SACM
Internet-Draft
Intended status: Informational
Expires: May 19, 2016

J. Fitzgerald-McKay, Ed.
Department of Defense
November 16, 2015

Endpoint Compliance Standard
draft-fitzgeraldmckay-sacm-endpointcompliance-01

Abstract

This document describes how published standards can be used to meet SACM endpoint compliance use cases.

Status of This Memo

This Internet-Draft will expire on May 19, 2016.

Copyright Notice

Table of Contents

1. Introduction

This document proposes leveraging the Network Enterprise Assessment (NEA) architecture [RFC5209], work from the Trusted Computing Group's (TCG) Trusted Network Connect (TNC) Work Group, and the ISO Software Identification (SWID) Tag Standard [ISO.19770-2] as a starting place for building an endpoint compliance solution.

The SACM Information Model [I-D.ietf-sacm-information-model] defines an internal collector to gather posture attributes from an endpoint. These posture attributes must be communicated to a server that can store the attributes in a data repository. This repository of endpoint identities and attributes is where work can take place to validate the attributes.

The NEA architecture was originally designed for access control use cases. Using the TLS-based Posture Transport Protocol (PT-TLS) [RFC6876], the same architecture can be reused to collect large amounts of compliance data. Work from the TCG's TNC work group expands on this, enabling standardized communication of SWID Tags to a NEA server. Based on these standards, SACM can define actions that can be performed on endpoint posture attributes to ensure compliance, including:

1. ensuring that all network-connected endpoints are known, and authorized to access network resources;

2. confirming that only authorized applications are running on the endpoint;

3. knowing that all applications are patched and up-to-date; and,

4. ensuring that applications with known vulnerabilities can be located and patched.

2. Focus on a Way Forward

In light of SACM's new focus and the need for quick wins that get SACM closer to its goals, we would like to open discussion on standardizing the collection, communication and evaluation of endpoint software load reports. This meets a number of SACM use cases [I-D.ietf-sacm-use-cases]. Many of these standards already exist and are captured in the TCG's Endpoint Compliance Profile [Endpoint-Compliance-Profile]. Implementations are also publically available, such as the strongSwan TNC implementation [strongSwan].

3. Existing Protocols and Schema for Internal Data Collection

The Trusted Computing Group's TNC Work Group has additional standards that could be incorporated into the NEA architecture to specify how internal data collection can be used for security automation. The Integrity Measurement Collector Interface (IF-IMC) [IF-IMC] could be used to describe a standardized interface between a posture collector and a NEA client on an endpoint. Likewise, the Integrity Measurement Verifier Interface (IF-IMV) [IF-IMV] could provide an interface between a posture validator and a NEA Server. Both of these standards are critical additions to the NEA architecture that improve the security and interoperability of the messaging between components.

The SACM Information Model calls out a number of components that tie directly to the existing NEA architecture. The Posture Collector described by NEA [RFC5209] is a SACM Internal Collector, and the Posture Validator is a SACM evaluator. The PT-TLS protocol standardized by NEA addresses the SACM Information Model's security considerations by providing an authenticated, confidential channel through which posture attribute-value pairs can be communicated, with assurance that the communicated data has not been modified.

In recent years, TNC has worked to specify SWID Message and Attributes for IF-M [SWID-Messages]. This standard uses NEA and TCG architectural elements to collect and validate software identities using the ISO Software Identification Tag Standard. It also enables a NEA server to automate the storage of SWID tags for later evaluation, separating collection and evaluation roles. Server Discovery and Validation [Server-Discovery] ensures that the endpoint only communicates with trusted servers.

4. An Architecture for Internal Data Collection

Using these standards, we can begin to build an architecture for internal data collection that addresses SACM's use cases. An endpoint is connected to the network, and using the Server Discovery

and Validation protocol, locates a trusted server, and connects to it over PT-TLS. A SWID Collector gathers SWID tags from a directory on the endpoint, and communicates them over IF-IMC to the Posture Broker (PB) Client. The Posture Broker Client then communicates this data to the Posture Transport Server via the Posture Broker Protocol [RFC5793].

While NEA included validation capabilities on its server, SACM requires the separation of collection and evaluation. Certain features of Posture Attribute validators, such as the evaluation of collected data against network policy or guidance, will be best performed at the data repository. Other features, such as the ability to request data from an endpoint, should remain on the server. SACM will have to decide how to best separate these function. For now, a SACM Server will work as a place holder for the PB Server plus any functionality from the NEA Posture Validator that the group chooses to retain on the server. The SACM Server will also be responsible for storing collected data in a data repository, where it will be made available to evaluators.

```
      Endpoint                          Server
+------------------+             +------------------+
|                  |             |                  |
| +--------------+ |             |
|                                           Evaluators
| |SWID Collector| |             |
|                                     +------------------+
| +--------------+ |             |                  |            Data
Repository          | +------------------+
|        |         |             |                  |
+-----------------+        | | +------------------+
|        | IF-IMC  |             |                  |
|                 |        | | |                  |
|        |         |             |                  |
|                 |        | | |                  |
| +--------------+ |             | +--------------+ |
|                 |        | | |                  |
| |   PB Client  | |             | | SACM Server  +------------
+                 +------------+                  |
| +--------------+ |             | +--------------+ |
|                 |        | | |                  |
|        |         |             |         |        |
|                 |        | | |                  |
|        | PB      |             |         | PB     |
|                 |        +-+-|                  |
|        |         |             |         |        |
+-----------------+            +------------------+
| +--------------+ |             | +--------------+ |
| |   PT Client  +-----------------+   PT Server  | |
| +--------------+ |   PT-TLS    | +--------------+ |
|                  |             |                  |
+------------------+             +------------------+
```

Figure 1

5. Future Work

This collection of standards provides a reasonable basis upon which we can build a SACM solution that focuses on the applications that are running on different types of endpoints, and the work that can be performed on this data when it is collected securely by an authorized server and stored in an data repository. We intend, in the coming months, to ask the TNC to submit these standards to SACM for inclusion in our first version solution, as they meet our newly scoped goals of collecting state information from a subset of endpoint types.

More work is needed to build out the capabilities in this set of standards. Agreeing to use them as a starting point will clarify our work and help scope out future efforts.

6. IANA Considerations

This memo includes no request to IANA.

7. Security Considerations

Each of the standards referenced in this internet draft contains its own security considerations section. This internet draft does not itself propose any new security considerations.

8. Informative References

[Endpoint-Compliance-Profile]
Trusted Computing Group, "TNC Endpoint Compliance Profile Specification", December 2014.

[I-D.ietf-sacm-information-model]
Waltermire, D., Watson, K., Kahn, C., and L. Lorenzin, "SACM Information Model", draft-ietf-sacm-information-model-02 (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.

[I-D.narten-iana-considerations-rfc2434bis]
Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", draft-narten-iana-considerations-rfc2434bis-09 (work in progress), March 2008.

[IF-IMC] Trusted Computing Group, "TCG Trusted Network Connect TNC IF-IMC, Verion 1.3", February 2013.

[IF-IMV] Trusted Computing Group, "TCG Trusted Network Connect TNC IF-IMV, Version 1.4", December 2014.

[ISO.19770-2]
"Information technology -- Software asset management -- Part 2: Software identification tag", ISO/IEC 19770-2, 2009.

[RFC3552] Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", BCP 72, RFC 3552, DOI 10.17487/RFC3552, July 2003, <http://www.rfc-editor.org/info/rfc3552>.

[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>.

[RFC5793] Sahita, R., Hanna, S., Hurst, R., and K. Narayan, "PB-TNC: A Posture Broker (PB) Protocol Compatible with Trusted Network Connect (TNC)", RFC 5793, DOI 10.17487/RFC5793, March 2010, <http://www.rfc-editor.org/info/rfc5793>.

[RFC6876] Sangster, P., Cam-Winget, N., and J. Salowey, "A Posture Transport Protocol over TLS (PT-TLS)", RFC 6876, DOI 10.17487/RFC6876, February 2013, <http://www.rfc-editor.org/info/rfc6876>.

[Server-Discovery]
Trusted Computing Group, "DRAFT: TCG Trusted Network Connect PDP Discovery and Validation, Version 1.0", August 2013.

[strongSwan]
strongSwan, "Trusted Network Connect (TNC) HOWTO", April 2015, <https://wiki.strongswan.org/projects/strongswan/wiki/TrustedNetworkConnect>.

[SWID-Messages]
Trusted Computing Group, "DRAFT: TCG Trusted Network Connect SWID Message and Attributes for IF-M, Version 1.0", March 2015.

Author's Address

Jessica Fitzgerald-McKay (editor)
Department of Defense
9800 Savage Road
Ft. Meade, Maryland
USA

Email: jmfitz2@nsa.gov