SACM Working Group
Internet-Draft
Intended status: InformationalNational Institute of Standards and Techno
Expires: May 4, 2017

D. Waltermire
S. Banghart

October 31, 2016

Definition of the ROLIE Software Descriptor Extension
draft-banghart-sacm-rolie-softwaredescriptor-00

Abstract

This document extends the Resource-Oriented Lightweight Information Exchange (ROLIE) core to add the information type category and related requirements needed to support Software Record and Software Inventory use cases. The 'software-descriptor' information type is defined as a ROLIE extension. Additional supporting requirements are also defined that describe the use of specific formats and link relations pertaining to the new information type.

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 May 4, 2017.

Table of Contents

1. Introduction

This document defines an extension to the Resource-Oriented Lightweight Information Exchange (ROLIE) protocol to support the publication of software descriptor information. Software descriptor information is information that characterizes:

an installable software package, or

information about static software components that may be installed by a software package or patch.

Software descriptor information includes identifying, versioning, software creation and publication, and file artifact information. Software descriptor information provides data about what might be installed, but doesn't describe where or how a specific software installation is installed, configured, or executed.

Software descriptor information can be used in the following ways:

Software providers can publish software descriptor information so that software researchers and users of software can understand the collection of software produced by a that software provider.

Organizations can aggregate and syndicate collections of software descriptor information provided by multiple software providers to support software-related analysis processes (e.g., vulnerability analysis) and value added information (e.g., software configuration checklist repositories) using identification and characterization information derived from software descriptor information.

End user organizations can consume sources of software descriptor information, and other related software vulnerability and configuration information to provide the data needed to automate software asset, patch, and configuration management practices.

This document supports these use cases by describing the content requirements for Collections of software descriptor information that are to be published to or retrieved from a ROLIE repository. This document also discusses requirements around the use of link relationships and describing the data model formats used in a ROLIE Entry describing a software descriptor information resource.

TODO: describe how this approach differs from the SWIMA approach.

2. Terminology

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 [RFC2119].

Definitions for some of the common computer security-related terminology used in this document can be found in Section 2 of [RFC5070].

3. New information-types

This document defines the following information type:

3.1. The "software-descriptor" information type

The "software-descriptor" information type represents any information that describes a piece of software. This document uses the definition of software provided by [RFC4949]. Note that as per this definition, this information type pertains to static software, that is, code on the disc. The software-descriptor information type is

intended to provide a category for information that does one or more of the following:

identifies and characterizes software This software identification and characterization information can be provided by a large variety of data, but always describes software in a pre-installed state.

provides software installer metadata This represents information about software used to install other software. This metadata identifies, and characterizes a software installation package or media.

describes stateless installation metadata Information that describes the software post-deployment, such as files that may be deployed during an installation. It is expected that this metadata is produced generally for a given installation, and may not exactly match the actual installed files on a given endpoint.

Provided below is a non-exhaustive list of information that may be considered to be of a software-descriptor information type.

- Naming information: IDs and names that aid in the identification of a piece of software

- Version and patching information: Version numbers, patch identifiers, or other information that

- Vendor and source information: Includes where the software was developed or distributed from, as well as where the software installation media may be located.

- Payload and file information: information that describes or enumerates the files and folders that make up the piece of software, and information about those files.

- Descriptive information and data: Any information that otherwise characterizes a piece of software, such as libraries, runtime environments, target OSes, intended purpose or audience, etc.

Note again that this list is not exhaustive, any information that in is the abstract realm of an incident should be classified under this information-type.

This information type does not include descriptions of running software, or state and configuration information that is associated with a software installation.

4. Usage of CSIRT Information Types in the Atom Publishing Protocol

This document does not specify any additional requirements for use of the Atom Publishing Protocol.

5. Usage of the software-descriptor Information Type in the atom:feed element

This document does not specify any additional requirements for use of the atom:feed element.

6. Usage of the software-descriptor Information Type in an atom:entry

This document specifies the following requirements for use of the software-descriptor information type with regards to Atom Entries.

6.1. Use of the atom:link element

This section defines the requirements around the use of atom:links in Entries. Each relationship should be named,described, and given a requirement level. TODO

Name	Description	Conformance
ancestor	Links to a software descriptor resource that defines an ancestor of the software being described by this Entry.	MAY
patches	Links to a software descriptor resource that defines the software being patched by this software	MAY
requires	Links to a software descriptor resource that defines a piece of software required for this software to function properly.	MAY
installs	Links to a software descriptor resource that defines the software being installed by this software.	MAY
installationrecord	Provides a link to a resource that describes an installation of this software.	MAY

Table 1: Link Relations for Resource-Oriented Lightweight Indicator Exchange

6.2. Use of the rolie:format element

New supported data formats would be described here alongside any other rolie:format requirements.

6.2.1. The ISO SWID 2016 format

The ISO SWID Tag 2016 format is a software descriptor and software record data format. It provides several tags: primary, which provides descriptive and naming information about software, patch, which describes non-standalone software meant to patch existing software, and corpus, which describes the software installation media that installs a given piece of software.

For a more complete overview as well as normative requirements, refer to TODO(ref?):ISO/IEC 19770-2

7. IANA Considerations

7.1. incident information-type

IANA has added an entry to the "ROLIE Security Resource Information Type Sub-Registry" registry located at <https://www.iana.org/assignments/rolie/category/information-type> .

The entry is as follows:

name: software-descriptor

index: TBD

reference: This document, Section 3.1

8. Security Considerations

9. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC5070] Danyliw, R., Meijer, J., and Y. Demchenko, "The Incident Object Description Exchange Format", RFC 5070, DOI 10.17487/RFC5070, December 2007, <http://www.rfc-editor.org/info/rfc5070>.

[RFC4949] Shirey, R., "Internet Security Glossary, Version 2", FYI 36, RFC 4949, DOI 10.17487/RFC4949, August 2007, <http://www.rfc-editor.org/info/rfc4949>.

Appendix A. Schema

This document does not require any schema extensions.

Appendix B. Examples of Use

TODO: Add examples of Use

Authors' Addresses

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

Email: david.waltermire@nist.gov

Stephen Banghart
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, Maryland 20877
USA

Email: stephen.banghart@nist.gov