



A FORUM TO INVESTIGATE/ADDRESS
COMMAND AND CONTROL
(PERTAINING TO CYBER DEFENSE)

16 Feb 2016

Agenda

2

- Background
 - ▣ Problem Statement
 - ▣ Formation of the Working Group
- Design Principles/ Scope
- Work In Progress
- Next Steps
- Updates

The Problem Statement

- Modern Cyber Defense implementations:
 - ▣ Integrate products in a proprietary or unique manner
 - ▣ Statically configured
 - ▣ Upgrades to the functional blocks are intensive
 - ▣ Modifications may impact the efficacy of the system
 - ▣ Adaptations to new TTPs hard to accomplished in cyber-relevant time
- Future Defense implementations must support:
 - ▣ Sharing of indicators
 - ▣ Coordination of responses between domains
 - ▣ Synchronization of cyber defense mechanisms
 - ▣ Automated, multi-part actions at machine speed
- Standardization is a Key Enabler for Unambiguous C2

Formation of the Working Group

4

- Stakeholders
 - ▣ USG: DHS IACD, NSA Active Cyber Defense
 - ▣ Industry
 - Orchestration Vendors
 - Network, Endpoint, Application Vendors
 - Financial Sector
 - ▣ Academia
- Course of Action Working Group
 - ▣ Kickoff on July 29, 2015
 - ▣ 90 minute Teleconference/Meetings (biweekly)
 - ▣ Full Day Workshops (Quarterly)

Defense in Cyber Relevant Time

OpenC2 Design Principles

5

- Lightweight
 - ▣ Efficient Machine to Machine communications
 - ▣ Minimize the set of 'core' actions
- Abstract
 - ▣ Focuses on 'What' to do vice 'How' to do it
 - ▣ Permits different levels of abstraction
- Extensible
 - ▣ Address requirements for operational environment
 - ▣ Extensions enable additional precision and flexibility
- Agnostic
 - ▣ Transport, Authentication , Integrity controls etc.
 - ▣ Enables flexibility w.r.t. implementation

Enable Unambiguous Machine to Machine
Command and Control Messages

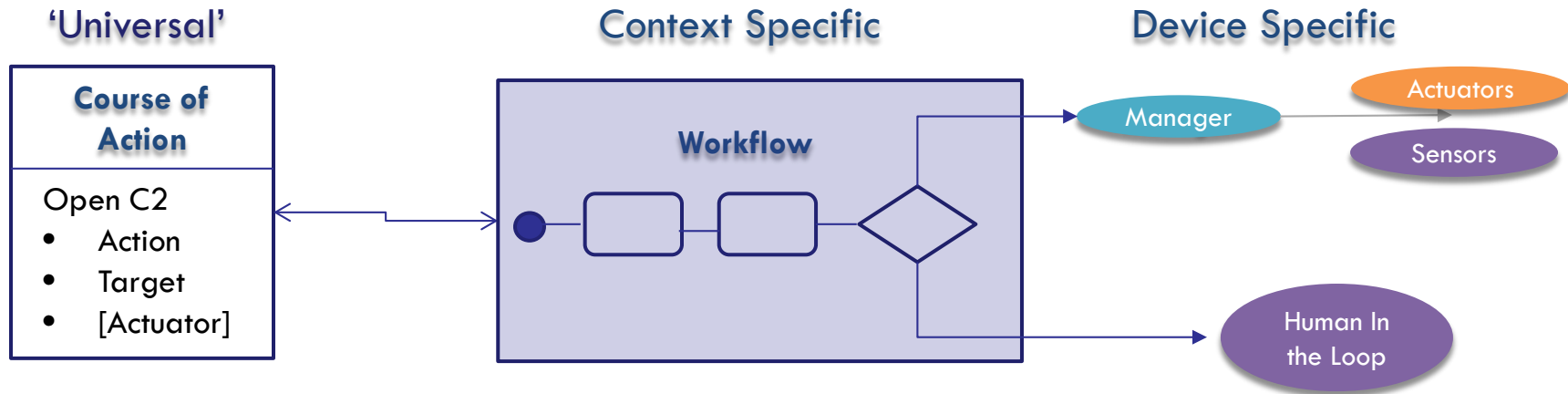
Additional Considerations

6

- External Dependencies
 - ▣ Transport Layer
 - ▣ Information Assurance
 - Authentication Mechanism
 - Integrity
 - Availability
 - Confidentiality
 - ▣ Message Prioritization
 - ▣ Message Identification/ Acknowledgment
- Message Types
 - ▣ Tasking/ Response
 - ▣ Notifications
 - ▣ Effects based

Conceptual Model

7



Course of Action

- Focused on desired effect.
- A set of activities to mitigate specific attack to an information system.

Workflow

- Derived from a Course of Action
- An ordered or coordinated set of steps

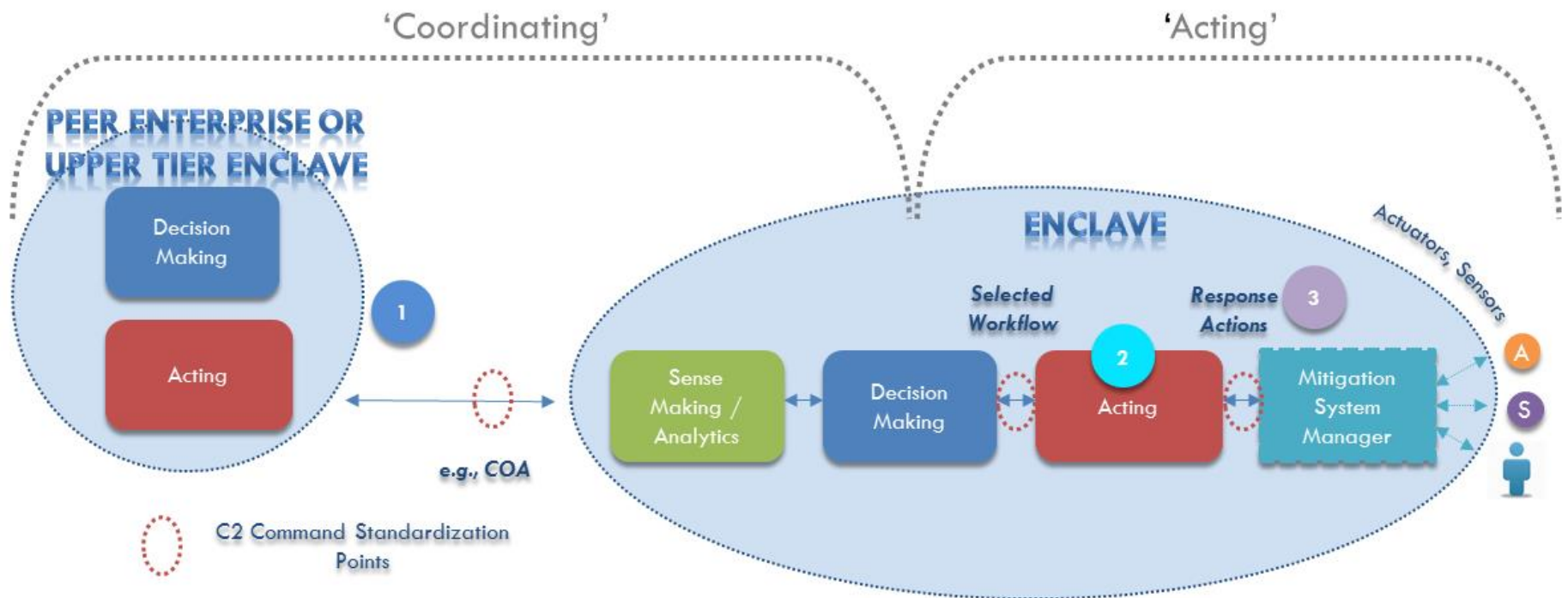
Response Action

- One or more instructions for a particular sensor or actuator

OpenC2 to Support Integrated Defensive Cyber Operations

8

- Coordination/ Sharing using OpenC2 commands (i.e., Course of Action)
- Execution using OpenC2 Commands (i.e., Workflow)



Work In Progress: Syntax

9

```
<ACTION> (  
    target (type=<TARGET_TYPE>, specifiers),  
    [actuator (type=<ACTUATOR_TYPE>, specifiers)],  
    [modifiers]  
)
```

- **ACTION** ('The Verb')
 - ▣ What is to be done
 - ▣ All OpenC2 commands have an Action
- **TARGET** ('The Object')
 - ▣ What is affected by the ACTION
 - ▣ All OpenC2 commands have a target
- **ACTUATOR** ('The Subject')
 - ▣ What is executing the ACTION on the TARGET
 - ▣ Optional In Higher Level Commands
- ***Specifiers***
 - ▣ Further identify TARGET(s) and ACTUATOR(s)
- ***Modifiers***
 - ▣ Provide additional information for the ACTION (optional)

OpenC2 Syntax Flexibility

10

ACTION	TARGET	SPECIFIER	ACTUATOR	SPECIFIER	MODIFIER
--------	--------	-----------	----------	-----------	----------

Effects-based (no actuator specified); suitable for coordinating across enclaves

DENY	ip	<i>address</i>			
------	----	----------------	--	--	--

Specify class of actuator

DENY	ip	<i>address</i>	network		
------	----	----------------	---------	--	--

Specify type of actuator

DENY	ip	<i>address</i>	network.router		
------	----	----------------	----------------	--	--

Specify particular actuator

DENY	ip	<i>address</i>	network.router	<i>BGP Speaker</i>	
------	----	----------------	----------------	--------------------	--

Add a modifier to specify the action

DENY	ip	<i>address</i>	network.router	<i>BGP Speaker</i>	Method= blackhole
------	----	----------------	----------------	--------------------	----------------------

Work in Progress: Lexicon

11

□ ACTIONS

- ▣ Converging on ~ 30 terms
- ▣ Modifiers

□ TARGETS

- ▣ Leveraging CybOX objects

□ ACTUATORS

▣ Categories

- Endpoint
- Network/ Platform
- Services/ Processes

- ▣ Researching the ISCM and SACM efforts

Next Steps

12

- Continue Development of the language (Version 1.0)
- Reference Implementations
 - NSA/ JHUAPL (Beginning January 2016)
 - NSA/G2 Corporation (Beginning January 2016)
 - NIST Cyber-security Center of Excellence (Future)
- Integrate with Trusted Cyber Sensor (ongoing)
- Definition of TLV (Future)

Future Steps

13

- Finalize Working Group Charter
 - ▣ Draft Charter
 - ▣ Membership Agreement in progress
- Increase Participation in the Working Group
 - ▣ Financial Sector, DHS, Malware Detection vendors
- Engage OASIS
 - ▣ OpenC2 and STIX efforts complement each other
 - ▣ STIX COA Profile in progress
- Web Presence
 - ▣ <https://github.com/OpenC2-org>

Questions?