

SACM Working Group
Internet-Draft
Intended status: Informational
Expires: September 14, 2017

H. Birkholz
Fraunhofer SIT
J. Lu
Oracle Corporation
J. Strassner
Huawei Technologies
N. Cam-Winget
Cisco Systems
March 13, 2017

Security Automation and Continuous Monitoring (SACM) Terminology draft-ietf-sacm-terminology-12

Abstract

This memo documents terminology used in the documents produced by SACM (Security Automation and Continuous Monitoring).

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 September 14, 2017.

Copyright Notice

Copyright (c) 2017 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 (<http://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
2.	Terms and Definitions	2
3.	IANA Considerations	21
4.	Security Considerations	21
5.	Acknowledgements	21
6.	Change Log	21
7.	Contributors	24
8.	Informative References	25
Appendix A.	The Attic	26
	Authors' Addresses	27

[1.](#) Introduction

Our goal with this document is to improve our agreement on the terminology used in documents produced by the IETF Working Group for Security Automation and Continuous Monitoring. Agreeing on terminology should help reach consensus on which problems we're trying to solve, and propose solutions and decide which ones to use.

[2.](#) Terms and Definitions

This section describes terms that have been defined by other RFC's and defines new ones. The predefined terms will reference the RFC and where appropriate will be annotated with the specific context by which the term is used in SACM.

Assertion: Defined by the ITU in [[X.1252](#)] as "a statement made by an entity without accompanying evidence of its validity". In the context of SACM, an assertion is the output of a SACM component in the form of a statement (including metadata about the data source and data origin, e.g. time stamps). While the validity of an assertion cannot be verified without, for example, an additional attestation protocol, an assertion (and therefore a statement, respectively) can be accompanied by evidence of the validity of its metadata provided by a SACM component.

Assessment: Defined in [[RFC5209](#)] as "the process of collecting posture for a set of capabilities on the endpoint (e.g., host-based firewall) such that the appropriate validators may evaluate the posture against compliance policy."

An assessment is a specific workflow that incorporates the SACM tasks discovery, collection and evaluation. A prominent instance

of the assessment workflow is illustrated in the Vulnerability Assessment Scenario [[I-D.ietf-sacm-vuln-scenario](#)].

Asset: Defined in [[RFC4949](#)] as "a system resource that is (a) required to be protected by an information system's security policy, (b) intended to be protected by a countermeasure, or (c) required for a system's mission". In the scope of SACM, an asset can be composed of other assets. Examples of Assets include: Endpoints, Software, Guidance, or X.509 public key certificates. An asset is not necessarily owned by an organization.

Asset Management: The process by which assets are provisioned, updated, maintained and deprecated.

Attribute: Defined in [[RFC5209](#)] as "data element including any requisite meta-data describing an observed, expected, or the operational status of an endpoint feature (e.g., anti-virus software is currently in use)." In the context of SACM, attributes are "atomic" information elements and an equivalent to attribute-value-pairs. Attributes can be components of Subjects.

Authentication: Defined in [[RFC4949](#)] as "the process of verifying a claim that a system entity or system resource has a certain attribute value."

Authorization: Defined in [[RFC4949](#)] as "an approval that is granted to a system entity to access a system resource."

Broker: A broker is a specific controller type that contains control plane functions to provide and/or connect services on behalf of other SACM components via interfaces on the control plane. A broker may provide, for example, authorization services and find, upon request, SACM components providing requested services.

Capability: In [[I-D.ietf-i2nsf-terminology](#)] a capability "defines a set of features that are available from a managed entity. Examples of "managed entities" are NSFs and Controllers, where NSF Capabilities and Controller Capabilities define functionality of an NSF and a Controller that may, but do not have to, be used, respectively. All Capabilities are announced through the Registration Interface."

In the context of SACM, the extent of a SACM component's ability is enabled by the functions it is composed of. Capabilities are announced by a SACM component via the SACM component registration task and can be discovered by or negotiated with other SACM components. For example, the capability of a SACM Provider may be

to provide endpoint management data, or only a subset of that data.

The SACM Vulnerability Assessment Scenario [[I-D.ietf-sacm-vuln-scenario](#)] defines the terms Endpoint Management Capabilities, Vulnerability Management Capabilities, and Vulnerability Assessment Capabilities, which illustrate specific sets of SACM capabilities, which are required to conduct workflows illustrated by the scenario definition.

Collection Result: Information about a target endpoint that is produced by a collector conducting a collection task. A collection result is composed as one or more content-elements.

Collection Task: The task by which endpoint attributes and/or corresponding attribute values about a target endpoint are collected. The collection tasks are targeted at specific target endpoints and therefore are targeted tasks.

There are three types of frequency collection tasks can be conducted with:

ad-hoc, e.g. triggered by a specific event or a query

scheduled, e.g. in regular intervals, such as every minute or weekly

continuously, e.g. a network behavior observation

There are three types of collection methods, each requiring an appropriate set of functions to be included in the SACM component conducting the collection task:

Self-Reporting: A SACM component located on the target endpoint itself conducts the collection task.

Remote-Acquisition: A SACM component located on an Endpoint different from the target endpoint conducts the collection task via interfaces available on the target endpoint, e.g. SNMP/NETCONF or WMI.

Behavior-Observation: A SACM component located on an Endpoint different from the target endpoint observes network traffic related to the target endpoint and conducts the collection task via interpretation of that network traffic.

Collector: A piece of software that acquires information about one or more target endpoints by conducting collection tasks. A

collector provides acquired information in the form of collection results via a set of registered capabilities that can be discovered by other SACM components.

A collector can be distributed across multiple endpoints, e.g. across a target endpoint and a SACM component. The separate parts of the collector can communicate with a specialized protocol, such as PA-TNC [[RFC5792](#)]. At least one part of a distributed collector has to take on the role of a provider of information by providing SACM interfaces to propagate capabilities and to provide SACM content in the form of collection results.

Configuration: A non-volatile subset of the endpoint attributes of a (target) endpoint that is intended to be unaffected by a normal reboot-cycle. Configuration is a type of imperative guidance that is stored in files (files dedicated to contain configuration and/or files that are software components), directly on block devices, or on specific hardware components that can be accessed via corresponding software components. Modification of configuration can be conducted manually or automatically via management (plane) interfaces that support management protocols, such as SNMP or WMI. A change of configuration can occur during both run-time and down-time of an endpoint. It is common practice to schedule a change of configuration during or directly after the completion of a boot-cycle via corresponding software components located on the target endpoint itself.

Examples: The static association of an IP address and a MAC address in a DHCP server configuration, a directory-path that identifies a log-file directory, a registry entry.

Configuration Drift: The discrepancy of a target endpoint's endpoint attributes representing the actual composition of a target endpoint (is-state) and its intended composition (should-state) in the scope of a valid target endpoint composition (could-state) due to continuous alteration of a target endpoint's composition over time. Configuration drift exists for both hardware components and software components. Typically, the frequency and scale of configuration drift of software components is significantly higher than the configuration drift of hardware components.

Consumer: A consumer is a SACM role that is assigned to a SACM component that contains functions to receive information from other SACM components.

Content Element: Content elements constitute the payload data (SACM content) transferred via statement Subjects emitted by providers of

information. Every content element Subject includes a specific content Subject and a corresponding content metadata Subject.

Content Metadata: Data about content Subjects. Every content-element includes a content metadata Subject. The Subject can include any information element that can annotate the content transefered. Examples include time stamps or data provenance Subjects.

Control Plane: Typically used as a term in the context of routing, e.g. [[RFC6192](#)]. In the context of SACM, the control plane is an architectural component providing common control functions to all SACM components, including authentication, authorization, (capability) discovery or negotiation, registration and subscription. The control plane orchestrates the flow on the data plane according to imperative guidance (i.e. configuration) received via the management plane. SACM components with interfaces to the control plane have knowledge of the capabilities of other SACM components within a SACM domain.

Controller: A controller is a SACM role that is assigned to a SACM component containing control plane functions that manage and facilitate information sharing or execute on security functions. There are three types of SACM controllers: Broker, Proxy, and Repository. Depending on its type, a controller can also contain functions that have interfaces on the data plane.

Data Confidentiality: Defined in [[RFC4949](#)] as "the property that data is not disclosed to system entities unless they have been authorized to know the data."

Data In Motion: Data that is being transported via a network; also referred to as "Data in Transit" or "Data in Flight". Data in motion requires a data model to transfer the data using a specific encoding. Typically, data in motion is serialized (marshalling) into a transport encoding by a provider of information and deserialized (unmarshalling) by a consumer of information. The termination points of provider of information and consumer of information data is transferred between are interfaces. In regard to data in motion, the interpretation of the roles consumer of information and provider of information depends on the corresponding OSI layer (e.g. on layer2: between interfaces connected to a broadcast domain, on layer4: between interfaces that maintain a TCP connection). In the context of SACM, consumer of information and provider of information are SACM components.

The SACM architecture and corresponding models focus on data in motion.

Data At Rest: Data that is stored in a repository. Data at rest requires a data model to encode the data to be stored. In the context of SACM, data at rest located on a SACM component can be provided to other SACM components via discoverable capabilities.

In the context of SACM, data models for data at rest are out of scope.

Data Integrity: Defined in [[RFC4949](#)] as "the property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner."

Data Origin: One or more properties (i.e. endpoint attributes) that enable a SACM component to identify the SACM component that initially acquired or produced data about a (target) endpoint (e.g. via collection from a data source) and made it available to a SACM domaini via a SACM statement. Data Origin can be expressed by an endpoint label information element (e.g. to be used as metadata in statement).

Data Plane (fix statement): Typically used as a term in the context of routing (and used as a synonym for forwarding plane, e.g. [[RFC6192](#)]). In the context of SACM, the data plane is an architectural component providing operational functions to enable a SACM component to provide and consume SACM statements and therefore SACM content (the "payload"). The data plane is used to conduct distributed SACM tasks by transporting SACM content using transporting encodings and corresponding operations defined by SACM data models.

Data Provenance: A historical record of the sources, origins and evolution of data that is influenced by inputs, entities, functions and processes. In the context of SACM, data provenance is expressed as metadata that identifies SACM statements and corresponding content elements a new statement is created from. In a downstream process, this references can cascade, creating a data provenance tree that enables SACM components to trace back the original data sources involved in the creation of SACM statements and take into account their characteristics and trustworthiness.

Data Source: One or more properties (i.e. endpoint attributes) that enable a SACM component to identify - and potentially characterize - a (target) endpoint that is claimed to be the original source of endpoint attributes in a SACM statement. Data Source can be expressed as metadata by an endpoint label information element or a corresponding subject of identifying endpoint attributes.

Endpoint: Defined in [[RFC5209](#)] as "any computing device that can be connected to a network. Such devices normally are associated with a particular link layer address before joining the network and potentially an IP address once on the network. This includes: laptops, desktops, servers, cell phones, or any device that may have an IP address."

To further clarify the [[RFC5209](#)] definition, an endpoint is any physical or virtual device that may have a network address. Note that, network infrastructure devices (e.g. switches, routers, firewalls), which fit the definition, are also considered to be endpoints within this document.

Physical endpoints are always composites that are composed of hardware components and software components. Virtual endpoints are composed entirely of software components and rely on software components that provide functions equivalent to hardware components.

The SACM architecture differentiates two essential categories of endpoints: Endpoints whose security posture is intended to be assessed (target endpoints) and endpoints that are specifically excluded from endpoint posture assessment (excluded endpoints).

Based on the definition of an asset, an endpoint is a type of asset.

Endpoint Attribute: In the context of SACM, endpoint attributes are information elements that describe an endpoint characteristic of a target endpoint. Endpoint Attributes typically constitute Attributes that can be bundled into Subject (e.g. information about a specific network interface can be represented via a set of multiple AVP).

Endpoint Characteristic: The state, configuration and composition an endpoint is in, including observable behavior, e.g. sys-calls, log-files, or PDU emission on a network.

Endpoint Characterization: The task by which a profile is composed out of endpoint attributes that describe the desired or expected posture of a type or class of target endpoints or even an individual target endpoint. The result of this task is an endpoint profile that is required as declarative guidance for the tasks of endpoint classification or posture assessment.

Endpoint Classification: The task by which a discovered target endpoint is classified. Endpoint classification requires declarative guidance in the form of an endpoint profile, discovery

results and potentially collection results. Types, classes or the characteristics of an individual target endpoint are defined via endpoint profiles.

Endpoint Label: In a SACM domain, every endpoint can be identified by an endpoint label. There are two prominent uses of endpoint labels in a SACM domain: to identify SACM components and to identify Target Endpoints. Both endpoint labels can be used in SACM content or in content metadata:

SACM Components are identified by: SACM component label / Data Origin

Target Endpoints are identified by: TE label / Data Source

An endpoint label is expressed as an artificially created ID that references a distinct set of identifying attributes (Target Endpoint Identifier). A target endpoint label is unique in a SACM domain and created by a SACM component that provides the appropriate function as a capability.

Endpoint Management Capabilities: An enterprise IT department's ability to manage endpoint identity, endpoint information, and associated metadata on an ongoing basis.

Evaluation Task: The task by which endpoint attributes are evaluated.

Evaluation Result: The resulting value from having evaluated a set of posture attributes.

Event: The change of a target endpoint characteristics at a specific point in time. In the context of SACM, an event is a statement (and therefore data in motion) that includes the new target endpoint characteristics and optional also the past ones, annotated with corresponding metadata (most prominently, the collection time of the data that constitutes the observation of the event regarding the target endpoint).

Excluded Endpoint: A specific designation, which is assigned to an endpoint that is not supposed to be the subject of a collection task (and therefore is not a target endpoint). Typically but not necessarily, endpoints that contain a SACM component (and are therefore part of the SACM domain) are designated as excluded endpoints. Target endpoints that contain a SACM component cannot be designated as excluded endpoints and are part of the SACM domain.

Expected Endpoint State: The required state of an endpoint that is to be compared against. Sets of expected endpoint states are transported as declarative guidance in target endpoint profiles via the management plane. This, for example, can be a policy, but also a recorded past state. An expected state is represented can be represented via an Attribute or an Subject that represents a set of multiple attribute value pairs.

SACM Function: A behavioral aspect or capacity of a particular SACM component, which belies that SACM component's purpose. For example, a SACM function with interfaces on the control plane can provide a brokering function to other SACM components. Via data plane interfaces, a function can act as a provider and/or as a consumer of information. SACM functions can be propagated as the capabilities of a SACM component and can be discovered by or negotiated with other SACM components.

Guidance: Input instructions to processes, such as automated device management or remediation, and SACM tasks, such as collection or evaluation. Guidance influences the behavior of a SACM component and is considered content of the management plane. In the context of SACM, guidance is machine-readable and can be manually or automatically generated or provided. Typically, the tasks that provide guidance to SACM components have a low-frequency and tend to be be sporadic.

There are two types of guidance:

Declarative Guidance: defines the configuration or state an endpoint is supposed to be in--without providing specific actions or methods to produce that desired state. Examples include Target Endpoint Profiles or network topology based requirements.

Imperative Guidance: prescribes specific actions to be conducted or methods to be used in order to achieve an outcome. Examples include a targeted Collection Task or the IP-Address of a SACM Component that provides a registration function.

Hardware Component: Hardware components are the distinguishable physical components that compose an endpoint. The composition of an endpoint can be changed over time by adding or removing hardware components. In essence, every physical endpoint is potentially a composite of multiple hardware components, typically resulting in a hierarchical composition of hardware components. The composition of hardware components is based on interconnects provided by specific hardware types (e.g. mainboard is a hardware type that provides local busses as an interconnect). In general, a hardware component can be distinguished by its serial number.

Occasionally, hardware components are referred to as power sucking aliens.

Hardware Inventory: The list of hardware components that compose a specific endpoint representing its hardware configuration.

Hardware Type: Hardware types define specific and distinguishable categories of hardware components that can be part of endpoints, e.g. CPU or 802.11p interface. Typically, hardware types can be distinguished by their vendor assigned names, names of standards used, or a model name.

Information Element: A representation of information about physical and virtual "objects of interests". Information elements are the building blocks that constitute the SACM information model. In the context of SACM, an information element that expresses a single value with a specific name is referred to as an Attribute (analogous to an attribute-value-pair). A set of attributes that is bundled into a more complex composite information element is referred to as a Subject. Every information element in the SACM information model has a unique name. Endpoint attributes or time stamps, for example, are represented as information elements in the SACM information model.

Information Model: An information model is an abstract representation of data, their properties, relationships between data and the operations that can be performed on the data. While there is some overlap with a data model, [\[RFC3444\]](#) distinguishes an information model as being protocol and implementation neutral whereas a data model would provide such details. The purpose of the SACM information model is to ensure interoperability between SACM data models (that are used as transport encoding) and to provide a standardized set of information elements for communication between SACM components.

Interaction Model: The definition of specific sequences regarding the exchange of messages (data in motion), including, for example, conditional branching, thresholds and timers. An interaction model, for example, can be used to define operations, such as registration or discovery, on the control plane. A composition of data models for data in motion and a corresponding interaction model is a protocol.

Internal Collector: Internal Collector: a collector that runs on a target endpoint to acquire information from that target endpoint. (TBD: An internal collector is not a SACM component and therefore not part of a SACM domain).

Management Plane: An architectural component providing common functions to steer the behavior of SACM components, e.g. its behavior on the control plane. Prominent examples include: modification of the configuration of a SACM component or updating a target endpoint profile that resides on an evaluator. In essence, guidance is transported via the management plane. Typically, a SACM component can fulfill its purpose without continuous input from the management plane. In contrast, without continuous availability of control plane functions a typical SACM component could not function properly. In general, interaction on the management plane is less frequent and less regular than on the control plane. Input via the management plane can be manual (e.g. via a CLI), or can be automated via management plane functions that are part of other SACM components.

Metadata: Data about data. In the SACM information model, data is referred to as Content. Metadata about the content is referred to as Content-Metadata, respectively. Content and Content-Metadata are combined into Subjects called Content-Elements in the SACM information model. Some information elements defined by the SACM information model can be part of the Content or the Content-Metadata. Therefore, if an information element is considered data or data about data depends on which kind of Subject it is associated with. The SACM information model also defines metadata about the data origin via the Subject Statement-Metadata. Typical examples of metadata are time stamps, data origin or data source.

Network Address: Network addresses are layer specific and follow layer specific address schemes. Each interface of a specific layer can be associated with one or more addresses appropriate for that layer. There is no guarantee that an address is globally unique. In general, there is a scope to an address in which it is intended to be unique.

Examples include: physical Ethernet port with a MAC address, layer 2 VLAN interface with a MAC address, layer 3 interface with multiple IPv6 addresses, layer 3 tunnel ingress or egress with an IPv4 address.

Network Interface: An endpoint is connected to a network via one or more network interfaces. Network interfaces can be physical or virtual. Network interfaces of an endpoint can operate on different layers, most prominently what is now commonly called layer 2 and 3. Within a layer, interfaces can be nested.

On layer 2, a root interface is typically associated with a physical interface port and nested interfaces are virtual interfaces. In the case of a virtual endpoint, a root interface

can be a virtual interface. Virtual layer 2 interfaces of one or more endpoints can also constitute an aggregated group of links that act as one.

On layer 3, nested interfaces typically constitute virtual tunnels or virtual (mesh) networks.

Examples include: physical Ethernet port, layer 2 VLAN interface, a MC-LAG setup, layer 3 Point-to-Point tunnel ingress or egress.

Posture: Defined in [[RFC5209](#)] as "configuration and/or status of hardware or software on an endpoint as it pertains to an organization's security policy."

This term is used within the scope of SACM to represent the configuration and state information that is collected from a target endpoint in the form of endpoint attributes (e.g. software/hardware inventory, configuration settings, dynamically assigned addresses). This information may constitute one or more posture attributes.

Posture Attributes: Defined in [[RFC5209](#)] as "attributes describing the configuration or status (posture) of a feature of the endpoint. A Posture Attribute represents a single property of an observed state. For example, a Posture Attribute might describe the version of the operating system installed on the system."

Within this document this term represents a specific assertion about endpoint configuration or state (e.g. configuration setting, installed software, hardware) represented via endpoint attributes. The phrase "features of the endpoint" highlighted above refers to installed software or software components.

Provider: A provider is a SACM role that is assigned to a SACM component that contains functions to provide information to other SACM components.

Proxy: A proxy is a specific controller type that provides data plane and control plane functions, information, or services on behalf of another component, which is not directly participating in the SACM architecture.

Repository: A repository is a specific controller type that contains functions to consume, store and provide information of a particular kind - typically data transported on the data plane, but potentially also data and metadata from the control and management plane. A single repository may provide the functions

of more than one specific repository type (i.e. configuration baseline repository, assessment results repository, etc.)

SACM Component: A component is defined in [\[I-D.ietf-i2nsf-terminology\]](#) as "an encapsulation of software that communicates using Interfaces. A Component may be implemented by hardware and/or Software, and be represented using a set of classes. In general, a Component encapsulates a set of data structures as well as a set of algorithms that implement the functions that it provides."

In the context of SACM, a set of SACM functions composes a SACM component. A SACM component conducts SACM tasks, acting on control plane, data plane and/or management plane via corresponding SACM interfaces. SACM defines a set of standard components (e.g. a collector, a broker, or a data store). A SACM component contains at least a basic set of control plane functions and can contain data plane and management plane functions. A SACM component residing on an endpoint assigns one or more SACM roles to the corresponding endpoint due to the SACM functions it is composed of. A SACM component "resides on" an endpoint and an endpoint "contains" a SACM component, correspondingly. For example, a SACM component that is composed solely of functions that provide information would only take on the role of a provider.

SACM Component Discovery: The task of brokering appropriate SACM components according to their capabilities or roles on request.

Input: Query

Output: a list of SACM components including metadata

SACM Component Label: A specific endpoint label that is used to identify a SACM component. In content-metadata, this label is called data origin.

SACM Content: The payload provided by SACM components to the SACM domain on the data plane. SACM content includes the SACM data models.

SACM Domain: Endpoints that include a SACM component compose a SACM domain. (To be revised, additional definition content TBD, possible dependencies to SACM architecture)

SACM Interface: An interface is defined in [\[I-D.ietf-i2nsf-terminology\]](#) as "A set of operations one object knows it can invoke on, and expose to, another object. This

decouples the implementation of the operation from its specification. An interface is a subset of all operations that a given object implements. The same object may have multiple types of interfaces to serve different purposes."

In the context of SACM, SACM Funktionen provide SACM Interfaces on the management, control, or data plane. Operations a SACM Interface provides are based on corresponding data model defined by SACM. SACM Interfaces are used for communication between SACM components.

SACM Role: A role is defined in [[I-D.ietf-i2nsf-terminology](#)] as "an abstraction of a Component that models context-specific views and responsibilities of an object as separate role objects that can be statically or dynamically attached to (and removed from) the object that the role object describes. This provides three important benefits. First, it enables different behavior to be supported by the same Component for different contexts. Second, it enables the behavior of a Component to be adjusted dynamically (i.e., at runtime, in response) to changes in context, by using one or more Roles to define the behavior desired for each context. Third, it decouples the Roles of a Component from the Applications that use that Component."

In the context of SACM, SACM roles are associated with SACM components and are defined by the set of functions and interfaces a SACM component includes. There are three SACM roles: provider, consumer, and controller. The roles associated with a SACM component are determined by the purpose of the SACM functions and corresponding SACM interfaces the SACM component is composed of.

Security Automation: The process of which security alerts can be automated through the use of different tools to monitor, evaluate and analyze endpoint and network traffic for the purposes of detecting misconfigurations, misbehaviors or threats.

Software Package: A generic software package (e.g. a text editor).

Software Component: A software package installed on an endpoint, including a unique serial number if present (e.g. a text editor associated with a unique license key).

Software Instance: A running instance of the software component (e.g. on a multi-user system, one logged-in user has one instance of a text editor running and another logged-in user has another instance of the same text editor running, or on a single-user system, a user could have multiple independent instances of the same text editor running).

State: A volatile subset endpoint attributes of a (target) endpoint that is affected by a reboot-cycle. Local state is created by the interaction of components with other components via the control plane, via processing data plane payload, or via the functional properties of local hardware and software components. Dynamic configuration (e.g. IP address distributed dynamically via an address distribution and management services, such as DHCP) is considered state that is the result of the interaction with another component that provides configuration via the control plane (e.g. provided by a DHCP server with a specific configuration).

Exmaples: The static association of an IP address and a MAC address in a DHCP server configuration, a directory-path that identifies a log-file directory, a registry entry.

Statement: A statement is a subject defined in the SACM information model.

When a statement is used to provide content to a SACM domain, it is a top-level subject that bundles Content Elements into one subject and includes metadata about the data origin.

Subject: A composite information element. Like Attributes, subjects have a name and are composed of attributes and/or other subjects. Every IE that is part of a subject can have a quantitiy associated with it (e.g. zero-one, none-unbounded). The content IE of a subject can be an unordered or an ordered list.

Supplicant: A SACM component seeking to be authenticated via the control plane for the purpose of participating in a SACM domain.

System Resource: Defined in [[RFC4949](#)] as "data contained in an information system; or a service provided by a system; or a system capacity, such as processing power or communication bandwidth; or an item of system equipment (i.e., hardware, firmware, software, or documentation); or a facility that houses system operations and equipment.

Target Endpoint: A target endpoint is an "endpoint under assessment" (even if it is not actively under assessment at all times) or "endpoint of interest". Every endpoint that is not specifically designated as an excluded endpoint is a target endpoint. A target endpoint is not part of a SACM domain unless it contains a SACM component (e.g. a SACM component that publishes collection results coming from an internal collector).

A target endpoint is similar to a device that is a Target of Evaluation (TOE) as defined in Common Criteria.

Target Endpoint Characterization Record: A set of endpoint attributes about a target endpoint that was encountered in a SACM domain, which are associated with a target endpoint by being included in the corresponding record. A characterization record is intended to be a representation of an endpoint. It cannot be assured that a record distinctly represents a single target endpoint unless a set of one or more endpoint attributes that compose a unique set of identifying endpoint attributes are included in the record. Otherwise, the set of identifying attributes included in a record can match more than one target endpoints, which are - in consequence - indistinguishable to a SACM domain until more qualifying endpoint attributes can be acquired and added to the record. A characterization record is maintained over time in order to assert that acquired endpoint attributes are either about an endpoint that was encountered before or an endpoint that has not been encountered before in a SACM domain. A characterization record can include, for example, acquired configuration, state or observed behavior of a specific target endpoint. Multiple and even conflicting instances of this information can be included in a characterization record by using timestamps and/or data origins to differentiate them. The endpoint attributes included in a characterization record can be used to re-identify a distinct target endpoint over time. Classes or profiles can be associated with a characterization record via the Classification Task in order to guide collection, evaluation or remediation tasks.

Target Endpoint Characterization Task: An ongoing task of continuously adding acquired endpoint attributes to a corresponding record. The TE characterization task manages the representation of encountered target endpoints in the SACM domain in the form of characterization records. For example, the output of a target endpoint discovery task or a collection task can be processed by the characterization task and added to the record. The TE characterization Task also manages these representations of target endpoints encountered in the SACM domain by splitting or merging the corresponding records as new or more refined endpoint attributes become available.

Input: discovered target endpoint attributes, endpoint attribute collection, existing characterization records

Output: target endpoint characterization records

Target Endpoint Classification Task: The task of associating a class from an extensible list of classes with an endpoint characterization record. TE classes function as imperative and declarative guidance for collection, evaluation, remediation and security posture assessment in general.

Input: endpoint characterization records (without classification), guidance (how to classify a record)

Output: endpoint characterization records (with classification)

Target Endpoint Discovery Task: The ongoing task of detecting previously unknown interaction of a potential target endpoint in the SACM domain. TE Discovery is not directly targeted at a specific target endpoint and therefore an un-targeted task. SACM Components conducting the discovery task as a part of their function are typically distributed and located, for example, on infrastructure components or collect from those remotely via appropriate interfaces. Examples of infrastructure components that are of interest to the discovery task include routers, switches, VM hosting or VM managing components, AAA servers, or servers handling dynamic address distribution.

Input: endpoint attributes acquired via local or remote interfaces

Output: endpoint attributes including metadata such as data source or data origin

Target Endpoint Identifier: The target endpoint discovery task and the collection tasks can result in a set of identifying endpoint attributes added to a corresponding Characterization Record. This subset of the endpoint attributes included in the record is used as a target endpoint identifier, by which a specific target endpoint can be referenced. Depending on the available identifying attributes, this reference can be ambiguous and is a "best-effort" mechanism. Every distinct set of identifying endpoint attributes can be associated with a target endpoint label that is unique in a SACM domain.

Target Endpoint Label: A specific endpoint label that refers to a target endpoint identifier used to identify a specific target endpoint (also referred to as TE label). In content-metadata, this label is called data source.

Target Endpoint Profile: A bundle of expected or desired configurations and states (typically a composition of endpoint attribute value pairs) that can be associated with a target endpoint. The corresponding task by which the association with a

target endpoint takes places is the endpoint classification. The task by which an endpoint profile is created is the endpoint characterization. A type or class of target endpoints is defined within a target endpoint profile, e.g. printer, smartphone, or an office PC.

SACM Task: A SACM task is conducted by one or more SACM functions that reside on a SACM component (e.g. a collection task or endpoint characterization). A SACM task can be triggered by other operations or functions (e.g. a query from another SACM component or an unsolicited push on the data plane due to an ongoing subscription). A task is part of a SACM process chain. A task starts at a given point in time and ends in a deterministic state. With the exception of a collection task, a SACM task consumes SACM statements provided by other SACM components. The output of a task is a result that can be provided (e.g. published) on the data plane. There following tasks are defined by SACM:

Target Endpoint Discovery

Target Endpoint Characterization

Target Endpoint Classification

Collection

Evaluation [TBD]

Information Sharing [TBD]

SACM Component Discovery

SACM Component Authentication [TBD]

SACM Component Authorization [TBD]

SACM Component Registration [TBD]

Timestamps : Defined in [[RFC4949](#)] as "with respect to a data object, a label or marking in which is recorded the time (time of day or other instant of elapsed time) at which the label or marking was affixed to the data object" and as "with respect to a recorded network event, a data field in which is recorded the time (time of day or other instant of elapsed time) at which the event took place.".

This term is used in SACM to describe a recorded point in time at which, for example, an endpoint attribute is created or updated by

a target endpoint and observed, transmitted or processed by a SACM component. Timestamps can be created by target endpoints or SACM components and are associated with endpoint attributes provided or consumed by SACM components. Outside of the domain of SACM components the assurance of correctness of time stamps is typically significantly lower than inside a SACM domain. In general, it cannot be simply assumed that the source of time a target endpoint uses is synchronized or trustworthy.

Vulnerability Assessment: The process of determining whether a set of endpoints is vulnerable according to the information contained in the vulnerability description information.

Vulnerability Description Information: Information pertaining to the existence of a flaw or flaws in software, hardware, and/or firmware, which could potentially have an adverse impact on enterprise IT functionality and/or security. Vulnerability description information should contain enough information to support vulnerability detection.

Vulnerability Detection Data: A type of imperative guidance extracted or derived from vulnerability description information that describes the specific mechanisms of vulnerability detection that is used by an enterprise's vulnerability management capabilities to determine if a vulnerability is present on an endpoint.

Vulnerability Management Capabilities: An enterprise IT department's ability to manage endpoint vulnerabilities and associated metadata on an ongoing basis by ingesting vulnerability description information and vulnerability detection data, and performing vulnerability assessments.

Vulnerability assessment capabilities: An enterprise IT department's ability to determine whether a set of endpoints is vulnerable according to the information contained in the vulnerability description information.

Workflow:

A workflow is a modular composition of tasks. A workflow can contain loops, conditionals, multiple starting points and multiple endpoints. The most prominent workflow in SACM is the assessment workflow.

3. IANA Considerations

This memo includes no request to IANA.

4. Security Considerations

This memo documents terminology for security automation. While it is about security, it does not affect security.

5. Acknowledgements

6. Change Log

Changes from version 00 to version 01:

- o Added simple list of terms extracted from UC draft -05. It is expected that comments will be received on this list of terms as to whether they should be kept in this document. Those that are kept will be appropriately defined or cited.

Changes from version 01 to version 02:

- o Added Vulnerability, Vulnerability Management, xposure, Misconfiguration, and Software flaw.

Changes from version 02 to version 03:

- o Removed [Section 2.1](#). Cleaned up some editing nits; broke terms into 2 sections (predefined and newly defined terms). Added some of the relevant terms per the proposed list discussed in the IETF 89 meeting.

Changes from version 03 to version 04:

- o TODO

Changes from version 04 to version 05:

- o TODO

Changes from version 05 to version 06:

- o Updated author information.
- o Combined "Pre-defined Terms" with "New Terms and Definitions".
- o Removed "Requirements language".

- o Removed unused reference to use case draft; resulted in removal of normative references.
- o Removed introductory text from [Section 1](#) indicating that this document is intended to be temporary.
- o Added placeholders for missing change log entries.

Changes from version 06 to version 07:

- o Added Contributors section.
- o Updated author list.
- o Changed title from "Terminology for Security Assessment" to "Secure Automation and Continuous Monitoring (SACM) Terminology".
- o Changed abbrev from "SACM-Terms" to "SACM Terminology".
- o Added [appendix T](#) The Attic to stash terms for future updates.
- o Added Authentication, Authorization, Data Confidentiality, Data Integrity, Data Origin, Data Provenance, SACM Component, SACM Component Discovery, Target Endpoint Discovery.
- o Major updates to Building Block, Function, SACM Role, Target Endpoint.
- o Minor updates to Broker, Capability, Collection Task, Evaluation Task, Posture.
- o Relabeled Role to SACM Role, Endpoint Target to Target Endpoint, Endpoint Discovery to Endpoint Identification.
- o Moved Asset Targeting, Client, Endpoint Identification to The Attic.
- o Endpoint Attributes added as a TODO.
- o Changed the structure of the Change Log.

Changes from version 07 to version 08:

- o Added Assertion, Collection Result, Collector, Excluded Endpoint, Internal Collector, Network Address, Network Interface, SACM Domain, Statement, Target Endpoint Identifier, Target Endpoint Label, Timestamp.

- o Major updates to Attributes, Broker, Collection Task, Consumer, Controller, Control Plane, Endpoint Attributes, Expected Endpoint State, SACM Function, Provider, Proxy, Repository, SACM Role, Target Endpoint.
- o Minor updates to Asset, Building Block, Data Origin, Data Source, Data Provenance, Endpoint, Management Plane, Posture, Posture Attribute, SACM Component, SACM Component Discovery, Target Endpoint Discovery.
- o Relabeled Function to SACM Function.

Changes from version 08 to version 09:

- o Updated author list.
- o Added Data Plane, Endpoint Characterization, Endpoint Classification, Guidance, Interaction Model, Software Component, Software Instance, Software Package, Statement, Target Endpoint Profile, SACM Task.
- o Removed Building Block.
- o Major updates to Control Plane, Endpoint Attribute, Expected Endpoint State, Information Model, Management Plane.
- o Minor updates to Attribute, Capabilities, SACM Function, SACM Component, Collection Task.
- o Moved Asset Characterization to The Attic.

Changes from version 09 to version 10:

- o Added Configuration Drift, Data in Motion, Data at Rest, Endpoint Management Capability, Hardware Component, Hardware Inventory, Hardware Type, SACM Interface, Target Endpoint Characterization Record, Target Endpoint Characterization Task, Target Endpoint Classification Task, Target Endpoint Discovery Task, Vulnerability Description Information, Vulnerability Detection Data, Vulnerability Management Capability, Vulnerability Assessment
- o Added references to i2nsf definitions in Capability, SACM Component, SACM Interface, SACM Role.
- o Added i2nsf Terminology I-D Reference.
- o Major Updates to Endpoint, SACM Task, Target Endpoint Identifier.

- o Minor Updates to Guidance, SACM Component Discovery, Target Endpoint Label, Target Endpoint Profile.
- o Relabeled SACM Task
- o Removed Target Endpoint Discovery

Changes from version 10 to version 11:

- o Added Content Element, Content Metadata, Endpoint Label, Information Element, Metadata, SACM Component Label, Workflow.
- o Major Updates to Assessment, Capability, Collector, Endpoint Management Capabilities, Guidance, Vulnerability Assessment Capabilities, Vulnerability Detection Data, Vulnerability Assessment Capabilities.
- o Minor updates to Collection Result, Control Plane, Data in Motion, Data at Rest, Data Origin, Network Interface, Statement, Target Endpoint Label.
- o Relabeled Endpoint Management Capability, Vulnerability Management Capability, Vulnerability Assessment.

Changes from version 11 to version 12:

- o Added Configuration, Endpoint Characteristic, Event, SACM Content, State, Subject.
- o Major Updates to Assertion, Data in Motion, Data Provenance, Data Source, Interaction Model.
- o Minor Updates to Attribute, Control Plane, Data Origin, Data Provenance, Expected Endpoint State, Guidance, Target Endpoint Classification Task, Vulnerability Detection Data.

[7.](#) Contributors

David Waltermire
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20877
USA

Email: david.waltermire@nist.gov

Adam W. Montville
Center for Internet Security
31 Tech Valley Drive
East Greenbush, NY 12061
USA

Email: adam.w.montville@gmail.com

David Harrington
Effective Software
50 Harding Rd
Portsmouth, NH 03801
USA

Email: ietfdbh@comcast.net

Brian Ford
Lancope
3650 Brookside Parkway, Suite 500
Alpharetta, GA 30022
USA

Email: bford@lancope.com

Merike Kaeo
Double Shot Security
3518 Fremont Avenue North, Suite 363
Seattle, WA 98103
USA

Email: merike@doubleshotsecurity.com

[8.](#) Informative References

[I-D.ietf-i2nsf-terminology]

Hares, S., Strassner, J., Lopez, D., Xia, L., and H. Birkholz, "Interface to Network Security Functions (I2NSF) Terminology", [draft-ietf-i2nsf-terminology-03](#) (work in progress), March 2017.

[I-D.ietf-sacm-vuln-scenario]

Coffin, C., Cheikes, B., Schmidt, C., Haynes, D., Fitzgerald-McKay, J., and D. Waltermire, "SACM Vulnerability Assessment Scenario", [draft-ietf-sacm-vuln-scenario-02](#) (work in progress), September 2016.

[RFC3444] Pras, A. and J. Schoenwaelder, "On the Difference between Information Models and Data Models", [RFC 3444](#), DOI 10.17487/RFC3444, January 2003, <<http://www.rfc-editor.org/info/rfc3444>>.

[RFC4949] Shirey, R., "Internet Security Glossary, Version 2", FYI 36, [RFC 4949](#), DOI 10.17487/RFC4949, August 2007, <<http://www.rfc-editor.org/info/rfc4949>>.

[RFC5209] Sangster, P., Khosravi, H., Mani, M., Narayan, K., and J. Tardo, "Network Endpoint Assessment (NEA): Overview and Requirements", [RFC 5209](#), DOI 10.17487/RFC5209, June 2008, <<http://www.rfc-editor.org/info/rfc5209>>.

[RFC5792] Sangster, P. and K. Narayan, "PA-TNC: A Posture Attribute (PA) Protocol Compatible with Trusted Network Connect (TNC)", [RFC 5792](#), DOI 10.17487/RFC5792, March 2010, <<http://www.rfc-editor.org/info/rfc5792>>.

[RFC6192] Dugal, D., Pignataro, C., and R. Dunn, "Protecting the Router Control Plane", [RFC 6192](#), DOI 10.17487/RFC6192, March 2011, <<http://www.rfc-editor.org/info/rfc6192>>.

[X.1252] "ITU-T X.1252 (04/2010)", n.d..

[Appendix A. The Attic](#)

The following terms are stashed for now and will be updated later:

Asset Characterization: Asset characterization is the process of defining attributes that describe properties of an identified asset.

Asset Targeting: Asset targeting is the use of asset identification and categorization information to drive human-directed, automated

decision making for data collection and analysis in support of endpoint posture assessment.

Client: An architectural component receiving services from another architectural component.

Endpoint Identification (TBD per list; was "Endpoint Discovery"):
The process by which an endpoint can be identified.

Authors' Addresses

Henk Birkholz
Fraunhofer SIT
Rheinstrasse 75
Darmstadt 64295
Germany

Email: henk.birkholz@sit.fraunhofer.de

Jarrett Lu
Oracle Corporation
4180 Network Circle
Santa Clara, CA 95054
USA

Email: jarrett.lu@oracle.com

John Strassner
Huawei Technologies
2330 Central Expressway
Santa Clara, CA 95138
USA

Email: john.sc.strassner@huawei.com

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

Email: ncamwing@cisco.com

