SACM                                                    N. Cam-Winget, Ed.
Internet-Draft                                                Cisco Systems
Intended status: Informational                                 L. Lorenzin
Expires: April 18, 2016                                       Pulse Secure
                                                              I. McDonald
                                                            High North Inc
                                                               A. Woland
                                                            Cisco Systems
                                                        October 16, 2015

         **Secure Automation and Continuous Monitoring (SACM) Architecture**
                     **draft-ietf-sacm-architecture-05**

Abstract

   This document defines an architecture for standardization of
   interfaces, protocols, and information models related to security
   automation and continuous monitoring.  It describes the basic
   architecture, components, and interfaces defined to enable the
   collection, acquisition, and verification of Posture and Posture
   Assessments.

Status of This Memo

Copyright Notice

Table of Contents

## 1.  Introduction

Several data models and protocols (including - but not limited to -
NEA, TCG TNC, SCAP, SWIDs, XMPP, etc.) are in use today that allow
different applications to perform the collection, acquisition, and
assessment of posture.  These applications can vary from being
focused on general system and security management to specialized
configuration, compliance, and control systems.  With an existing
varied set of applications, there is a strong desire to standardize
data models, protocols, and interfaces to better allow for the
automation of such data processes.

This document addresses general and architectural requirements
defined in [I-D.ietf-sacm-requirements].  The architecture described
enables standardized collection, acquisition, and verification of
Posture and Posture Assessments.  This architecture includes the
components and interfaces that can be used to better identify the
Information Model and type(s) of transport protocols needed for
communication.

This document uses terminology defined in
[I-D.ietf-sacm-terminology].

## 1.1.  Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
"SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this
document are to be interpreted as described in RFC 2119 [RFC2119].

When the words appear in lower case, their natural language meaning
is used.

## 2.  Problem Statement

Securing information and the systems that store, process, and
transmit that information is a challenging task for organizations of
all sizes, and many security practitioners spend much of their time
on manual processes.  Administrators can't get technology from
disparate sources to work together; they need information to make
decisions, but the information is not available.  Everyone is
collecting the same data, but storing it as different information.
Administrators therefore need to collect data and craft their own
information, which may not be accurate or interoperable because it's
customized by each administrator, not shared.

Security automation and continuous monitoring require a large and
broad set of mission and business processes; to make the most
effective use of technology, the same data must support multiple
processes.  The need for complex characterization and assessment
necessitates components and functions that interoperate and can build
off each other to enable far-ranging and/or deep-diving analysis.
SACM is standardizing an information model, data models, operations,
and transports that will allow for administrators to share with
others and to use data from others interoperably.

## 3.  Architectural Overview

At a high level, the SACM architecture describes "Where" and "How"
information and assessment of posture may be collected, processed
(e.g. normalization, translation, aggregation, etc.), assessed,

exchanged, and/or stored.  This section provides an architectural
overview of

o  the basic architectural building blocks, which - in combination -
   constitute SACM components (the entities, the "where"), and

o  the relationships and interaction between these building blocks on
   the data plane and control plane (communications and flows between
   entities, the "how").

The SACM architecture provides the basic means to describe and
compose SACM components.  Components enable the basic functionality
in SACM, such as Endpoint Attribute Collection or Target Endpoint
Posture Assessment.

The role(s) a component plays in the SACM architecture are determined
by the function(s) that component instantiates.  Three main component
roles are defined: a Consumer (Cs), a Provider (Pr), and a Controller
(Cr) used to facilitate some of the security functions such as
authentication and authorization and other metadata functions.  See
Section 3.1 for details on roles.

In SACM, components are composed of functions, the modular building
blocks in the SACM architecture.  The SACM architecture defines the
purpose of these functions.  Attributes and operations used by
component functions are described in other SACM documents.  See
Section 5 for details on component functions.

Functions use SACM interfaces for communications between components.
Interfaces handle management and control functions (such as
authentication, authorization, registration, and discovery), and
enable SACM components to share information (via publication, query,
and subscription).  Three primary interfaces are defined: an
interface for management and control (A), an interface for data
communication between the controller and providers or consumers (B),
and an interface for data communication directly between a provider
and a consumer (C).  See Section 4 for details on interfaces.

Figure 1 illustrates the relationships between component roles and
interfaces:

```
                +---------------------------------------+
                | +---------------------------------------+
                | | +---------------------------------------+
                | | |                                       |
                +-| |           Consumer (Cs)               |
                  +-|                                       |
                   +---------------------------------------+
                    /   \         /   \           /   \
                   /     \       /     \         /     \
                  -     -     -  d  -        -       -
                   || ||A       | a |B        |    |C
                   || ||        | t |         |    |
                  -     -     -  a  -         |    |
                   \     /       \     /      |    |
                    \   /         \   /       |    |
                 /|--------------------|\      |    |
               /|----/                  \--------| d |--|\
              /     /    Controller (Cr)     \ ctrl | a |    \
              \     \                         / plane | t |    /
               \|----\                     /--------| a |--|/
                \|--------------------|/      |    |
                    /   \         /   \       |    |
                   /     \       /     \      |    |
                  -     -     -  d  -        |    |
                   || ||A       | a |B        |    |C
                   || ||        | t |         |    |
                  -     -     -  a  -        -       -
                   \     /       \     /       \       /
                    \   /         \   /         \     /
                 +----------------------------------+
                 |                                  |-+
                 |           Provider (Pr           | |
                 |                                  | |-+
                 +----------------------------------+ | |
                    +----------------------------------+ |
                       +----------------------------------+
```
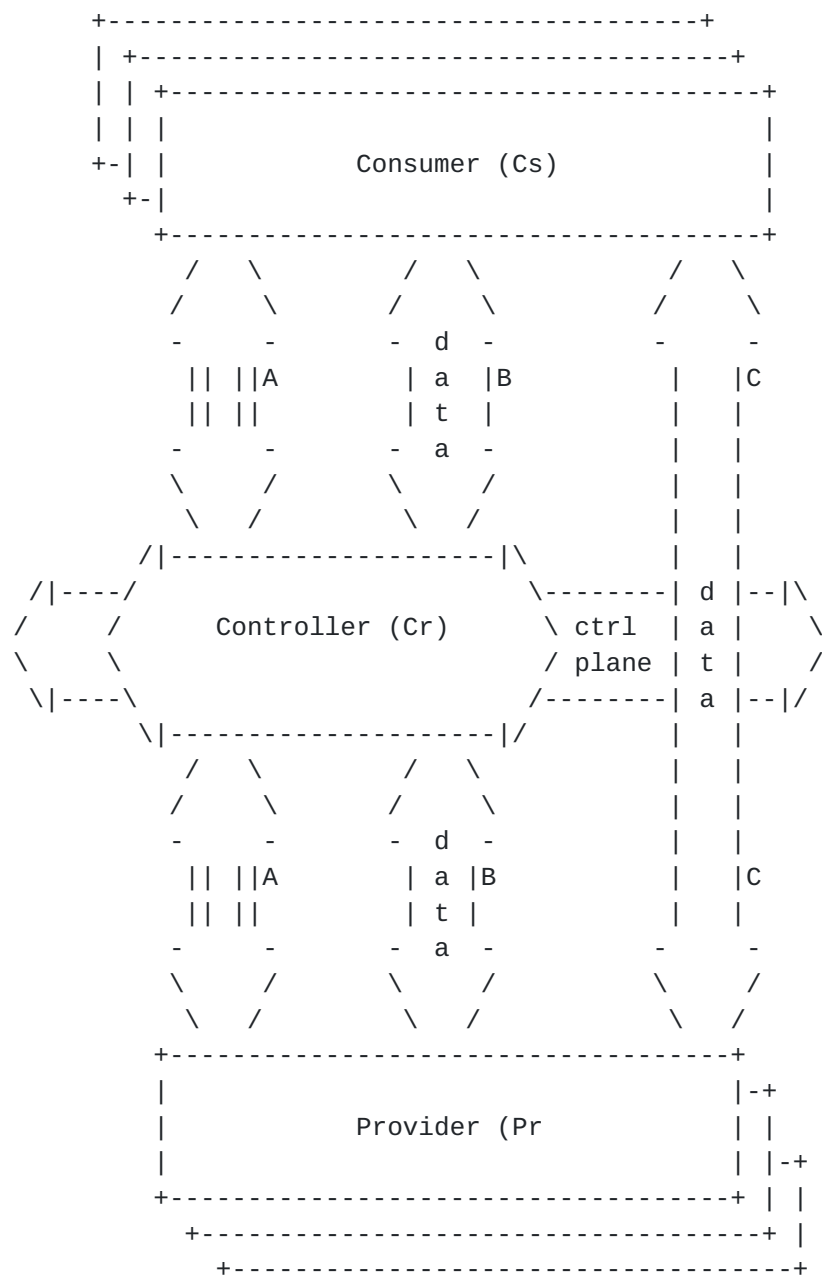
                    Figure 1: Simple Architectural Model

## [3.1](#). Component Roles

   An endpoint, as defined in [[I-D.ietf-sacm-terminology](#)], can operate
   in two primary ways: as the target of an assessment, and/or as a
   functional component of the SACM architecture that can instantiate
   one or more functions (see [Section 5](#)).  In the SACM architecture,

individual endpoints may be a target endpoint, a component, or both
simultaneously.  An endpoint acting as a component may perform one or
more roles.  Components can take on the role(s) of Provider,
Consumer, and/or Controller.

### 3.1.1.  Provider

The Provider (Pr) is the component that contributes Posture
Assessment Information and/or Guidance either spontaneously or in
response to a request.  A Provider can be a Posture Evaluator,
Posture Collector, Data Store (see Section 3.1.3), or an application
that has aggregated Posture Assessment Information that can be
shared.

The Provider implements the capabilities and functions that must be
handled to share or provide Posture Assessment information.

One means by which a Provider shares information, is in response to a
direct request from a Consumer.

A Provider may also share information spontaneously.  Use cases such
as the change in a posture state require that a Provider be able to
provide such changes or updates especially to Consumers such as
Security Information and Event Management (SIEM) systems; similarly,
SIEM applications that are providing live information require any
such updates or changes to posture information to be provided
spontaneously.  Authorization for the enabling for these unsolicited
messages happens through the Controller at the time that both
Provider and Consumers request authorization for (spontaneous)
messages.

The information provided, may be filtered or truncated to provide a
subset of the requested information to honor the request.  This
truncation may be performed based on the Consumer's request and/or
the Provider's ability to filter.  The latter case may be due to
security considerations (e.g. authorization restrictions due to
domain segregation, privacy, etc.).

The Provider may only be able to share the Posture Assessment
Information using a specific data model and protocol.  It may use a
standard data model and/or protocol, a non-standard data model and/or
protocol, or any combination of standard and non-standard data models
and protocols.  However, it must support either one or more standard
data models, or one or more standard protocols.  It may also choose
to advertise its capabilities through a metadata abstraction within
the data model itself, or through the use of the registration
function of the Controller (see Section 3.1.4).

The Provider must be authorized to provide the Posture Assessment
Information for specific consumers.

### 3.1.2.  Consumer

The Consumer (Cs) is the component that requests or accepts Posture
Assessment Information and/or Guidance.  A Consumer can be a Posture
Evaluator, Report Generator, Data Store (see Section 5.2), or an
application that consumes Posture Assessment Information in order to
perform another function.

As described in Section 2.2 of the SACM Use Cases
[I-D.ietf-sacm-use-cases], several usage scenarios are posed with
different application types requesting posture assessment
information.  Whether it is a configuration verification system; a
checklist verification system; or a system for detecting posture
deviations, compliance or vulnerabilities, they all need to acquire
information about Posture Assessment.  The architectural component
performing such requests is a Consumer.

The Consumer implements the capabilities and functions that must be
handled in order to enable a Posture Assessment Information Request.
Requests can be either for a single posture attribute or a set of
posture attributes; those attributes can be the raw information, or
an evaluation result based upon that information.  The Consumer may
further choose to query for the information directly (one-time
query), or to request for updates to be provided as the Posture
Assessment Information changes (subscription).  A request could be
made directly to an explicitly identified Provider, but a Consumer
may also desire to obtain the information without having to know the
available Providers.

There may be instances where a Consumer may be requesting information
from various Providers and, due to its policy or application
requirements, may need to be better informed of the Providers and
their capabilities.  In those use cases, a Consumer may also request
to discover the respective capabilities of those Providers using the
discovery function of the Controller (see Section 3.1.4) or may
request metadata reflecting the capabilities of the Providers.

The Controller (described below) must authorize a Consumer to acquire
the information it is requesting.  The Consumer may also be subject
to limits or constraints on the numbers, types, sizes, and rate of
requests.

### 3.1.3.  Types of Providers and Consumers

SACM Providers and Consumers can perform a variety of SACM-related
tasks.  For example, a Collector can perform Collection tasks; an
Evaluator can perform Evaluation tasks.  A single Provider or
Consumer may be able to perform only one task, or multiple tasks.
SACM defines the following types of Providers/Consumers:

### 3.1.3.1.  Collector

A collector consumes Guidance and/or other Posture Assessment
Information; it provides Posture Assessment Information.  Collectors
may be internal or external.  As a SACM component, a Collector may be
a Consumer as it may consume guidance information and may also be a
Provider as it may publish the collected information.

### 3.1.3.1.1.  Internal Collector

An internal collector is a collector that runs on the endpoint and
collects posture information locally.

### 3.1.3.1.2.  External Collector

An external collector is a collector that observes endpoints from
outside.  These collectors may be configured and operated to manage
assets for reasons including, but not limited to, posture assessment.
Collectors that are not primarily intended to support posture
assessment (e.g. intrusion detection systems) may still provide
information that speaks to endpoint posture (e.g. behavioral
information).

Examples:

o  A RADIUS server, which collects information about which endpoints
   have logged onto the network

o  A network profiling system, which collects information by
   discovering and classifying network nodes

o  A Network Intrusion Detection System (NIDS) sensor, which collects
   information about endpoint behavior by observing network traffic

o  A vulnerability scanner, which collects information about endpoint
   configuration by scanning endpoints

o  A hypervisor, which collects information about endpoints running
   as virtual guests in its host environment

o  A management system that configures and installs software on the
   endpoint, which collects information based on its provisioning
   activities

### 3.1.3.1.3.  Collector Interactions With Target Endpoints

TODO - examples of endpoint interactions with local internal
collector (e.g.  NEA client), endpoint with remote internal collector
(SNMP query), and external collector (sensor)

### 3.1.3.2.  Evaluator

An evaluator consumes Posture Assessment Information, Evaluation
Results, and/or Guidance; it provides Evaluation Results.  An
evaluator may consume endpoint attribute assertions, previous
evaluations of posture attributes, or previous reports of Evaluation
Results.

TODO: update the terminology doc to reflect this definition

Example: a NEA posture validator [RFC5209]

### 3.1.3.3.  Report Generator

A report generator consumes Posture Assessment Information,
Evaluation Results, and/or Guidance; it provides reports.  These
reports are based on:

o  Endpoint Attribute Assertions, including Evaluation Results

o  Other Reports (e.g., a weekly report may be created from daily
   reports)

It may summarize data continually, as the data arrives.  It also may
summarize data in response to an ad hoc query.

### 3.1.3.4.  Data Store

A data store consumes any data; it provides any data.

### 3.1.4.  Controller

The Controller (Cr or Controller) is a component defined to
facilitate the overall SACM management and control system functions.
This component is responsible for handling the secure communications
establishment (such as the authentication and authorization) between
Providers and Consumers.  In addition, the Controller may also handle
how the data may be routed.  While the architecture defines the

Controller as a single component, implementations may implement this
to suit the different deployment and scaling requirements.  In
particular, for the data handling, SACM defines three types of
Controller:

Broker:  Intermediary negotiating connection between Provider and
 Consumer.  Implements only control plane functions.  A Controller
 acting as a Broker:

  *  Receives a request for information from a Consumer and instructs
     the Consumer where and how retrieve the requested information.

  *  Receives a publication request from a Provider and instructs the
     Provider where and how to deliver the published information.

  *  The information itself is neither distributed nor stored by the
     Controller.

 Proxy:  Intermediary negotiating on behalf of a Consumer or Provider.
  Implements both control and data plane functions.  A Controller
  acting as a Proxy:

   *  Receives a request for information from a Consumer, retrieves the
      information from the appropriate Providers, and provides the
      information to the Consumer.

   *  Receives a publication request from a Provider, accepts the
      published information, and distributes it to appropriate
      consumers.

   *  The information itself is distributed by, but not stored by, the
      Controller.

 Repository:  Intermediary receiving and storing data from a Provider,
  and providing stored data to a Consumer.  Implements both control
  and data plane functions.  A Controller acting as a Repository:

   *  Receives a request for information from a Consumer, retrieves the
      information from its data stores, and provides the information to
      the Consumer.

   *  Receives a publication request from a provider, stores the
      published information, and distributes it to appropriate
      Consumers.

   *  The information itself is both handled by and stored by the
      Controller.

A single instantiation of a Controller may be a Broker, Proxy, or
Repository, or any combination thereof.

Through the use of a discovery mechanism, Consumers can have
visibility into the Providers present, the type(s) of Posture
Assessment Information available, and how it can be requested.
Similarly, a Provider may need to publish what Posture Assessment
Information it can share and how it can share it (e.g. protocol,
filtering capabilities, etc.).  Enabling this visibility through a
Controller or through metadata publication also allows for the
distinct definition of security considerations (e.g. authorized
registration / publication of capabilities by Providers) beyond how a
Provider may define its own capability.

Beyond the control and management functions for the SACM system, a
Controller may also provide proxy or broker or repository (and
possibly routing) services in the data plane.  In the deployment
scenario where Providers do not assert the need to know their
Consumers and/or vice versa, the Controller can thus provide the
appropriate services to ensure the Posture Assessment Information is
appropriately communicated from the Providers to the authorized
Consumers.

The Controller, acting as a management control plane, helps define
how to manage an overall SACM system that allows for Consumers to
obtain the desired Posture Assessment Information without the need to
distinctly know and establish one (Consumer) to many (Provider)
connections.  Similarly, a Provider may not need to distinctly know
and establish one (Provider) to many (Consumer) connections; e.g. the
Controller enables the means to allow a SACM system to support many
to many connections.  Note that the Controller also allows for the
direct discovery and connection between a Consumer and Provider.

As a SACM component, the Controller may be instantiated within a
system or device acting as a Provider or a Consumer (or both), or as
its own distinct Controller entity.  In a rich SACM environment, it
is feasible to instantiate a Controller that provides both the
management (and control) functions for SACM as well as providing the
data plane services for the actual data, e.g.  Posture Assessment
Information flow.  Note that Controllers may be implemented to only
provide control plane functions (broker), or both control plane
functions and data plane services (proxy or repository).

## [4](#). Interfaces between Consumers, Providers, and Controllers

A SACM interface is a transport carrying operations (e.g. publication
via a RESTful API).  As shown in Figure 1, communication can proceed
with the following interfaces and expected functions and behaviors:

A:  interface "A" shown in Figure 1 handles the management and
control functions that are needed to establish, at minimum, a secure
communication between Consumers and Providers.  The interface must
also handle the functions to allow for the discovery and
registration of the Providers as well as the ways in which Posture
Assessment Information can be provided (or requested).

B:  interface "B" shown in Figure 1 enables Providers to share their
Posture Assessment Information spontaneously; similarly, it enables
Consumers to request information without having to know the
identities (or reachability) of all the Providers that can fulfill
Consumers' requests.

C:  interface "C" shown in Figure 1 illustrates the ability and
desire for Consumers and Providers to be able to communicate
directly when a Provider is sharing Posture Assessment Information
directly to a Consumer.  The interface allows for the different data
models and protocols to be used between a Consumer and a Provider
with the expectation that the appropriate authentication and
authorization mechanisms have been employed to establish a secure
communication link between the Consumer and the Provider.
Typically, it is expected that the secure link establishment occurs
as a management or control function through the abstracted
Controller role (e.g. the Controller could be a broker or could be
embedded in a Consumer or a Provider).

A variety of protocols, such as SNMP, NETCONF, NEA protocols
[RFC5209], and other similar interfaces, may be used for collection
of data from the target endpoints by the Posture Information
Provider.  Those interfaces are outside the scope of SACM.

## 5.  Component Functions

SACM components are composed of a variety of functions, which may be
instantiated on a single endpoint or on separate standalone endpoints
providing various roles.  An endpoint MUST implement one or more of
these functions to be considered a SACM component.  A SACM solution
offers a set of functions across a set of SACM components.

The functions described here are the minimum set that is mandatory to
implement in a SACM solution.  A SACM solution MAY implement
additional functions.

## 5.1.  Control Plane Functions

Control plane functions represent various services offered by the
Controller to the Providers and Consumers to facilitate sharing of

information.  Control plane functions include, but are not limited
to:

Authentication:  The authentication of Consumers and Providers
 independent of the actual information-sharing communication channel.
 While authentication between peers (e.g. a Consumer and a Provider)
 can be achieved directly through peer to peer authentication (using
 TLS for instance), there are use cases where:

  *  Consumers may request information independent of knowing the
     identities of the Providers.

  *  Providers may want to share the information without prior
     solicitation.

To address the above use cases, the architecture must account for an
abstraction where a Controller may be defined to effect the
authentication of the Consumers and Providers independent of the
actual information-sharing communication channel.  Consumers and
Providers that consume or publish information without requiring
knowledge of the Providers and Consumers respectively would function
in a SACM system where the Controller is a distinct entity.  As a
distinct SACM component, the Controller would authenticate Providers
and Consumers.

Authorization:  The restriction of Posture Assessment Information
 sharing between the Consumers and Providers.  At minimum, a
 management function must define the necessary policies to control
 what Providers can publish and Consumers to accept.  The Controller
 is the authority for the type of Posture Information that a Provider
 can publish and a Consumer can accept.  If a Controller is a Broker,
 then it may only grant authorization to the capabilities requested
 by the Provider or Consumer.  When acting as a Proxy, as part of its
 authorization, the Controller may further obscure or block
 information being shared by a Provider as it distributes it to a
 Consumer.  Similarly, a Repository may block information as recieved
 by the Provider and pass to the Consumer and to its storage the
 resulting authorized information.  A Provider may also enforce its
 own authorization based upon its connection to a Controller; though,
 in the case where an application includes both the Provider and
 Controller roles, it can choose to implement all authorization on
 the Controller.  Similarly, a Consumer may enforce its own
 authorization of what data it can receive based on the Controller
 (or Provider) it is communicaticating with; in the case where an
 application includes both the Consumer and Controller roles, it can
 choose to implement all the authorization on the Controller.

   Identity Management:  Since Identity Management for authentication
      and authorization policies is best performed via a centralized
      component, the Controller also facilitates this function.

      The Controller needs to be able to identify the endpoints
      participating as SACM components and the roles that they play.
      Similar to how access control may be effected via Authentication,
      Authorization, and Accounting Systems (e.g.  AAA services), the
      same principle is defined; as AAA services depend on Identity
      Management services, the Controller will need a similar function
      and interface to Identity Management services.  Note that
      implementations of this function is abstractly centralized, but to
      address scalability and the need to manage different resources
      (e.g. users, processes and devices) a distributed system that is
      centrally coordinated may be used.

   Registration/Discovery:  A SACM ecosystem needs to provide the
      ability for devices to discover Providers, Consumers, Controllers
      and their respective capabilities.  For a Consumer to be able to
      obtain the information of interest must either configure itself to
      know what Providers to communicate with directly (and their known
      capabilities, such as the supported data model and information
      provided) or can dynamically discover the information that is
      available.  Similarly, Providers may need to either be configured to
      know who to publish the information to, or can dynamically discover
      its Consumers.

      In the case where there is a Controller, the capabilities of the
      Controller must also be advertised so that Providers and Consumers
      may know how the data is being handled as well (e.g. if acting as a
      Broker or Repository).  The Controller also provides the function of
      registering the Providers and Consumers; the registration function
      enables the Controller to also affect the authorization afforded to
      the Provider or Consumer.

## [5.2](#).  Data Plane Functions

   There are three basic functions to facilitate data flow:

   Subscription:  A Consumer that wants to recieve information from a
      specific Provider or from the Controller advertising the
      availability of specific information (that may come from more than
      one Provider) will effectively subscribe to recieve the information
      spontaneously and continuously as new information as subscribed to
      becomes available.

   Publication  A Provider being registered through the Controller to
      provide specific information, may publish the information either

directly to the Consumers or to the Controller that is acting as the
broker or respository.

Query/Response  A Consumer may contact the Provider directly and
 request the information through a query operation; and in response,
 the Provider would send the information directly to the Consumer.

## 6.  Component Capabilities

TODO: add a discussion of "capability" as being able to talk a
specific data model, data operations, or SACM transport

TODO: data plane capabilities / control plane capabilities can be
discovered via querying the controller

## 7.  Example Illustration of Functions and Workflow

TODO: once the group reaches consensus on content for the previous
sections, revise all this text based upon the agreed-upon
architecture

```
                +-------------------------------+
                | +-----------------------------+
                | |                             |
                +-|        Controller (Cr)      |
                  +-----------------------------+
                    //   /           \    \\
                   //   /             \    \\
                A //   /               \    \\ A
                 //   /                 \    \\
                //   /  B             B   \    \\
               //   /                       \    \\
    +----------------------+          +-----------------------+
    | +--------------------+    A     | +---------------------+
    | |                    |==========| |                     |
    | |    Consumer (C)    |----------| |      Provider (P)    |
    +-|                    |    C    +-|                     |
      +--------------------+          +---------------------+
```
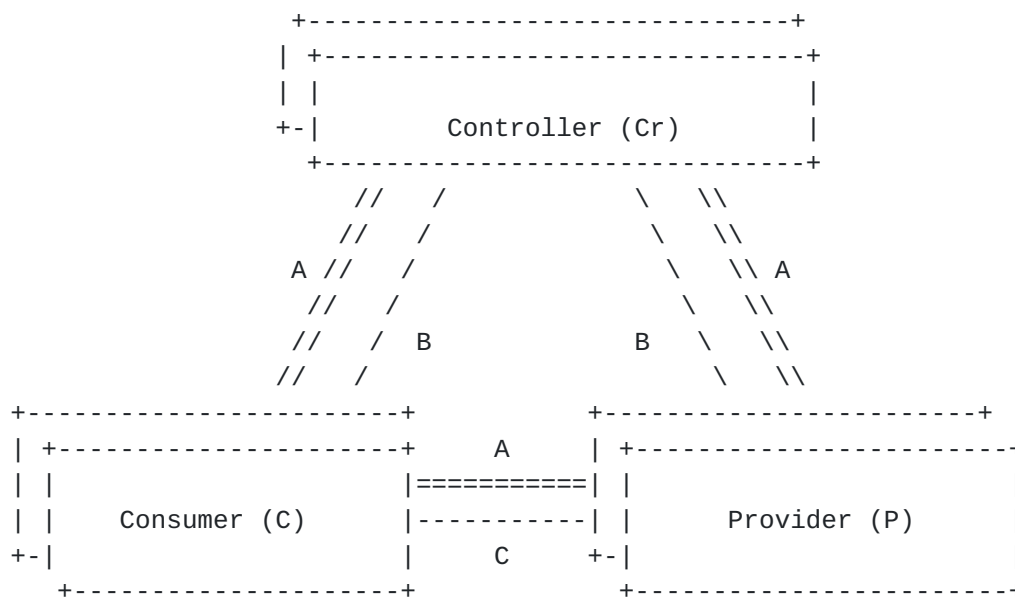
Figure 2: Communications Model

SACM's focus is on the automation of collection, verification and
update of system security configurations pertaining to endpoint
assessment.  In order to carry out these tasks, the architectural
components shown in Figure 1 can be further refined as:

Providers:  a Provider may be dedicated to perform either the
   collection, aggregation or evaluation of one or more posture
   attributes whose results can be conveyed to a Consumer.  In this
   example form of the SACM architecture model, these are shown as
   Collection, Evaluation, and Results Providers.  Note that there may
   be posture attributes or posture assessment information that
   articulates Guidance information which may or may not be present in
   the architecture.

Consumers:  a Consumer may request or receive one or more posture
   attributes or posture assessment information from a Provider for
   their own use.  In this example form of the SACM architecture model,
   these are shown as Collection, Evaluation, and Results Consumers.
   Note that there may be posture attributes or posture assessment
   information articulating Guidance information which may or may not
   be present in the architecture to be provided or consumed.

Data Stores:  a Data Store is both a Provider and a Consumer, storing
   one or more posture attributes or assessments for endpoints.  It
   should be understood that these repositories interface directly to a
   Provider or Consumer (and Guidance) but the interfaces used to
   interact between them is outside the scope of SACM (e.g. no
   interface arrows are shown in the architecture).

Figure 3 illustrates an example flow for how Posture Assessment
Information may flow.

```
                                 +-------------+
                                 |Evaluation   |
                  +-------------+ |Guidance     +--+
                  |Endpoint     | |Function     |  |
      +-------+   |             | +------------+  |
      |       |   |             |                 |
      |       +-------+-----+         +-----v-------+
      | Collection     |              |Evaluation   |
    +-> Function   +--+--------+       |Function     |
    | |            |Collection |    +-----------+  +----------+
    | +------------+Provider   |    |           |---|          |
    |              |           |    |Collection |  |Evaluation|
    |              |           |    |Consumer   |  |Provider  |
    |              +----+------+    +----^------+  +---+------+
   ++---------+        |                 |             |
   |Collection|    +-----v------+        |             |
   |Guidance  |    |            |     +---+--------+    |
   |Function  |    |Collection  |     |Collection  |    |
   |          |    |Consumer    |-----|Provider    |    |
   +----------+    +------------+     |            |    |
                                     +------------+    |
                    | Collection |                     |
                    | Data Store |                     |
                    +------------+                     |
                                                       |
        +--------------+         +--------------+      |
        |Evaluation    |         |Evaluation    |      |
        |Results       |         |Consumer      |  <-----+
        |Provider      |---------|              |      |
        +-----+--------+         +--------------+
              |       |Results Reporting|
              |       |Function         |
              |       +------------^----+
              |                    |
        +-----v--------+     +----+------+
        |Evaluation    |     |Reporting  |
        |Results       |     |Guidance   |
        |Consumer      |     |Data Store |
        +---+----------+     +-----------+ +-------------+
            |                             | Results      |
          +---------------------------> Data Store    |
                                          |             |
                                          +-------------+
```
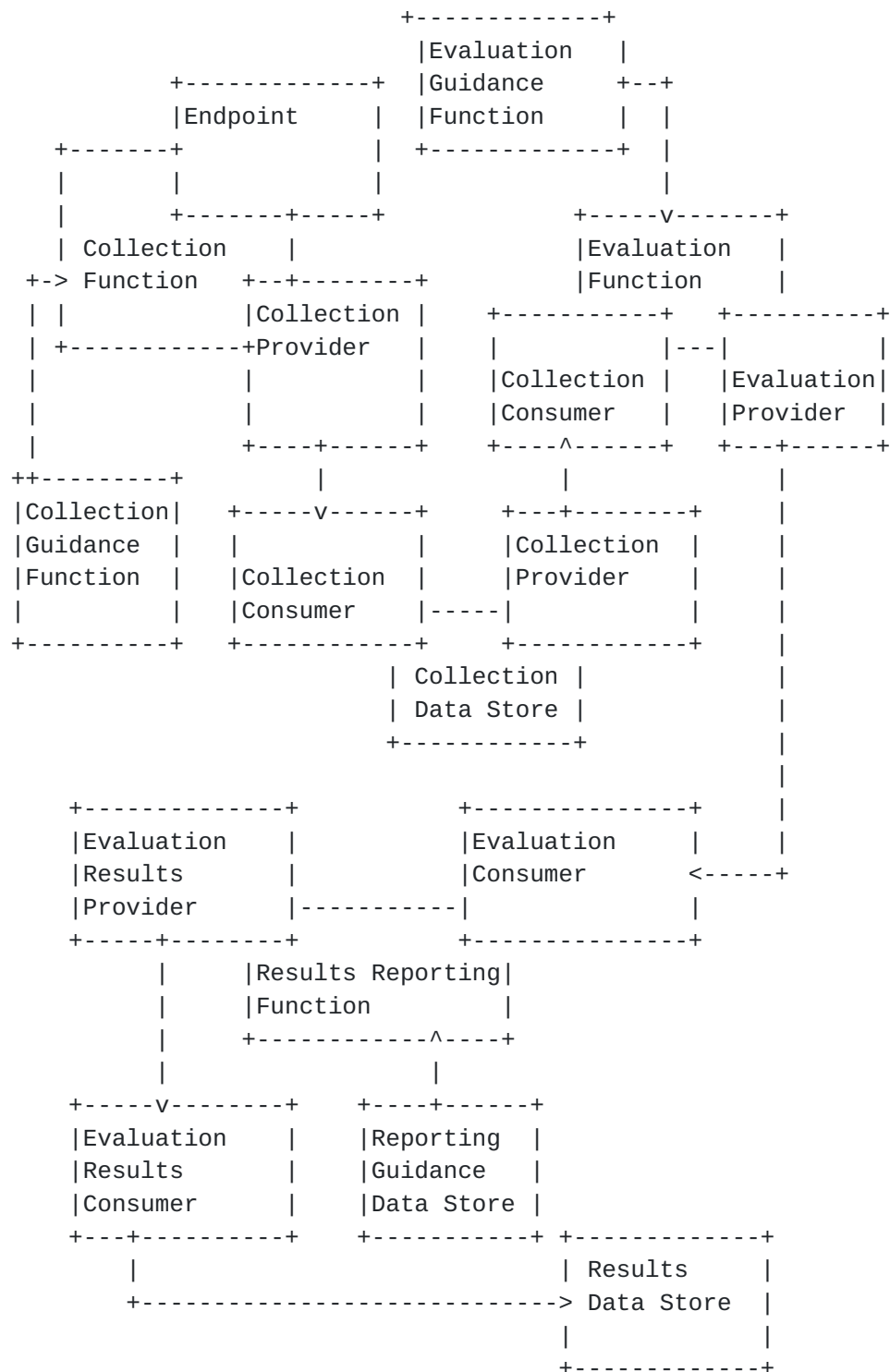
                    Figure 3: Example Posture Information Flow

   TODO - add example of / more content around interactions with
   endpoint, possible communications patterns

## 8.  Acknowledgements

   The authors would like to thank Jim Bieda, Henk Birkholz, Jessica
   Fitzgerald-McKay, Trevor Freeman, Adam Montville, and David
   Waltermire for participating in architecture design discussions,
   reviewing, and contributing to this draft.

## 9.  IANA Considerations

   This memo includes no request to IANA.

## 10.  Security Considerations

   The SACM architecture defines three main components that interface
   with each other both for management and control (in the control
   plane) and for the sharing of Posture Assessment Information.
   Considerations for transitivity of trust between a Provider and
   Consumer can be made if there is a well understood trust between the
   Provider and the Controller and between the Consumer and Controller.
   The trust must include strong mutual authentication, at minimum,
   between the Provider and Controller and between the Consumer and
   Controller.

   To address potential Man-in-the-Middle (MitM) attacks, it is also
   strongly recommended that the communications be secured to include
   replay protection and message integrity (e.g. transport integrity and
   if required, data integrity).  Similarly, to avoid potential message
   disclosure (e.g. where privacy may be needed), confidentiality should
   also be provided.

   As the Controller provides the security functions for the SACM
   system, the Controller should provide strong authorizations based on
   either or both business and regulatory policies to ensure that only
   authorized Consumers and obtaining Posture Assessment Information
   from authorized Providers.  It is presumed that once authenticated
   and authorized, the Provider, Controller or Consumer is deemed
   trustworthy; though note that it is possible that the modules or
   devices hosting the SACM components may be compromised as well (e.g.
   due to malware or tampering); however, addressing that level of
   trustworthiness is out of scope for SACM.

   As the data models defined through the interfaces are transport
   agnostic, the Posture Assessment Information data in the interfaces
   may leverage the transport security properties as the interfaces are
   transported between the Provider, Consumer and Controller.  However,

there may be other devices, modules or components in the path between
the Provider, Consumer and Controller that may observe the interfaces
flowing through them.

## 11.  References

### 11.1.  Normative References

[I-D.ietf-sacm-requirements]
           Cam-Winget, N. and L. Lorenzin, "Secure Automation and
           Continuous Monitoring (SACM) Requirements", draft-ietf-
           sacm-requirements-08 (work in progress), July 2015.

[I-D.ietf-sacm-terminology]
           Birkholz, H., "Secure Automation and Continuous Monitoring
           (SACM) Terminology", draft-ietf-sacm-terminology-07 (work
           in progress), July 2015.

[I-D.ietf-sacm-use-cases]
           Waltermire, D. and D. Harrington, "Endpoint Security
           Posture Assessment - Enterprise Use Cases", draft-ietf-
           sacm-use-cases-10 (work in progress), July 2015.

[RFC2119]  Bradner, S., "Key words for use in RFCs to Indicate
           Requirement Levels", BCP 14, RFC 2119,
           DOI 10.17487/RFC2119, March 1997,
           <http://www.rfc-editor.org/info/rfc2119>.

### 11.2.  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>.

[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>.

Authors' Addresses

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


Email: ncamwing@cisco.com


Lisa Lorenzin
Pulse Secure
2700 Zanker Rd, Suite 200
San Jose, CA  95134
US


Email: llorenzin@pulsesecure.net


Ira E McDonald
High North Inc
PO Box 221
Grand Marais, MI  49839
US


Email: blueroofmusic@gmail.com


Aaron Woland
Cisco Systems
1900 South Blvd. Suite 200
Charlotte, NC  28203
US


Email: loxx@cisco.com