HS SEDI
Homeland Security Systems Engineering and Development Institute

MAEC™

v1.1 Update

December 14, 2010

Ivan Kirillov

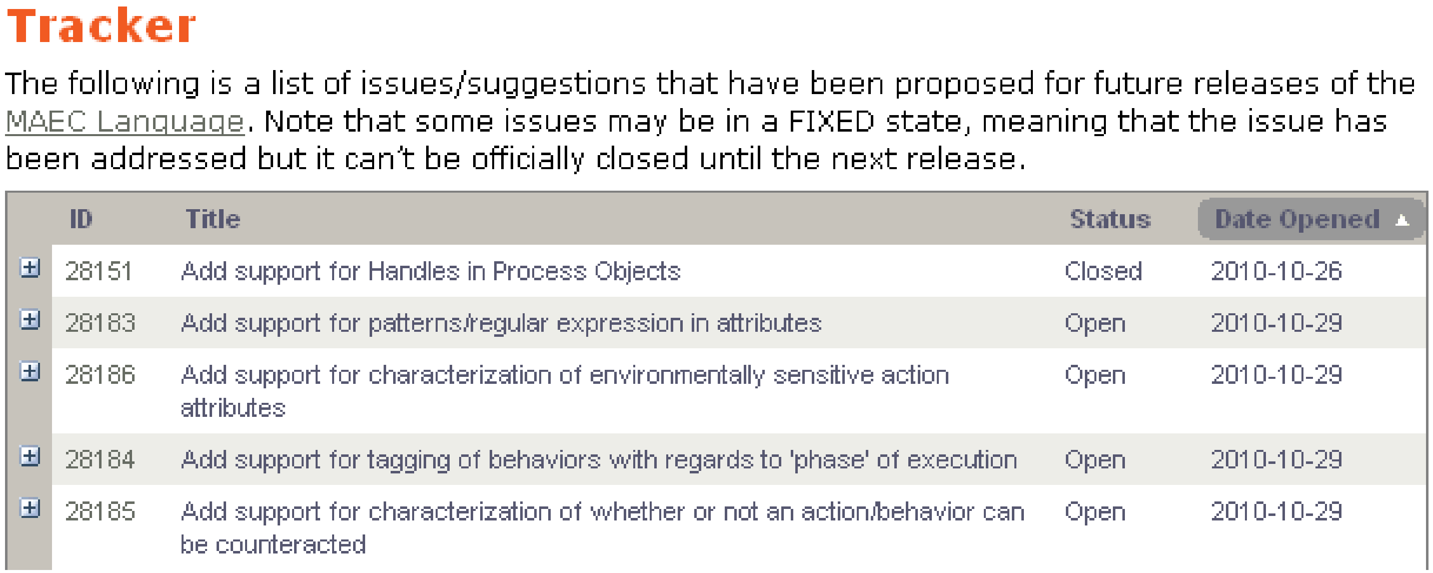
Homeland Security

Fixed/Resolved Issues from v1.01 (1/2)

- **Added support for handles in process objects**
  - New element under Process_Object_Attributes
- **Added processor family class attribute for CodeType**
  - Can be used for specifying processor architecture, using enumerated list of architectures, e.g.
    - X86-32
    - X86-64
    - ARM
    - PowerPC
    - etc.
- **Added support for differentiating between locally & externally bound sockets**
  - New internal_bound_address/external_bound_address elements under Network_Object_Attributes
- **APICall/Code elements made optional under ActionImplementationType**

Fixed/Resolved Issues from v1.01 (2/2)

- **Other, minor tweaks**
  - Defined patterns for IDs
    - Format derived from OVAL, e.g. MAEC:test:act:1 (for an action)
  - Added some enumerated entities
  - Changed some xs:sequence elements to xs:choice
- **All of this can be seen on the new issue tracker at maec.mitre.org:**



Tracker

The following is a list of issues/suggestions that have been proposed for future releases of the MAEC Language. Note that some issues may be in a FIXED state, meaning that the issue has been addressed but it can't be officially closed until the next release.

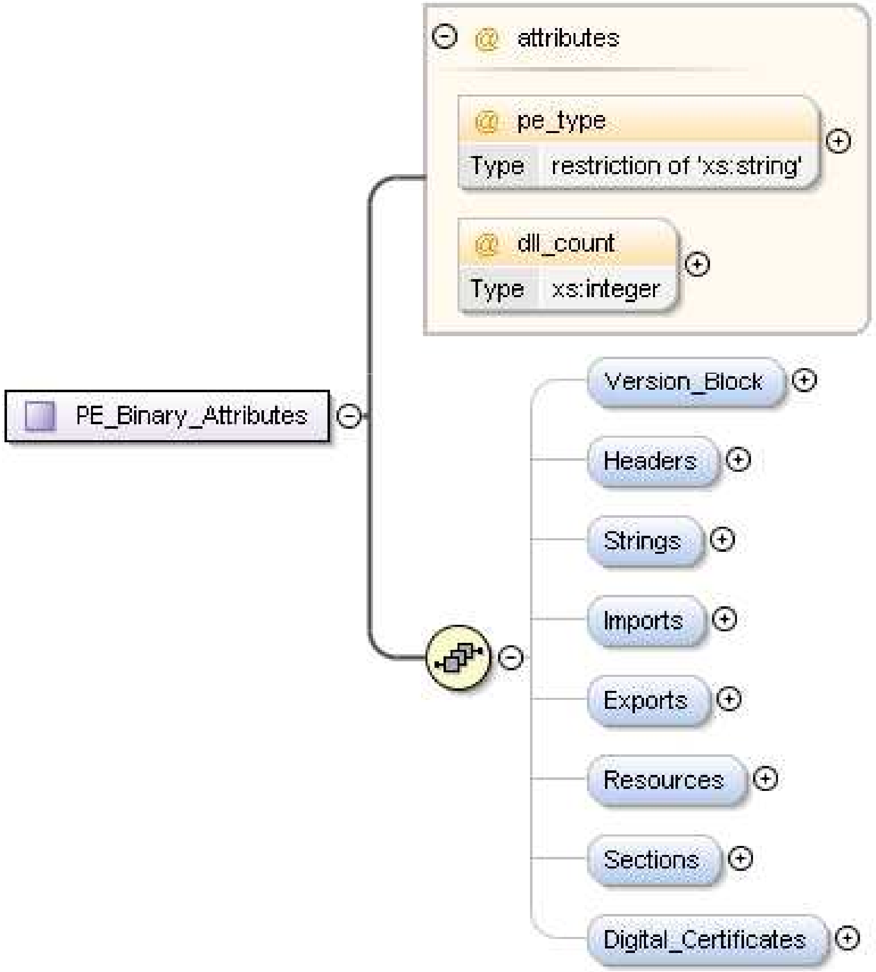
	ID	Title	Status	Date Opened ▲
⊞	28151	Add support for Handles in Process Objects	Closed	2010-10-26
⊞	28183	Add support for patterns/regular expression in attributes	Open	2010-10-29
⊞	28186	Add support for characterization of environmentally sensitive action attributes	Open	2010-10-29
⊞	28184	Add support for tagging of behaviors with regards to 'phase' of execution	Open	2010-10-29
⊞	28185	Add support for characterization of whether or not an action/behavior can be counteracted	Open	2010-10-29

v1.1 Additions – PE Binary Attributes (1/2)

- **Permits characterization of PE binary metadata**
  - Allows MAEC to capture data obtained through static analysis
  - Useful for attribution, detection, etc.
- **Compiled list of attributes, based on community input**
  - See discussion list thread, Handshake discussion
- **High-level overview:**
  - Headers
  - Strings
  - Imports
  - Exports
  - Resources
  - Sections
  - Digital Certificates

v1.1 Additions – PE Binary Attributes (2/2)

- **For testing, created new schema**
  - Available on Handshake



Future MAEC Schema Additions (1/2)

- **Observables schema integration**
  - Shared between MAEC, CAPEC, and CEE
  - Likely replacement for current method of characterizing objects
- **Addition of document metadata attributes**
  - PDF/Office docs
  - Useful for identifying toolkits and other forms of attribution
- **Add support for defining string composition**
  - Many malware strings are randomized or otherwise generated based on some entity (e.g. hostname)
- **Partitioning of enumerations into separate namespace**
  - Permits easy maintenance
  - Allows for addition of entities without alteration of main schema
  - Fixes utility of having ‘other’ for representing a value not found in the enumerations

Future MAEC Schema Additions (2/2)

- **Additional network attributes**
  - Netflow
  - Specific Layer 7 (Protocol) Attributes
  - Metadata
- **Additional memory attributes**
  - IDT addresses, IRP function addresses, etc.
  - Especially relevant to memory forensics
    - E.g. those extracted by Volatility
- **Refinement of behaviors and associated relationships**
- **Support for patterns/regular expression in attributes and elements**
- **Others – any requests?**
  - Post on the discussion list or Handshake, and we will add them to the MAEC issue tracker

Summary

- **MAEC v1.1 will focus on minor fixes, along with the addition of PE binary attributes**

- **ETA: December**
  - Preview copy is already up on Handshake

- **Please submit issues or suggestions to us, and we'll make sure they're discussed and posted to the tracker**

References

- **MAEC Issue Tracker:**
  - http://maec.mitre.org/language/tracker.html
- **Handshake (invitation needed):**
  - http://handshake.mitre.org
- **PE Attribute Discussion:**
  - http://making-security-measurable.1364806.n2.nabble.com/PE-Static-Analysis-Attributes-tp5722339p5722339.html;cid=1291836911437-873