Network Working Group
Internet Draft
Intended status: Informational
Expires: April 2013

S. Hanna
Juniper Networks
October 15, 2012

Standard Assessment Protocols and Formats for SACM
draft-hanna-sacm-assessment-protocols-00.txt

Abstract

The draft charter for the SACM BOF at IETF 85 calls for the development of "continuous assessment interfaces". This draft points out several existing documents that provide a good start in this area.

Status of this Memo

This Internet-Draft will expire on April 15, 2013.

Copyright Notice

Table of Contents

1. Introduction

The draft charter for the SACM BOF at IETF 85 [1] calls for the development of "continuous assessment interfaces". This text from the draft charter provides more detail about what's desired:

> 2. Define, either by normative reference, adoption, or creation, a set of standards that can be used to continuously assess and report on the state of systems, composed of many different types of devices and networks, operated by varying personnel, to ensure security process effectiveness in a pre-defined or ad-hoc manner. This area of focus provides for integration protocols supporting plug and play continuous assessment and security automation networking within an enterprise.

Actually, there are several specifications from IETF and other organizations that provide a very good start on addressing this problem. More work is certainly needed but the SACM BOF should be aware of these documents.

2. Languages and Enumerations

The SCAP specification [2] lists a large number of languages and enumerations that are useful for remote security assessment: XCCDF [3], OVAL [4], OCIL [5], Asset Identification [6], CCE [7], CPE [8], and CVE [9]. Since there is a great deal of implementation experience with these specifications, they should certainly be considered by the SACM BOF or any successor Working Group.

3. Protocols

The IETF NEA Working Group has defined an architecture and a layered set of protocols for remote assessment of endpoint security posture: the NEA Architecture [10], PA-TNC [11], PB-TNC [12], PT-TLS [13], and PT-EAP [14]. These protocols are designed to be used either at the time that an endpoint connects to a network or continuously after the endpoint is connected to the network.

The NEA protocols are based on the Trusted Network Connect (TNC) protocols, which were created by the Trusted Computing Group (TCG) and donated to the IETF. The TCG contributed the TNC specifications to the IETF in full compliance with BCP 78 [15] and BCP 79 [16], transferring change control and copyright to the IETF (among other things). The IETF took full advantage of this change control, adopting the TNC standards through an open and competitive process but adapting them to the IETF’s needs and processes. For example, the IETF renamed all the TNC protocols: IF-M became PA-TNC, IF-TNCCS became PB-TNC, IF-T Binding for TLS became PT-TLS, and IF-T Binding for Tunneled EAP Methods became PT-EAP.

Because the NEA protocols are based on the TNC protocols, they benefit from the experiences of and feedback from millions of users, thousands of customers, and dozens of vendors and open source implementers who have used the TNC protocols. For example, users strongly prefer quick and efficient checks when waiting to get on the network. Therefore, all the NEA protocols use a binary encoding and minimize round trips. Still, vendors need extensibility so the NEA specs permit vendor-specific extensions while requiring that vendors work without them.

Two of the NEA protocols (PA-TNC and PB-TNC) were published as Proposed Standards in 2010. At the same time, the TCG issued updated TNC protocol specs (IF-M 1.0 [17] and IF-TNCCS 2.0 [18]) that correspond exactly to the NEA specs, thus ensuring that the two architectures remain in alignment. The other two NEA specs (PT-TLS and PT-EAP) are expected to be published as Proposed Standards within the next few months. TCG may reasonably be expected to again issue updated versions of the corresponding TNC specs to maintain alignment. Customer and vendor adoption is expected to be rapid for these specs since the old versions were widely implemented and the new specs are a simple upgrade from the old. Even vendors who have long used proprietary protocols have indicated their plans to support the new open standard protocols.

4. Merging The Two

While the NEA protocols define the format for some simple posture checks (anti-virus or host firewall status, OS patch level), they do not define standards that approach the level of detail that sophisticated enterprise customers need and can achieve with SCAP.

At the same time, SCAP does not define any standards for gathering SCAP content from an endpoint. This is left to the vendor, resulting in a situation where each vendor must place a software agent on the endpoint in order to assess that endpoint (or settle for an external scan, which has lower fidelity).

What’s needed to fully satisfy the SACM BOF’s charter item on continuous assessment interfaces is a standard for conveying the SCAP languages and enumerations in the NEA protocols.

Fortunately, the TCG has recently published exactly this document. The TCG’s SCAP Messages for IF-M specification [19] was published for Public Review on TCG’s web site on October 3, 2012. This document describes how SCAP content should be carried over the NEA (TNC) protocols. It includes support for provisioning SCAP content to endpoints, for rapidly and efficiently gathering assessment results when a device connects to the network, for gathering exhaustive information in the background after the device is connected to the network, and for continuously monitoring changes to configuration.

While the TCG has not made any official statements about its intent with respect to donating this specification to IETF, I believe that the TCG would be glad to do so if the IETF charters a Working Group to work on continuous assessment interfaces. I should know about this. I’m co-chair of the TCG’s Trusted Network Connect Work Group.

5. Next Steps

The SACM BOF participants should review the new SCAP Messages for IF-M specification to see if it meets their needs. If they find deficiencies, they should notify the TCG by sending email to SCAP-Messages-Comments@trustedcomputinggroup.org.

Within IETF, we should review and discuss these documents to see if they are relevant to the SACM effort. Do they meet the need for continuous assessment interfaces that was described in the proposed SACM charter? If not, what changes are needed? Could those changes be made using these specs as a starting point, assuming that the TCG donated the specs to the IETF with all rights and full change control? And should this work happen in a new Working Group or should it happen in the NEA Working Group, which already has five years of experience with this topic.

The IETF discussions should happen on the sacm@ietf.org list. I would also be glad to lead a discussion of this topic at the SACM BOF at IETF 85.

6. Security Considerations

This document describes several existing standards relating to endpoint assessment and configuration management. Each of these specifications includes its own Security Considerations section so the reader is referred to those documents for more details.

7. IANA Considerations

This document has no actions for IANA.

8. References

8.1. Informative References

[1] SACM BOF Draft Charter, http://www.ietf.org/mail-archive/web/sacm/current/msg00628.html

[2] U.S. NIST, "The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.2", NIST Special Publication 800-126 Revision 2, September 2011.

[3] U.S. NIST, "Specification for the Extensible Configuration Checklist Description Format (XCCDF) Version 1.2", NIST Interagency Report 7275 Revision 4, September 2011.

[4] The MITRE Corporation, "The OVAL(R) Language Specification Version 5.10.1", January 2012.

[5] U.S. NIST, "Specification for the Open Checklist Interactive Language (OCIL) Version 2.0", NIST Interagency Report 7692, April 2011.

[6] U.S. NIST, "Specification for Asset Identification 1.1", NIST Interagency Report 7693, June 2011.

[7] The MITRE Corporation, http://cce.mitre.org

[8] U.S. NIST, http://scap.nist.gov/specifications/cpe

[9] The MITRE Corporation, http://cve.mitre.org

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

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

[12] 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.

[13] Sangster, P., N. Cam-Winget, and J. Salowey, "PT-TLS: A TCP-based Posture Transport (PT) Protocol", draft-ietf-nea-pt-tls-07.txt (work in progress), August 2012.

[14] Cam-Winget, N. and P. Sangster, "PT-EAP: Posture Transport (PT) Protocol For EAP Tunnel Methods", draft-ietf-nea-pt-eap-03.txt (work in progress), July 2012.

[15] Bradner, S. and J. Contreras, "Rights Contributors Provide to the IETF Trust", RFC 5378, November 2008.

[16] Bradner, S., "Intellectual Property Rights in IETF Technology", RFC 3979, March 2005.

[17] Trusted Computing Group, "IF-M: TLV Binding", Version 1.0, Revision 37, March 2010.

[18] Trusted Computing Group, "IF-TNCCS: TLV Binding", Version 2.0, Revision 16, January 2010.

[19] Trusted Computing Group, "SCAP Messages for IF-M", Version 1.0, Revision 16, October 2012.

9. Acknowledgments

This document was prepared using 2-Word-v2.0.template.dot.

Author’s Address

Steve Hanna
Juniper Networks, Inc.
79 Parsons Street
Brighton, MA 02135
USA
Email: shanna@juniper.net