Schema

title:	OpenC2 Language Objects
module:	/oasis-open.org/openc2/v1.0/openc2-lang
version:	wd07
description:	Datatypes that define the content of OpenC2 commands and responses.
exports:	OpenC2-Command, OpenC2-Response
imports:	slpf: /oasis-open.org/openc2/v1.0/ap-slpf
	jadn: /oasis-open.org/openc2/v1.0/jadn

3.2 Structure Types

3.2.1 OpenC2-Command

The OpenC2 Command describes an action performed on a target. It can be directive or descriptive depending on the context.

OpenC2-Command (Record)

ID	Name	Type	#	Description
1	action	Action	1	The task or activity to be performed (i.e., the 'verb')
2	target	Target	1	The object of the action. The action is performed on the target
3	actuator	Actuator	0..1	The subject of the action. The actuator executes the action on the target
4	args	Args	0..1	Additional information that applies to the command
5	id	Command-ID	0..1	Identifier used to link responses to a command

3.2.2 Action

Action (Enumerated)

ID	Name	Description
1	scan	Systematic examination of some aspect of the entity or its environment in order to obtain information.
2	locate	Find an object physically, logically, functionally, or by organization.
3	query	Initiate a request for information.
4	report	Task an entity to provide information to a designated recipient.
5	notify	Set an entity's alerting preferences.
6	deny	Prevent a certain event or action from completion, such as preventing a flow from reaching a destination or preventing access.
7	contain	Isolate a file, process, or entity so that it cannot modify or access assets or processes.
8	allow	Permit access to or execution of a target.
9	start	Initiate a process, application, system, or activity.
10	stop	Halt a system or end an activity.
11	restart	Stop then start a system or activity.
12	pause	Cease operation of a system or activity while maintaining state.
13	resume	Start a system or activity from a paused state.
14	cancel	Invalidate a previously issued action.
15	set	Change a value, configuration, or state of a managed entity.
16	update	Instruct a component to retrieve, install, process, and operate in accordance with a software update, reconfiguration, or other update.
17	move	Change the location of a file, subnet, network, or process.
18	redirect	Change the flow of traffic to a destination other than its original destination.
19	create	Add a new entity of a known type (e.g., data, files, directories).
20	delete	Remove an entity (e.g., data, files, flows.
21	snapshot	Record and store the state of a target at an instant in time.
22	detonate	Execute and observe the behavior of a target (e.g., file, hyperlink) in an isolated environment.
23	restore	Return a system to a previously known state.
24	save	Commit data or system state to memory.
25	throttle	Adjust the rate of a process, function, or activity.
26	delay	Stop or hold up an activity or data transmittal.
27	substitute	Replace all or part of the payload.
28	copy	Duplicate a file or data flow.
29	sync	Synchronize a sensor or actuator with other system components.
30	investigate	Task the recipient to aggregate and report information as it pertains to a security event or incident.
31	mitigate	Task the recipient to circumvent a problem without necessarily eliminating the vulnerability or attack point.
32	remediate	Task the recipient to eliminate a vulnerability or attack point.

3.2.3 Target

OpenC2 Target datatypes

Target (Choice)

ID	Name	Type	Description
1	artifact	Artifact	An array of bytes representing a file-like object or a link to that object.
2	command	Command-ID	A reference to a previously issued OpenC2 command
3	device	Device	The properties of a hardware device
4	directory	Directory	The properties common to a file system directory
5	disk	Disk	A disk drive
6	disk_partition	Disk-Partition	A single partition of a disk drive
7	domain_name	Domain-Name	A netowrk domain name
8	email_addr	Email-Addr	A single email address
9	email_message	Email-Message	An instance of an email message, corresponding to the internet message format described in RFC 5322 and related RFCs
10	file	File	Properties of a file
11	ip_addr	IP-Addr	The representation of one or more IP addresses (either version 4 or version 6) expressed using CIDER notation
13	mac_addr	Mac-Addr	A single Media Access Control (MAC) address
14	memory	Memory	A memory object
15	ip_connection	IP-Connection	A network connection that originates from a source and is addressed to a destination
16	openc2	OpenC2	A set of items used with the query action to determine an actuator's capabilities
17	process	Process	Common properties of an instance of a computer program as executed on an operating system
18	software	Software	High-level properties associated with software, including software products
19	uri	URI	A uniform resource identifier
20	user_account	User-Account	An instance of any type of user account, including but not limited to operating system, device, messaging service, and social media platform accounts
21	user_session	User-Session	A user session
22	volume	Volume	A generic drive volume
23	windows_registry_key	Windows-Registry-Key	The properties of a Windows registry key
24	x509_certificate	X509-Certificate	The properties of an X.509 certificate, as defined by ITU recommendation X.509
1024	slpf	slpf:Target	Targets defined in the Stateless Packet Filter profile

3.2.4 Actuator

Actuator (Choice)

ID	Name	Type	Description
1	generic	Specifiers	Generic actuator specifiers
1024	slpf	slpf:Specifiers	Specifiers as defined in the Stateless Packet Filter profile, oasis-open.org/openc2/oc2ap-slpf/v1.0/csd01

3.2.5 Specifiers

Specifiers (Map)

ID	Name	Type	#	Description
1	actuator_id	URI	0..1	Network locater of the actuator
2	asset_id	String	0..1	Hardware identifier of a physical actuator device, such as a serial number or inventory barcode

3.2.6 Args

Args (Map)

ID	Name	Type	#	Description
1	start_time	Date-Time	0..1	The specific date/time to initiate the action

	2	stop_time	Date-Time	0..1	The specific date/time to terminate the action
	3	duration	Duration	0..1	The length of time for an action to be in effect
	4	response_requested	Response-Type	0..1	The type of response required for the action
1024		slpf	slpf:Args	0..1	Command arguments defined in the Stateless Packet Filter profile

3.2.7 OpenC2-Response

OpenC2-Response (Record)

ID	Name	Type	#	Description
1	id	Command-ID	1	Id of the ommand that induced this response
2	status	Status-Code	1	An integer status code
3	status_text	String	0..1	A free-form human-readable description of the response status
4	*	Results	1	Data or extended status information that was requested from an OpenC2 command

3.2.8 Status-Code

Status-Code (Enumerated.Tag)

Value	Description
102	Processing -- An interim response used to inform the client that the server has accepted the request but not yet completed it.
200	OK -- The request has succeeded.
301	Moved Permanently -- The target resource has been assigned a new permanent URI
400	Bad Request -- The server cannot process the request due to something that is perceived to be a client error (e.g., malformed request syntax.)
401	Unauthorized -- The request lacks valid authentication credentials for the target resources or authorization has been refused for the submitted credentials.
403	Forbidden -- The server understood the request but refuses to authorize it.
500	Server Error -- The server encountered an unexpected condition that prevented it from fulfilling the request.
501	Not Implemented -- The server does not support the functionality required to fulfill the request.

3.2.9 Results

Results (Map)

ID	Name	Type	#	Description
1	strings	String	0..n	Generic set of string values
2	ints	Integer	0..n	Generic set of integer values
3	kvps	KVP	0..n	Generic set of string values
4	versions	Version	0..n	Generic set of string values
5	profiles	Uname	0..n	Generic set of string values
6	schema	Schema	0..n	Generic set of string values
7	actions	ActionTargets	0..n	Generic set of string values
1024	slpf	slpf:Results	0..n	Results from Stateless Packet Filter profile

3.2.10 KVP

KVP (Array)

ID	Type	#	Description
1	Identifier	1	"key": name of this item
2	String	1	"value": string value of this item

3.2.11 ActionTargets

ActionTargets (Array)

ID	Type	#	Description
1	Action	1	"action": An action supported by this actuator
2	Target.*	1..n	"targets": List of targets applicable to this action

3.2.12 Artifact

Artifact (Record)

ID	Name	Type	#	Description
1	mime_type	String	0..1	Permitted values specified in the IANA Media Types registry
2	*	Payload	0..1	choice of literal content or URL to obtain content
3	hashes	Hashes	0..1	Specifies a dictionary of hashes for the contents of the payload

3.2.13 Payload

Payload (Choice)

ID	Name	Type	Description
1	payload_bin	Binary	Specifies the data contained in the artifact.
2	url	URI	MUST be a valid URL that resolves to the un-encoded content

3.2.14 OpenC2

A target used to query Actuator for its supported capabilities

OpenC2 (ArrayOf.Query-Item ['max', 'min'])

3.2.15 Query-Item

Results to be included in response to query openc2 command

Query-Item (Enumerated)

ID	Name	Description
1	versions	OpenC2 language versions supported by this actuator
2	profiles	List of profiles supported by this actuator
3	schema	Definition of the command syntax supported by this actuator
4	pairs	List of supported actions and applicable targets

3.2.16 IP-Connection

5-tuple that specifies a tcp/ip connection

IP-Connection (Record)

ID	Name	Type	#	Description
1	src_addr	IP-Addr	0..1	source address
2	src_port	Port	0..1	source TCP/UDP port number
3	dst_addr	IP-Addr	0..1	destination address
4	dst_port	Port	0..1	destination TCP/UDP port number
5	layer4-protocol	L4-Protocol	0..1	Protocol (IPv4) / Next Header (IPv6)

3.2.17 L4-Protocol

protocol (IPv4) or next header (IPv6) field - any IANA value, RFC 5237

L4-Protocol (Enumerated)

ID	Name	Description
1	icmp	Internet Control Message Protocol – RFC 792
6	tcp	Transmission Control Protocol – RFC 793
17	udp	User Datagram Protocol – RFC 768
132	sctp	Stream Control Transmission Protocol – RFC 4960

3.2.18 File

File (Map)

ID	Name	Type	#	Description
1	name	String	0..1	The name of the file as defined in the file system
2	path	String	0..1	The absolute path to the location of the file in the file system
3	hashes	Hashes	0..1	One or more cryptographic hash codes of the file contents

3.2.19 Response-Type

Response-Type (Enumerated)

ID	Name	Description
0	none	No response
1	ack	Respond when command received
2	complete	Respond when all aspects of command completed

3.2.20 Process

Process (Map)

ID	Name	Type	#	Description
1	pid	Integer	0..1	Process ID of the process
2	name	String	0..1	Name of the process
3	cwd	String	0..1	Current working directory of the process
4	executable	File	0..1	Executable that was executed to start the process
5	parent	Process	0..1	Process that spawned this one
6	command_line	String	0..1	The full command line invocation used to start this process, including all arguments

3.2.21 Hashes

Cryptographic Hash values

Hashes (Map)

ID	Name	Type	#	Description
1	md5	Binary	0..1	Hex-encoded MD5 hash as defined in RFC3121
4	sha1	Binary	0..1	Hex-encoded SHA1 hash as defined in RFC3174
6	sha256	Binary	0..1	Hex-encoded SHA256 as defined in RFC6234

3.2.22 Device

Device (Map)

ID	Name	Type	#	Description
1	hostname	Hostname	1	A hostname that can be used to connect to this device over a network
2	description	String	0..1	A human-readable description of the purpose, relevance, and/or properties of the device
3	device_id	String	0..1	An identifier that refers to this device within an inventory or management system

3.3 Primitive Types

Name	Type	Description
Command-ID	String	Uniquely identifies a particular command – TBD syntax
Date-Time	String (date-time)	RFC 3339 date-time
Duration	String (duration)	RFC 3339 / ISO 8601 duration
Domain-Name	String (hostname)	Domain name, RFC 1034, section 3.5
Email-Addr	String (email)	Email address, RFC 5322, section 3.4.1
IP-Addr	String (ip)	IPv4 or IPv6 address per RFC 2673 section 3.2, and RFC 4291 section 2.2
Mac-Addr	String (mac)	48 bit Media Access Code address
Port	String (port)	Service Name or Transport Protocol Port Number, RFC 6335
Version	String	Version string – TBD syntax
URI	String (uri)	Uniform Resource Identifier