SACM
Internet-Draft
Intended status: Informational
Expires: December 26, 2014

N. Cam-Winget, Ed.
B. Ford
Cisco Systems
L. Lorenzin
Juniper Networks
I. McDonald
High North Inc
A. Woland
Cisco Systems
June 24, 2014

Secure Automation and Continuous Monitoring (SACM) Architecture
draft-camwinget-sacm-architecture-00

Abstract

This document describes an 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 December 26, 2014.

Table of Contents

1. Introduction

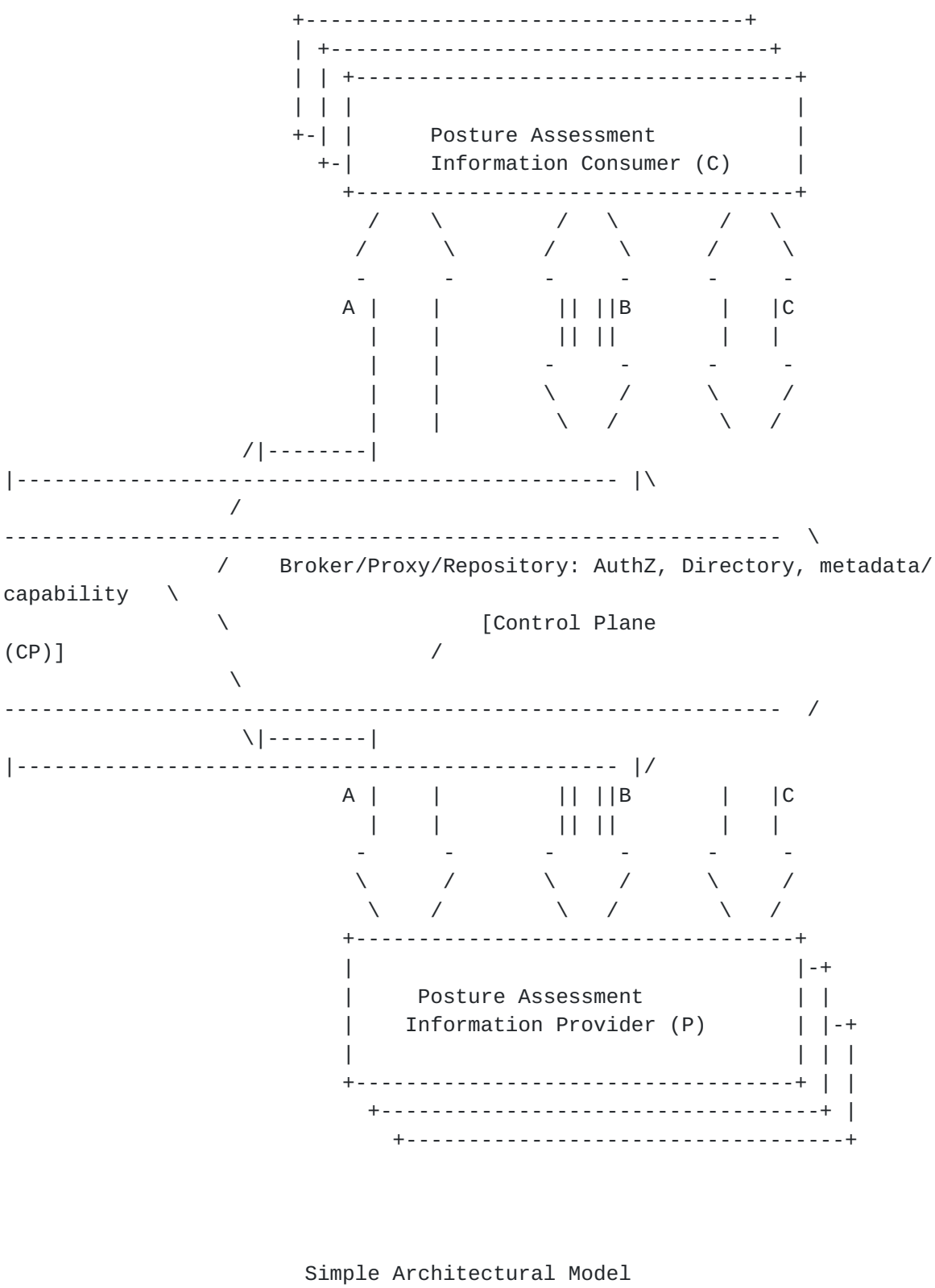
Several data models and protocols are in use today that allow different applications to perform the collection, acquisition and assessment of posture. These applications can vary from being focused on general system and security management to specialized configuration, compliance and control systems. 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 describes an architecture to enable standardized collection, acquisition, and verification of Posture and Posture Assessments. The architecture will include the components and interfaces that can be used to better identify the Information Model, type(s) of transport protocols needed for communication, and further, provide a model from which requirements can be drawn.

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

2. Architectural Overview

Figure 1 shows a proposed SACM architecture. Three main functional components are defined: a Posture Assessment Information Consumer (C), a Posture Assessment Information Provider (P) and a Control Plane (CP) used to facilitate some of the security functions such as authentication and authorization and other metadata functions.



Simple Architectural Model

The functional components in the proposed architecture are further described in this section.

2.1. 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 defines the capabilities and functions that must be handled in order to facilitiate 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.

The Control Plane (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.

2.2. Posture Assessment Information Provider

The Posture Assessment Information Provider (P or Provider) is the component that contributes Posture Assessment Information 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 defines the capabilities and functions that must be handled to share or provide Posture Assessment information. A Provider may provide the information spontaneously, or in response to a direct request from a Consumer. The information may be filtered or truncated to honor the request either by the Consumer's request, or the Providers's ability to filter (or provide only a subset of the requested information) or 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.

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.

2.3. Control Plane

The Control Plane may be an abstracted component but is distinctly defined as a component to execute on some of the security functions and overall system functions. Some of the functions include:

Authentication: with use cases where Consumers may request information independent of knowing the identities of the Providers and Providers may want to share the information unsolicited, the architecture must account for an abstraction where a control plane or a broker may be defined to affect the authentication of the Consumers and Providers independent of the actual information sharing communication channel.

Authorization: to address security for how Posture Assessment Information is shared between the Consumers and Providers, at minimum a management function to define those policies are needed. However, with the introduction of the control plane with use cases where R's may request information independent of knowing the identities of the P's and Providers (P's) wanting to share the information unsolicited, the architecture must account for an abstraction where a control plane or a broker may be defined to affect the authentication of the R's and P's 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 Control Plane also provides those services.

Discovery/Registration: 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; that is, through the 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 its "capability" for the Posture Assessment Information it can share and how it can share it (e.g. protocol or with filtering capabilities). Enabling this function through a broker or control plane 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.

The Control Plane also 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 (Consumers) to many (Provider) connections. Note that the Control Plane also allows for the direct discovery and connection between a Consumer and Provider.

2.4. Interfaces between Consumers, Providers and Control Plane

As shown in Figure 1, communication can proceed with the following interfaces and expected functions and behaviors:

A: interface "A" 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 control plane component (e.g. the control plane could be a proxy or could be embedded in a Consumer or a Provider).

B: interface "B" 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).

C: interface "C" 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.

3. Acknowledgements

The authors would like to thank Jessica Fitzgerald-McKay, Trevor Freeman, Jim Bieda and Adam Montville for participating in the architecture design discussions that lead to this draft.

4. IANA Considerations

This memo includes no request to IANA.

5. Security Considerations

TBD. This section will need to cover the AAA and confidentiality/ integrity of the data and data transports to be considered. Also, the considerations for the interfaces (which may be covered in transports) between the Consumers, Providers, and the Control Plane.

6. References

6.1. Normative References

[I-D.ietf-sacm-terminology]
Waltermire, D., Montville, A., Harrington, D., and N. Cam-Winget, "Terminology for Security Assessment", draft-ietf-sacm-terminology-04 (work in progress), May 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.

6.2. 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

Brian Ford
Cisco Systems
5507-10 Nesconset Hwy #242
Mt Sinai, NY 11766
US

Email: brford@cisco.com

Lisa Lorenzin
Juniper Networks
3614 Laurel Creek Way
Durham, NC 27712
US

Email: llorenzin@juniper.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