SACM
Internet-Draft
Intended status: Informational
Expires: July 7, 2015

N. Cam-Winget, Ed.
Cisco Systems
L. Lorenzin
Pulse Secure
I. McDonald
High North Inc
A. Woland
Cisco Systems
January 3, 2015

Secure Automation and Continuous Monitoring (SACM) Architecture draft-ietf-sacm-architecture-02

Abstract

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

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on July 7, 2015.

Copyright Notice

Copyright (c) 2015 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of

publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction

Several data models and protocols 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]. This document describes an architecture to enable 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].

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 of 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.

[NCW]This is a very broad problem statement that am not sure belongs in the Architecture specification. Why does the charter not suffice? What is the purpose of inserting this section in this draft?

3. Architectural Overview

At a high level, the architecture describes 'How' and 'Where' information and assessment of posture may be collected, processed or assessed. Three main functional components are defined: a Posture Assessment Information Consumer (Cs), a Posture Assessment Information Provider (P), and a Controller (Cr) used to facilitate some of the security functions such as authentication and authorization and other metadata functions.

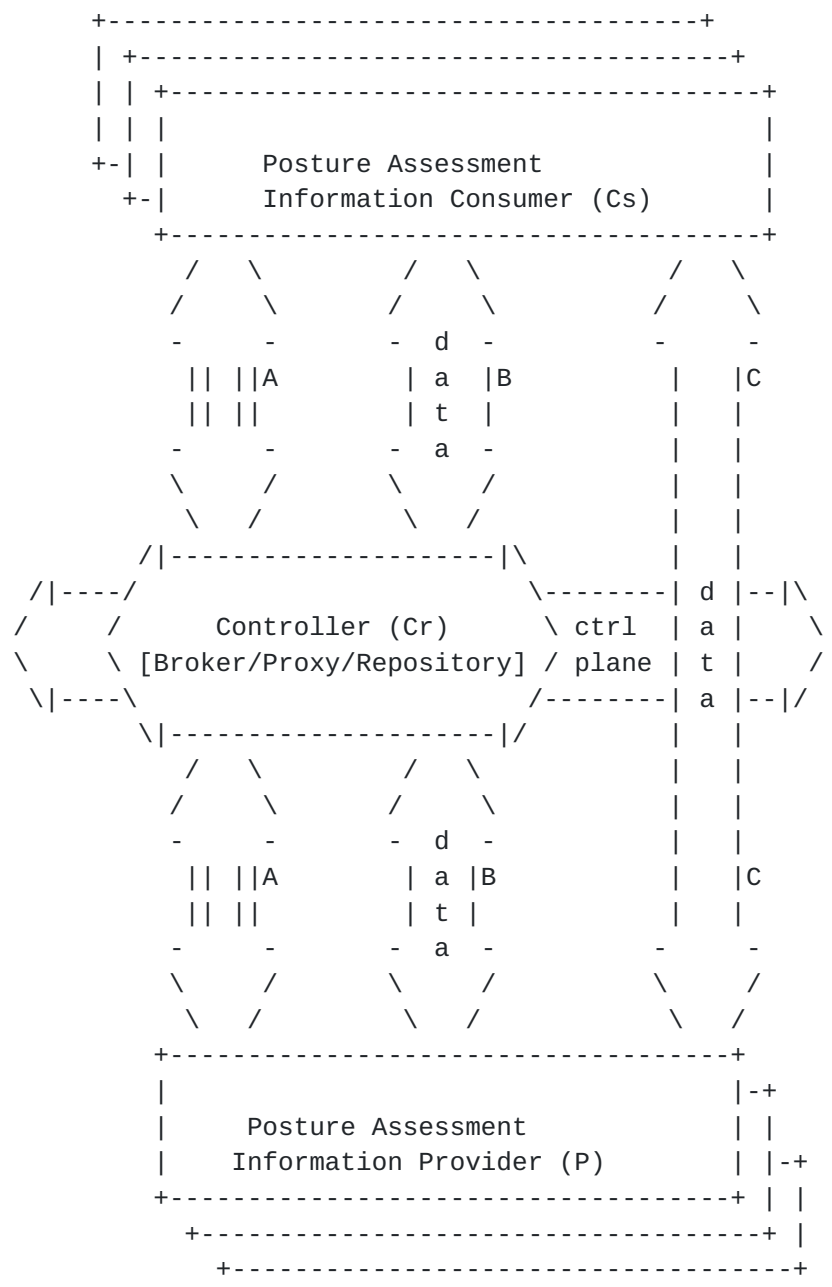

Figure 1: Simple Architectural Model

3.1. Component Roles

An endpoint, as defined in [I-D.ietf-sacm-terminology], can function 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 capabilities (see Section 4). Individual endpoints may

be a target endpoint, or a component, or both simultaneously. Components can take on the role of Posture Assessment Information Provider, Posture Assessment Information Consumer, and/or Controller.

3.1.1. Posture Assessment Information Provider

The Posture Assessment Information Provider (P or Provider) 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, 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.

A Provider may provide information spontaneously, or in response to a direct request from a Consumer. The information 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. 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 3.1.3) [QUESTION: Are these different?].

The Provider must be authorized to provide the Posture Assessment Information and further, be authorized to do so with the specific data models and protocols.

3.1.2. Posture Assessment Information Consumer

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. Thus, the architectural component to enable such requests is defined as a Posture Assessment Information Consumer (C or Consumer).

The Consumer implements the capabilities and functions that must be handled in order to facilitate a Posture Assessment Information Request. Requests can be either for a single posture attribute or a set of posture attributes where those attributes can be the raw information or an evaluated or assessed state 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 Posture Assessment Information Provider (P or 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 3.1.3).

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. Controller

The Controller is a component defined to facilitate information brokering or proxing and to execute on security functions and overall SACM management and control system functions including:

Authentication: The architecture must account for an abstraction where a Controller may be defined to affect the authentication of Consumers and Providers independent of the actual information sharing communication channel. This supports 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.

Authorization: To restrict how Posture Assessment Information is shared between the Consumers and Providers. At minimum a management function must define the necessary policies.

The introduction of the Controller supports use cases where:

* Consumer's may request information independent of knowing the identities of the Provider's

* Providers may want to share information unsolicited

The architecture must account for an abstraction where a Controller may be defined to affect the authentication of the Consumers and Providers independent of the actual information sharing communication channel.

Identity Management: As typically, Identity Management for authentication and authorization policies are best defined through a centralized component, the Controller also provides these services.

Registration/Discovery: A discovery mechanism is required to facilitate the interaction of Providers that may have different Posture Assessment Information and potentially limited (or a rich set) of ways in which they can share the information. Through the use of a discovery mechanism, Consumers can have visibility of the Providers present and the type(s) of Posture Assessment Information that is available and how it can be requested. Similarly, a Provider may need to register what Posture Assessment Information it can share and how it can share it (e.g. protocol or with filtering capabilities). Enabling this function through a Controller also allows for the distinct definition of security considerations (e.g. authorized registration of capabilities and of Providers) beyond how a Provider may define its own capability.

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

Data Store: as a broker, the Controller may also include data stores to affect the appropriate buffering, aggregation or filtering as required to deliver the data as communicated from the Provider to the Consumer.

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 a one (Consumer) to many (Provider) connections. Similarly, a Provider may not need to distinctly know and establish a 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 the same system or device acting as a Provider, 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 provide the proxying, brokering or routing functions for the actual data, e.g. Posture Assessment Information flow. Note that Controllers may be implemented to only provide the management and control functions or only the data proxy/broker function or both.

3.2. Interfaces between Consumers, Providers, and Controllers

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 demonstrates 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 proxy or could be embedded in a Consumer or a Provider).

TODO - add text around the usage of various protocols for endpoint data collection (SNMP, NETCONF, etc.?)

4. Component Capabilities

TODO: Intro text about capabilities

4.1. Control Plane Capabilities

TODO: Intro text about control plane capabilities

TODO: Determine whether broker, proxy, and repository need to be full subsections or paragraphs in this section.

Broker: Intermediary negotiating connection between provider and consumer.

Proxy: Intermediary negotiating on behalf of a consumer.

Repository: Intermediary receiving and storing data from a provider, and providing stored data to a consumer.

4.2. Data Plane Capabilities

TODO: Intro text about data plane capabilities

4.2.1. Collector

A collector consumes Guidance and/or other Posture Assessment Information; it provides Posture Assessment Information. Collectors may be internal or external.

4.2.1.1. Internal Collector

TODO

4.2.1.2. 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:

- A RADIUS server whereby an endpoint has logged onto the network

- A network profiling system, which discovers and classifies network nodes
- A Network Intrusion Detection System (NIDS) sensor
- A vulnerability scanner
- A hypervisor that peeks into the endpoint, the endpoint being a virtual machine
- A management system that configures and installs software on the endpoint

4.2.1.3. Collector Interactions With Target Endpoints

TODO

4.2.2. 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.

[kkw-i don't think this conflicts with the definition in the terminology doc re: that evaluation tasks evaluate posture attributes.]

[cek-I like the change. I think it *does* require a change in the terminology doc, though.]

Example: a NEA posture validator [RFC5209]

[jmf- a NEA posture validator is not an example of this definition. A NEA posture assessment is, maybe?]

[cek-Why isn't a NEA posture validator an example?]

4.2.3. Report Generator

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

- Endpoint Attribute Assertions, including Evaluation Results
- Other Reports (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.

4.2.4. Data Store

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

5. Example Illustration of Capabilities and Workflow

TODO: revise all this text

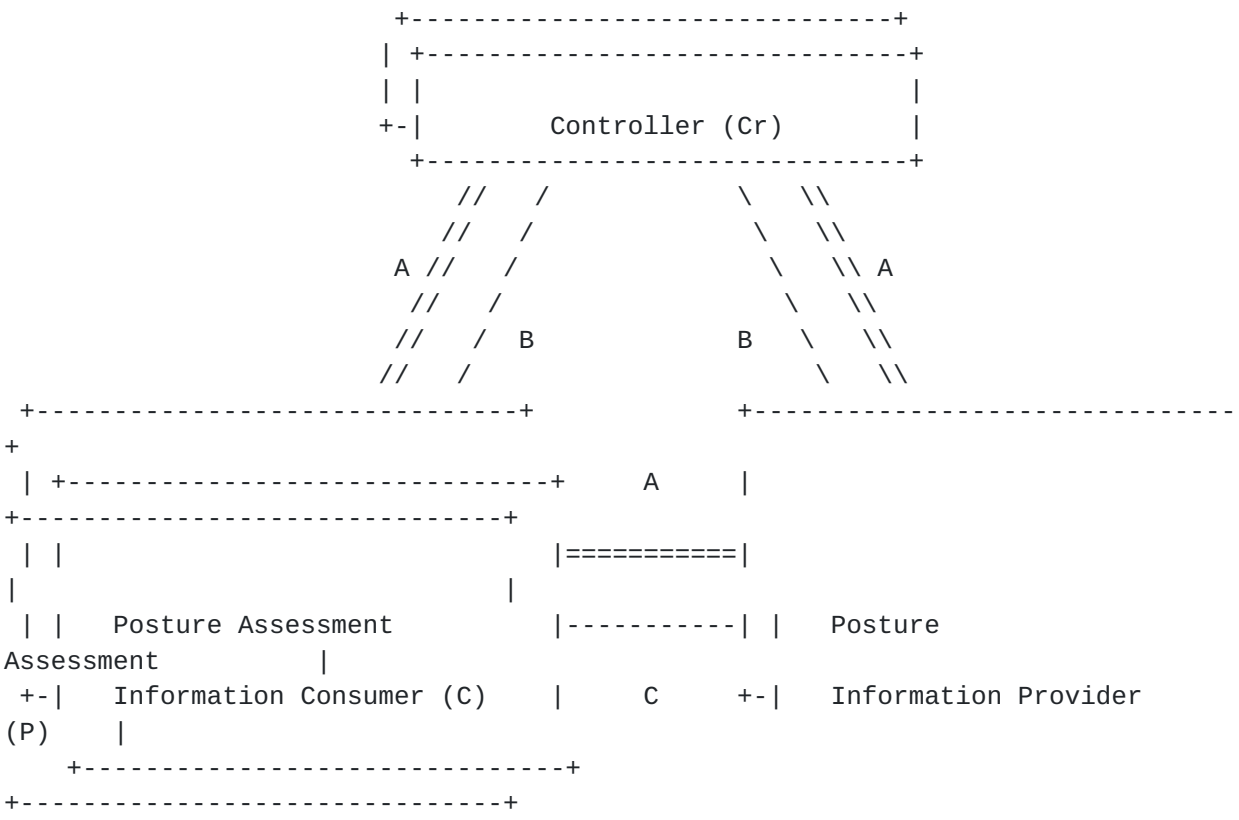

Figure 2: Communications Model

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:

Posture Assessment Information 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 Posture Assessment Information 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.

Posture Assessment Information Consumers: a Consumer may request or receive one or more posture attributes or posture assessment information from a Posture Assessment Information 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.

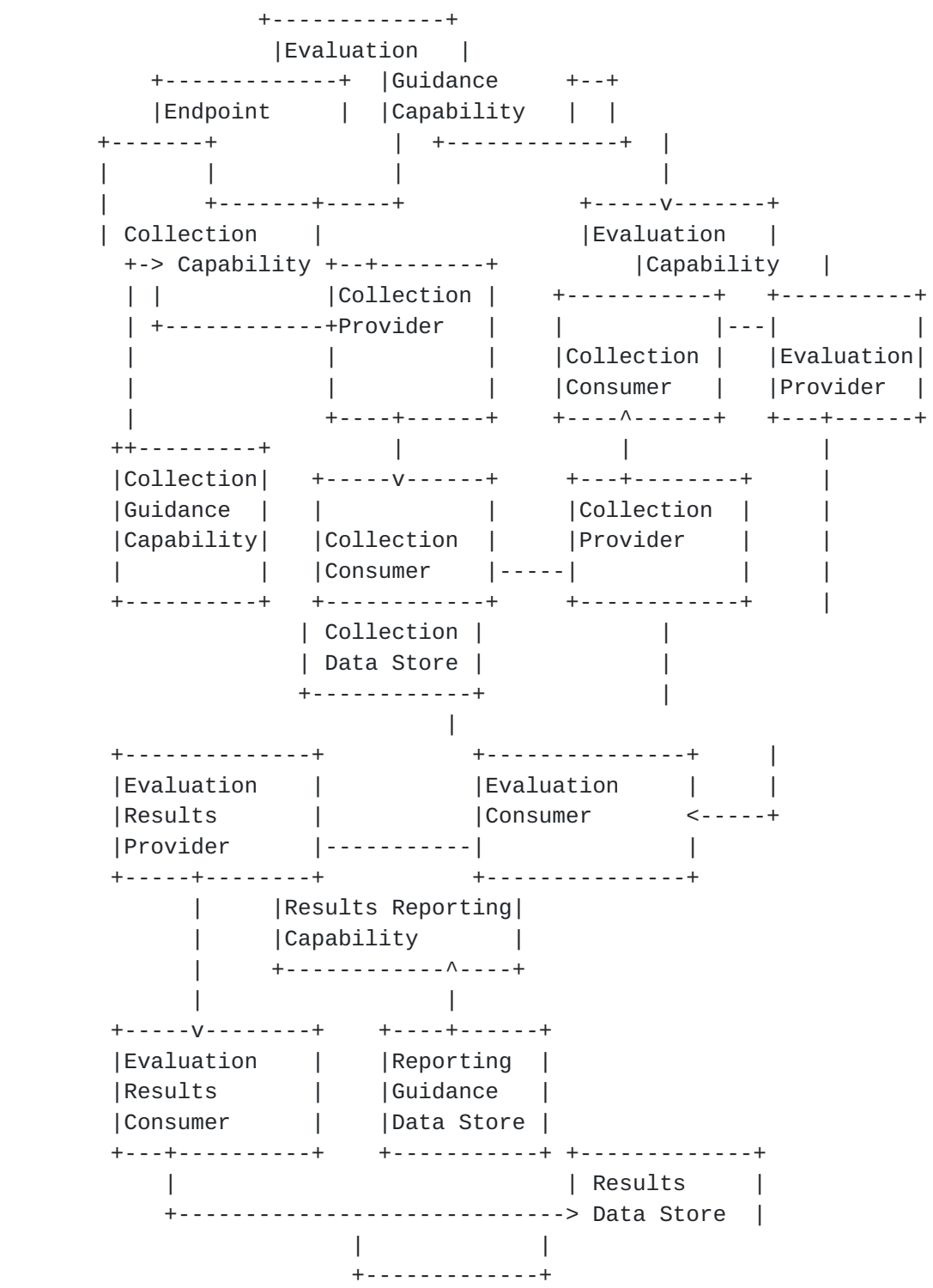

Figure 3: Example Posture Information Flow

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

6. 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.

7. IANA Considerations

This memo includes no request to IANA.

8. 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 (MiM) 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 tampering, 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.

9. References

9.1. Normative References

[I-D.ietf-sacm-requirements]
Cam-Winget, N. and L. Lorenzin, "Secure Automation and Continuous Monitoring (SACM) Requirements", draft-ietf-sacm-requirements-02 (work in progress), October 2014.

[I-D.ietf-sacm-terminology]
Waltermire, D., Montville, A., Harrington, D., and N. Cam-Winget, "Terminology for Security Assessment", draft-ietf-sacm-terminology-05 (work in progress), August 2014.

[I-D.ietf-sacm-use-cases]
Waltermire, D. and D. Harrington, "Endpoint Security Posture Assessment - Enterprise Use Cases", draft-ietf-sacm-use-cases-07 (work in progress), April 2014.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

9.2. Informative References

[RFC3444] Pras, A. and J. Schoenwaelder, "On the Difference between Information Models and Data Models", RFC 3444, January 2003.

[RFC5209] Sangster, P., Khosravi, H., Mani, M., Narayan, K., and J. Tardo, "Network Endpoint Assessment (NEA): Overview and Requirements", RFC 5209, June 2008.

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