SACM Working Group   H. Birkholz
Internet-Draft   Fraunhofer SIT
Intended status: Informational   J. Lu
Expires: June 17, 2019   Oracle Corporation
                                                          J. Strassner
                                                    Huawei Technologies
                                                         N. Cam-Winget
                                                          Cisco Systems
                                                          A. Montville
                                                                    CIS
                                                      December 14, 2018

        Security Automation and Continuous Monitoring (SACM) Terminology
                      draft-ietf-sacm-terminology-16

Abstract

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

Status of This Memo

Copyright Notice

Table of Contents

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. Note that explanatory or
   informational augmentation to definitions are segregated from the
   definitions themselves. The definition for the term immediately
   follows the term on the same line, whereas expositional text is
   contained in subsequent paragraphs immediately following the
   definition.

   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 SACM Statement (including metadata
      about the data source and data origin, e.g. timestamps). While
      the validity of an assertion about Content and Content Metadata
      cannot be verified without, for example, Integrity Proofing of the

Data Source, an assertion (and therefore a SACM statement,
respectively) of the validity of Statement Metadata can by enabled
by including corresponding Integrity Evidence created by the Data
Origin.

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."

Attribute: Is a data element, as defined in [RFC5209], that is
   atomic.

   In the context of SACM, attributes are "atomic" information
   elements and an equivalent to attribute-value-pairs. Attributes
   can be components of Subjects, the basic composite definitions
   that are defined in the SACM Information Model.

Capability: A set of features that are available from a SACM
   Component.

   See also "capability" in [I-D.ietf-i2nsf-terminology].

   In the context of SACM, the extent of a SACM component's ability
   is enabled by the functions it is composed of. Capabilities are
   registered at a SACM broker (potentially also at a proxy or a
   repository component if it includes broker functions) by a SACM
   component via the SACM component registration task and can be
   discovered by or negotiated with other SACM components via the
   corresponding tasks. For example, the capability of a SACM
   provider may be to provide target endpoint records (declarative
   guidance about well-known or potential target endpoints), or only
   a subset of that data.

   A capability's description is in itself imperative guidance on
   what functions are exposed to other SACM components in a SACM
   domain and how to use them in workflows.

   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 on an enterprise IT
   department's point of view and therefore compose sets of
   declarative guidance.

Collection Result: Is a composition of one or more content elements
   carrying information about a target endpoint, that is produced by
   a collector when conducting a collection task.

Collection Task: A targeted task that collects attributes and/or
   corresponding attribute values from target endpoint.

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

   ad-hoc, e.g. triggered by a unsolicited query

   conditional, e.g. triggered in accordance with policies included
   in the compositions of workflows

   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 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
      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 scheduled 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 disposition of endpoint characteristics to
      change 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 SACM Role that requires a SACM Component to include SACM
      Functions enabling it 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
      transferred. Examples include time stamps or data provenance
      Subjects.

   Control Plane: An architectural component that provides common
      control functions to all SACM components.

Typically used as a term in the context of routing, e.g.
[RFC6192]. SACM components may include 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 managing and
   facilitating 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.

Data At Rest: Data that is stored.

   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.

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: The SACM Component that initially acquired or produced
    data about an endpoint.

    Data Origin enables 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 domain 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: Is an architectural component providing operational
    functions enabling information exchange that is not command and
    control or management related.

    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, which composes
    the actual SACM content. The data plane in a SACM domain is used
    to conduct distributed SACM tasks by transporting SACM content via
    specific transport encodings and corresponding operations defined
    by SACM data models.

Data Provenance: An historical record of the sources, origins and
    evolution, as it pertains to data, that is influenced by inputs,
    entities, functions and processes.

    Additional Information - 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: Is an endpoint from which a particular set of
    attributes and/or attribute values have been collected.

    Data Source enables 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."

      Additional Information - The [RFC5209] definition continues, "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: Is a discreet endpoint characteristic that is
      computably observable.

      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 Characteristics: The state, configuration and composition
      of the software components and (virtual) hardware components a
      target endpoint is composed of, including observable behavior,
      e.g. sys-calls, log-files, or PDU emission on a network.

      In SACM work-flows, (Target) Endpoint Characteristics are
      represented via Information Elements.

   Endpoint Characterization Task: The task of endpoint
      characterization that uses endpoint attributes that represent
      distinct endpoint characteristics.

Endpoint Classification: The categorization of of the endpoint into
   one or more taxonomic structures.

   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 Classification Task: The task of endpoint classification
   that uses an endpoint's characteristics to determine how to
   categorize the given endpoint into one or more taxonomic
   structures.

Endpoint Label: A unique label associated with a unique endpoint.

   Endpoint specializations have corresponding endpoint label
   specializations. For example, an endpoint label used on a SACM
   Component is a SACM Component Label.

Endpoint Management Capabilities: Enterprise IT management
   capabilities that are tailored to manage endpoint identity,
   endpoint information, and associated metadata.

Evaluation Task: A task by which an endpoint's asserted attribute
   value is evaluated against a policy-compliant attribute value.

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

Expected Endpoint Attribute State: The policy-compliant state of an
   endpoint attribute that is to be compared against.

   Sets of expected endpoint attribute 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 by an
   Attribute or a Subject that represents a set of multiple attribute
   value pairs.

Guidance: Machine-processable input directing SACM processes or
   tasks.

   Examples of such processes/tasks include automated device
   management, remediation, collection, 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 sporadic.

There are two types of guidance:

Declarative Guidance: Guidance that 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: Guidance that 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.

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.

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

Hardware Component: A distinguishable physical component used to
   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.
FRU in a chassis are connected via redundant busses). In general,
a hardware component can be distinguished by its serial number.
Occasionally, hardware components are referred to as power sucking
aliens.

Information Element: A representation of information about physical
   and virtual "objects of interest".

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 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: A collector that runs on a target endpoint to
acquire information from that target endpoint.

Management Plane: An architectural component providing common
functions to steer the behavior of SACM components, e.g. their
behavior on the control 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.

Network Address: A layer-specific address that follows a layer-
specific address scheme.

The following characteristics are a summery derived from the
Common Information Model and ITU-T X.213. Each Network Interface
of a specific layer can be associated with one or more addresses
appropriate for that layer. There is no guarantee that a network

address is globally unique. A dedicated authority entity can
provide a level of assurance that a network address is unique in
its given scope. In essence, there is always a scope to a network
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
(Hardware Component) or logical (virtual Hardware component, i.e.
a dedicated Software Component). 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.

In SACM, the association of Endpoints and Network Addresses via
Network Interfaces is vital to maintain interdependent autonomous
processes that can be targeted at Target Endpoints, unambiguously.

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

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.

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 assigned to a SACM component
      that provides role-specific functions to provide information to
      other SACM components.

   Repository: A repository is a controller that contains functions to
      consume, store and provide information of a particular kind.

      Such information is 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 Broker Controller: A SACM Broker Controller is a controller
      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.

   SACM Component: Is a component, as defined in
      [I-D.ietf-i2nsf-terminology], that is composed of SACM
      capabilities.

      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 discovering the capabilities
provided by SACM components within a SACM domain.

This is likely to be performed via an appropriate set of control
plane functions.

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 Function: A behavioral aspect of a SACM component that provides
external SACM Interfaces or internal interfaces to other SACM
Functionse.

For example, a SACM Function with SACM Interfaces on the Control
Plane can provide a brokering function to other SACM Components.
Via Data Plane interfaces, a SACM 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.

SACM Interface: An interface, as defined in
[I-D.ietf-i2nsf-terminology], that provides SACM-specific
operations.

[I-D.ietf-i2nsf-terminology] defines interface as a "set of
operations one object knows it can invoke on, and expose to,
another object," and further defines interface by stating that an
interface "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 Functions 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 Proxy Controller: A SACM Proxy Controller is a controller 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.

SACM Role: Is a role, as defined in [I-D.ietf-i2nsf-terminology],
that requires the SACM Component assuming the role to bear a set
of SACM functions or interfaces.

SACM Roles provide 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.

SACM Statement: Is an assertion that is made by a SACM Component.

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

Security Automation is intended to identify target endpoints that
cannot be trusted (see "trusted" in [RFC4949]. This goal is
achieved by creating and processing evidence (assessment
statements) that a target endpoint is not a trusted system
[RFC4949].

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

   Software Component: A software package installed on an endpoint.

      The software component may include a unique serial number (e.g. a
      text editor associated with a unique license key).

   Software Instance: A running instance of a software component.

      For example, 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 set of 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 (e.g. provided by a DHCP
      server with a specific configuration).

      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.

   Statement: A statement is the root/top-level subject defined in the
      SACM information model.

      A statement is used to bundle Content Elements into one subject
      and includes metadata about the data origin.

   Subject: A semantic composite information element pertaining to a
      system entity that is a target endpoint.

      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.

      In contrast to the definitions of subject provided by [RFC4949], a
      subject in the scope of SACM is neither "a system entity that

causes information to flow among objects or changes the system
state" nor "a name of a system entity that is bound to the data
items in a digital certificate".

In the context of SACM, a subject is a semantic composite of
information elements about a system entity that is a target
endpoint. Every acquirable subject-as defined in the scope of
SACM-about a target endpoint represents and therefore identifies
every subject-as defined by [RFC4949]-that is a component of that
target endpoint. The semantic difference between both definitions
can be subtle in practice and is in consequence important to
highlight.

Supplicant: A 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: Is an endpoint that is under assessment at some
   point in, or region of, time.

   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 and as referenced
   by {{RFC4949}.

Target Endpoint Address: An address that is layer specific and which
   follows 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.

   Target Endpoint Characterization: The description of the distinctive
      nature of a target endpoint, that is based on its characteristics.

   Target Endpoint Characterization Record: A set of endpoint
      attributes about a target endpoint that was encountered in a SACM
      domain, which are associated with that target endpoint as a result
      of a Target Endpoint Characterization Task.

      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.

   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.

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.

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: An endpoint label that identifies a specific
    target endpoint.

Target Endpoint Profile: A bundle of expected or desired component
    composition, configurations and states that is associated with a
    target endpoint.

    The corresponding task by which the association with a target
    endpoint takes places is the endpoint classification task. The
    task by which an endpoint profile is created is the endpoint
    characterization task. A type or class of target endpoints can be
    defined via a target endpoint profile. Examples include:
    printers, smartphones, or an office PC.

    In respect to [RFC4949], a target endpoint profile is a protection
    profile as defined by Common Criteria (analogous to the target
    endpoint being the target of evaluation).

SACM Task: Is a task conducted within the scope of a SACM domain by
    one or more SACM functions that achieves a SACM-defined outcome.

    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.

The 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".

   A timestamp always requires context, i.e. additional information
   elements that are associated with it. Therefore, all timestamps
   wrt information elements are always metadata. Timestamps in SACM
   Content Elements may be generated outside a SACM Domain and may be
   encoded in an unknown representation. Inside a SACM domain the
   representation of timestamps is well-defined and unambiguous.

Virtual Endpoint: An endpoint composed entirely of logical system
   components (see [RFC4949]).

   The most common example is a virtual machine/host running on a
   target endpoint. Effectively, target endpoints can be nested and
   at the time of this writing the most common example of target
   endpoint characteristics about virtual components is the
   EntLogicalEntry in [RFC6933].

   Vulnerability Assessment: An assessment specifically tailored to
      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 IT management capability
      tailored toward managing 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 assessment capability that
      is tailored toward determining whether a set of endpoints is
      vulnerable according to vulnerability description information.

   Workflow: A workflow is a modular composition of tasks that 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 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.

Changes from version 12 to version 13:

o Added Virtual Component.

o Major Updates to Capability, Collection Task, Hardware Component,
   Hardware Type, Security Automation, Subject, Target Endpoint,
   Target Endpoint Profile.

o Minor Updates to Assertion, Data Plane, Endpoint Characteristics.

Changes from version 13 to version 14:

o Handled a plethora of issues listed in GitHub.

o Pruned some commonly understood terms.

o Narrowing term labels per their definitions.

o In some cases, excised expositional text.

o Where expositional text was left intact, it has been separated
   from the actual definition of a term.

Changes from version 14 to version 16:

o moved obsolete definitions into the Appendix (attic).

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. References

8.1. Normative References

   [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,
              <https://www.rfc-editor.org/info/rfc5792>.

   [RFC6933] Bierman, A., Romascanu, D., Quittek, J., and M.
              Chandramouli, "Entity MIB (Version 4)", RFC 6933,
              DOI 10.17487/RFC6933, May 2013,
              <https://www.rfc-editor.org/info/rfc6933>.

8.2. 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-06 (work in
              progress), July 2018.

   [I-D.ietf-netmod-entity]
              Bierman, A., Bjorklund, M., Dong, J., and D. Romascanu, "A
              YANG Data Model for Hardware Management", draft-ietf-
              netmod-entity-08 (work in progress), January 2018.

   [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,
              <https://www.rfc-editor.org/info/rfc3444>.

   [RFC4949] Shirey, R., "Internet Security Glossary, Version 2",
              FYI 36, RFC 4949, DOI 10.17487/RFC4949, August 2007,
              <https://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,
              <https://www.rfc-editor.org/info/rfc5209>.

   [RFC6192] Dugal, D., Pignataro, C., and R. Dunn, "Protecting the
              Router Control Plane", RFC 6192, DOI 10.17487/RFC6192,
              March 2011, <https://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: Is a system resource, as defined in [RFC4949], that may 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 IT process by which assets are provisioned,
      updated, maintained and deprecated.

   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

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

      Email: adam.w.montville@gmail.com