be standard or implementation-specific.

G-010 Data Isolation: A method for partitioning of data must be supported, to accommodate considerations such as geographic, regulatory, overlay boundaries and federation, where an organization may want to differentiate between information that can be shared outside its own domain and information that cannot. As with the requirement for data integrity, this method is required to be available (i.e. all data-handling components must support it), but is not required to be used in all cases.

G-011 Modularity: Announcement and negotiation of functional capabilities (such as authentication protocols, authorization schemes, data models, transport protocols, etc.) must be supported, enabling a SACM component to make inquiries about the capabilities of other components in the SACM ecosystem.

G-012 Versioning and Backward Compatibility: Announcement and negotiation of versions, includsive of exisiting capabilities (such as transport protocols, data models, specific attributes within data models, standar attribute expression sets, etc.) must be supported. Negotiation for both versioning and capability negotiation is needed to accommodate future growth and ecosystems with mixed capabilities.

G-013 Discovery: The solution must provide a mechanism for components to discover what information is available across the ecosystem (i.e. a method for cataloging data available in the ecosystem and advertising it to consumers), and where to go to get a specific piece of that information. For example, providing a method by which a node can locate the advertised information so that

consumers do not have to have a priori knowledge to find available information.

G-014 Synchronization: Request and response operations must be timestamped, and published information must capture time of publication. Actions or decisions based on time-sensitive data (such as user logon/logoff, endpoint connection/disconnection, endpoint behavior events, etc.) are all predicated on a synchronized understanding of time. A method for detecting and reporting time discrepancies must be provided.

G-015 Collection separation: The request for a data item must include enough information to properly identify the item to collect, but the request shall not be a command to directly execute nor directly applied as arguments to a command. The purpose of this requirement is primarily to reduce the potential attack vectors, but has the additional benefit of abstracting the request for collection from the collection method thereby allowing more flexibility in how collection is implemented.

G-016 Collection composition A collection request can be composed of other collection requests (which yield collected values). This must be able to be expressed as part of the collection request so that these references can be resolved at the point of collection without having to interact with the requester.

## 2.2. Requirements based on Use Cases

This section describes the requirements that may apply to information models, data models, protocols or transports as identified by the use cases in [I-D.ietf-sacm-use-cases] and referenced by the section numbers from that draft.

REQ-001 Attribute Dictionary: Use Cases in the whole of Section 2 describe the need for an Attribute Dictionary. With SACM's scope focused on Posture Assessment, the attribute collection and aggregation must have a well understood set of attributes inclusive of their meaning or usage intent.

REQ-002 Information Model: Use Case 2.1.1 describes the need for an Information Model to drive content definition. As SACM endeavors to reuse already existing standards which may have their own data models defined by instantiating an information model, the data models can be mapped to SACM's information model. See [RFC3444] for a description and distinctions between an information and data model.

REQ-003 Data Model to Protocol mapping: Use Case 2.1.1 describes the need to instantiate a data model that can map to the SACM protocols for posture content operations such as publication, query, change detection and asynchronous notifications.

REQ-004 Endpoint Discovery: Use Case 2.1.2 describes the need to discover endpoints and their composition.

REQ-005 Attribute based query: Use Case 2.1.2 describes the need for the data model to support a query operation based on a set of attributes to facilitate collection of information such as posture assessment, inventory (of endpoints or endpoint components) and configuration checklist. .

REQ-006 Information based query with filtering: Use Case 2.1.3 describes the need for the data model to support the means for the information to be collected through a query mechanism. Furthermore, the query operation requires filtering capabilities to allow for only a subset of information to be retrieved. The query operation may be a synchronous request or asynchronous request.

REQ-007 Asynchronous publication, updates or change modifications with filtering: Use Cases 2.1.3, 2.1.4 and 2.1.5 describe the need for the data model to support the means for the information to be published asynchronously. Similarly, the data model must support the means for a requestor to obtain updates or change modifications asynchronously. Like the query operation, these update notifications can be set up with a filter to allow for only a subset of posture assessment information to be obtained.

REQ-008 Data model scalability: Use Cases 2.1.4 and 2.1.5 describes the need for the data model to support scalability. For example, the query operation may result in a very large set of attributes as well as a large set of targets.

REQ-009 Separation of Collection Request and Collection Action: the data model must distinguish the means to request for a data item to include enough information to properly identify the item to collect but the request could be separate and distinct from the actual method or process used to fulfill the request.

## 2.3. Requirements for the Information Model

It is expected that as applications may produce Posture assessment information, they may share it using a specific data model. Similarly, applications consuming or requesting Posture Assessment information, may require it based on a specific data model. Thus, while there may exist different data models and schemas, they should

adhere to a SACM information model that meets a set of requirements defined in this section.

The specific requirements include:

IM-001 Uniqueness of objects of reference, such as endpoints, IP addresses, etc.

IM-002 Mechanism to resolve or tolerate ambiguity in referents (e.g. same IP address used in two separate networks)

IM-003 Support for rootless searches and wildcard searches

IM-004 Ability to start a search anywhere in the tree, rather than at a specific leaf

IM-005 Data lifetime management (longevity or expiration of data)

IM-006 Data ephemerality (update vs. notify)

IM-007 Looseness of coupling between producer and consumer

IM-008 Ability to identify data from a specific producer

IM-009 Metadata cardinality - single-valued vs. multi-valued

IM-010 Capability negotiation - what data types and schemas are supported

IM-011 Provenance of data - for example:

* Publisher identity, classification, trustworthiness, authoritativeness

* Freshness of data

* Method by which data was generated (i.e. self-reported, reported by aggregator, result of scan, etc.)

* Location of data

* Delta results vs. total results

IM-012 Freshness: Published data must be associated with the time of origination - separately from the time of publication required in G-014 - so consumers can make decisions about the relevance of the data based on its currency and/or age.

## 3. Acknowledgements

The authors would like to thank Barbara Fraser, Jim Bieda and Adam Montville for reviewing and contributing to this draft.

## 4. IANA Considerations

This memo includes no request to IANA.

## 5. Security Considerations

This document defines the requirements for SACM. As such, it is expected that several data models, protocols and transports may be defined or reused from already existing standards. This section will highlight security considerations that may apply to SACM based on the architecture and standards applied in SACM.

To address security and privacy considerations, the data model, protocols and transport must consider authorization based on consumer function and privileges, to only allow authorized consumers and providers to access specific information being requested or published.

To enable federation across multiple entities (such as across organizational or geographic boundaries) authorization must also extend to infrastructure elements themselves, such as central controllers / brokers / data repositories.

In addition, authorization needs to extend to specific information or resources available in the environment. In other words, authorization should be based on both subject (the information requestor) and object (the information requested). The method by which this authorization is applied is unspecified.

## 6. References

### 6.1. Normative References

[I-D.ietf-sacm-terminology]
Waltermire, D., Montville, A., Harrington, D., and N. Cam-Winget, "Terminology for Security Assessment", draft-ietf-sacm-terminology-05 (work in progress), August 2014.

[I-D.ietf-sacm-use-cases]
Waltermire, D. and D. Harrington, "Endpoint Security Posture Assessment - Enterprise Use Cases", draft-ietf-sacm-use-cases-07 (work in progress), April 2014.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

### 6.2. Informative References

[RFC3444] Pras, A. and J. Schoenwaelder, "On the Difference between Information Models and Data Models", RFC 3444, January 2003.

[RFC5209] Sangster, P., Khosravi, H., Mani, M., Narayan, K., and J. Tardo, "Network Endpoint Assessment (NEA): Overview and Requirements", RFC 5209, June 2008.

Authors' Addresses

Nancy Cam-Winget
Cisco Systems
3550 Cisco Way
San Jose, CA 95134
US

Email: ncamwing@cisco.com

Lisa Lorenzin
Juniper Networks
3614 Laurel Creek Way
Durham, NC 27712
US

Email: llorenzin@juniper.net