Security Automation and Continuous Monitoring WG
Internet-Draft
Intended status: Informational
Expires: February 16, 2015

D. Waltermire
NIST
A. Montville
Tripwire
D. Harrington
Effective Software
N. Cam-Winget
Cisco Systems

August 15, 2014

Terminology for Security Assessment
draft-ietf-sacm-terminology-05

Abstract

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

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 February 16, 2015.

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.

This document is expected to be a temporary work product, and will probably be incorporated into the architecture or other document.

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.

2.1. Pre-defined Terms

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 this document 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.

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)."

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.

Based on the previous definition of an asset, an endpoint is a type of asset.

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] distinguished an information model as being protocol and implementation neutral whereas a data model would provide such details.

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 this document to represent the state information that is collected from an endpoint (e.g. software/hardware inventory, configuration settings). The state information may constitute one to many 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 state (e.g. configuration setting, installed software, hardware). The phrase "features of the endpoint" refers to installed software or software components.

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.

2.2. New Terms and Definitions

This section defines terms that are not explictly defined in the IETF.

Asset characterization

Asset characterization is the process of defining attributes that describe properties of an identified asset.

Asset Management

The process by which assets are provisioned, updated, maintained and deprecated.

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.

Broker

An entity providing and/or connecting services on the behalf of other architectural components. Within the SACM Architecture, for example, a broker may provide authorization services and find, upon request, entities providing requested services.

Building Block

For SACM, a building block is a unit of functionality that may apply to more than one use case and can be supported by different components of an architectural model.

Capability

The extent of an architectural component's ability. For example, a Posture Information Provider may only provide endpoint management data, and then only a subset of that data.

Client

An architectural component receiving services from another architectural component.

Collection Task

The process by which posture attributes or values are collected.

Consumer

An architectural component receiving information from another architectrual component.

Evaluation Task

The process by which posture attributes are evaluated.

Endpoint Target

The endpoint of interest.

Endpoint Discovery

The process by which an endpoint can be identified.

Evaluation Result

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

Expected Endpoint State

The required state of an endpoint that is to be compared against.

Function

A behavioral aspect of a particular architectural component, which belies that component's purpose. For example, the Management Plane can provide a brokering function to other SACM architectrual components.

Management Plane (TBD per list; was "Control Plane")

Architectural component providing common functions to all SACM participants, including authentication, authorization, capabilities mappings, and the like.

Provider

An architectural component providing information to another architectrual component.

Proxy

An architectural component providing functions, information, or services on behalf of another component, which is not directly participating in the architecture.

Repository

An architectural component intended to store information of a particular kind. A single repository may provide the functions of more than one repository type (i.e. configuration baseline repository, assessment results repository, etc.)

Role

A label representing a collection of functions provided by a particular architectural component.

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.

Supplicant

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

2.3. 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].

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

6.1. ietf-sacm-terminology-01- to -02-

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.

6.2. ietf-sacm-terminology-01- to -02-

Added Vulnerability, Vulnerability Management, xposure, Misconfiguration, and Software flaw.

6.3. ietf-sacm-terminology-02- to -03-

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.

7. References

7.1. Normative References

[I-D.ietf-sacm-use-cases]
Waltermire, D. and D. Harrington, "Endpoint Security Posture Assessment - Enterprise Use Cases", draft-ietf-sacm-use-cases-06 (work in progress), March 2014.

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

7.2. Informative References

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

[RFC4949] Shirey, R., "Internet Security Glossary, Version 2", RFC 4949, August 2007.

[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

David Waltermire
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, Maryland 20877
USA

Email: david.waltermire@nist.gov

Adam W. Montville
Tripwire
101 SW Main Street, 15th floor
Portland, Oregon 97204
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
US

Email: ncamwing@cisco.com