Information Model Update

SACM WG Virtual Interim Meeting

01/25/2016

Agenda

- Status
- Overview of IPFIX IM Syntax
- Examples
- Next steps

Status

- Updated to -03[1]
  - Submitted version based on previous changes (basically what was on GitHub)
  - A few other minor updates (e.g. Use Cases I-D published as an RFC, etc.)

- Selected the IPFIX IM syntax for the SACM IM[2]
  - IM for IPFIX [RFC 7012][3]
  - Export of Structured Data in IPFIX [RFC 6313][4]
  - Guidelines for Authors and Reviewers of IPFIX IEs [RFC 7013][5]
  - IANA Registry of IPFIX IEs[6] (reuse where possible)

[1] http://www.ietf.org/mail-archive/web/sacm/current/msg03689.html

[2] http://www.ietf.org/mail-archive/web/sacm/current/msg03705.html

[3] https://datatracker.ietf.org/doc/rfc7012/

[4] https://datatracker.ietf.org/doc/rfc6313/

[5] https://datatracker.ietf.org/doc/rfc7013/

[6] http://www.iana.org/assignments/ipfix/ipfix.xhtml

Overview of the IPFIX IM Syntax (1)

- All Information Elements (IEs) MUST have the following properties
  - name
  - elementId
  - description
  - dataType
  - status

- IEs MAY have the following properties
  - dataTypeSemantics
  - units
  - range
  - reference

- Organization-specific IEs MUST have a enterpriseId property

Overview of the IPFIX IM Syntax (2)

- IEs can be combined using the following abstract types
  - basicList – represents a list of zero or more instances of any IE
  - subTemplateList – represents a list of zero or more instances of a single, specific Template
  - subTemplateMultiList – represents a list of zero or more instances of any Template

Example 1 – Network Interface

```
elementId: 1
name: interfaceName
dataType: string
status: current
description: A short name uniquely describing an interface,
             eg "Eth1/0". See [RFC2863] for the definition
             of the ifName object.
---
elementId: 2
name: interfaceIndex
dataType: unsigned32
status: current
description: The index of an interface installed on an
             endpoint. The value matches the value of
             managed object 'ifIndex' as defined in
             [RFC2863]. Note that ifIndex values are not
             assigned statically to an interface and that
             the interfaces may be renumbered every time
             the device's management system is re-
             initialized, as specified in [RFC2863].
---
elementId: 3
name: interfaceMacAddress
dataType: macAddress
status: current
description: The IEEE 802 MAC address associated with a
             network interface on an endpoint.
---
```

```
elementId: 5
name: interfaceFlags
dataType: unsigned16
status: current
description: This information element specifies the flags
             associated with a network interface. Possible
             values include:
                 -0x1   interface is up
                 -0x2   broadcast address valid
                 -0x4   turn on debugging
                 -0x8   is a loopback net
                 -0x10  interface is point-to-point link
                 ...
---
elementID: 6
name: networkInterface
dataType: basicList
status: current
description: Information about a network interface
             installed on an endpoint. The following high-
             level diagram describes the structure of
             networkInterface information element.

             networkInterface = (basicList, allof,
                 interfaceName,
                 interfaceIndex,
                 macAddress,
                 ifType,
                 flags
             )
---
```

Example 2 – Software Instance

```
elementId: 7
name: softwareIdentifier
dataType: string
status: current
description: A globally unique identifier for a particular
             software application.
---
elementId: 8
name: title
dataType: string
status: current
description: The title of the software application.
---
elementId: 10
name: simpleVersion
dataType: simpleVersionType
status: current
description: The version string for a software application
             that follows the simple versioning scheme.
---
elementId: 11
name: rpmVersion
dataType: rpmVersionType
status: current
description: The version string for a software application
             that follows the RPM versioning scheme.
---
```

```
elementId: 13
name: softwareVerison
dataType: basicList
status: current
description: The version of the software application.
             Software applications may be versioned using a
             number of schemas. The following high-level
             diagram describes the structure of the
             softwareVersion information element.

             softwareVersion(basicList, exactlyOneOf,
                 simpleVersion,
                 rpmVersion,
                 ...
             )
---
elementId: 15
name: softwareInstance
dataType: subTemplateMultiList
status: current
description: Information about an instance of software
             installed on an endpoint. The following
             high-level diagram describes the structure of
             softwareInstance information element.

             softwareInstance = (subTemplateMultiList, allof,
                 softwareIdentifier,
                 title,
                 creator,
                 softwareVersion,
                 lastUpdated
             )
---
```

Next steps

- Specify existing SACM IEs in the IPFIX IM syntax
- Solicit WG for feedback on mandatory-to-implement IEs
  - Architecture and Requirements
  - Vulnerability Assessment Scenario
  - Existing data models (SCAP, CIM, SWID, APP-ID, etc.)
- Define mandatory-to-implement IEs in the IM
  - We need help

1. http://www.ietf.org/mail-archive/web/sacm/current/msg03163.html