Paper Proposal for CARIS2: Coordinating Attack Response at Internet Scale

Information Sharing, Security Models, and Cyber Defense

The Charles Stark Draper Laboratory and the U.S. National Security Agency

Michael Jerge, Chelse Swoopes, Mike Ridge, and Joseph Brule

This paper supplements the discussion on "Trust, Privacy, and Data Markings" formulated at the first *Coordinating Attack Response at Internet Scale (CARIS) Workshop*. It has long been understood that there are benefits to security from information sharing across enterprises and third-parties for the purpose of preventing and mitigating internet attacks. Heretofore, the type of information sharing previously mentioned was seen as a nontrivial task that required the efforts of many disciplines, including legal, and information technology. Additional factors included the fear of staining reputation and cultural norms against data sharing. This way of thinking, in turn, led organizations to withhold information necessary for combating cyber-attacks at the internet scale, which created additional challenges for effectively combating these types of attacks.

Modern information security models, such as the NIST Risk Management Framework (RMF), are rigid in nature and do not allow for the flexibility and adaptability required for innovative cyber defense mechanisms because these models are primarily optimized for compliance, not resiliency. While it is true that the NIST RMF contains elements for continuous monitoring of controls and processes, this monitoring only emphasizes auditing the processes and controls that were established at the initial categorization, thereby impeding adaptation to changing tides. The motivation for continuous monitoring is currently focused on compliance and auditing, not near real time cyber situational awareness. System designs are becoming more complex and sophisticated, resulting in a terrain increasingly favorable to an attacker. William Bray said in his "Department of the Navy Systems Engineering Transformation" presentation, that the static and serial systems engineering processes are an inhibiting factor in creating effective cyber defenses in the evolving cyber environment. Complexity stymies creativity, which is tantamount to innovation. Hence, while cyber tools are being developed to address this changing environment, they are difficult to deploy because of the static security frameworks.

The solution is to create risk frameworks that do not merely enforce compliance, but rather enable dynamic change within the structure, such as the Baldrige Excellence Framework used for leadership and performance management. Attack mitigation is cyclical in nature, in that it requires constant, reliable "system status" information being available to the defense mechanisms. Proper, timely information cannot be conveyed within the constraints of rigid monolithic structures. While security baselines within the framework offer low cost security capabilities, they ultimately do not solve problems, as evidenced by the annual Verizon breach reports. Rigid monolithic structures impede information sharing and the coordination of efforts between departments within organizations and municipal governments.

This is not to say that the current frameworks are poorly built. On the contrary, frameworks such as the one created by NIST work well for understanding one's residual risk. The trouble comes when the environment creates fractured blocks that do not conform to transient properties in a cyber-related time frame. Collaboration is necessary for optimal results. Standard requirements are thus necessary for creating a strategy centered around defending infrastructure in the event of cyber-attacks. For example white box switches are beneficial in creating a landscape in which to develop and operate innovative security requirements, representing the foundational building block of the "networking ecosystem required to enable organizations to pick and choose the elements they need their respective objectives." A similar type of foundation is needed for both policies and services management.

Cyber systems are subject to a global threat from adversaries that are increasingly dynamic and operate at machine speed. Modern cyber defense products tend to operate in isolation and often statically configured. The use of statically configured point defenses against a global attack surface is not tenable. Future systems need to a coordinated defenses operating in cyber relevant time. Creating coordinated cyber defense systems in the absence of standards is impractical. The integration of a suite of monolithic products may result in redundant cyber defense functions, incompatible functions and capability gaps. The functional blocks within a given product may be tightly coupled with other functions and the may not be directly accessible by way of an API. Typically, integration efforts are expensive, require customized interfaces, and if tightly coupled, difficult to maintain or modernize. The need for Coordination of Attack Response at Internet Scale is hardly a contentious topic; however, discussions, strategies and efforts towards these ends have limited efficacy should the approaches fail to consider the postulate, 'Internet Scale' involves two attributes: (i) any information model must be widely understood and unambiguous (a

semantic metric) and (ii) a cyber-response must occur within cyber relevant time (a temporal metric). Engineering strategies, design principles and approaches must support or at least be consistent with this postulate if we are to achieve coordinated response at scale. We consider the following engineering principles to be consistent towards this goal.

- Separation of Concerns: Decouple the functional blocks within a cyber-defense system to the greatest extent practical.
- Standards based Interfaces: All inputs and outputs (i.e. the primitives) must be standards based.
- All designs and implementations are public knowledge (an extension of Kerckhoff's principle).

The Open Command and Control (OpenC2) effort is a technical committee within the OASIS International Standards Body. The purpose of OpenC2 is to define a standardized language for command and control of cyber defense technologies. It will address the acting portion of cyber defense by focusing on the creation of specification that enable unambiguous machine-to-machine communications and assumes the other functional blocks are in place. These assumptions permit OpenC2 to define a simple and low overhead language that is agnostic of any particular transport protocol or information assurance implementation.

OpenC2 makes three key assumptions with respect to cyber-attacks and defense. In the context of cyber defense, the high-level action that defenders take has been stable for years (such as block, deny, redirect). Similarly, what we are acting on has also been stable for quite some time (such as malicious files, compromised users, compromised devices, and unauthorized users). The area of active research, development and innovation takes place in the cyber defense products. For example, virus scanners have evolved from static signature based to sophisticated Bayesian classifiers and machine learning.

OpenC2 will produce a 'Language Specification' that defines the actions (what we are doing) and targets (what we are acting on). The Language Specification defines the syntax of the language and the means to extend the language. The language specification is consistent with the first two assumptions.

OpenC2 will create a suite of 'Actuator Profile' specifications. In the context of OpenC2, an actuator is the entity that executes the command. The purpose of the actuator profile is to identify the appropriate actions and targets that are applicable or make sense in the context of a particular cyber defense function. A suite of Actuator Profile specifications allows vendors to focus on what is relevant to their product, accommodates new technologies and functions while minimizing the need to revise the language specification. This is consistent with the third assumption. OpenC2 will also create a suite of 'Implementation' specifications. By design, OpenC2's scope is limited to the 'acting' portion of cyber defense however, a command and control system requires an assured message fabric and the components of the cyber defense system must be on a standard transport infrastructure in order to interoperate. A given implementation specification will leverage pre-existing standards and protocols to provide transport, key management, information assurance, audit, logging and other external dependencies. By design, OpenC2 is agnostic of the transport layer. This will permit cyber-ecosystems to select the optimal message fabric for their particular requirements and still utilize OpenC2.

OpenC2 is striving to standardize the command and control of cyber defense technologies. The Language Specification will define the semantics of the language and at a high level will capture the breadth of cyber defense technologies. Actuator profiles will refine the language in the context of particular cyber defense functions. The Actuator profiles will specify to vendor community how to ensure that their products are OpenC2 compliant. Similarly, the actuator profiles will provide a means for the system integrators to determine what a particular product does so that meaningful comparisons are possible. The Implementation Specifications will document how a system integrator can achieve interoperability of cyber defense functions and address matters that are critical to the success of a command and control system, but beyond the scope of 'response'. Ultimately, this suite of documents will enable the mission owner to acquire an OpenC2 enabled enterprise that can be tailored for a particular cyber ecosystem.