Introducing
draft-stoecker-danyliw-rfc5070bis-00

Paul Stoecker <paul.stoecker@rsa.com>
Roman Danyliw <rdd@cert.org>
IETF 86
March 12, 2013
Defining the Scope

RFC 5070-bis
“Define end notes, relationships between nodes, and actions done to them” ?

RFC 5901
Domain Name
Windows Registry Keys
Files
Mail Headers
HTTP Headers

IODEF Extensions
SCI
CVRF
CVSS
MMDEF
OCIL
XCCDF
CPE
CCSS

Other Community Efforts
CVE
MAEC
OVAL
CEE
CWE
STIX
CAPEC
Open IOC
Enumerated Value Extensibility: Current

Positive
• All “standardized” enumerated values can be checked with XML validation from an RFC-derived schema
• XML validation will not fail on enumerated values

Negative
• No IETF repository for “accepted” additional enumerate values
• Even “widely accepted” additional enumerated values will have to use ext-attribute

<class attribute1="ext-value" ext-attribute="additional-value1">
Enumerated Value Extensibility: Candidate #1

**Positive**
- Public repository and documented process for adding new “accepted” enumerated value

**Negative**
- XML validate using RFC-derived schema will break on new “accepted” enumerated values
Changes from RFC 5070

• All submitted RFC5070 Errata has been implemented with the exception of #17

• Addition of xmlns:ds and import of same namespace (per RFC5091)

• New @indicator_uid and @indicator_set_id attributes to “highlight” (reference) items in the document that can be used as indicators

• Added support for new indicator data types:
  – Service/{Email,EmailSubject,X-Mailer}
  – RecordItem/{FileName,FileHash,WindowsRegistryKey}
  – SoftwareType/HTTPUserAgent
@Indicator-UID and @Indicator-set-ID

- Uniquely reference data in the document that can be used as indicators
- Support relationships between indicators in the same document and across documents
- Quickly find only the indicators and treat the rest as of the information as context
Adding Domain Name Information

• Domain names and associated meta-data is missing. Use of RFC 5901 shows it’s needed.
• There are different options:
  1. Add DNS class in RFC5070-bis (Node/System/RecordData).
  2. Change RFC5901 (current doesn’t represent all DNSfields).
  3. Bring in another schema. (ARF doesn’t seem to cover.)
Other Outstanding Issues

• Revisit internationalization (i.e., @language, @encoding, and MLSTRING)
• Review enum existing values particularly @restriction, NodeRole@category, HistoryItem@action, Impact@type
• Add better reference for RecordPattern@type=regex
• Explore additional annotative for Node/System (e.g., geolocation, Address/url vs. Address@category=url)
• Explore how much more Filesystem, Mail, HTTP, and Windows Registry information to add
• Review specification of Reference
• ... what else?