A SUITE OF SPECIFICATIONS TO ENABLE CYBER SECURITY

Joe Brule
Co-chair,
OASIS OpenC2 TC

OCT 16, 2018
Agenda

- Background and Motivation
- Strategy
- Desired Endstate
- Prototype efforts
- Findings
- Status and Way Forward
- Video Demonstration
So How’s It Working Out For You?

- **Cyber Attacks**
  - Sophisticated
    - Adaptive
    - Automated
  - Occur in Seconds

- **Cyber Response**
  - Slow
  - Manual

- **Malware as a Service (MAAS)**
  - Cost for a DDoS ~ $38/hr. or 10,000 zombies (World mix) ~ $200

- **Defenders**
  - Economic Impact of Cyber-crime ~ 0.8% GDP
  - NOTE: Global Defense Budget ~ 2.2% GDP
Another View
With more detail...
Integration in the Absence of Standards
What Can Go Wrong?

:\(\text{Your PC ran into a problem and needs to collect some error info, and then restart.}\)

If you'd like to know more, you can search online for the error: HAL_INITIALIZATION_FAILED.
The Motivation and Vision

- **Challenge**
  - Coordinated Defense in Cyber Relevant Time

- **Vision: Future Cyber Defense Tactics**
  - Sharing of indicators
  - Coordination of response actions
  - Automated, multi-part actions at machine speed

- **Strategy**
  - Decouple Functional Blocks and Standardize Interfaces
  - Identify and fill gaps as they pertain to Cyber Threat Indicator Sharing and Response
  - Participate in a diverse and collaborative environment

Standardization is a Key Enabler for Automation
OpenC2 at a glance

- Focuses on ‘Act’ portion of cyber-defense
- OpenC2 assumes the following has been done:
  - Sensing; ‘What’ triggers the action
  - Analytics; ‘Why’
  - Decision; ‘Which’ action
  - Message Fabric; ‘Transport’ and ‘Assurance’
- Leverage pre-existing protocols and efforts
- Unambiguous Machine-to-Machine Communication
- Simplicity
  - Low overhead on sensor and actuator
OpenC2 is Part of a Bigger Picture

- **STIX**
  - Standard Threat INTEL object
  - Supports Analysis

- **MQTT**
  - Standard Transfer Protocol
  - Supports Pub/Sub Architecture

- **OpenC2**
  - Standard Command Language
  - Supports Acting/Response

OpenC2 is part of a Suite of OASIS Standards
OpenC2 Subcommittee Foci

- Language Specification
  - Actions
  - Default Target namespace
  - Semantics, syntax
  - Minimum to implement

- Actuator Profiles
  - Scope and applicability
  - Required and optional Actions/Target Pairs in the context of the Actuator
  - Specifiers and options for a class of actuators

- Implementation Guides
  - All other integration aspects
  - Use of other standards to address ‘External Dependencies’

OpenC2 is not ‘a’ specification; It is a Suite
End State: OpenC2 Enabled Enterprise

- Enterprise Owner: RFP language:
  - ‘Complies with OpenC2 specifications’
  - ‘micro-satellite formation fliers utilizing COAP’
  - ‘ground segment logically separates…’

- Integrators: Select appropriate Implementation Specification and cyber defense components.

- Vendors: Implement one or more ‘Actuator Profiles’
Scope (Integrators point of view)

IMPLEMENTATION SPECIFICATIONS

- HTTP/TLS
- COAP
- OPEN DXL

RFP
- SWaP constrained
- Ground Segment Logically Isolates
- ...

PRODUCTS (defined in terms of actuator profiles)
- Cloud Service Provided Firewall
- ‘Backbone’ Router
- Next Generation Proxy
Scope (Vendors point of view)

PROFILES
- DAR Analytic
- Stateless Packet Filtering
- Routing
- DIT Analytic
- SDN Controller
- Others

VENDORS
- Cloud Service Provided Firewall
- ‘Backbone’ Router
- Next Generation Proxy
Early OpenC2 Prototypes

- Abstract Use Case
  - Mitigate Evil Domain
  - Local Orchestrator
    - Deny Evil Domain
    - Scan Evil.pdf
    - Contain Evil
  - Firewall executes command
- Implement on OpenC2 Message Fabric
Possible Implementation

- Orchestrators and Actuators converge on the OpenC2 message fabric
- OpenC2 ‘Proxy’ maps to hardware API
- Converging on Message Fabric Facilitates implementation
Change out the Actuators

- Allows Corporate wide sharing of cyber defense tactics
- Minimizes impact when changing components
Abstracts the cyber-defense function

- Deny Command is executed REGARDLESS of product
- Simplifies integration of new technologies that achieve similar actions
- Unified tactical approach independent of equipment set
Recent OpenC2 Integration Fabric

Legend
- Docker container
- Logical module

Orchestrator
- Core
- Buffer
- Serialize
- HTTPS
- Serialize
- MQTT

Devices
- HTTPS
- Deserialize
- Buffer
- ISR actuator
- EW actuator
- JSON device
- MQTT
- Deserialize
- Buffer
- ISR actuator
- EW actuator
- JSON device
- MQTT
- Deserialize
- Buffer
- EW actuator
- CBOR device
- other actuator
Deny
- Firewalls will interpret as a Rule (multiple examples)
- Routers will interpret as ACL (Cisco CTIA)
- Servers will interpret as permissions

Locate
- LYCAN use case returns GPS coordinate for an IP

Allow
- Mathematical compliment for Deny

What will Unmanned Platforms do with these?
Existing Universal Controller Requirements & Architecture

Architecture Extensible to RAS ICD Systems

RQ-20 Puma (LRR)
RQ-11 Raven (MRR)
Short Range Recon (SRR)
Lethal Maneuver Aerial Munition System (LMAMS)
PD-100 / Soldier Borne Sensor (SBS)

Unmanned Systems Waveform/Common Robotic System (Communication Link) (CRS(LR))
OSD Unmanned Control Segment (UCS)

SPAWAR MOCU 3.0/4.0

PM UAS
PM UAS
PEO Missiles & Space
PEO Soldier

IOP/JAUS
IOP/JAUS
IOP/JAUS
IOP/JAUS
IOP/JAUS

SMET

MTRS Inc II
MTRS MK II
CRS(I)
CRS(H)

CRS(I) (including Universal Controller) currently in EMD Phase

All graphics are notional to convey the general size and type of system

CRS(I) Universal Controller CDD Language: 6.2.2
(U) KPP 6 - Unmanned System Control.
The CRS (I) OCU must have the ability to achieve and maintain active and/or passive control of any current Army and Marine Corps PoR battalion and below level Unmanned (Air or Ground) System (UxS) and/or their respective payloads in less than three (T), one (O) minute(s).
Array of Monopole Antennas
Maintain RF Situational Awareness

- **Scenario:** Concern that a burst SOI may be operating in the vicinity
  - OpenC2 commands to establish an array of antennas
    - Issue SYNC {list of identifiers}
      - Instructs UAV’s to fly in formation
      - UAV’s ‘elect’ designated router
      - Responds with Designated router
    - Issue COPY {RF range, duration}
  - End State:
    - An Array of Monopole Antennas maintaining a copy of collected signals over the past two seconds

**SYNC:** Synchronize a sensor or actuator with other system components

**COPY:** Duplicate an object, file, data flow or artifact.
Determine Emitter Location

- OpenC2 Commands to acquire Line of Bearing
  - Issue ‘SCAN {SOI}’ to UAVs
    - Nodes review past two seconds and respond with TOA and coordinates
  - Issue ‘LOCATE {matrix}’ to ISR analytics
    - Returns coordinates of emitter

- Alternative OpenC2 Commands (low SNR environment)
  - Issue ‘REPORT {SOI, LOB} to designated router
    - Issues SCAN to each UAV
    - Distributed Matrix calculations for n-channel DF
    - Designated router returns LOB and coordinates of origin

**SCAN:** Systematic examination of some aspect of the entity or its environment in order to obtain information.

**LOCATE:** Find an object physically, logically, functionally, or by organization.
Other Scenarios

- **Avoid Radar Detection:** Analytics have determined that a potential adversary is using a radar signal to determine the physical location of the task force
  - Issue DENY [center freq, rule_number]
    - The UAV’s emit a radar jamming signal
  - Issue DELETE [rule_number]

- **Include Other Sensors:** Unmanned platforms based from an adjacent carrier group is providing ISR
  - Allow [list identifiers] to the ingress of the draper tool providing key management
    - The TRANSEC key is provided to the peer task force
Findings

- Maintained Separation of Concerns
- Agnostic of Topology
  - STAR utilizing HTTPS
  - Pub/sub utilizing MQTT
- Agnostic of serialization
  - JSON, CBOR
- Same ‘Strategic’ effect achieved from the commands
  - Deny [RF] (Jamming signal sent)
  - Allow [asset_id] (Provide TRANSEC key)
  - Locate [RF signal]
    - Scan [SOI] returns TOA and GPS coordinate
    - N-channel array provides line of bearing
Status of OpenC2 TC

- **Language Specification**
  - Final issues worked out at Oct 1, 2 F2F
  - To be released for Public Comment October 17

- **Actuator Specifications**
  - StateLess Packet Filter Profile (October 4)
  - Stateful Packet Filter
  - Endpoint Remediation
  - ISR Profile

- **Transfer Specifications**
  - HTTP/TLS (October 4)
  - OpenDXL
  - CoAP
OpenC2 as a Concept
At the Language Level
OpenC2 at the Actuator Profile Level
So Where do You Come in?

- OpenC2 Technical Committee
  - 132 members
  - Representing 51 Organizations

- Of those 132 members:
  - ~ 104 have ONE thing in common…
  - What about the other 20 percent?

- Request of Stakeholders
  - Identify Use Cases
  - Create Custom Actuator Profiles
  - Identify Message Fabric
Why I never do Live Demos…

TIME FOR A LIVE DEMO

WHAT COULD GO WRONG?
Thank you!
Questions?
Backups
OpenC2 Codebases:

- **Lycan Series**
  - Translation of OpenC2 JSON to objects and back
  - Python, Java and BEAM

- **OCAS**
  - Simulator to validate and verify OpenC2 interface

- **Python API’s**
  - OpenC2 API to accept & Convert OpenC2 commands to Python
  - Yuuki and Orchid are codebase
  - Reactor Master and Reactor Relay are Deployed

- **OpenC2 Integration and Test Fabric**
  - MQTT, HTTPS
  - JSON, CBOR, Protobuf
  - Imports ANY schema
<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>scan</td>
<td>Systematic examination of some aspect of the entity or its environment.</td>
</tr>
<tr>
<td>2</td>
<td>locate</td>
<td>Find an object physically, logically, functionally, or by organization.</td>
</tr>
<tr>
<td>3</td>
<td>query</td>
<td>Initiate a request for information.</td>
</tr>
<tr>
<td>6</td>
<td>deny</td>
<td>Prevent a certain event or action from completion, such as preventing a flow from reaching a destination or preventing access.</td>
</tr>
<tr>
<td>7</td>
<td>contain</td>
<td>Isolate a file, process, or entity so that it cannot modify or access assets or processes.</td>
</tr>
<tr>
<td>8</td>
<td>allow</td>
<td>Permit access to or execution of a target.</td>
</tr>
<tr>
<td>9</td>
<td>start</td>
<td>Initiate a process, application, system, or activity.</td>
</tr>
<tr>
<td>10</td>
<td>stop</td>
<td>Halt a system or end an activity.</td>
</tr>
<tr>
<td>11</td>
<td>restart</td>
<td>Stop then start a system or an activity.</td>
</tr>
<tr>
<td>14</td>
<td>cancel</td>
<td>Invalidate a previously issued action.</td>
</tr>
<tr>
<td>15</td>
<td>set</td>
<td>Change a value, configuration, or state of a managed entity.</td>
</tr>
</tbody>
</table>
## OpenC2 Actions

**Type:** Action (Enumerated)

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>update</td>
<td>Instruct a component to retrieve, install, process, and operate in accordance with a software update, reconfiguration, or other update.</td>
</tr>
<tr>
<td>18</td>
<td>redirect</td>
<td>Change the flow of traffic to a destination other than its original destination.</td>
</tr>
<tr>
<td>19</td>
<td>create</td>
<td>Add a new entity of a known type (e.g., data, files, directories).</td>
</tr>
<tr>
<td>20</td>
<td>delete</td>
<td>Remove an entity (e.g., data, files, flows).</td>
</tr>
<tr>
<td>22</td>
<td>detonate</td>
<td>Execute and observe the behavior of a target (e.g., file, hyperlink) in an isolated environment.</td>
</tr>
<tr>
<td>23</td>
<td>restore</td>
<td>Return a system to a previously known state.</td>
</tr>
<tr>
<td>28</td>
<td>copy</td>
<td>Duplicate an object, file, data flow or artifact.</td>
</tr>
<tr>
<td>30</td>
<td>investigate</td>
<td>Task the recipient to aggregate and report information as it pertains to a security event or incident.</td>
</tr>
<tr>
<td>32</td>
<td>remediate</td>
<td>Task the recipient to eliminate a vulnerability or attack point.</td>
</tr>
</tbody>
</table>
## OpenC2 Syntax Extensibility

<table>
<thead>
<tr>
<th>ACTION</th>
<th>TARGET</th>
<th>SPECIFIER</th>
<th>ACTUATOR</th>
<th>SPECIFIER</th>
<th>OPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Effects-based (no actuator specified); suitable for coordinating across enclaves</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DENY</td>
<td>ip</td>
<td>address</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Specify class of actuator

<table>
<thead>
<tr>
<th>ACTION</th>
<th>TARGET</th>
<th>SPECIFIER</th>
<th>ACTUATOR</th>
<th>SPECIFIER</th>
</tr>
</thead>
<tbody>
<tr>
<td>DENY</td>
<td>ip</td>
<td>address</td>
<td>Stateless Packet Filter</td>
<td></td>
</tr>
</tbody>
</table>

### Specify group of actuators

<table>
<thead>
<tr>
<th>ACTION</th>
<th>TARGET</th>
<th>SPECIFIER</th>
<th>ACTUATOR</th>
<th>SPECIFIER</th>
<th>OPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>DENY</td>
<td>ip</td>
<td>address</td>
<td>Stateless Packet Filter</td>
<td>Perimeter</td>
<td></td>
</tr>
</tbody>
</table>

### Specify particular actuator

<table>
<thead>
<tr>
<th>ACTION</th>
<th>TARGET</th>
<th>SPECIFIER</th>
<th>ACTUATOR</th>
<th>SPECIFIER</th>
<th>OPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>DENY</td>
<td>ip</td>
<td>address</td>
<td>Stateless Packet Filter</td>
<td>identifier</td>
<td></td>
</tr>
</tbody>
</table>

### Add an option to refine the action

<table>
<thead>
<tr>
<th>ACTION</th>
<th>TARGET</th>
<th>SPECIFIER</th>
<th>ACTUATOR</th>
<th>SPECIFIER</th>
<th>OPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>DENY</td>
<td>ip</td>
<td>address</td>
<td>Stateless Packet Filter</td>
<td>Perimeter</td>
<td>SLPF: Reject</td>
</tr>
</tbody>
</table>
OpenC2 External Dependencies

- OpenC2 is necessary but insufficient
- OpenC2 Assumes
  - Decision has been made
  - Action is warranted
  - The command can get there intact and securely.
  - Recipient is authenticated and authorized.
- OpenC2 Focuses on the ACTING portion of cyber Defense

OpenC2 Implementations will FAIL without a robust means to convey commands!
Threats against Inter-enclave C2 – an actor may:

- alter C2 message to degrade or halt defensive responses,
- send spoofed commands to open up enclave B to attack,
- view C2 traffic to gain warning of defensive responses,
- disrupt network services to prevent delivery of C2 messages.
Dependencies & Security
Threats against intra-enclave C2 – an actor may:

- alter C2 messages to degrade or halt defensive responses,
- send false commands to open up an enclave for attack,
- Spoof C2 replies to disrupt defense or confuse defenders,
- Flood devices to prevent delivery of C2 messages.
OpenC2 Derived Security Requirements

To combat or mitigate threats against inter- and intra-enclave cases, OpenC2 may need:

- **Confidentiality** – ability to control visibility of OpenC2 messages to only authorized recipients.
- **Integrity** – assurance that OpenC2 message sent is the message received
- **Authorization** – limit sending and receiving to authorized parties only
- **Authentication/Proof-of-Origin** – ability for all recipients to know the source of a message or identify of the sender
- **Availability** – assurance that messages can always be sent
- **Reliability** – assurance that messages are delivered to all intended recipients
End Notes

- Contribution: Status and Way Forward Brief by Joe Brule, Executive Director, OpenC2
- Cisco® is a registered trademark of Cisco Systems, Inc.
- Oasis® is a registered trademark of Oasis, Inc.
- Yuuki © Joshua Brule
- OrchID © OpenC2
- OCAS © sFractal Consulting