Cyber Grand Challenge

CFE Event Plan

July 26, 2016

Defense Advanced Research Projects Agency
Information Innovation Office
675 North Randolph Street
Arlington, VA 22203-2114

CYBER

GRAND_CHALLENGE

Table of Contents

1 Introduction

The CGC Final Event (CFE) will be computed according to the following event plan. While great effort has been made to test the CFE competition infrastructure and allow finalist testing of Cyber Reasoning Systems (CRS), CFE itself will be the first time finalist CRSs can interact inside the competition infrastructure; unexpected results may occur. This event plan defines the procedures to be followed by the CFE referees during the computation of the CFE.

2 Establishment of Air Gap

An air gap around the competition infrastructure and finalist CRSs will be established prior to the computation of CFE in order to enforce the autonomy policy of CFE as defined in A171 of the CGC FAQ and the CGC Rules.
Air Gap certification requires the removal of all wireless communications devices from inside the air gap and the disconnection of all wired communications cables that transit the air gap wall. Once the air gap is certified, no digital media or communications cables will enter the air gap. Only CGC referees and officials appointed by DARPA may enter the air gap after a sweep by DARPA physical security. Data may *exit* the air gap by use of the Air Gap Robot or other unidirectional media transfers approved by the CGC PM.

3 Prior to CFE Computation

Once the Air Gap has been established and prior to CFE Computation, the competition infrastructure will be converted from sparring mode which isolates the CRSs to a networked competition mode.

4 CFE Computation Commencement

CFE Computation is scheduled to commence after 0900 Pacific Time on August 4th, 2016 following the concurrence of the DARPA Program Manager, the CFE Command Center and the CGC referees.

5 CFE Computation Conclusion

CFE Computation is scheduled to conclude after 40 scored rounds have been computed (per CGC FAQ A169) and any of the following conditions occurs:

- 96 rounds complete.
- Computation reaches 1900 Pacific Time on August 4th, 2016. A round after the 40th round whose computation time occludes 1900 Pacific Time will be included in computation.
- The DARPA CGC PM declares computation finished due to a risk to the CFE.

6 Round Timing

Round timing will be consistent with CGC FAQ A157. Each round of play will last about 270 seconds under nominal conditions. Each unscored break can be extended

by the competition infrastructure or the CFE referees should a potential risk to event execution occur; examples of these risks can be found in CGC FAQ entry A168.

7 Handling Risks to Event Execution

7.1 Risk Investigation Process

When alerted to a risk to event execution, an annotation will be made in the event log with a description of the risk, the time of the alert, the round in which it was observed and the CRS(s) affected if known. The risk will be investigated by the referees at which point investigation updates may be included in the event log. Once the risk is resolved, mitigated or accepted, the event log will be annotated with the time of closure, a description of the action(s) taken and the CRS(s) affected.

7.1.1 Publishing the Event Log

The CFE Event Log will be published following the conclusion of CFE.

7.2 Categories of Risks

There are several categories of anticipated risks:

- Infrastructure stoppage
- Infrastructure non-stoppage
- CRS failure

7.2.1 Infrastructure Stoppage Risks

The CFE infrastructure automatically pauses CFE when alerted to a multitude of internal consistency errors. These include missing log files, unreachable hosts, host software configuration changes, infrastructure software errors, etc. Alternately the CFE referees will manually pause the competition in order to investigate a risk to the competition infrastructure. Infrastructure stoppage errors are investigated per the Risk Investigation Process and may result in the Risk Actions documented below.

7.2.2 Infrastructure Non-Stoppage Risks

Infrastructure non-stoppage risks are unconfirmed risks that do not warrant automatic competition stoppage; they will be investigated according to the Risk Investigation Process. Once identified, conditions for which the risk of remediation outweighs the risk of inaction may redefine nominal conditions and will not cause other action. During an investigation, a non-stoppage risk may be promoted to a stoppage risk per the judgement of the referees.

7.2.3 CRS Failure

The CRSs are passively observed by the referees by monitoring CRS interactions with the Team Interface API, by periodic checks of the hardware fault indicators and by passively monitoring the High Performance Computing (HPC) power consumption. Should a finalist CRS appear to have a failure then it will be investigated according to the below CRS Failure Investigation Process.

7.2.3.1 CRS Failure Investigation Process

If a CRS Failure is suspected, the DARPA Program Manager will be notified of a potential CRS failure and referees will be tasked to investigate the potential root

cause. Should the root cause be determined to be a competition infrastructure issue it will handled per Infrastructure Stoppage Risks. Should the root cause be determined to be a finalist HPC hardware failure then the procedure published in Section 6 ("System Recovery") of the Finalist Event Information will begin.

7.3 Risk Actions

One or more of the below actions may be initiated in order to mitigate a risk to the event according to the judgement of the referees. The action(s) taken will be recorded in the Event Log.

7.3.1 End of Competition

The DARPA CGC PM may choose to end the competition immediately due to risk; for examples of these risks please see CGC FAQ A169.

7.3.2 Infrastructure Hardware Replacement

Should the competition infrastructure experience or indicate an impending hardware failure that would pose a risk to the event, the CFE referees will determine the optimal hardware replacement approach. Options include computer replacement, component replacement, or utilizing spare infrastructure already inside the air gap.

7.3.3 Software Modification

At any time, per the expert judgement of the referees, the competition infrastructure software may be modified. When possible, software modifications will be put in place during an unscored break.

7.3.4 Challenge Set Removal

A Challenge Set that creates a risk to the event may be removed from the competition. When possible, removal will take place during an unscored break. The challenge set schedule committed in this Event Plan will not be modified except to remove a CS for reasons of risk reduction.

7.3.5 Discarding Rounds

In the event of a failure or risk a round may be discarded. For instance, if a defended host belonging to a CRS fails, the round in which the failure occurred would be discarded. In a manner consistent with A152 of the CGC FAQ, no provisions will be made for expected HPC node failures.

7.3.6 Attacks against the Competition

All finalists are signatories to the CGC Event Participation Agreement; the Conduct section of this agreement provides guidance on attacks against the competition itself. If an attack against the competition is identified, the competition will be paused and the DARPA Program Manager notified. The competition will not continue until the DARPA Program Manager approves the results of the investigation and the remediation actions.

8 Certification of Event Log and Event Plan

Modifications to the Event Plan may be made at the sole discretion of the DARPA CGC PM. The Event Log will be certified by the DARPA CGC PM prior to release.

9 Hashes

Hash of CFE scoring formula:

```
1ce168b27b5f5411c0eefba8389f64b281e9bff7c006a77d3cecdf3e355
1e7c0d8f3f5a9d7c1c690284b9c1fecc8320b
```

Hash of CFE CS schedule:

```
42059960f5f96a2337841916f1b14e813c9328a7b9dc0c05051a515762d
bab96419ccf5a33bb6eca4b5e230e68bee453
```