SACM Working Group   H. Birkholz
Internet-Draft   Fraunhofer SIT
Intended status: Informational   J. Lu
Expires: September 22, 2016   Oracle Corporation
                                                       N. Cam-Winget
                                                        Cisco Systems
                                                       March 21, 2016

        Secure Automation and Continuous Monitoring (SACM) Terminology
                      draft-ietf-sacm-terminology-09

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.

   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 a collection result that includes
      metadata about the data source (and optionally a timestamp
      indicating the point in time the assertion was created at). The
      validity of an assertion cannot be verified.

   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."

      Within SACM the use of the term is expanded to support other uses
      of collected posture (e.g. reporting, network enforcement,
      vulnerability detection, license management). The phrase "set of
      capabilities on the endpoint" includes: hardware and software
      installed on the endpoint."

   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)." If not indicated otherwise,
attributes in SACM are represented and processed as attribute
value pairs.

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: The extent of an SACM component's ability enabled by the
functions it is composed of. Capabilities are propagated by a
SACM component 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.

Collection Result: Information about a target endpoint that is
produced by a collector conducting a collection task. A
collection result is composed of one or more endpoint attributes.

Collection Task: The task by which endpoint attributes and/or
corresponding attribute values about a target endpoint are
collected. There are three types of collection tasks, 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 to SACM components in the
      form of collection results. A SACM component that consumes
      collection results may take on the role of a provider and publish
      the collection results in a SACM domain. (TBD: A collector may
      not be a SACM component and therefore not part of a SACM domain).

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

   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. The control plane
      orchestrates the flow on the data plane according to guidance and/
      or input from 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 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 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).

Data Plane: 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.

Data Source: One or more properties that enable a SACM component to
   identify an (target) endpoint that is claimed to be the original
   source of received data.

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.

   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 a characteristic of a target
   endpoint. Endpoint Attributes typically constitute atomic
   information elements (AVP) that can be bundled into composite

information elements (e.g. information about a specific network
interface can be represented via a set of multiple AVP).

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 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 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.

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

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

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 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 a atomic information element or an composite
information element 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 to processes and tasks, such as collecting,
assessing or reporting. Guidance influences the behavior of a
SACM component and is considered content of the management plane.
Guidance 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. A prominent example
of guidance are target endpoint profiles, but guidance can have
many forms, including:

Configuration, e.g. a SACM component's name, or a CMDB's IPv6
address.

Profiles, e.g. a set of expected states for network behavior
associated with target endpoints employed by specific users.

Policies, e.g. an interval to refresh the registration of a SACM
component, or a list of required capabilities for SACM components
in a specific location.

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: For now this is a Place-Holder. Is an
interaction model that defines, for example, the operations on the
control plane, such as registration or SACM component discovery,
required?

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.

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 interfaces. Interfaces can be physical or virtual.
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 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 Role: 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 functions and corresponding
   interfaces the SACM component is composed of.

SACM Component: 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 function by which a SACM component
      (e.g. by role, capabilities, or data provided/consumed) can be
      discovered.

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

   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).

   Statement: The output of a provider, e.g. a report or an assertion
      acquired via a collection result from a collector, that includes
      metadata about the data origin and the point in time the statement
      was created at. A statement can be accompanied by evidence of the
      validity of its metadata.

   Supplicant: The entity seeking to be authenticated by the Management
      Plane for the purpose of participating in the SACM architecture.

   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 Discovery: The function by which target endpoints
   can be discovered. The output of target endpoint discovery
   typically includes identifying endpoint attributes.

Target Endpoint Identifier: The target endpoint discovery process
   and collection tasks targeted at target endpoints can result in a
   set of identifying endpoint attributes. This set of identifying
   endpoint attributes is used as a target endpoint identifier
   referring to a specific target endpoint. 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 unique
   target endpoint label.

Target Endpoint Label: 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 contains an appropriate
   function.

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 a 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: [TBD conflicts in definitions of specific tasks] 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 due to a subscription on the data plane).
   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 content.
   The output of a task is a result that can be provided (e.g.

published) on the data plane. There are six fundamental tasks
defined in SACM:

Asset Classification: Map the assets on the target endpoints to
asset classes. This enables identification of the attributes
needed to exchange information pertaining to the target endpoint.
[the label now conflicts with Endpoint Classification]

Attribute Definition: Define the attributes desired to be
collected from each target endpoint. This is what we want to know
about a target endpoint. For instance, organizations will want to
know what software is installed and its many critical security
attributes such as patch level.

Policy Definition: This is where an organization can express its
policy for acceptable or problematic values of an endpoint
attribute. The expected values of an endpoint attribute are
determined for later comparison against the actual endpoint
attribute values during the evaluation process. Expected values
may include both those values which are good as well as those
values which represent problems, such as vulnerabilities. The
organization can also specify the endpoint attributes that are to
be present for a given target endpoint.

Information Collection: Collect information (attribute values)
from the target endpoint to populate the endpoint data.

Endpoint Assessment: Evaluate the actual values of the endpoint
attributes against those expressed in the policy. (An evaluation
result may become additional endpoint data).

Result Reporting: Report the results of the evaluation for use by
other components. Examples of use of a report would be additional
evaluation, network enforcement, vulnerability detection, and
license management.

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 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.

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.

[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

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

      Email: ncamwing@cisco.com

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

      Email: jarrett.lu@oracle.com

      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

[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>.

[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

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

   Email: ncamwing@cisco.com