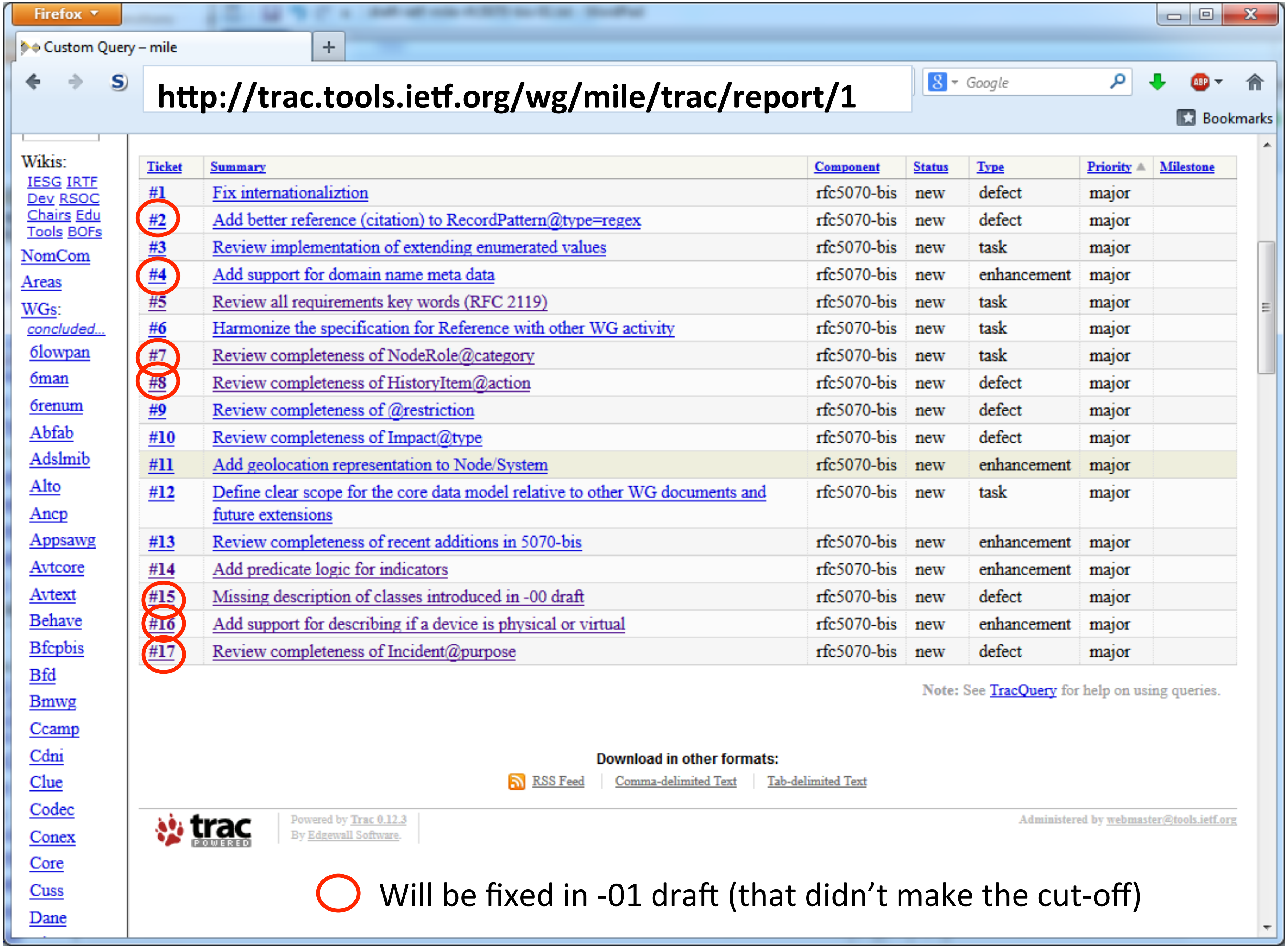
draft-ietf-mile-rfc5070-bis-00

Roman Danyliw <rdd@cert.org>

IETF 87

July 30, 2013



http://trac.tools.ietf.org/wg/mile/trac/report/1

Wikis:
IESG IRTF
Dev RSOC
Chairs Edu
Tools BOFs
NomCom
Areas
WGs:
concluded...
6lowpan
6man
6renum
Abfab
Adslmib
Alto
Ancp
Appsawg
Avtcore
Avtext
Behave
Bfcpbis
Bfd
Bmwg
Ccamp
Cdni
Clue
Codec
Conex
Core
Cuss
Dane

Ticket	Summary	Component	Status	Type	Priority ▲	Milestone
#1	Fix internationaliztion	rfc5070-bis	new	defect	major	
○ #2	Add better reference (citation) to RecordPattern@type=regex	rfc5070-bis	new	defect	major	
#3	Review implementation of extending enumerated values	rfc5070-bis	new	task	major	
○ #4	Add support for domain name meta data	rfc5070-bis	new	enhancement	major	
#5	Review all requirements key words (RFC 2119)	rfc5070-bis	new	task	major	
#6	Harmonize the specification for Reference with other WG activity	rfc5070-bis	new	task	major	
○ #7	Review completeness of NodeRole@category	rfc5070-bis	new	task	major	
○ #8	Review completeness of HistoryItem@action	rfc5070-bis	new	defect	major	
#9	Review completeness of @restriction	rfc5070-bis	new	defect	major	
#10	Review completeness of Impact@type	rfc5070-bis	new	defect	major	
#11	Add geolocation representation to Node/System	rfc5070-bis	new	enhancement	major	
#12	Define clear scope for the core data model relative to other WG documents and future extensions	rfc5070-bis	new	task	major	
#13	Review completeness of recent additions in 5070-bis	rfc5070-bis	new	enhancement	major	
#14	Add predicate logic for indicators	rfc5070-bis	new	enhancement	major	
○ #15	Missing description of classes introduced in -00 draft	rfc5070-bis	new	defect	major	
○ #16	Add support for describing if a device is physical or virtual	rfc5070-bis	new	enhancement	major	
○ #17	Review completeness of Incident@purpose	rfc5070-bis	new	defect	major	

Note: See TracQuery for help on using queries.

Download in other formats:

RSS Feed | Comma-delimited Text | Tab-delimited Text

trac POWERED

Powered by Trac 0.12.3
By Edgewall Software.

Administered by webmaster@tools.ietf.org

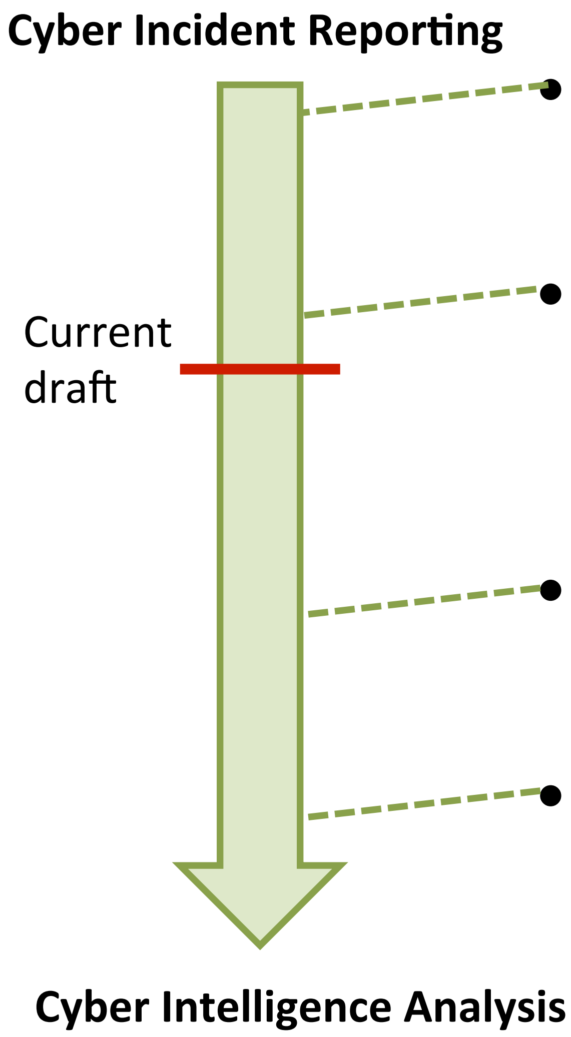
○ Will be fixed in -01 draft (that didn't make the cut-off)

Checking Scope

	Classes of Data	Description
1	**Cyber Intelligence Analysis**	Describes the characteristics of the threat
2	**Cyber Incident Reporting**	Describes a particular cyber event
3	**Cyber Event Mitigation**	Describes a proactive or reactive mitigation
4	**Cyber Information Sharing**	Describes the meta-data necessary to share information with a third party

- What data should be represented in a extension rather than in the code data model?

Cyber Intelligence Scope



- Describe the source and target of the event
- Describe a technical pattern of a given tactic used in an attack (e.g., indicators or signatures)
- Describe the actors perpetrating the attack?
- Characterize the capabilities and intent of the actors?

Cyber Intelligence Scope (2)

- What other indicator data fields should be add?
  - File information (e.g., size, attributes, ACLs, ADS, PE information)
  - Process information (e.g., pids, chains, loaded libraries)
  - Mutex names
  - Device state (e.g., ARP or routing table, disk geometry, BIOS, network settings)
  - Email (e.g., arbitrary headers, structure of contents)
    - Currently already support From, Subject, X-Mailer
  - HTTP (e.g., arbitrary headers)
    - Currently already support URL and UserAgent
  - TLS Certificate or certificate chains
  - External signatures languages (e.g., Yara, snort, Bro)

- Explicitly express a relationships between indicators?
  - e.g., "(From: Email1 and Email1) OR (X-Mailer)"
- Absence of an indicator?
- Valid time to apply the indicator (EventData/StartTime and EndTime?)

@Indicator-UID and @Indicator-set-ID

```
<System category="source">
  <Node>
    <Address category="ipv4-addr"
             indicator-uid="csirt-2013-9083-3094f"
             indicator-set-id="csirt-28897283">
...
<History>
  <HistoryItem indicator-uid="csirt-2013-3283-2389"
               indicator-set-id="csirt-28897283‟
               action=‟investigate”>
...
```

Applies to:

```
<HistoryItem>
<Expectation>
<Reference>
<Assessment>
<Address>
<Service>
<EmailDetails>
<RecordData>
<RegistryKeyItem>
<FileName>
```

Missing:

```
<DomainData>?
```

- Uniquely reference data in the document that can be used as indicators
  - *Quickly find only the indicators and treat the rest as of the information as context*
- Implementation experience
  - Are the attributes at the right top level class?
  - Is there a need to further describe the `indicator-set-id`?

Cyber Intelligence Scope (3)

```
+-------------------+
| RelatedActivity   |
+-------------------+
| ENUM restriction  |<>--{1..*}--[ IncidentID ]
|                   |<>--{1..*}--[ URL        ]
+-------------------+
```

- What further relationships between incident reports should be provided?
  - Label describing activity as a campaign (e.g., APT1)
  - `Confidence` in this label or `IncidentID`
  - Description explaining the means or rational for this attribution

Cyber Incident Reporting Scope

- What other data fields should be add?
  - `Expectation` and `HistoryItem`
    - Predefined course of action -- add another class (other than `Description`) to encode the action when `@action="other"?`
    - Add a cost metric to the action?
    - Add an efficacy statement to the action?
  - `System`
    - Asset Number (needed if System/AdditionalData/Platform used?)
    - Add `Contact` (needed if EventData/Contact?)
    - Indicator of ownership (e.g., Corporate, Partner, Personally)?
    - What specific location information is needed beyond System/Location?
  - `Contact`
    - Add `Contact/Title` (e.g., *Mr.* Smith, *Captain* Johnson)?
    - Split `Contact/ContactName` into a given name and surname?
    - Add `Contact/Department?`
    - Add `Contact/NetworkUserId` (e.g., LOCALNET\john)?

Cyber Incident Reporting Scope (2)

- Assessment
  - Summary of impact to business/mission (add Incident/ Assessment/Description? Some enumerate qualitative impact?)
  - Enumerate intended purpose of attack (e.g., theft-of-IP, degradation of service, fraud)?

Cyber Information Sharing Scope

- How should indicator matches be returned?
- How should document updates be sent?

Discussion