Revising IODEF and Updating Guidance

Rosella Mattioli
Presented by Kathleen Moriarty
MILE, IETF 84
Review

• Update process
• Use case driven
• Collaboration
• Consensus process
• Voice your opinion on the mailing list!!!
RFC5070-bis
Suggested Changes

• Ability to extend attribute values via IANA tables
• Fix internationalization issues
• Add granularity of confidence ratings to specific indicators without having to separate out EventData instances
• Add support for URLs as an indicator type
  – Currently requires an extension (RFC5901)
• Fix discrepancies/typos
Contact Class

• LEA and Vulnerability Reporter
  – May require new enumeration values either in:
    • the schema,
    • the escape value, or
    • extending attribute values through an IANA registry

• Should an element be added to handle PGP since it is widely used in the community?

• Representing sensor information requires a cross reference to System@category
  – May need guidance?
Time Representation

• Most values needed are covered, however
  – Do we need a value for next validation time?
  – Do we need a way to recommend an action for a period of time?
Addresses

• Most address information is covered, gap exists for domain data
• Should classes and elements of RFC5901 be included directly in IODEF as a more generic class regarding domain data?
  – DomainData
  – DomainContacts
  – Nameserver elements
• Where should they be placed? Same as in RFC5901 or re-aligned for broader use case?
  – Embed it in System or Node classes -OR-
  – Create a new class?
System@category

• The current values include:
  – infrastructure, intermediate, sensor, source and target
  – While attacker and destination could be considered as covered by source and target, they probably don't completely comply with the definition within RFC 5070.
    • How is this handled, change or updated guidance?

• Values not covered:
  – Sinkhole, command&control, data exfiltration destination is not covered, do we add it?
  – The Node Address list is limited to describe on node (source and target), is there a need to include multiple addresses (multiple sources and multiple targets) for watchlist distributions to condense the XML or is the separation preferred?

• Do we update the guidance or the schema to address?
Status of an Address

• system@spoofed has the current values:
  – Yes, no, unknown
• RFC5901 has the following values
  – system@status:
    • Spoofed, fraudulent, innocent-hacked, innocent-hijacked, unknown
  – domain@status:
    • reservedDelegation, assignedAndActive, assignedAndInactive, assignedAndOnHold, revoked, transferPending, registryLock, registrarLock
    • Specific to fraud
• Missing clear representation for:
  – offline/ online
  – allocated /unallocated
  – advertised/ unadvertised
  – Inconsistent
• How do we resolve this?
  – Update IODEF?
  – Create a new status class in RFC5070 to better address?
  – Use the IANA registry to extend in the future for new values
Impact@type

- **impact@type values**
  - Overlap between attack vectors and impacts hampers a clear identification of the occurring incident within the IODEF data model without the use of the Fraud extension

- **impact@type**
  - 1. admin. Administrative privileges were attempted.
  - 2. dos. A denial of service was attempted.
  - 3. file. An action that impacts the integrity of a file or database was attempted.
  - 4. info-leak. An attempt was made to exfiltrate information.
  - 5. misconfiguration. An attempt was made to exploit a mis-configuration in a system.
  - 6. policy. Activity violating site's policy was attempted.
  - 7. recon. Reconnaissance activity was attempted.
  - 8. social-engineering. A social engineering attack was attempted
  - 9. user. User privileges were attempted.
  - 10. unknown. The classification of this activity is unknown.
  - 11. ext-value. An escape value used to extend this attribute.

- **RFC5901 fraud@type includes the following values:**
  - Phishing; recruiting; malware distribution; fraudulent site; Dnsspoof

- **Do we need other values as well to represent today’s incident/indicator types?**
Support for Malware

• No class specific to Malware samples, need to describe:
  – Malware infections associated with an incident
  – RFC5901 contains
    • fraudType attribute value for “malware distribution”,
    • LureSource class includes “includedMalware”, “FilesDownloaded” and “WindowsRegistryKeyModified” classes

• Considerations:
  – Malware indicators should be hashes (MD5 or SHA1), and data model should include filetype and version
  – Name of the malware file should be defined using CARO Malware Naming Schemei
  – High level characterization helps handler to quickly identify the threat
    • IODEF Fraud extension too generic for a complete in-depth categorization of sample
    • Lacks of detailed information regarding behaviors and other
  – Useful to have high-level enumerations and definitions
    • Use of IANA registry to extend list of enumerated values could be helpful
    • CSIRTs can map their own dictionaries and insert their internal characterizations/names as a subset

Text from MILE mailing list, contributors: Rosella Mattioli, Tom Millar, and SM
Support for Malware

• Options to Solve:
  – Improve guidance of current IODEF data model and related extensions
  – Implement high-level taxonomy of malware types as proposed in the present ontology conceptualization and leave further characterization to the interoperability with other cyber security formats
    • What can/should be referenced here: OpenIOC, CAPEC, MAEC, CybOX, etc.? -OR-
      • Is a high-level solution enough without needing another specification?
  – Create a new class, structure, or extend the Method class?
    • Extend to include enumerated category values regarding attack and malware type
    • Provide high level categorization of attack/malware type to handler, provide consistency for future aggregation, comparison, and statistics
Support for Sinkholes and Command and Control Data Feeds

• Difficult to express in current IODEF data model

• Need support for additional elements to describe these events, such as:
  – URLs visited
  – Infection types
  – Country where IP is located

• Consensus on providing guidance on representation structure is important
Internationalization Support

• Review of RID (RFC6045-bis) and the IODEF Template for Extensions highlighted issues in IODEF internationalization guidance.

• Need to review and fix
  • Use of MLSTRING,
  • Add internationalization of the NodeName element of the Node class, and possibly other locations.
IODEF Guidance

• The MILE charter an item to provide guidance on IODEF and to change IODEF where needed to enable lightweight exchanges.
  – Many capabilities are enabled through IODEF to enable lightweight exchanges. Do we need to create more formal guidance?
  – Review existing guidance in IODEF for commonly shared watch lists of data and other data types.
  – Are there other guidance changes that will assist with effective exchanges?
  – Guidance for the use of 'formatid' may be very helpful to enable the ability to exchange some common data sets with reduced context to reduce the size of exchanges.
  – Guidance is needed to provide consistent interpretations of when an item should be shared via IODEF and when an extension is needed

• As RFC5070-bis is edited, is a complimentary guidance document needed?
• Additional guidance on some enumeration values, such as the use of low/med/high for confidence ratings to help with consistency?
Engaging in the IETF

• Meetings are held three times a year
  – Participation can be in person or remote via MeetEcho

• All decisions are finalized on the mailing list

• Join MILE@ietf.org mailing list
  – Participate in an existing thread
  – Start a thread on any questions based on review of a draft
  – Start a thread on work to be proposed related to MILE
  – Submit a draft in context of the charter or related work
    • post to the mailing list for consideration as a working group item

• Participation is as an individual
See you on the Mailing List!