---

title: Collaborative Automated Course of security Action Operations (CACAO)

abbrev: CACAO

docname: draft-jordan-cacao-charter-00

date: 2018-11-30

keyword: course of action

ipr: trust200902

area: General

workgroup: IETF

keyword: Internet-Draft

category: info

stand\_alone: yes

pi: [toc, sortrefs, symrefs]

coding: us-ascii

author:

-

   ins: B. Jordan

   name: Bret Jordan

   organization: Symantec Corporation

   street: 350 Ellis Street

   city: Mountain View

   code: CA 94043

   country: USA

   email: bret\_jordan@symantec.com

-

   ins: A. Thomson

   name: Allan Thomson

   organization: LookingGlass Cyber

   street: 10740 Parkridge Blvd, Suite 200

   city: Reston

   code: VA 20191

   country: USA

   email: athomson@lookingglasscyber.com

--- abstract

This is the charter for the Working Group: Collaborative Automated Course of Action Operations (CACAO) for Attack Defense

--- middle

**# Problem**

Threat actors and intrusion sets are advancing at an increasing rate relative to security attacks defense (including, attack detect and mitigation). Yet, defenders who detect an attack is ongoing usually have to manually identify and process prevention, mitigation, and (candidate) remediation actions to protect their systems, networks, data, and users. Moreover, there are no standard means to easily and dynamically share (candidate) mitigation actions and operational experience among a trusted set of network operators facing similar attacks.

Due to the increasing sophistication, and amplitude of security attacks, the need for a secured collaborative mechanism that would enable system and network operators to efficiently react (or proactively act) to threats in machine relevant time has raised significantly. While some attacks may be well known to certain security experts and researchers they are hardly documented in a way that would enable automated mitigation or remediation. Also, new attacks may emerge and candidate mitigation actions may not be widely and promptly disseminated among networks and systems under or (being targets to) such attacks.

Standard data models for describing attacks, prevention and mitigation actions, as well as proposed remediation actions are necessary for collaborative security defenders to respond more quickly and reduce the risk of being exposed to an attack. Distributed responses and coordination means would thus help to efficiently soften and mitigated distributed attacks at the largest scales.

**# Working Group**

To enable efficient collaboration and facilitate the sharing of security practices among network operators for the sake of optimized, anticipating and dynamically responsive security policy enforcement defense, the Collaborative Automated Course of security Action Operations (CACAO) working group will focus on documenting a solution to securely share the actions needed to anticipate, prevent, mitigate, and remediate threats among trusted parties. This effort will include the specification of a data model, data serialization, and a transport mode for sharing, and processing security actions.

Each collaborative course of action will consist of a sequence of actions that can be coordinated and deployed across a set of (heterogeneous) systems such that both the actions requested and the resultant outcomes may be monitored and verified. Means to link an action with an attack will be considered.

The primary focus of this working group will be the definition and the distribution of the sequence of actions. Where possible, the wg will leverage existing efforts that may define the atomic actions to be included in a process or sequence. The WG won’t consider how shared actions are used/enforced by a receiving party, but will focus on the required data to be shared among trusted parties, and the companion interfaces and protocol exchanges.

The mechanisms for sharing actions must be reliable and must be immune against misuse that would lead to exacerbate an attack or by introducing new attack vectors.

The WG will reuse existing protocols, wherever appropriate. Modifications to existing protocols will be achieved in coordination with the corresponding WGs.

**# Goals**

This working group has the following major goals:

* Document the use cases and requirements
* Describe a functional architecture which identifies the required functional entities and required interfaces and protocols for CACAO.
* Create a data model that can capture and enable collaborative courses of action among a set of trusted parties that can be used to automate the enforcement of appropriate security policies or the execution of proper mitigation actions
* Identify and document the configuration for a series of protocols that can be used to distribute courses of action in both direct delivery and publish-subscribe methods
* Define and create a series of tests and documents to assist with interoperability
* Document applicability statements for some attack types (DDoS, for example).

**# Deliverables**

The working group plans to create informational and standards track documents some of which may be published through the IETF RFC stream:

* CACAO Use Cases
* CACAO Requirements
* CACAO Functional Architecture: Roles and Interfaces
* CACAO Data Model
* CACAP Applicability Statement: The DDoS Case

The WG may decide to not publish the uses cases and requirements as RFCs. The decision will be made during the lifetime of the WG.

Within the first year, the working group aims to:

* Describe a solution for capturing and distributing multiple sequenced atomic actions, whether they be manual or automated.
* Publish a standards track draft solution that can be used by organizations and vendors to create and distribute Courses of Action.