OpenC2 Open Command and Control (OpenC2): A Forum to Promote Global Development and Adoption of Command and Control.

Today, cyber-attacks are increasing in terms of complexity, speed, and dynamics. Advanced cyber actors now use highly-sophisticated, dynamic attack steps with automation, and these trends are likely to continue.

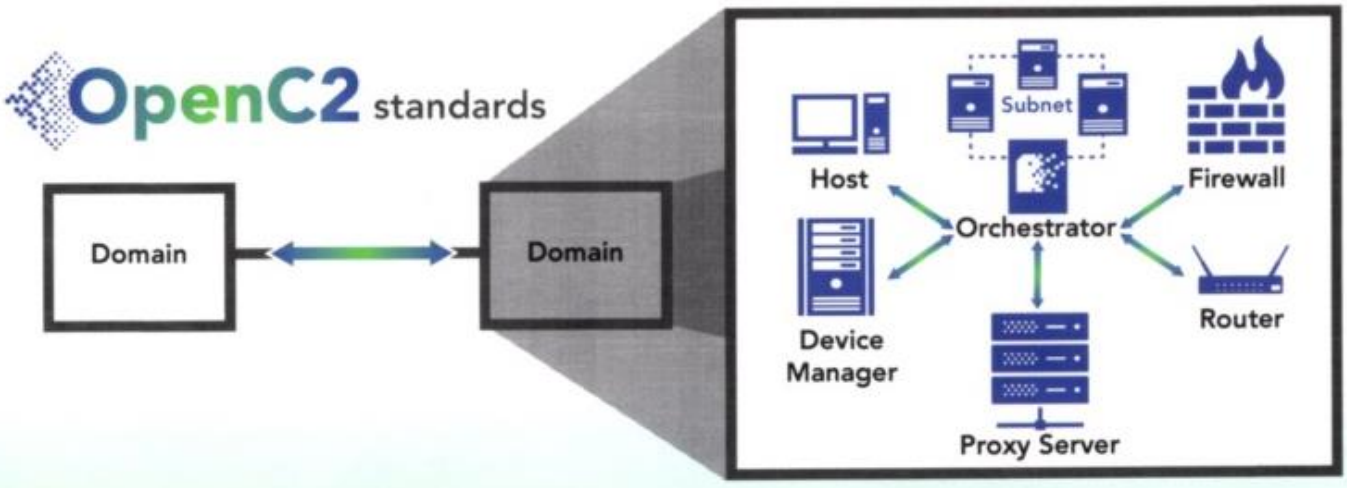
Modern defense systems are typically statically configured and integrate products in a nonstandard way. Upgrading or modifying the functional blocks within the cyber-defenses is intensive, may impact the efficacy of the system as a whole, and in many cases cannot be realized in cyber-relevant time.

Future defenses will require the integration of new functional blocks, coordination of responses between domains, synchronization of cyber defense mechanisms, and automated actions at machine speed against current and pending attacks. Standard interfaces and protocols to facilitate the integration of components resulting in a more flexible and interoperable cyber defense system. *A defined, standardized, and unambiguous machine-to-machine command and control language will help realize this vision.*

Our Vision

The OpenC2 Forum defines a language at a level of abstraction that will enable unambiguous command and control of cyber defense technologies. OpenC2 is broad enough to provide flexibility in the implementations of devices and accommodate future products and will have the precision necessary to achieve the desired effect.

Figure 1: The Open Command and Control (OpenC2) Language Description Document defines a language and lexicon at a level of abstraction that will enable the coordination and execution of command and control of cyber defense components between domains and within a domain.



Inter-Domain Coordination

Intra-Domain Execution

Who Are We?

The OpenC2 Forum is an industry driven group that is currently chaired by the Technical Director of the National Security Agency's Capabilities Directorate. The OpenC2 Forum is open to cyber security stakeholders such as product vendors, system integrators, and academics. ***We have 33 member organizations from across the world and counting.***

Our Design Philosophy

OpenC2 focuses on machine-to-machine command and control. By leveraging pre-existing standards for transport, information assurance, configuration management, and other aspects of the system to the greatest extent practical, OpenC2 is able to be both architecture and vendor agnostic.

We strive for simplicity to facilitate adoption and minimize the processing overhead. OpenC2 is defined at an abstract level and will support different encodings.

We collaborate with other cyber security and threat standardization efforts and make every effort to ensure that our artifacts are compatible with little to no overlap.

Our Current and Near Term Activities

- Final Release Candidate of the Language Description Document: Specifies a lexicon for the actions, defines the syntax for a command, presents representative use cases and provides illustrative examples.
- Information Assurance Implementation Considerations: OpenC2 leverages pre-existing protocols and in of itself does not provide security. The IA Implementation Considerations document provides guidance for the IA related external dependencies.
- JSON Abstract Encoding Notation (JAEN): JAEN specifies actions, targets, and actuators to build and validate OpenC2 commands.
- Prototype Use Case Implementations: Our members have created an open source codebase in Python, Erlang, and Java. We have demonstrated that OpenC2 is compatible with significantly different implementation choices such as the Actor Model, Multiple Dispatch on Type, and Object Oriented Programming.
- Actuator Profiles: Profiles specify the minimum to implement and define appropriate extensions.
- Sample Commands and Codebase: Extensive library available to validate commands.
- Reference implementation suitable for an enterprise that addresses external dependencies such as message format, communication protocol, information assurance, and other aspects.

We Are Defending Against a Global Attack Surface Operating at Net Speed

Join Us Today: Together, We Will Succeed

OpenC2 HTTP://OPENC2.ORG