INTERNET-DRAFT   R. Housley
Intended Status: Informational   Vigil Securiy
Expires: January 12, 2014   S. Turner
                                                              IECA
                                                     July 11, 2013

sacm: Asset Identifier
draft-handt-sacm-asset-identifiers-00

Abstract

This document examines the asset identifiers available for sacm and it proposes that OIDs (Object Identifiers) be selected as the asset identifier format.

Status of this Memo

Copyright and License Notice

1. Introduction

The meaning of the terms identity, identification, and identifier are often conflated. This document uses and proposes that sacm use the terms as defined in [RFC4949], where system entity is replace by asset:

- Asset identity is "the collective aspect of a set of attribute values (i.e., a set of characteristics) by which [an asset] is recognizable or known."

- Asset identification is an "act or process that presents an identifier to a system so that the system can recognize [an asset] and distinguish it from other [assets]."

- An asset identifier is a "data object -- often, a printable, non-blank character string -- that definitively represents a specific identity of [an asset], distinguishing that identity from all others."

You've got an identity, we've got an identity, we've all got an identity. Even assets have at least one identity. For the purpose of this document, an asset is any computing based hardware and the software, including operating system, that runs on the hardware. Examples of computing devices include laptops, tablets, servers, routers, and telephones but as more and more devices are computerized this could expand to the break room's toaster [Arkko].

Obviously, assets exist therefore they have an identity and because they exist (and they cost money to build or buy) enterprises will manage them. It cost money to buy the asset so there is little doubt they should be tracked to make sure at minimum the asset does not find itself disappeared. More to the point, enterprises do not wish their assets to misbehave. When the toaster starts acting like a flame thrower, it is a very bad day in the break room.

Identifiers are an easy way to sum up the asset's identity that uniquely identifies it from other assets of the same type. If there's two toasters in the break room and only one is misbehaving,

then it would be good to know which one is misbehaving; it's even more important to know which asset is misbehaving if there are ninety thousand IP-based sensors in a building and one is acting up.

The identifier is also import because asset identifiers enable authenticated identities that in turn serve as basis for security services such as peer entity authentication.

This document examines the proposes that OIDs (Object Identifiers) be used as the asset identifier in sacm (a proposed wg at the time this was submitted).

2. Identifiers

Identifiers are a dime a dozen. Some make sense and some do not. This section will examine some options, but first it propose some requirements.

For asset identification to work, application developers, os (operating system) vendors, and hardware manufacturers need to be the ones assigning identifiers. Interacting with a 3rd party to obtain an identifier would add unacceptable complexity.

Asset identifiers need not include all of the identity's attribute values in the identifier. In the same way an X.509 certificate often only includes a country name, organization, and common name but not hair color, height and weight.

Asset identifiers need not have any inherent semantic meaning that's the job for metadata.

2.1. Identifier Format Options

2.1.1. CPE

Common Platform Enumeration (CPE) "is a structured naming scheme for information technology systems, software, and packages" and it is a "method of describing and identifying classes of applications, operating systems, and hardware devices present among an enterprise's computing assets." It is a product of US NIST (National Institute of Standards and Technology) Computer Security Division, Information Technology Laboratory, sponsored by the US DHS's (Department of Homeland Security's) National Cyber Security Division. All intellectual property has been transferred to NIST [CPE-IPR].

CPE is a four part document set [CPE]. CPE's specifications define the naming scheme (the format and binding of names) and matching rules for the names. Also defined is a dictionary (aka repository or

directory) that holds the names and metadata about the names that can be accessed for lookups and searches presumably to ensure there's no duplication amongst the names. Finally, an application language is defined for applicability statements (aka logical expressions) using WFNs (Well-Formed Names) "to tag checklists, policies, guidance, and other documents with information about the product(s) to which the documents apply."

In terms of asset identifiers, the naming document applies as well as the requirements in the directory document for which of the 7 WFN name attributes are required. The remaining documents, the name matching, the application language, and the rest of the directory document, are not germane to the asset identifier topic.

A WFN (Well-Formed Name), as defined in the CPE naming document, is "a logical construct only" and "is not intended to be a data format, encoding, or any other kind of machine-readable representation for machine interchange and processing." The URI (Uniform Resource Identifiers) [RFC3986] and formatted string bindings are the machine-readable representation for machine interchange and processing. A WFN has 7 naming attributes (whose purposes are pretty self-explanatory so this document does not copy the definitions but instead leaves it to the motivated reader to read NIST's specifications): part, vendor, product, version, update, edition, language, sw_edition, target_sw, target_hw, other. Part (application, operating system, hardware), vendor, product, and version must be present, as specified in the directory document.

A major issue with a WFN as the asset identifier is it's scope. CPE provides identifiers for platforms, including both hardware and software, but not to the level necessary to act as the asset identifier because it lacks the ability to disambiguate between hardware of software of the same type.

Another major issue with CPE is process by which one is obtained; an application needs to be submitted to NVD (National Vulnerability Database), which is run by the USG (United States Government). This simple fact likely renders CPE, as it is currently specified and operated, as unsatisfactory as the basis for sacm because there will be some non-US entity unwilling or unable to submit an application.

3.1.2.2. SWID

Software Identifier (SWID), documented in ISO/IEC 19770-2:2009, is as its name implies an identifier for software. SWIDs can be assigned by software developers or by organizations that purchased software without a SWID.

Complaints about SWID include:

- o The standards is not free. In terms of IETF process, this is not show stopper. The standard must be publicly available and it even it costs some.

- o SWIDs aren't free. This is not entirely clear because there appeared to be a way for opensource software to receive a tag.

  Note that Software Entitlement (SWEN) Tags, documented in ISO/IEC 19770-3, are likely a non-starter in the IETF because of DRM issues.

  The reason SWIDs obviously can't be the identifier is that

3.1.2.3. Protocol Identifiers

Protocol identifiers encompass identifiers such as MAC (Media Access Control), IPv4 [RFC791], IPv6 [RFC2460], as well as IPv6's CGAs (Cryptographically Generated Addresses) [RFC3972][RFC4581][RFC4982] and UUIDs (Universal Unique Identifiers) [RFC4122]. None of these are appropriate for the asset identifier for sacm because of their scope.

3.1.2.6. OIDs

OIDs are abstract and can actually represent anything. OIDs are cheap, and there are ways to get them for free. OIDs can be obtained from the IANA PEN (Private Enterprise Number) Registry [IANA-PEN] or from the ITU's UUID OID page [I-UUID].

OIDs are also already used by management protocols SNMP and for identifying hardware modules for firmware distribution [RFC4108].

4. Recommendations

Select OIDs as the asset identifier format.

5. Security Considerations

Identifiers that include inherent semantic meaning may divulge information about that asset if the identifier is not protected at rest and in transit.

6. IANA Considerations

There are no IANA considerations present in this document.

If OIDs are chosen as the asset identifier, then entities wishing to use OIDs may obtain them using the procedures

7. References

7.1 Normative References

[RFC4949] Shirey, R., "Internet Security Glossary, Version 2", FYI 36, RFC 4949, August 2007.

7.2 Informative References

[RFC791] Postel, J., "Internet Protocol", STD 5, RFC 791, September 1981.

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[RFC3972] Aura, T., "Cryptographically Generated Addresses (CGA)", RFC 3972, March 2005.

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, January 2005.

[RFC4108] Housley, R., "Using Cryptographic Message Syntax (CMS) to Protect Firmware Packages", RFC 4108, August 2005.

[RFC4122] Leach, P., Mealling, M., and R. Salz, "A Universally Unique IDentifier (UUID) URN Namespace", RFC 4122, July 2005.

[RFC4581] Bagnulo, M. and J. Arkko, "Cryptographically Generated Addresses (CGA) Extension Field Format", RFC 4581, October 2006.

[RFC4982] Bagnulo, M. and J. Arkko, "Support for Multiple Hash Algorithms in Cryptographically Generated Addresses (CGAs)", RFC 4982, July 2007.

[CPE] https://nvd.nist.gov/cpe.cfm
https://csrc.nist.gov/publications/nistir/ir7695/NISTIR-7695-CPE-Naming.pdf

https://csrc.nist.gov/publications/nistir/ir7696/NISTIR-7696-CPE-Matching.pdf

https://csrc.nist.gov/publications/nistir/ir7697/NISTIR-7697-CPE-Dictionary.pdf

https://csrc.nist.gov/publications/nistir/ir7698/NISTIR-7698-CPE-Language.pdf

[CPE-IPR] https://cpe.mitre.org/index.html

[IANA-PEN] http://pen.iana.org/pen/PenApplication.page

[I-UUID] http://www.itu.int/ITU-T/asn1/uuid.html#registration

[Arkko] http://online.wsj.com/article/SB10001424052702303544604576434013394780764.html

Authors' Addresses

Russ Housley
Vigil Security, LLC
918 Spring Knoll Drive
Herndon, VA 20170
USA

Email: : housley@vigilsec.com

Sean Turner
IECA, Inc.
3057 Nutley Street, Suite 106
Fairfax, VA 22031
USA

Email: turners@ieca.com