SACM C. Coffin
Internet-Draft D. Haynes
Intended status: Informational C. Schmidt
Expires: January 7, 2016 The MITRE Corporation
J. Fitzgerald-McKay
Department of Defense
July 6, 2015

SACM ECP Mapping
draft-haynes-sacm-ecp-mapping-00

Abstract

This document builds upon [I-D.fitzgeraldmckay-sacm-endpointcompliance] to demonstrate how published IETF, ISO, and TCG standards, available today, can be used to accomplish the use cases outlined in [I-D.ietf-sacm-use-cases].

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

In [I-D.fitzgeraldmckay-sacm-endpointcompliance], several existing standards are identified as aligning with the needs of SACM and are suggested for possible incorporation, either by reference or by adoption, into the set of solutions in the SACM architecture. These standards include the suite of network interfaces defined in the IETF Network Endpoint Assessment (NEA) workgroup, and some additional specifications from the Trusted Computing Group's (TCG's) Trusted Network Communications (formerly Trusted Network Connect) (TNC) [TNC] workgroup. The NEA architecture [RFC5209] is based on the TNC architecture and both are interoperable. The NEA/TNC architecture provide standards-based mechanisms to collect endpoint state and configuration information and securely transmit it to some authority where the information is evaluated against criteria. This aligns closely with the overall SACM goals of "...an architecture to enable standardized collection, acquisition, and verification of Posture and Posture Assessments." This document provides a more detailed mapping of the NEA specifications, as well as some additional TNC specifications that standardize additional behaviors within the NEA/TNC architecture, to the use cases defined for SACM.

At the heart of this proposal is the Endpoint Compliance Profile (ECP) [Endpoint-Compliance-Profile]. The ECP is a high-level standard describing a specific combination and application of NEA and TNC protocols and interfaces specifically designed to support ongoing monitoring of endpoint state and the controlled exposure of collected information to appropriate security applications. The ECP uses the components specified in the NEA/TNC architecture and also defines roles for the additional TNC specifications mentioned in [I-D.fitzgeraldmckay-sacm-endpointcompliance], namely IF-IMC [IF-IMC], IF-IMV [IF-IMV], SWID Message and Attributes for IF-M [SWID-Messages], and Server Discovery and Validation. (The latter is

referred to as PDP Discovery and Validation [Server-Discovery] in the ECP as the ECP predated the expansion of that specification's scope.) The ECP dictates the use of specific standards and also clarifies requirements for optional features in order to better standardize assessment practices. The following sections outline how the use of standards in accordance with the ECP can also meet SACM's use cases.

In the descriptions below, IETF NEA terminology is used where possible. The table below indicates TNC and NEA terms for corresponding standards and functional units. TCG terms that do not have a NEA counterpart but which are mentioned in the ECP are also identified.

+--------------------------------------+-------------------+

TCG Standards	IETF Standards
IF-T TLS	PT-TLS (RFC 6876)
IF-T EAP	PT-EAP (RFC 7171)
IF-TNCCS	PB-TNC (RFC 5793)
IF-M	PA-TNC (RFC 5792)
TNC	NEA (RFC 5209)
IF-IMC	-
IF-IMV	-
SWID Message and Attributes for IF-M	-
Server Discovery and Validation	-
Endpoint Compliance Profile	-

Table 1: Mapping Between TNC and NEA Standards

TCG Terminology	IETF Terminology
Access Requestor	NEA Client
Policy Decision Point	NEA Server + added enforcement capabilities
Integrity Measurement Collector	Posture Collector
Integrity Measurement Validator	Posture Validator
TNC Client	Posture Broker Client
TNC Server	Posture Broker Server
Network Access Requestor	Posture Transport Client
Network Access Authority	Posture Transport Server

Table 2: Mapping Between TNC and NEA Functional Units

The following sections describe where each of the standards mentioned in the ECP fit into use cases 2, 3, and 4 of [I-D.ietf-sacm-use-cases]. Use case 1 is a much higher-level set of capabilities and requirements and so is not treated separately.

2. Endpoint Identification and Assessment Planning

The Endpoint Identification and Assessment Planning use case (section 2.1.2 of [I-D.ietf-sacm-use-cases]) involves "discovery of endpoints, understanding their composition, identifying the desired state to assess against, and calculating what posture attributes to collect to enable evaluation." Several of the TNC specifications and architectural components identified in the ECP are directly applicable to these activities.

The first step in the assessment process is to discover the endpoints on the network. The NEA Architecture allows enterprises to enforce a policy where endpoints (a.k.a., NEA Clients) are only allowed onto the network if they contact a NEA Server and provide measurements to demonstrate their compliance with enterprise policy. In such an enterprise, this would ensure that all endpoints on the network were known. Added security and flexibility for this activity can be provided by the Server Discovery and Validation specification, which can be leveraged to ensure that NEA Clients are connecting to trusted servers before they register themselves and send sensitive information.

When a NEA Client first connects to a NEA Server, and on an as-needed basis after that, it can be required to provide posture information that helps to identify the endpoint on the network and characterize its nature, which is critical in determining if an endpoint qualifies as the target of an assessment. Posture information is collected by Posture Collectors on the NEA Client. Once collected, the Posture Collectors securely transmit the attributes back to the Posture Validators on the NEA Server via the PA-TNC (NEA "application" layer) [RFC5792], PB-TNC (NEA "routing" layer) [RFC5793] and either PT-TLS or PT-EAP (NEA "transport" layer) protocols. The collected posture information may also be stored in a CMDB or data repository for later use in assessment targeting and evaluation. Beyond any identifying information collected by the Posture Collectors, the PT-TLS [RFC6876] and PT-EAP [RFC7171] protocols both support certificate-based authentication of the client.

The NEA/TNC architecture is designed to be highly flexible and extensible. The IF-IMC (connecting Posture Collectors to Posture Broker Clients) and IF-IMV (connecting Posture Validators to Posture Broker Servers) interfaces allow a range of Posture Collectors and Posture Validators, respectively, to be employed. The standard

interfaces mean that new Collector/Validator pairs supporting different types of posture information can be easily added to the assessment infrastructure to meet the needs of individual enterprises. For example, SWID Message and Attributes for IF-M defines a standard way to collect and transport a NEA Client's SWID tag inventory information, which can be very useful in understanding a NEA Client's role and its exposure to software vulnerabilities.

Once posture information has been collected, the Posture Validators evaluate the information. Based on this evaluation, the Validators can suggest access control decisions, recommend further assessment of the NEA Client, or take other actions. For example, a NEA Client can be required to provide a SWID tag inventory (using the SWID Message and Attributes for IF-M protocol) when it initially seeks to connect to an enterprise, when a Posture Collector detects a change to the SWID tag inventory, or when it is requested by the NEA Server. The Posture Validator that receives this information might examine the SWID tags of a particular NEA Client and discover that the NEA Client is running a web server. Based on this, the NEA Client may be subject to additional assessment in its role as a web server for the enterprise. Another NEA Client may submit a SWID tag for a piece of software with a known vulnerability. Based on this, the Posture Validator may determine that this NEA Client requires further examination to determine whether mitigating steps have been taken to protect it from the vulnerability.

3. Endpoint Posture Attribute Value Collection

The Endpoint Posture Attribute Value Collection use case (section 2.1.3 of [I-D.ietf-sacm-use-cases]) follows from the previous use case. The overall goal of this use case is to determine which additional endpoint posture attribute values are needed and then perform the collection. The use case that follows (2.1.4 Posture Attribute Evaluation) uses the attribute values to perform an evaluation of the attributes and their values as part of an overall assessment.

In the current use case, the NEA Client(s) in question have already been authenticated and have been granted access to the network. The NEA Client(s) have also been identified and characterized (i.e., OS type and version, hardware platform, etc.) based on the collected information. Some attribute and attribute values from this step may be cached or stored in a CMDB or data repository and may be used within the current use case.

Now that the NEA Client is part of the network, a more extensive assessment and/or periodic reassessments can be performed in order to ensure detailed, ongoing compliance with policies. The data

collected during this activity could include additional or updated identification and characterization attributes or information to support assessment against checklists or other guidance. Depending on the needs of the enterprise and the nature of the guidance it uses, different Posture Collector/Validator pairs can be employed to gather and transmit this information. As mentioned earlier, the IF-IMV and IF-IMC standards allow these Collectors/Validators to be added to the assessment infrastructure seamlessly. If different information needs to be delivered to different NEA Servers for assessment, the Server Discovery and Validation can help NEA Clients identify and validate the authenticity of those servers.

Multiple events could trigger a posture attribute value collection. Some of those events could be triggered on the NEA Client, such as the detection of a change in posture. Other events could trigger the NEA Server to collect attributes, such as the detection of specific network events or net flows, the receipt of new guidance, requirements for periodic reassessment, or a manually triggered assessment by an administrator. All such triggers are supported by the NEA architecture. In particular, Posture Collectors can be instructed to monitor for changes in their attribute set of interest and automatically report events of interest to Posture Validators. Similarly, Posture Validators can be triggered to gather information from a NEA Client in a variety of ways. The process of attribute exchange uses the same set of NEA protocols here as outlined in the preceding use case, namely PA-TNC, PB-TNC, and PT-TLS or PT-EAP.

The SWID Message and Attributes for IF-M specification provides an excellent example of this capability. The SWID IMV (a Posture Validator) can request a variety of types of information about an endpoint's SWID tag collection based on guidance, a periodic trigger, and/or manual requests. The SWID IMC (a Posture Collector) can also be instructed to monitor the NEA Client's SWID tag collection for changes, and can be instructed to report certain types of changes to the NEA Server automatically. The former capability allows on-demand updates of a NEA Client's SWID tag collection, while the latter allows the NEA Server to be automatically informed of any changes to the NEA Client's SWID tag collection (or subsets thereof) in real time.

4. Posture Attribute Evaluation

The Posture Attribute Evaluation use case (section 2.1.4 of [I-D.ietf-sacm-use-cases]) involves the analysis of posture attribute values, collected from the NEA Client, against the expected values of the posture attributes in order to determine a result. This result can be used to initiate follow up actions. The NEA architecture provides a framework in which this use case can be achieved.

Once a NEA Client resides on the network, the NEA architecture supports a number of triggers that can result in the reassessment of that NEA Client. These triggers and the resulting attribute collection are discussed in more detail in the Endpoint Posture Attribute Value Collection use case described in the preceding section.

This SACM use case emphasizes posture change detection on an endpoint as a triggering condition. As noted earlier, NEA supports this by allowing Posture Collectors to monitor the NEA Client and automatically push information about changes of interest. Such Posture Collectors may be configurable to be selective in what they report in order to ensure NEA Servers are not deluged by irrelevant data. For example, the SWID Message and Attributes for IF-M specification supports configuring SWID IMCs with lists of specific tags to monitor and/or can be configured only to report how a NEA Client's SWID tag collection has changed since the last update.

Once the Posture Validator has the required inputs to carry out the evaluation, it can perform this evaluation and return a result. The result of this evaluation is passed to the Posture Broker Server which then initiates any necessary response. For example, upon evaluation of a NEA Client's SWID tag collection, it might be determined that a newly installed piece of software is not on the organization's whitelist of authorized software. Depending on enterprise policy, this may result in a simple alert to an administrator, or something as proactive as removal of the NEA Client from the enterprise network.

5. Conclusion

Several years ago, the Trusted Computing Group offered several of their TNC standards to the IETF and these eventually became the NEA standards. If SACM feels that the additional TNC standards discussed here have value, it is hoped that TCG will again be willing to offer them for IETF adoption. Doing this does more than just provide a shortcut to the publication of useful, tested IETF RFCs - it helps unify the approaches of TCG and IETF rather than creating multiple separate solutions to the challenges of automated cyber defense. Consolidating standards around a proven approach not only accelerates standards development but aids consumers by avoiding a multiplicity of competing standards.

More generally, this document shows that the described TNC and NEA standards align well with SACM use cases. While they do not address every identified building block of these use cases, they address a large number of them, and the NEA/TNC architecture supports extension points where other standards can be applied to address any missing capabilities. By the same token, because the NEA/TNC architecture so closely aligns with SACM needs, developing a new solution would lead to redundant, competing solutions for many of the activities that SACM seeks to support. For these reasons, the authors urge SACM to consider use of NEA/TNC standards in general, and the ECP in particular, in the development of the SACM architecture.

6. IANA Considerations

This memo includes no request to IANA.

All drafts are required to have an IANA considerations section (see the update of RFC 2434 [I-D.narten-iana-considerations-rfc2434bis] for a guide). If the draft does not require IANA to do anything, the section contains an explicit statement that this is the case (as above). If there are no requirements for IANA, the section will be removed during conversion into an RFC by the RFC Editor.

7. Security Considerations

All drafts are required to have a security considerations section. See RFC 3552 [RFC3552] for a guide.

8. Informative References

[Endpoint-Compliance-Profile]
Trusted Computing Group, "TNC Endpoint Compliance Profile Specification, Version 1.0", December 2014.

[I-D.fitzgeraldmckay-sacm-endpointcompliance]
Fitzgerald-McKay, J., "Endpoint Compliance Standard", draft-fitzgeraldmckay-sacm-endpointcompliance-00 (work in progress), May 2015.

[I-D.ietf-sacm-use-cases]
Waltermire, D. and D. Harrington, "Endpoint Security Posture Assessment - Enterprise Use Cases", draft-ietf-sacm-use-cases-09 (work in progress), March 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, Version 1.3", February 2013.

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

[RFC3552] Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", BCP 72, RFC 3552, July 2003.

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

[RFC5792] Sangster, P. and K. Narayan, "PA-TNC: A Posture Attribute (PA) Protocol Compatible with Trusted Network Connect (TNC)", RFC 5792, March 2010.

[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, March 2010.

[RFC6876] Sangster, P., Cam-Winget, N., and J. Salowey, "A Posture Transport Protocol over TLS (PT-TLS)", RFC 6876, February 2013.

[RFC7171] Cam-Winget, N. and P. Sangster, "PT-EAP: Posture Transport (PT) Protocol for Extensible Authentication Protocol (EAP) Tunnel Methods", RFC 7171, May 2014.

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

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

[TNC] Trusted Computing Group, "TCG Trusted Network Connect TNC Architecture for Interoperability, Version 1.5", February 2012.

Authors' Addresses

Chris Coffin
The MITRE Corporation
202 Burlington Road
Bedford, MA 01730
USA

Email: ccoffin@mitre.org

Daniel Haynes
The MITRE Corporation
202 Burlington Road

Bedford, MA 01730
USA

Email: dhaynes@mitre.org

Charles Schmidt
The MITRE Corporation
202 Burlington Road
Bedford, MA 01730
USA

Email: cmschmidt@mitre.org

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

Email: jmfitz2@nsa.gov