OpenC2

BIWEEKLY FORUM MEETING

05 Jan 2017

Agenda

- □ Language Description Document Updates
- □ Open Issues
- □ STIX/OpenC2 Subgroup Report
- □ Actuator Profile Subgroup Report
- □ Path to Standardization

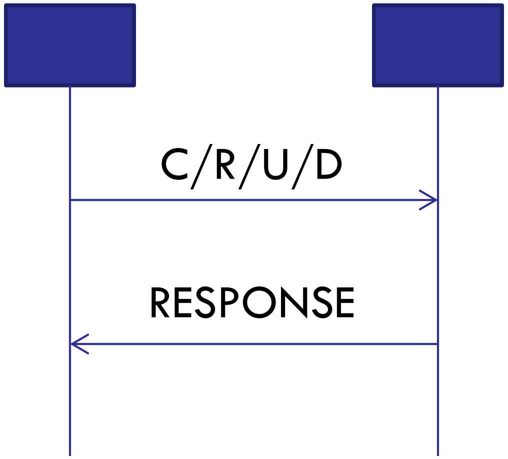
Language Description Document Updates

- Add "respond-to" universal modifier
- Add modifier datatypes: command_id, location
- Update actions
  - Update CRUD semantics
  - Update NOTIFY definition
- Update target vocabulary
  - Data model
  - STIX 2.0 Cyber Observables

CRUD Semantics

Create	SET
Read	QUERY
Update	SET
Delete	DELETE

- Remove MODIFY
  - Redundant with SET



Remove GET

- LDD: "The GET action tasks an entity to retrieve a specific object."
- Act of "getting" embedded into other actions.
- E.g., `update (source = <patch-url>)`

- Rationale:
  Data retrieval is always followed by an action.

Distinguishing REPORT and NOTIFY

- REPORT
  - The REPORT action tasks an entity to provide information to a designated recipient of the information.
- NOTIFY
  - The NOTIFY action is used to set an entity's alerting preferences.

Target Data Model

- Legacy Target Data Model
  - Data model prefix = “cybox:"
  - JSON object definitions derived from CybOX 2.1 XML schemas
  - Augmented with one ‘homegrown’ object (“data”)
  - Defined in OpenC2 spec
- New Target Data Model
  - Data model prefix = “openc2:”
  - Derived from STIX 2.0 Cyber Observable objects
    - Same information, but with streamlined JSON syntax
  - Still under development
    - "target-mapping" on Google Docs
    - Need help completing and validating the mapping

STIX/OpenC2 Subgroup Report

Firewall Profile Report

- Uploaded to Googledocs
  - Section 1
    - Should Scope be subdivided?
  - Section 2
    - Agreement on MTI and optional?
- Pending
  - Example OpenC2 commands
  - Derive
    - Target data model,
    - Actuator specific Modifiers
    - Response
- Approach?
  - Use case driven?
  - Derive from Vendor?
  - Hybrid?

Announcements/ Updates

- Draft SC3 Charter
- CTI TC Meeting
- RSA
  - Slick Sheet and Slides
  - Birds of a Feather?
- Path to Standardization (not necessarily in order)
  - Formalize Outreach to OASIS
  - Stabile LDD
  - OpenC2 Data Model (derived from SOX)
  - Profile(s) and Guide
  - Implementation Guide