sacm
Internet-Draft
Intended status: Standards Track
Expires: January 26, 2020

C. Inacio
CMU

July 25, 2019

SACM Information Model
draft-inacio-sacm-infomodel-00

Abstract

This defines the information model for the Security Automation and Continuous Monitoring (SACM) standards. The working group faces a set of complex issues when trying to define an information model that complicates this effort:

- There are many standards in the SACM space which are not interoperable

- There exists an extremely large and diverse set of data types which are desirable to exchange

- Many data types depend on the operating systems from which they are collected; making a universal typing harder

- A goal of SACM is to cover a diverse set of system types

These complex needs create a information model which is difficult to unify within the environment. Instead, this information model design is focused on minimum needed functionality with the desire to include a type system design into the information model allowing for easy expandability. It is envisioned that this information model will serve the following purposes:

- Enough well specified elements in order to exchange key data fields between systems

- Sufficient typing system to expand key fields over time and use of a registry to standardize common expansions

- Meta information such that compplete information exchange using various other formats understood by all parties can be used as needed to exchange complete records on demand

- Sufficient action verbs defined to allow orchestration between various systems to allow unified control of federated components

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

The set of elements which are desired to standarize are the subset of data elements used within the SACM standards and related standards. To this end, the core capability to reasonably identify a network end point and minimally describe an event along with enough information that two parties involved in the communication may determine a way forward for further information exchange. The minimal set of activity and endpoint identifiers will allow parties participating in SACM communications to effectively search their respecitive data stores for relevent and related information and respond to queries or accept events in kind.

This information model is intended to describe a minimal number of elements which enable this functionality, but also sufficiently describe the attributes which can define those elements. This combination of information intends to provide enough meta information about information elements to allow both in protocol definition of types in possible data models as well as clear construction of future standardized element definitions. Conversely, this information model is not attempting to define all possible information elements that need to be exchanged. Many information elements, especially those related to host monitoring, are heavily related to the operating system and related software for proper context - beyond the initial scope of this standard.

1.1. Conventions and Terminology

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 BCP 14 [RFC2119][RFC8174] when, and only when, they appear in all capitals, as shown here.

Additionally, the key words "*MIGHT*", "*COULD*", "*MAY WISH TO*", "*WOULD PROBABLY*", "*SHOULD CONSIDER*", and "*MUST (BUT WE KNOW YOU WON'T)*" in this document are to interpreted as described in RFC 6919 [RFC6919].

2. Minimal Needed Information Elements

IP Address, hostname, time/date, SWID/CoSWID ID's, firmware versions, serial number, MAC address, certificate ID

3. Information Element Metadata

name, basic_data_type, octet_length, data_use_type (label, counter, gauge), description, std/vendor type, structure/composite

The following fields are defined in the set of metadata about each information element

name:
A descriptive but concise name to be used for human understanding

basic data type:
A fundamental data type supported by the this information model. The predefined types include unsigned integers, signed integers, octet array, string, IP addresses, MAC addresses

octet length:
The number of octets maximally used for this information

data use type:
This refines the basic data type expressing the usage of the value. For example, some integers represent mathematical values and may be added together (counts for example) while some things may be expressed as an integer, but are really a type of label (e.g. IP address)

description:
A longer textual description of this data type

registration domain:
The domain in which this information element is defined.

composite structure:
The definition of the composite structure of following elements, e.g. list, set, map

3.1. Information Elements

3.1.1. IPv4 Address

Field	Value
Name	IPv4
Basic data type	32-bit unsigned integer
Octet length	4
Data use type	Label
Description	An Internet Protocol version 4 address
Registration domain	standard
Composite structure	N/A
Comments	

3.1.2. IPv6 Address

Field	Value
Name	IPv6
Basic data type	octet array
Octet length	16
Data use type	Label
Description	An Internet Protocol version 6 address
Registration domain	standard
Composite structure	N/A
Comments	

3.1.3. Hostname

Field	Value
Name	Hostname
Basic data type	string
Octet length	up to 256
Data use type	Label
Description	Fully qualified domain name of endpoint system
Registration domain	standard
Composite structure	N/A
Comments	

3.1.4. AssettID

Field	Value
Name	AssettID
Basic data type	string
Octet length	up to 256
Data use type	Label
Description	AssettID of topic assett
Registration domain	standard
Composite structure	N/A
Comments	

3.1.5. MACAddress

Field	Value
Name	MACAddress
Basic data type	string
Octet length	6
Data use type	Label
Description	IEEE 802 Hardware Address
Registration domain	standard
Composite structure	N/A
Comments	

3.1.6. Timestamp

Field	Value
Name	timestamp
Basic data type	ISO time formatted string
Octet length	variable
Data use type	time/date
Description	time date string
Registration domain	standard
Composite structure	N/A
Comments	

3.1.7. Action

Field	Value
Name	Action
Basic data type	enumeration
Octet length	2
Data use type	label
Description	
Registration domain	standard
Composite structure	
Comments	RunAssessment, AssessmentResult, Subscribe, PubEvent,

3.1.8. Action Parameters

Field	Value
Name	Action Parameters
Basic data type	list
Octet length	variable
Data use type	variable
Description	parameters for the action command, defined per action command
Registration domain	standard
Composite structure	list
Comments	

3.1.9. AdditionalDataType

Field	Value
Name	AdditionalDataType
Basic data type	16-bit integer
Octet length	2
Data use type	label
Description	An enumeration of registered additional data types that can be contained in the AdditionalData field
Registration domain	standard
Composite structure	N/A
Comments	

3.1.10. AdditionalData

Field	Value
Name	AdditionalData
Basic data type	octet-array
Octet length	variable
Data use type	opaque
Description	This is an envelope to contain other standardized data exchange formats
Registration domain	standard
Composite structure	N/A
Comments	formats like OVAL or IF-MAP may be contained in here

3.1.11. Extra

[ed: remove before publication]

Field	Value
Name	
Basic data type	
Octet length	
Data use type	
Description	
Registration domain	standard
Composite structure	
Comments	

4. Updates

- 25-July-2019 - initial document

5. IANA Considerations

This will create a IANA registery of elements, eventually. IANA language to be added

6. Security Considerations

To be completed.

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>.

[RFC6919] Barnes, R., Kent, S., and E. Rescorla, "Further Key Words for Use in RFCs to Indicate Requirement Levels", RFC 6919, DOI 10.17487/RFC6919, April 2013, <https://www.rfc-editor.org/info/rfc6919>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

Appendix A. Acknowledgements

The contributions of the SACM working group have greatly impacted the thinking presented here. In particular, we wish to thank Bill Munyan, Adam Monteville, and Henk Birkholz.

Author's Address

Christopher Inacio
Carnegie Mellon University
4500 5th Ave.
Pittsburgh PA 15213
United States

Email: inacio@cert.org