Schema

title:	OpenC2 Command Definitions
module:	openc2
version:	wd06
description:	Datatypes that define the content of OpenC2 commands and responses.

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 target entity or its environment in order to obtain information.
2	locate	Find the target 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 other 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 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.

ID	Name	Description
22	detonate	Execute and observe the behavior of a target (e.g., file, hyperlink) in an isolated environment.
23	restore	Return the 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 data, content or 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	
4	directory	directory	
5	disk	disk	
6	disk_partition	disk-partition	
7	domain_name	domain-name	
8	email_addr	email-addr	
9	email_message	email-message	
10	file	file	
11	ipv4_addr	ipv4-addr	
12	ipv6_addr	ipv6-addr	
13	mac_addr	mac-addr	
14	memory	memory	
15	ip_connection	ip-connection	
16	openc2	openc2	OpenC2 - query actuator for supported capabilities, negotiate connection
17	process	process	
18	software	software	
19	uri	uri	
20	user_account	user-account	
21	user_session	user-session	
22	volume	volume	
23	windows_registry_key	windows-registry-key	
24	x509_certificate	x509-certificate	
1024	slpff	Slpff-Target	Targets defined in the Stateless Packet Filter Firewall profile

3.2.4 Actuator

Actuator (Choice)

ID	Name	Type	Description
100	spff	SpffSpecifiers	Specifiers as defined in the Stateless Packet Filtering Firewall profile, docs.oasis-open.org/openc2/oc2ap-spff/v1.0/csd01

3.2.5 Args

Args (Map)

ID	Name	Type	#	Description
1	start_time	Date-Time	0..1	The specific date/time to initiate the action
2	end_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
100	spff	SpffArgs	0..1	Command arguments defined in the Stateless Packet Filtering Firewall profile

3.2.6 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

3.2.7 Status-Code

{u'compact': True}

Status-Code (Enumerated)

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.

3.2.8 artifact

artifact (Record)

ID	Name	Type	#	Description
1	mime_type	String	0..1	Permitted values specified in the IANA Media Types registry

ID	Name	Type	#	Description
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

3.2.9 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

3.2.10 openc2

A target used to query Actuator for its supported capabilities
{u'aetype': u'Query-Item', u'max': 3, u'min': 0}

3.2.11 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

3.2.12 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	layer4-protocol	0..1	Protocol (IPv4) / Next Header (IPv6)

3.2.13 layer4-protocol

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

layer4-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

3.2.14 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

3.2.15 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

3.2.16 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

3.2.17 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

3.2.18 device

TODO: Add inventory device-id?

device (Map)

ID	Name	Type	#	Description
1	description	String	0..1	
2	device_type	String	0..1	
3	manufacturer	String	0..1	
4	model	String	0..1	
5	serial_number	String	0..1	
6	firmware_version	String	0..1	
7	system_details	String	0..1	

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
ipv4-addr	String (ipv4)	IPv4 address or range in CIDR notation, RFC 2673, section 3.2
ipv6-addr	String (ipv6)	IPv6 address or range, 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