

Welcome! [Login](#)[HOME](#) | [DOCUMENTS](#) | [REGISTRATION](#) | [FORUM](#)

DARPA CYBER GRAND CHALLENGE COMPETITOR PORTAL

Welcome to the CGC Competitor Portal, the official competitor information site for DARPA's fully automated computer security challenge. This site provides official access to all DARPA Cyber Grand Challenge documentation, rules, announcements, software, forums, team registration and team login.

Details about the Cyber Grand Challenge and some of the other registered teams can be found at <http://www.cybergrandchallenge.com>

Accept the Challenge!

NEWS

10/3/2014 CGC DECREE OS Update Posted. Visit the [Forum page](#) for more information.

8/29/2014 Frequently Asked Questions updated August 29, 2014. Go to [Documents](#) for the new update.

6/3/2014 Cyber Grand Challenge Announces 1st Group of Teams, Final Event at DEF CON. Visit <http://www.darpa.mil/NewsEvents/Releases/2014/06/03.aspx> for more information.

6/3/2014 CGC Reddit AMA today 10:00 – 4:00pm EST. <http://www.reddit.com/r/IAmA/comments/...>

6/3/2014 CGC Releases Source and Binaries! Visit the Forum page for more information.

5/28/2014 CGC Kick Off is June 3rd! See the Forum post "[CGC Kick Off - June 3, 2014](#)" for important information.

2/12/2014 CGC Architecture Proposer's Day scheduled for February 18, 2014. Go to www.sa-meetings.com/CGCArchitectureProposersDay to register.

11/27/2013 West Coast Competitor Day scheduled for Dec 9, 2013. Go to <http://www.sa-meetings.com/darpacgcccompetitordaywest> to register.

11/26/2013 East Coast Competitor Day scheduled for Dec 3, 2013. Go to <http://www.sa-meetings.com/darpacgcccompetitorday> to register.

10/29/2013 DARPA Cyber Grand Challenge Team Registration Opens!








10/22/2013 DARPA Announces Cyber Grand Challenge

[CONTACT US](#)[PRIVACY POLICY](#)[TERMS OF USE](#)[DARPA HOME](#)

This is an Official U.S. Department of Defense Web Site sponsored by the Defense Advanced Research Projects Agency.

Welcome! [Login](#)[HOME](#) | [DOCUMENTS](#) | [REGISTRATION](#) | [FORUM](#)








CHALLENGE DOCUMENTS

-  [Cyber Grand Challenge Rules - Version 2](#)
-  [Frequently Asked Questions - Version 8, August 29, 2014](#)
-  [Cyber Grand Challenge \(CGC\) Extended Application - May 16, 2014.](#)
-  [Master Schedule - June 23, 2014.](#)
-  [Site Visit Procedures - May 29, 2014.](#)
-  [Technical Paper Guidelines - May 29, 2014.](#)
-  [CQE Scoring Document - Version 1.1, July 7, 2014.](#)

DECREE

[DARPA Experimental Cyber Research Evaluation Environment](#)
[Source code repository](#)
[Package repository](#)
[IDA Pro CGC Platform Binaries](#)

ARCHIVE

-  [DARPA-SN-14-20: Cyber Grand Challenge \(CGC\) Architecture Proposers' Day. - Closed](#)
-  [DARPA-BAA-14-03: Cyber Grand Challenge \(CGC\) Competition Architecture. - Closed](#)
-  [DARPA-BAA-14-03: Attachment 1--CGC Non-Disclosure Agreement. - Closed](#)
-  [DARPA-BAA-14-05: Cyber Grand Challenge: Automated Cyber Reasoning--Amendment 2 - Closed](#)
-  [Competitor Day CGC Program Presentation](#)
-  [Competitor Day Contracts Office Presentation](#)
-  [ISSTA 2014 Presentation](#)

[CONTACT US](#)[PRIVACY POLICY](#)[TERMS OF USE](#)[DARPA HOME](#)

This is an Official U.S. Department of Defense Web Site sponsored by the Defense Advanced Research Projects Agency.
Accessibility/Section 508

News

Cyber Grand Challenge Announces 1st Group of Teams, Final Event at DEF CON

June 03, 2014

Teams from around the world start two-year track towards the world's first tournament of fully automated network security systems

Computer security experts from academia, industry and the larger security community have organized themselves into more than 30 teams to compete in DARPA's Cyber Grand Challenge—a first-of-its-kind tournament designed to speed the development of automated security systems able to defend against cyberattacks as fast as they are launched. DARPA also announced today that it has reached an agreement to hold the 2016 Cyber Grand Challenge final competition in conjunction with DEF CON, one of the largest computer security conferences in the world.

DARPA's Cyber Grand Challenge takes aim at an increasingly serious problem: the inadequacy of current network security systems, which require expert programmers to identify and repair system weaknesses—typically after attackers have taken advantage of those weaknesses to steal data or disrupt processes. Such disruptions pose greater risks than ever as more and more devices, including vehicles and homes, get networked in what has become known as “the Internet of things.”

“Today's security methods involve experts working with computerized systems to identify attacks, craft corrective patches and signatures and distribute those correctives to users everywhere—a process that can take months from the time an attack is first launched,” said Mike Walker (http://www.darpa.mil/Our_Work/I2O/Personnel/Mr_Michael_Walker.aspx), DARPA program manager. “The only effective approach to defending against today's ever-increasing volume and diversity of attacks is to shift to fully automated systems capable of discovering and neutralizing attacks instantly.”

To help accelerate this transition, DARPA launched the Cyber Grand Challenge, the first computer security tournament designed to test the wits of machines, not experts. The Challenge plans to follow a “capture the flag” competition format that experts have used for more than 20 years to test their cyber defense skills. That approach requires that competitors reverse engineer software created by challenge organizers and locate and heal its hidden weaknesses in a live network competition.

The longest-running annual capture-the-flag challenge for experts is held at an annual conference known as DEF CON, and under the terms of a new agreement the Cyber Grand Challenge final competition is scheduled to co-locate with the DEF CON Conference in Las

Vegas in 2016. The co-location of those two events means the first all-computer capture-the-flag competition would occur alongside the conference that has hosted and defined the capture-the-flag competition format for the past 22 years.

At the event, computers that have made it through a series of qualifying events over the next two years would compete head-to-head in a final tournament. Custom data visualization technology is under development to make it easy for spectators—both a live audience at the conference and anyone watching the event's video stream worldwide—to follow the action.

DARPA anticipates that the **two-year Challenge** and its culmination in an event synchronized with DEF CON will not only accelerate the development of capable, automated network defense systems, but also encourage the diverse communities now working on computer and network security issues in the public and private sectors to work together in new ways. This dynamic is crucial if information security practitioners are to pull ahead of adversaries persistently looking to take advantage of network weaknesses.

During a **kickoff event today**, DARPA released **DECREE**, an open-source extension built atop the Linux operating system. Constructed from the ground up as a platform for operating small, isolated software test samples—and incompatible with any other software in the world—DECREE aims to provide a safe research and experimentation environment for the Cyber Grand Challenge. As part of today's launch, Walker and other organizers are hosting a six-hour interactive conversation with potential competitors and members of the public on Reddit, a community discussion site, from 10 a.m. to 4 p.m. ET.

As of today, 35 teams from around the world have registered with DARPA to construct and program high-performance computers capable of competing in the Cyber Grand Challenge. Most competitors have entered on the **"open track"** available to self-funded teams. A parallel **"proposal track"** consists of teams invited and partially supported by DARPA to develop automated network defense technology. Those teams represent a mix of participants from industry and academia and will receive seed funding from DARPA until their performance is tested in open competition involving all teams at a major qualification event scheduled for June 2015. Additional teams may register to participate through **November 2, 2014.**

- For All Secure
- GrammaTech
- Lekkertech
- SIFT
- SRI
- Trail of Bits
- University of California, Berkeley

The winning team from the CGC finals stands to receive a cash prize of **\$2 million**. Second place can earn **\$1 million** and third place **\$750,000**.

Details about the Cyber Grand Challenge and some of the other registered teams can be found at www.cybergrandchallenge.com (<http://www.cybergrandchallenge.com/>) .

###

Associated images posted on www.darpa.mil (<http://www.darpa.mil/>) and video posted at www.youtube.com/darpatv (<http://www.youtube.com/darpatv>) maybe reused according to the terms of the DARPA User Agreement, available here: <http://go.usa.gov/nYr> (<http://go.usa.gov/nYr>) .

Tweet @darpa

Media Queries

Please direct all media queries to Outreach@darpa.mil

Images



[Click for High-Resolution Image](#)

Computer security experts from academia, industry and the larger security community have organized themselves into more than 30 teams to compete in DARPA's Cyber Grand Challenge—a first-of-its-kind tournament designed to speed the development of automated security systems able to defend against cyberattacks as fast as they are launched. DARPA also announced today that it has reached an agreement to hold the 2016 Cyber Grand Challenge final competition in conjunction with DEF CON, one of the largest computer security conferences in the world.

Additional Info



News

DARPA Announces Cyber Grand Challenge

October 22, 2013

First-of-its-kind cyber defense tournament seeks to drive automation revolution in information security

What if computers had a “check engine” light that could indicate new, novel security problems? What if computers could go one step further and heal security problems before they happen?

To find out, the Defense Advanced Research Projects Agency (DARPA) intends to hold the Cyber Grand Challenge (CGC)—the first-ever tournament for fully automatic network defense systems. DARPA envisions teams creating automated systems that would compete against each other to evaluate software, test for vulnerabilities, generate security patches and apply them to protected computers on a network. To succeed, competitors must bridge the expert gap between security software and cutting-edge program analysis research. The winning team would receive a cash prize of \$2 million.

“DARPA’s series of vehicle Grand Challenges were the dawn of the self-driving car revolution,” said Mike Walker, DARPA program manager. “With the Cyber Grand Challenge, we intend a similar revolution for information security. Today, our time to patch a newly discovered security flaw is measured in days. Through automatic recognition and remediation of software flaws, the term for a new cyber attack may change from zero-day to zero-second.”

Highly trained experts capable of reasoning about software vulnerabilities, threats and malware power modern network defense. These experts compete regularly on a global “Capture the Flag” tournament circuit, improving their skills and measuring excellence through head-to-head competition. Drawing on the best traditions of expert computer security competitions, DARPA aims to challenge unmanned systems to compete against each other in a real-time tournament for the first time.

“The growth trends we’ve seen in cyber attacks and malware point to a future where automation must be developed to assist IT security analysts,” said Dan Kaufman, director of DARPA’s Information Innovation Office, which oversees the Challenge.

The competition is expected to draw teams of top experts from across a wide range of computer security disciplines including reverse engineering, formal methods, program analysis and computer security competition. To encourage widespread participation and teaming, DARPA plans to host teaming forums on the CGC website at www.darpa.mil/cybergrandchallenge.

For the first time, a cyber competition would take place on a network framework purpose-built to interface with automatic systems. Competitors would navigate a series of challenges, starting with a qualifying event in which a collection of software must be automatically analyzed. Competitors would qualify by automatically identifying, analyzing and repairing software flaws.

DARPA intends to invite a select group of top competitors from the qualifying event to the Cyber Grand Challenge final event, slated for early to mid-2016. In that competition, each team's system would automatically identify software flaws, scanning the network to identify affected hosts. Teams would score based on how capably their systems could protect hosts, scan the network for vulnerabilities and maintain the correct function of software. The winning team from the CGC finals would receive a cash prize of \$2 million, with second place earning \$1 million and third place taking home \$750,000.

A Broad Agency Announcement (BAA) with specific information for potential competitors is available at <http://go.usa.gov/WqcH>. Competitors can choose one of two routes: an unfunded track in which anyone capable of fielding a capable system can participate, and a funded track in which DARPA awards contracts to organizations presenting the most compelling proposals.

DARPA also plans in the near future to issue a second BAA for proposals to develop technologies to support the competition. Support technologies will include accessible visualization of a real-time cyber competition event, as well as custom problem sets. That BAA will be available on the Federal Business Opportunities website.

The program anticipates hosting two Challengers' Days—one at DARPA's offices in Arlington, Va., and the other on the West Coast—where interested competitors can learn more about the event. More information, including up-to-date rules and prize amounts, is available at www.darpa.mil/cybergrandchallenge.

Media Queries

Please direct all media queries to Outreach@darpa.mil

Images



[Click for High-Resolution Image](#)

Computer security experts from academia, industry and the larger security community have organized themselves into more than 30 teams to compete in DARPA's Cyber Grand Challenge—a first-of-its-kind tournament designed to speed the development of

automated security systems able to defend against cyberattacks as fast as they are launched. DARPA also announced today that it has reached an agreement to hold the 2016 Cyber Grand Challenge final competition in conjunction with DEF CON, one of the largest computer security conferences in the world.

Additional Info

- Cyber Grand Challenge (CGC)

Tweet 194

g+1 85

Like < 717

Cyber Grand Challenge

Rules

May 16, 2014

Version 2



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



Document Change Summary

[illegible]

Table of Contents

1	Introduction	5
1.1	Vision	5
1.2	Overview	5
1.3	Objectives	6
2	Applying to the Cyber Grand Challenge (CGC)	7
2.1	Eligibility	7
2.2	Proposal Track Applications	8
2.3	Open Track Applications	8
3	Cyber Grand Challenge Events	9
3.1	Cyber Grand Challenge Qualification Event (CQE).....	9
3.1.1	Preparing for CQE	9
3.1.2	CQE Scoring.....	9
3.1.3	Advancement to CFE.....	10
3.1.4	Finalists	10
3.2	Cyber Grand Challenge Final Event (CFE).....	11
3.2.1	CFE Trials	11
3.2.2	CFE Format.....	12
3.2.3	CFE Scoring.....	12
3.2.4	CFE Technical Paper	13
3.2.5	CFE Prizes	13
4	Full Automation Requirement.....	13
5	Intellectual Property	14
6	Additional Information	14
7	Scope and Precedence.....	16

1 Introduction

1.1 Vision

Top computer security experts test their skill head-to-head in competitive “Capture the Flag” contests. These contests provide a competition rating for the ability of experts to locate and comprehend security weaknesses.

The Defense Advanced Research Projects Agency (DARPA) Cyber Grand Challenge (CGC) will utilize a series of competition events to test the abilities of a new generation of fully automated cyber defense systems. During a final competition event, automated Cyber Reasoning Systems will compete against each other in real time. This event will be held in a public setting and documented for research purposes.

The CGC seeks to engender a new generation of autonomous cyber defense capabilities that combine the speed and scale of automation with reasoning abilities exceeding those of human experts.

1.2 Overview

The Department of Defense (DoD) maintains information systems using a software technology base comprised of Commercial Off The Shelf (COTS) operating systems and applications. This COTS technology base is common to the DoD, industry, and the Defense Industrial Base, and the continual discovery of potential vulnerabilities in this software base has led to a constant cycle of intrusion, compromise discovery, patch formulation, patch deployment and recovery. This defensive cycle is currently performed by highly trained software analysts; it is the role of these analysts to reason about the function of software, identify novel threats and remove them. Manual analysis of code and threats is an artisan process, often requiring skilled analysts to spend weeks or months analyzing a problem. The size of the technology base also contributes to the difficulty of manually discovering vulnerabilities.

At the present time, automated program analysis capabilities are able to assist the work of human software analysts. These automation technologies include Dynamic Analysis, Static Analysis, Symbolic Execution, Constraint Solving, Data Flow Tracking, Fuzz Testing, and a multitude of related technologies. In the Cyber Grand Challenge, a competitor will improve and combine these semi-automated technologies into an unmanned Cyber Reasoning System (CRS) that can autonomously reason about novel program flaws, prove the existence of flaws in networked applications, and formulate effective defenses. The performance of these automated systems will be evaluated through head-to-head tournament style competition.

The CGC program will draw widespread attention to the technology issues associated with autonomous software comprehension and motivate entrants to overcome technical challenges to realize truly effective autonomous cyber defense. This program

will challenge the most capable and innovative companies, institutions, and entrepreneurs to produce breakthroughs in capability and performance.

1.3 Objectives

Currently, network Intrusion Detection Systems, software security patches, and vulnerability scanners are all forms of **signature based defense**: defensive systems which act on discrete quanta of human knowledge ("signatures"). Human analysts develop these signatures through a process of reasoning about software. In fully autonomous defense, a cyber system capable of reasoning about software will create its own knowledge, autonomously emitting and using knowledge quanta such as vulnerability scanner signatures, intrusion detection signatures, and security patches.

The objective of this program is to identify effective, integrated automation of cyber reasoning tasks as assessed by the Areas of Excellence (AoE) in Table 1. These AoE address the protection of compiled test software ("Challenge Binaries" or "CBs") operated on a closed, monitored network ("Competition Framework").

	Areas of Excellence (AoE)	CGC Qualification Event (CQE)	CGC Final Event (CFE)
1	Autonomous Analysis: The automated comprehension of computer software (e.g., CBs) provided through a Competition Framework.	<input type="checkbox"/>	<input type="checkbox"/>
2	Autonomous Patching: The automatic patching of security flaws in CBs provided through a Competition Framework.	<input type="checkbox"/>	<input type="checkbox"/>
3	Autonomous Vulnerability Scanning: The ability to construct input which when transmitted over a network provides proof of the existence of flaws in CBs operated by competitors. These inputs shall be regarded as Proofs of Vulnerability.	<input type="checkbox"/>	<input type="checkbox"/>
4	Autonomous Service Resiliency: The ability to maintain the availability and intended function of CBs provided through a Competition Framework.	<input type="checkbox"/>	<input type="checkbox"/>
5	Autonomous Network Defense: The ability to discover and mitigate security flaws in CBs from the vantage point of a network security device.		<input type="checkbox"/>

Table 1 - Areas of Excellence

2 Applying to the Cyber Grand Challenge (CGC)

DARPA provides two parallel paths for participating in the CGC: the Proposal Track and the Open Track. Rankings in the CGC Qualifying Event (CQE) and the CGC Final Event (CFE) will be based on the same technical evaluation criteria and scoring mechanisms for all competitors, irrespective of track. Proposal Track and Open Track teams that successfully pass the CQE will be invited to compete in the CFE. See Section 3 for a detailed description of the CQE and CFE.

2.1 Eligibility¹

A CGC Team is comprised of an entrant (US Entity² or individual), an individual team leader and an optional set of team members (individuals). Individual entrants may be the same individual named as team leader. If the entrant is a US Entity rather than an individual, the team must identify an entrant official. Teams may enter under an official affiliation (e.g., a university or corporation). Teams may also have an official set of sponsors.

Cyber Grand Challenge Team				
Entrant	Team Leader	Team Member(s)	Sponsor(s)	Official Affiliation
Required	Required	Optional	Optional	Optional
US Entity or individual(s)	Individual	Individual(s)	US Entity or individual(s)	US Entity

The CGC is open to team members of all nationalities and of all ages with the following caveats:

- CGC participation by minors requires authorization by a parent or guardian.
- An entrant must be a U.S. citizen, permanent resident, or US Entity.
- An individual, organization, or sponsor is not eligible to apply or participate if he, she, or it is on the Specially Designated Nationals list.³

Teams are intended to be wholly separate entities that do not share members, unique technology, official affiliations or financial interest.

¹ This section specifically refers to eligibility to participate in CGC events; eligibility to receive prizes is based on 15 U.S.C. § 3719. See DARPA-BAA-14-03 and DARPA-BAA-14-05 for specifics regarding eligibility to propose to those solicitations.

² Within these Rules, a US Entity is defined as a private entity incorporated in and maintaining a primary place of business within the United States; see 15 U.S.C. § 3719(g)(3).

³ <http://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx>.

Federal entities (from the US or any other country) are not eligible to participate as entrants, sponsors or official affiliates. Federal employees acting within the scope of their employment are not eligible to participate as entrants, entrant officials, team leaders or team members.

A Federal employee acting outside the scope of his or her employment should consult his or her ethics official before participating in the Challenge. DARPA employees and support contractors, their spouses, dependents, and household members are not eligible to participate.

Any personnel funded by DARPA to support the Cyber Grand Challenge are not eligible to participate. This group includes, but is not limited to, any party funded under DARPA-BAA-14-03 as well as any Federally Funded Research and Development Center (FFRDC) or Government personnel whose scope of work covers CGC architecture development.

DARPA reserves the right to disqualify a participant whose actions are deemed to violate the spirit of the competition for any reason, including but not limited to, the violation of relevant laws or regulations in the course of participation in the Challenge.

See Section 6 for additional information.

2.2 Proposal Track Applications

Proposal Track teams will be competitively selected on the basis of proposals submitted in response to DARPA-BAA-14-05. See DARPA-BAA-14-05 for Proposal Track deadlines and procedures related to submissions and selections. Proposal Track teams receiving an award through Broad Agency Announcement (BAA) DARPA-BAA-14-05 may not participate in the Open Track.

2.3 Open Track Applications

There is no fee for entry. Application materials are available on the Cyber Grand Challenge website (www.darpa.mil/cybergrandchallenge) and must be submitted in accordance with the instructions outlined herein. The application procedure is a two-step process consisting of an initial application and an extended application. All parts of both applications must be received by DARPA no later than 12:00 noon (U.S. Eastern Time), ~~June 3, 2014~~ November 2, 2014.

DARPA will acknowledge receipt of complete applications via e-mail. Upon receipt of each team's Cyber Grand Challenge Initial Application, DARPA will assign a team reference number which should be included on all team correspondence with DARPA.

The Initial Application must be submitted online at:
www.darpa.mil/cybergrandchallenge.

The Extended Application may be submitted through one of the detailed methods below.

(1) E-mailed to CyberGrandChallenge@darpa.mil. E-mails must include "Extended Application" and the team reference number in the subject line.

(2) Mailed/hand-carried directly to DARPA. Application materials must be addressed to:

DARPA/I2O
Attn: Cyber Grand Challenge
675 North Randolph Street
Arlington, VA 22203-2114

Application materials received after the deadline specified herein will be disposed of in a secure manner. Application materials will not be returned. Incomplete applications will not be accepted. DARPA may disqualify any team which does not meet the eligibility requirements specified herein.

3 Cyber Grand Challenge Events

3.1 Cyber Grand Challenge Qualification Event (CQE)

Finalists for the CFE will be determined at the CQE. The CQE is tentatively scheduled for June 3, 2015. During the CQE, all Proposal Track and Open Track competitors will receive an identical corpus of Challenge Binaries (CBs): insecure software which must be analyzed and secured. The goal of the CQE is to use an autonomous system to locate and mitigate flaws in the CBs and return a corpus of CB data to DARPA for scoring.

3.1.1 Preparing for CQE

Competitors will have the opportunity to participate in two preliminary Scored Events that will be similar in format to the CQE. Participation in these Scored Events is optional and success in these events will not be evaluated as part of CGC scoring. Each Scored Event is an opportunity for competitors to gain an understanding of the format, procedure, and scoring mechanism to be used during the CQE. These events are tentatively scheduled for December 2, 2014 and April 6, 2015.

3.1.2 CQE Scoring

Proposal Track and Open Track competitors will receive a score based on their ability to locate and mitigate flaws in CB software while minimizing damage to the function of each CB. The CQE will involve securing a corpus of over 100 CBs. For each CB, a CRS will demonstrate the location of existing flaws by formulating inputs that activate a software

flaw, crash or fault. To demonstrate the mitigation of flaws, each CRS will provide a secured version of each CB. Scoring will reflect performance in CQE AoE 1 - 4 as indicated in Table 1. A CRS must mitigate a flaw in at least one CB while retaining some CB functionality in order to receive a score greater than zero.

3.1.3 Advancement to CFE

Using a scoring methodology derived from AoE 1 - 4, DARPA will score and rank teams from the Proposal Track and Open Tracks. Based on this scoring, DARPA will invite some teams to the CFE as finalists. Finalists invited by DARPA will:

- Have submitted a CQE Technical Paper accepted by DARPA,
- Achieve a top ranking, non-zero CQE score, and
- Have successfully demonstrated their system to DARPA during a site visit.

3.1.3.1 CQE Technical Paper

To receive an invitation to the CFE, a team must submit an acceptable CQE technical paper to DARPA describing their CRS. CQE technical papers will be evaluated and approved according to the CGC Technical Paper Guidelines to be posted on the CGC website: www.darpa.mil/cybergrandchallenge. DARPA will review each technical paper and communicate acceptance of papers to each team leader. CQE Technical Papers are due March 5, 2015.

3.1.3.2 Site Visit

After CQE performance, teams must demonstrate the function of their system during a team site visit. DARPA will travel to an acceptable location (within the United States) identified by each eligible team. DARPA will release the Site Visit Procedures on or before June 3, 2014. Each team leader and CRS must be present at the site visit. DARPA will bring a corpus of CB software to the demonstration for analysis by the CRS. DARPA will assess the CRS using the CQE AoE listed in Table 1. During the site visit, teams should be prepared to demonstrate the CRS to the satisfaction of the DARPA team.

3.1.4 Finalists

Proposal Track teams invited to the CFE as finalists will continue to be funded by DARPA through their period of performance, in accordance with the terms of their awards. (See DARPA-BAA-14-05 for details). Proposal Track teams are not eligible to win prizes at the CQE stage.

Open Track teams invited to the CFE as finalists will receive a cash prize and retain eligibility to compete in the CFE. The anticipated amount of CQE prizes is \$750,000 per invited team.

3.2 Cyber Grand Challenge Final Event (CFE)

The CGC Champion will be determined at the CFE, tentatively scheduled for July 17, 2016. The CFE will consist of a real time, all-computer tournament scored over all Areas of Excellence from Table 1.

3.2.1 CFE Trials

To demonstrate readiness for the CFE, each finalist CRS will be required to pass a series of three Trials. These Trials (described below) are intended to demonstrate the field-worthiness of each finalist CRS and present an opportunity for competitors to debug and refine interactions with the Competition Framework prior to CFE competition. Over a three-week period, DARPA will provide each finalist with access to the Competition Framework to allow a demonstration match against a simulated opponent.

Trial 1 demonstrates ability in Area of Excellence 4. To pass this trial, each CRS will receive a Challenge Binary from the Competition Framework and field it on a networked host without disrupting its intended function.

Trial 2 demonstrates ability in Areas of Excellence 2 and 5. To pass this trial, competitor systems receive a Challenge Binary from the Competition Framework and field it on a networked host while preventing attempts by a simulated competitor to activate any flaws in the CB.

Trial 3 demonstrates ability in Area of Excellence 3. To pass this trial, competitor systems receive a Challenge Binary from the Competition Framework, identify its presence and remotely activate a flaw in the CB as it exists on a networked host operated by a simulated opponent.

Note that the Trials do not address Area of Excellence 1. Challenge Binaries for the Trials will be provided to competitors beforehand, and competitors are welcome to field signatures, patches, and vulnerability scans which have been hand crafted prior to the Trials.

DARPA will provide notification to each finalist as each Trial is completed. Upon completion of all three Trials, DARPA will issue a certification to each successful finalist. DARPA may, at its sole discretion, disqualify any finalist team which does not complete the Trials within the three week period.

The CFE Trial series is the only CGC event in which automated program analysis is not required. See Section 4 for further information on automation requirements.

3.2.2 CFE Format

During the CFE, each finalist will field a CRS. Each CRS will interface with the CGC Competition Framework via a networked interface to be specified by DARPA in the CGC Competition Framework API. This interface will provide each CRS with access to CBs as well as a networked host on which each CB must be fielded. During the CFE, each CRS will be responsible for maintaining and securing CB software provided by the Competition Framework; each CRS will be responsible for deploying this software on a networked host. Each CRS will have the ability to administer its own networked host, as well as connect to networked hosts operated by other finalists. Each CRS will work to challenge other finalists by emitting Proofs of Vulnerability (Area of Excellence 3) directed at the networked hosts operated by competitors. In turn, each CRS will work to repel such proofs from its own system, utilizing AoE 1, 2, and 5. The Competition Framework will provide extensive monitoring of the health of all CB software in operation, noting when competitors fail to keep software running and undamaged (Area of Excellence 4).

The CFE is designed to pose realistic defense challenges. For this reason, the CRS confronts the CFE network from the vantage point of a real world network defender. Each CRS will have the ability to deploy CBs to a networked host as well as monitor and modify network traffic to a networked host. Teams will not have the ability to alter the operating system or hardware of the networked host, or harness the execution of CBs as they operate in situ. For this reason, approaches that require a defended host to use custom hardware, custom operating system modifications, or harnessed software execution will be unable to interface with the Competition Framework.

A CRS observing network traffic during the CFE will be prevented from identifying the originating system of each connection via technical means imposed by the Competition Framework. Due to this limitation, decisions about network traffic made by a CRS must be made based on the contents of the network traffic rather than network addressing information.

3.2.3 CFE Scoring

The scoring methodology for the CFE will be announced by DARPA following the selection of CFE finalists. The scoring methodology will reflect successful cyber reasoning during a live exercise utilizing the CFE AoE identified in Table 1. This score will include the following considerations:

- A successful CRS will mitigate all vulnerabilities in the CB software running on its networked host, using whatever combination of networked defense or security patching is appropriate, without degrading the availability or correct function of each CB.

- A successful CRS will challenge the CB software maintained by competitors on their networked hosts; this will be accomplished by emitting Proofs of Vulnerability to the CB software.
- An unsuccessful CRS will fail to maintain the function of CB software on its networked host.
- An unsuccessful CRS will repeatedly allow Proofs of Vulnerability from other competitors to activate flaws in CB software.

At the conclusion of the event, DARPA will consult with event monitors to confirm the scoring results and the integrity of the competition.

3.2.4 CFE Technical Paper

All CFE participants must submit a CFE Technical Paper to DARPA describing their CRS in its final competition state, as well as lessons learned during CFE. CFE technical papers will be evaluated and approved according to the CGC Technical Paper Guidelines. DARPA will review each technical paper and communicate acceptance of papers to each performer. CFE Technical Papers are due within three weeks of the conclusion of the CFE.

3.2.5 CFE Prizes

Based on finalized scoring, DARPA will determine 1st, 2nd, and 3rd place winners to receive prizes. Following receipt and acceptance of final CFE Technical Papers from each winning team, DARPA will publicly announce the 1st, 2nd and 3rd place winners.

DARPA anticipates prizes in the following amounts:

- 1st place: \$2,000,000
- 2nd place: \$1,000,000
- 3rd place: \$750,000

Both Proposal Track and Open Track teams are eligible to receive prizes following the CFE.

4 Full Automation Requirement

Both the CQE and the CFE require a fully automated solution – no human assistance is permitted during either event in any cyber reasoning processes, including reverse engineering and patch formulation. Human assistance or other violation of these rules during CGC events will result in team disqualification and further actions as appropriate under Federal law and regulation. DARPA will preserve the integrity of competition within the CGC with safeguards to be developed during the program. These safeguards

will not be shared as sharing may cause the methods to be ineffective. For this reason, all safeguard inspection schedules, methods, and capabilities will not be disclosed to any Challenge participant for any reason. Any information regarding human interference in cyber reasoning processes during any CGC event should be sent to CyberGrandChallenge@darpa.mil.

5 Intellectual Property

DARPA claims no rights to software developed by Open Track competitors as a result of participation in the CGC. DARPA does not intend to disclose the CQE and CFE Technical Papers outside the Government, with the following exception: CGC Technical Papers may be handled by DARPA support contractors for administrative purposes and/or to assist with technical evaluation. All DARPA support contractors performing this role are bound by nondisclosure agreements. DARPA does not intend to disclose CGC Technical Papers to contractors to duplicate, commercialize, or for reprourement or reverse engineering purposes.

Proposal Track competitors should refer to DARPA-BAA-14-05 for specific information on intellectual property (IP) licensing rights related to their participation.

6 Additional Information

The development of revolutionary technologies is a key objective of the CGC. Teams are invited to communicate directly with DARPA regarding any rule that restricts their ability to demonstrate technical achievement and innovative solutions. Questions regarding rules should be sent to CyberGrandChallenge@darpa.mil.

DARPA may modify the rules at any time and for any reason, including the accommodation of a promising technical approach that would have been excluded by the rules.

DARPA unilaterally reserves the right to cancel or modify the CQE and CFE at its sole discretion. Considerations may include availability of funds and technical viability.

Participation in the CQE and CFE will be governed by Event Participation Agreements to be released by DARPA⁴. These Agreements will define the boundaries of competition within each event as well as assign IP rights to data transmitted during each event to DARPA. Acceptance of the Event Participation Agreements is mandatory for event participation. All data generated by each CRS during the CFE, to include network traffic, modified CBs, network host status, and other output data will be logged by the Competition Framework. These logs will be released into the public domain.

⁴ The Event Participation Agreements will be posted on the CGC website at www.darpa.mil/cybergrandchallenge.

The CGC prize is authorized under 15 U.S.C. § 3719. The CGC program will incentivize innovation using multiple cash prizes.⁵

In accordance with 15 U.S.C. § 3719, to be eligible to win a prize in this Challenge, an individual must have applied to participate in the Challenge in accordance with the instructions outlined herein. The entrant (described in section 2.1) shall be the prize recipient. The prize recipient shall be a citizen, a permanent resident of the United States, or a US Entity. Tax treatment of prizes will be handled in accordance with U.S. Internal Revenue Service guidelines.

Application information collected by DARPA will be used solely for the purpose of administering the CGC. Use of application information is governed by the Privacy Policy posted on the Cyber Grand Challenge website.

Teams may be listed on the CGC website to enable the event to be tracked by interested members of the public. The name and photographs of the winning teams may be posted on the DARPA website and released to the media.

DARPA reserves the right to disqualify a participant whose actions are deemed to violate the spirit of the competition for any reason, including but not limited to, the violation of relevant laws or regulations in the course of participation in the CGC.

By applying to and/or participating in the CGC, applicants and participants agree to follow these rules. Applicants and participants must agree to assume any and all risks and waive claims against the Federal Government and its related entities, except in the case of willful misconduct, for any injury, death, damage, or loss of property, revenue, or profits, whether direct, indirect, or consequential, arising from participation in the competition, whether the injury death, damage, or loss arises through negligence or otherwise.

DARPA does not authorize or consent to CGC participants infringing on any U.S. patent or copyright while participating in the CGC. No illegal activities may be undertaken for the purpose of participation in the Cyber Grand Challenge.

The appearance and reference to any person, name, place, film, artwork or any other images that are used in connection with the CGC does not constitute or imply endorsement by the U.S. Department of Defense or by DARPA.

Questions regarding the rules, privacy policy, or other aspects of the CGC may be directed to CyberGrandChallenge@darpa.mil.

⁵ Trophies will be substituted for cash prizes in the absence of sufficient funds.

7 Scope and Precedence

The rules outlined herein apply to all applicants and participants in the CGC. However, nothing in these rules, to include this document and any subsequent CGC rules documents, may be interpreted as modifying the statement of work or authorizing work outside the terms and conditions of any existing agreements or contracts with DARPA.

DARPA will release additional documents with rules updates, procedures, and other information for teams. These additional documents carry the full authority of the rules in this document.

Additional documents to be released include the following, at a minimum:

CGC Documents:

- CGC Master Schedule
- CGC Technical Paper Guidelines
- CGC Site Visit Procedures
- CGC Extended Application

CGC Qualification Event (CQE) Documents:

- CQE Procedures
- CQE Scoring Guide

CGC Final Event (CFE) Documents:

- Competition Framework API Document
- CFE Procedures
- CFE Scoring Guide

All documents including this Rules document will be posted and updated on the CGC website, www.darpa.mil/cybergrandchallenge. All CGC documents including these Rules should be considered living documents, subject to update and clarification throughout the CGC program.

Cyber Grand Challenge

Frequently Asked Questions (FAQ)

October 21, 2014



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



CYBER
GRAND_CHALLENGE

Document Change Summary

[illegible]

Q74: I am a foreign national who is eligible to participate per the CGC Rules. I have created a US-based LLC with a US-based Registered Agent to serve as the Entrant for my CGC team; this LLC is also eligible to participate per the CGC Rules. Is this approach compliant with the CGC Rules?

A74: Yes.

Q73: What happens when a connection is made to a DECREE service?

A73: *inetd-style*. A new instance is created to handle the new connection. This new instance is torn down after the connection terminates.

Q72: What types of connections will be made during CQE scoring?

A72: Multiple connections will be made from Service Pollers. Multiple connections will also be made from Proof of Vulnerability modules. Service Polls and PoV modules will never share connections.

Q71: What types of connections will be made during CFE scoring?

A71: Multiple connections will be made from service pollers. Multiple connections will also be made from logic built by competitors. Service polls and competitor logic will never share connections.

Q70: What other access to Cyber Grand Challenge is available to competitors outside of the cybergrandchallenge@darpa.mil email box and the FAQ responses?

A70: In the interests of conducting a fair and equitable global competition, access to challenge information is made available electronically to all competitors. All competitors whether next door or across the globe, may submit questions through the mailbox, and responses will be communicated through this FAQ.

Q69: Are CFE finalists required to bring hardware to compete in CFE?

A69: No. Finalists will have the option of either:

1. Bringing a competition system to CFE in accordance with A31, or
2. Competing in CFE on a DARPA-provided compute cloud instance after having accepted the DARPA Cloud Agreement.

Each DARPA-provided compute cloud instance will be on the order of hundreds of x86-64 cores.

Further details regarding the Cloud Agreement and system specifications will be released at a later date.

Q68: What information will be released to competitors after Scored Event #1?

A68: Please note that information release after Scored Events will be entirely different from the post-CQE information release addressed in A25. After Scored Event #1, the following information will be released publicly:

- The names of the seven top-scoring teams in rank order.
- A list of SHA-256 hashes for submitted Challenge Binaries and their associated scores and corresponding reference CB name.
- A list of SHA-256 hashes for PoVs and their associated scores and corresponding reference CB name.

Please note, these released hash lists will not correlate scored submissions to teams. Competitors will be required to calculate SHA-256 hashes of their submitted inputs in order to determine their scores.

Q67: How will ranking occur in Scored Event #1?

A67: Multiple submissions may be scored; hash list information on multiple submissions will be available via the hash list format (A68). Ranks will be determined using the score assigned to each team's final submission.

Q66: What will CQE Challenge Bundle contain?

A66: At the beginning of CQE, competitors will gain access to CQE Challenge Bundle (bundle will contain a collection of Reference CBs, as well as some pcap recordings of some service poll interactions between Service Pollers and these Reference CBs). These service poll interaction samples, where present, are not guaranteed to be complete.

Q65: What will Scored Event Challenge Bundles contain?

A65: Scored events are intended to provide technical preparation for CQE; therefore the Scored Event Bundles will mirror the format of the CQE Challenge Bundle to the greatest extent possible. Competitors should note that the CQE Bundle will be much larger than the Scored Event Bundles. These Scored Event Bundles may also re-use previously released CBs.

Q64: What is DECREE?

A64: DECREE is an open-source extension built atop the Linux operating system. Constructed from the ground up as a platform for operating small, isolated software test samples that are incompatible with any other software in the world—DECREE aims to provide a safe research and experimentation environment for the Cyber Grand Challenge.

DECREE binaries and source are available:

<http://repo.cybergrandchallenge.com/>
<http://github.com/cybergrandchallenge/>

Q63: How should issues in DECREE be reported?

A63: Email cybergrandchallenge@darpa.mil

Q62: Will all advanced application defenses that prevent arbitrary code from running increase the security score in CQE?

A62: No. CGC scoring does not require arbitrary code execution, therefore mechanisms which frustrate arbitrary code execution will not necessarily prevent scoring events. In CQE, competitors have the opportunity to mitigate denial of service flaws. See also Q4.

Q61: Will the Reference Patched CB perform differently than the Original CB?

A61: A diverse group of software authors are building a large corpus of CBs for CGC incorporating many classes of vulnerabilities. These CB authors are required to provide a single Reference Patched CB that passes the same functionality test suite as the Original CB and is not susceptible to any of the reference PoVs.

Q60: How does the Inter Process Communication (IPC) work in Challenge Binaries (CBs)?

A60: DECREE precludes communication via shared memory, network, or persistent storage between different CBs as well as different connections serviced by the same CB.

In order to offer a rich CB portfolio with broad CWE coverage including concurrency issues, DARPA allows for the use of a CGC IPC mechanism within a single CB, which works as follows. Each CB may be composed of multiple binaries running in distinct processes. The CGC competition framework will launch all of the binaries associated with the challenge. Each of these processes will be pre-connected with file descriptors to communicate with the others via `receive()` and `transmit()` system calls (see Figure 1) in a manner determined by the CB author (see Figure 2). Example IPC CBs will be provided prior to the first CQE Scored Event.

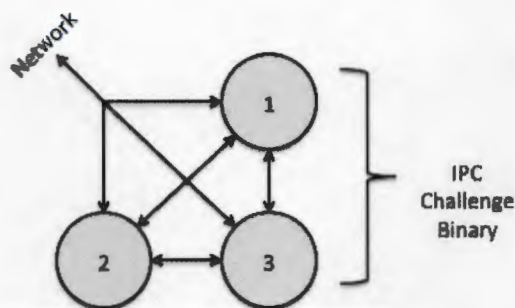


Figure 1: File descriptor connections

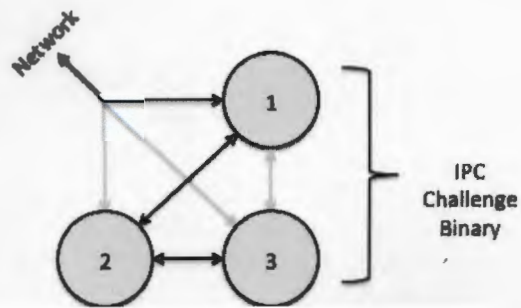


Figure 2: Example use of IPC inter-connections

Q59: What is the scoring method for CQE?

A59: DARPA held a period of public comment for the CFE and CQE scoring methods, and feedback from the CGC community was received and reviewed by DARPA. Updated scoring methods for CQE and CFE were released on Monday, March 10, 2014. These scoring methods are consistent with the Cyber Grand Challenge Rules. See also Q/ A 26, 27, and 30.

CQE scoring is the product of three assessed quantities: Availability score, Security score, and Evaluation score. These scores map to the Areas of Excellence (AoE) located in the Cyber Grand Challenge Rules as follows:

Availability: Area of Excellence 4

Security: Area of Excellence 2

Evaluation: Area of Excellence 3

During CQE, the CBs distributed by DARPA shall be referred to as “reference CBs”, not to be confused with replacement CBs submitted by competitors. PoVs used by DARPA for scoring will be referred to as “reference PoVs”. PoVs submitted by competitor systems to DARPA during CQE will be referred to as “submitted PoVs”.

DARPA will score one replacement CB and one submitted PoV per reference Challenge Binary. CQE Scores will be assessed per reference Challenge Binary (“CB score”). Each CB score will be calculated as follows:

$$\text{Availability} * \text{Security} * \text{Evaluation}$$

Availability:

This quantity shall vary as a multi-step function between 0 and 1, with 1 being a perfect score. Performance and Retained Functionality will be measured, with Availability being set to the minimum of these quantities.

- Performance of a submitted CB will decrement based on the greatest measured increase in system resource utilization. These measured increases include file size, execution time, and memory usage. For each of these measured quantities, a maximum acceptable increase is indicated below, after which Performance begins to decrement:
 - File size: +40%
 - Execution time: +10%
 - Memory usage: +10%
- Retained Functionality will be the percentage of test cases the replacement CB passes.

Competitors are advised that use of a multi-step function imposes a faster-than-linear Availability dropoff based on damage to Performance or Retained Functionality.

Security:

This quantity shall be determined using two quantities, Reference and Consensus:

- Reference: The number of reference PoVs which do not prove vulnerability in the replacement CB, divided by the number of reference PoVs
- Consensus: This quantity will be set to 0 or 1:
 - 0: Any submitted PoV proved vulnerability in the replacement CB
 - 1: No submitted PoV proved vulnerability in the replacement CB

If Reference is zero, Security will be set to zero.

If Reference is nonzero, Security will be calculated as follows:

$$1 + (\text{Reference} + \text{Consensus}) / 2$$

Evaluation:

This quantity will be set to 1 or 2:

- 1: The PoV emitted by this CRS did not prove vulnerability in the reference CB
- 2: The PoV emitted by this CRS did prove vulnerability in the reference CB

A CRS's total score at the end of CQE shall be the sum of that CRS's CB scores.

Q58: What is the scoring method for CFE?

A58: DARPA held a period of public comment for the CFE and CQE scoring methods, and feedback from the CGC community was received and reviewed by DARPA. Updated scoring methods for CQE and CFE were released on Monday, March 10, 2014. These scoring methods are consistent with the Cyber Grand Challenge Rules. See also Q/ A26, 27, and 30.

CFE scoring is the product of three assessed quantities: Availability score, Security score, and Evaluation score. These scores map to the Areas of Excellence (AoE) located in the Cyber Grand Challenge Rules as follows:

Availability: Area of Excellence 4

Security: AoE 2 and 5

Evaluation: Area of Excellence 3

CFE scoring will take place over many rounds. Scores will be assessed per Challenge Binary per round ("CB round score"); it follows that the sum of the CB round scores for a single CRS will be the total score for that system. Each CB round score will be calculated as follows:

$$\text{Availability} * \text{Security} * \text{Evaluation}$$

Availability:

This quantity shall vary as a multi-step function between 0 and 1, with 1 being a perfect score. Performance and Retained Functionality will be measured, with Availability being set to the minimum of these quantities.

- Performance of a submitted CB will decrement based on the greatest measured increase in system resource utilization. These measured increases include file size, execution time, and memory usage. For each of these measured quantities, a maximum acceptable increase is indicated below, after which Performance begins to decrement:
 - File size: +20%
 - Execution time: +5%
 - Memory usage: +5%
- Retained Functionality will be the percentage of network test cases the replacement CB passes.

Competitors are advised that use of a multi-step function imposes a faster-than-linear Availability dropoff based on damage to Performance or Retained Functionality.

Security:

This quantity will be set to 1 or 2:

- 1: At least one PoV from a competitor proved vulnerability in this CB during this round
- 2: No PoVs from competitors proved vulnerability in this CB during this round

Evaluation:

This quantity will vary between 1 and 2:

- 1: No PoVs emitted by this CRS proved vulnerabilities in this CB service on competitor systems
- $1 + (x / (N - 1))$ PoVs emitted by this CRS for this CB service proved vulnerability in x competitor systems, where N is the number of CRSs participating in CFE.

A CRS's total score at the end of CFE shall be the sum of that CRS's CB round scores.

Q57: What is the API to the CGC environment?

A57: The following C language function prototypes are provided:

```
void _terminate(unsigned int status);
int allocate(size_t length, int prot, void **addr);
int deallocate(void *addr, size_t length);
int fdwait(int nfds, fd_set *readfds, fd_set *writefds,
           struct timeval *timeout, int *readyfds);
int random(void *buf, size_t count, size_t *rnd_bytes);
int receive(int fd, void *buf, size_t count, size_t
           *rx_bytes);
int transmit(int fd, const void *buf, size_t count, size_t
           *tx_bytes);
```

These function prototypes are notional and may be improved due to feedback prior to CGC kickoff.

Q56: Can foreign nationals participate in this challenge?

A56: This question is addressed in the CGC Rules Section 2 and Section 6. Foreign nationals may participate in Cyber Grand Challenge within a team which conforms to the CGC Rules.

Q55: DARPA-BAA-14-05 mentions DARPA-BAA-14-03, which describes the architecture framework. Where is DARPA-BAA-14-03?

A55: DARPA anticipates DARPA-BAA-14-03 to be published in the near future.

Q54: Does DARPA have a complete government team or are there opportunities for CGC support in development, judging, operating, etc.?

A54: DARPA anticipates a second BAA with other opportunities within this challenge.

Q53: Can foreign teams apply for the funding also or can teams have foreign members?

A53: Review the eligibility section of DARPA-BAA-14-05 (3.1.4) and the Rules (2.1).

Q52: Is this 6.1 or 6.2 money?

A52: DARPA anticipates 6.2 funds for awards under DARPA-BAA-14-05 and DARPA-BAA-14-03.

Q51: Does fundamental versus non-fundamental affect desirability?

A51: See DARPA-BAA-14-05 section 2.2.

Q50: Are there any restrictions on foreign subcontractors? If so, what are the restrictions?

A50: See section 3.1.3 of DARPA-BAA-14-05.

Q49: Will the proposal evaluations favor small business, or is it a level playing field based on merit?

A49: See section 5 of DARPA-BAA-14-05. All proposals are evaluated on the same criteria.

Q48: Are the deliverables and payment percentages in DARPA-BAA-14-05 fixed, or can we propose alternatives?

A48: They are notional, not fixed. You can propose alternatives.

Q47: Can you clarify the length of the periods of performance for the base and option periods?

A47: Under DARPA-BAA-14-05, each period of performance is 12 months. The schedule in DARPA-BAA-14-05 is notional. Plan for all activities to take place within two 12 month phases.

Q46: Is it possible to combine with another group after the CQE?

A46: Yes.

Q45: Can an organization have two teams, one for Open track and one for Proposal track?

A45: This is excluded in the Rules. Teams are intended to be wholly separate.

Q44: If I submit a proposal to the Competition BAA (DARPA-BAA-14-05) and do not get selected, can I submit to the Architecture BAA (DARPA-BAA-14-03)?

A44: There's nothing to prevent you from submitting to both, but you cannot be selected for award under both. In the event that a proposer submits an otherwise selectable proposal to both DARPA-BAA-14-05 and DARPA-BAA-14-03, the decision as to which proposal to consider for award is at the discretion of the Government.

Q43: Must we deliver a working spreadsheet as part of the proposal for DARPA-BAA-14-05 or is that just DARPA's preference? You said it would be "helpful" versus "required?"

A43: Per section 4.2.1.2 of DARPA-BAA-14-05, the cost proposal should include a spreadsheet file (.xls or equivalent format) that provides formula traceability among all components of the cost proposal. The spreadsheet file must be included as a separate component of the full proposal package.

Q42: Can we talk to the Contracting Officer before a proposal is submitted?

A42: Reference Section 7 of DARPA-BAA-14-05, questions should be submitted to CGC-CompetitorBAA@darpa.mil.

Q41: Are there two BAA's anticipated for this program, the Architecture BAA (DARPA-BAA-14-03) and the Competition BAA (DARPA-BAA-14-05)?

A41: Yes.

Q40: What is the eligibility for using an OT for prototypes (845)?

A40: See DARPA's contract management website (http://www.darpa.mil/Opportunities/Contract_Management/Other_Transactions_and_Technology_Investment_Agreements.aspx) for information regarding OT for Prototype awards.

Q39: Is the electronic submittal system similar to T-FIMS?

A39: Yes.

Q38: Could the amounts of the project be larger if an entity supplied a cost share beyond the \$750k?

A38: Yes.

Q37: With regard to Section 4.2.1.2.3 of DARPA-BAA-14-05, where are government rates and Defense Contract Audit Agency (DCAA) rates defined?

A37: FAR Part 42 discusses procedures for establishing forward pricing rates. Information is also available on the Defense Contract Management Agency's (DCMA) Website <http://guidebook.dcma.mil/41/>. You do not have to have DCMA approved

rates to propose and receive an award under DARPA-BAA-14-05. Section 4.2.1.2.3 requires a proposer to justify its proposed direct labor rates and provides several examples of how that can be accomplished.

Q36: With regard to Section 4.2.1.1.1 of DARPA-BAA-14-05, where are the types of businesses described?

A36: Business sizes are defined by the Small Business Administration (<http://www.sba.gov/content/table-small-business-size-standards>). A definition of HBCU and Minority Institutions can be found in DFARS 252.226-7000 (<http://www.acq.osd.mil/dpap/dars/dfars/html/current/252226.htm#252.226-7000>).

Q35: Is there a limit to the number of teams awarded or total amount of grants?

A35: No grants will be awarded under DARPA-BAA-14-05, only Firm-Fixed-Price Procurement Contracts and Other Transactions. Under DARPA-BAA-14-05, DARPA anticipates multiple awards of \$750,000 per phase of a two-phase effort; however, per the BAA, the number/amount of awards will depend on the quality of the proposals received and the availability of funds.

Q34: Will accepted proposals become public?

A34. DARPA will not publish awarded proposals under DARPA-BAA-14-05. Per section 4.2.2 of the BAA, DARPA treats proposals as source selection information (see FAR 2.101 and 3.104) and protects them as such, using secure handling and destruction procedures.

Q33: During CFE, how will a CRS monitor and modify traffic to a networked host?

A33:

Monitor:

During CFE, each competitor CRS will receive a read-only stream of all Competitor CRS network traffic directed toward its network host over the CFE network.

Modify:

Competitor systems will be provided with access to a DARPA-managed network appliance within the competition framework which will allow for traffic modification between the CFE network and the network host defended by the CRS. The managed appliance will use filters provided by the CRS through the Competition Framework API. Filters need not modify traffic; depending on their formulation they may modify traffic, alert, or take no action. Like Challenge Binaries, filters provided by a CRS will be distributed to all competitor systems for purposes of

consensus evaluation (Shannon's Maxim). Alerts generated on the managed appliance by fielded filters will be communicated back to the CRS through the Competition Framework API. These CRS-provided filters will conform to a subset of the open source Snort rule syntax; this subset will be published by DARPA prior to kickoff of Cyber Grand Challenge.

Q32: How will CRS hardware interface with the CQE event?

A32: CQE is an Internet-accessible event that will not require a CRS to be physically present at an event location. Section 3.1 of the CGC Rules provides information on the CQE Corpus and workflow. Competitors should note the requirements of the post-CQE Site Visit from the CGC Rules, Section 3.1.3.2.

Q31: How will CRS hardware interface with the competition framework during CFE?

A31: A CRS used in CFE must fit entirely in a single, standard 19" 42U rack. CFE will take place at a physical location to be specified by DARPA. Competitor systems must be physically present at the CFE Compute Location in order to interface directly with the competition framework. Further details about available power, cooling, and infrastructure will be published as Cyber Grand Challenge progresses.

Q30: When will CQE and CFE scoring be finalized?

A30: DARPA is currently holding a period of public comment for the CFE and CQE scoring methods. Feedback should be addressed to cybergrandchallenge@darpa.mil. Scoring will be open for a period of public comment concluding on Friday, February 14, 2014. A final scoring algorithm for CQE and CFE will be released on Monday, March 10, 2014. Like the current proposed scoring algorithms, the final scoring methods will be consistent with the Cyber Grand Challenge Rules. See also Q/ A 26 and 27.

Q29: What constitutes a Proof of Vulnerability in CFE?

A29: Proof of Vulnerability (PoV) may be demonstrated during CFE by interacting with the Competition Framework via two different methods.

Method 1: Registers

To prove that a remote CB is vulnerable, a Method 1 PoV shall redirect execution to an instruction pointer value negotiated with the Competition Framework API. Execution must fault at this value. At time of fault, one general purpose register must also be set to a second value negotiated with the Competition Framework API. This redirection will create an effect detectable by instrumentation operated on the competition framework.

Method 2: Memory

To prove that a remote CB is vulnerable, a Method 2 PoV will retrieve a value present in the memory of a competitor CB. This value must be retrieved from a memory range specified by the Competition Framework API, must be of a size specified by the Competition Framework API, and must be submitted through the Competition Framework API. This submittal will create an effect detectable by instrumentation operated on the competition framework.

Q28: What constitutes a Proof of Vulnerability in CQE?

A28: A CQE Proof of Vulnerability will cause a CB to crash in a manner consistent with memory corruption flaws with security impact, e.g., a segmentation fault or illegal instruction fault.

Q27: What is the scoring method for CQE?

A27: ~~The below scoring method candidate will be open for public comment until Friday, February 14, 2014.~~

~~CQE scoring is the product of three assessed quantities: Availability score, Security Score, and Evaluation score. These scores map to the Areas of Excellence (AoE) located in the Cyber Grand Challenge Rules as follows:~~

~~Availability: Area of Excellence 4~~

~~Security: Area of Excellence 2~~

~~Evaluation: Area of Excellence 3~~

~~During CQE, the CBs distributed by DARPA shall be referred to as “reference CBs”, not to be confused with replacement CBs submitted by competitors. PoVs used by DARPA for scoring will be referred to as “reference PoVs”. PoVs submitted by competitor systems to DARPA during CQE will be referred to as “submitted PoVs”.~~

~~CQE Scores will be assessed per Challenge Binary (“CB score”). Each CB score will be calculated as follows:~~

$$\text{Availability} * \text{Security} * \text{Evaluation}$$

~~Availability:~~

~~This quantity shall vary as a multi-step function between 0 and 1, with 1 being a perfect score. Performance and retained functionality will be measured, with Availability being set to the minimum of these quantities. Competitors are advised that slowing down the function of a replacement CB will result in a faster-than-linear Availability score dropoff.~~

Security:

~~This quantity will be calculated as follows: $1 + (\text{Reference} + \text{Consensus}) / 2$~~

~~—Reference: The number of reference PoVs which do not prove vulnerability in the replacement CB, divided by the number of reference PoVs~~

~~—Consensus:~~

~~This quantity will be set to 0 or 1:~~

~~○ 0: Any submitted PoV proved vulnerability in the replacement CB~~

~~○ 1: No submitted PoV proved vulnerability in the replacement CB~~

Evaluation:

~~This quantity will be set to 1 or 2:~~

~~—1: A PoV emitted by this CRS did not prove vulnerability in the reference CB~~

~~—2: A PoV emitted by this CRS did prove vulnerability in the reference CB~~

~~A CRS's total score at the end of CQE shall be the sum of that CRS's CB scores.~~

Q26: What is the scoring method for CFE?

~~This scoring method candidate will be open for public comment until Friday, February 14, 2014.~~

~~A26: CFE scoring is the product of three assessed quantities: Availability score, Security Score, and Evaluation score. These scores map to the Areas of Excellence (AoE) located in the Cyber Grand Challenge Rules as follows:~~

~~Availability: Area of Excellence 4~~

~~Security: AoE 2,5~~

~~Evaluation: Area of Excellence 3~~

~~CFE scoring will take place over many rounds. Scores will be assessed per Challenge Binary per round ("CB round score"); it follows that the sum of the CB round scores for a single CRS will be the total score for that system. Each CB round score will be calculated as follows:~~

$$\text{Availability} * \text{Security} * \text{Evaluation}$$

Availability:

~~This quantity shall vary as a multi-step function between 0 and 1, with 1 being a perfect score. Performance and retained functionality will be measured, with Availability being set to the minimum of these quantities. Competitors are advised that slowing down the function of a replacement CB will result in a faster than-linear Availability score dropoff.~~

Security:

~~This quantity will be set to 1 or 2:~~

- ~~— 1: At least one PoV from a competitor proved vulnerability in this CB during this round~~
- ~~— 2: No PoVs from competitors proved vulnerability in this CB during this round~~

~~Evaluation:~~

~~This quantity will vary between 1 and 2:~~

- ~~— 1: No PoVs emitted by this CRS proved vulnerabilities in this CB service on competitor systems~~
- ~~— $1 + (x / (N - 1))$ PoVs emitted by this CRS for this CB service proved vulnerability in x competitor systems, where N is the number of CRSs participating in CFE.~~

~~A CRS's total score at the end of CFE shall be the sum of that CRS's CB round scores.~~

Q25: What will be publicly released Post-CQE?

A25: DARPA intends to release the following items post-CQE:

- Reference CBs (initial Corpus distributed for CQE)
- PoVs, including both reference PoVs and PoVs gathered during the CQE
- Replacement CBs from the CQE, including reference patched CBs
- PCAP of traffic used during CQE evaluation
- Reference service pollers for each CB
- Reference CB source code
- A detailed list of scores for each CB for each finalist
- Team rankings (including Open Track and Proposal Track)

DARPA may modify this list of intended deliverables at its sole discretion.

Q24: What information about challenge binaries will be provided ahead of time (e.g., sample input and response; interaction protocol, API for service, etc.)?

A24: DARPA will provide an interface document detailing the methods CBs will use to interface with their execution environment.

Q23: What will we know about challenge network configuration (e.g., address ranges) before the final event?

A23: The CFE network topology will be known prior to CFE. In addition, competitors will have the opportunity to test technology interoperability during CFE Trials.

Q22: Will the execution environment be provided to the teams?

A22: A sample environment will be provided prior to the program commencing (proposal track awards have been finalized and open track teams have been registered/ accepted) in the form of a virtual machine.

Q21: Will sample inputs be provided with some of the challenge binaries in the CQE corpus?

A21: Yes.

Q20: Can secure replacement CBs be submitted by a CRS throughout CFE?

A20: Yes.

Q19: What is the impact of submitting a replacement CB?

A19: The submission of secure replacements may be rate limited by the Competition Framework API, and fielding a replacement CB may impact service availability.

Q18: Are there networking constraints on patching? Reaching out to remote servers? May CBs communicate with the CRS while executing on the network host?

A18: During CFE, Challenge Binaries will not have the ability to initiate connections.

Q17: During CFE, for network defense, will existing tools for scanning and defending (TCP/ UDP/ NMAP, wireshark, snort, etc.) work, or must we develop new tools? Do you expect the teams to develop program analysis tools themselves or use off-the-shelf ones?

A17: DARPA will not dictate what automated approaches are acceptable within a CRS.

Q16: During CFE, what information (data sources) will our CRS have access to? Specifically will our CRS have access to crash logs, core dumps, and full network traffic feed?

A16: During CFE, a CRS will have access to a read only network tap. During CFE, a CRS will have the ability to request some CB status information through the Competition Framework API. Data sources automatically generated by a CRS internally will not be dictated by DARPA.

Q15: During CFE, how many networked hosts will competitors be responsible for monitoring/protecting?

A15: One.

Q14: During CFE, will competitors have access to the network host?

A14: A CRS will have the ability to query the Competition Framework API for some CB status information. A CRS will have the ability to field replacement CBs through the Competition Framework API.

Q13: During CFE, will you be issuing new binaries to teams after competition start, or will you give all binaries to teams before start?

A13: During CFE, a CRS will be notified that a CB is available through the Competition Framework API.

Q12: What programming languages will CBs be written in?

A12: The C family of languages.

Q11: Does the U.S. Government assert any intellectual property rights to CRS source code developed by open track competitors?

A11: No.

Q10: What type of security vulnerabilities will CGC address?

A10: CGC Challenge Binaries shall contain traditional memory corruption flaws. A subset of relevant flaw types drawn from the MITRE Common Weakness Enumeration entries as found on <http://cwe.mitre.org/> follows; teams are encouraged to make use of this list as a starting point, not a reference.

CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

CWE-121: Stack-based Buffer Overflow

CWE-122: Heap-based Buffer Overflow

CWE-123: Write-what-where Condition

CWE-124: Buffer Underwrite ('Buffer Underflow')

CWE-128: Wrap-around Error

CWE-129: Improper Validation of Array Index

CWE-130: Improper Handling of Length Parameter Inconsistency

CWE-131: Incorrect Calculation of Buffer Size

CWE-134: Uncontrolled Format String

CWE-135: Incorrect Calculation of Multi-Byte String Length

CWE-147: Improper Neutralization of Input Terminators

CWE-158: Improper Neutralization of Null Byte or NUL Character

CWE-170: Improper Null Termination
CWE-190: Integer Overflow or Wraparound
CWE-191: Integer Underflow (Wrap or Wraparound)
CWE-193: Off-by-one Error
CWE-194: Unexpected Sign Extension
CWE-195: Signed to Unsigned Conversion Error
CWE-196: Unsigned to Signed Conversion Error
CWE-401: Improper Release of Memory Before Removing Last Reference
CWE-409: Improper Handling of Highly Compressed Data (Data Amplification)
CWE-415: Double Free
CWE-416: Use After Free
CWE-457: Use of Uninitialized Variable
CWE-466: Return of pointer value outside of expected range
CWE-467: Use of sizeof() on a Pointer Type
CWE-468: Incorrect Pointer Scaling
CWE-469: Use of Pointer Subtraction to Determine Size
CWE-763: Release of Invalid Pointer or Reference
CWE-786: Access of Memory Location Before Start of Buffer
CWE-787: Out-of-bounds Write
CWE-788: Access of Memory Location After End of Buffer
CWE-805: Buffer Access with Incorrect Length Value
CWE-806: Buffer Access Using Size of Source Buffer
CWE-822: Untrusted Pointer Dereference
CWE-823: Use of Out-of-range Pointer Offset
CWE-824: Access of Uninitialized Pointer
CWE-825: Expired Pointer Dereference

Q9: What constitutes a software flaw in Cyber Grand Challenge?

A9: DARPA CGC will not provide a formal definition of a software flaw; this question lies outside the scope of the challenge. The CGC will operate in the tradition of existing cyber competitions: a flaw is proven when an input delivered from the network to a flawed software program (CB) creates an effect detectable by instrumentation operated by the competition framework. CGC Challenge Binaries will contain memory corruption flaws representative of flaws categorized by the MITRE CWE¹, however, Competitor Systems may prove any software flaw they discover through automated reasoning. A list of representative CWE categories will be released prior to the kickoff of Cyber Grand Challenge.

Q8: What platform will CGC run on?

A8: CGC Challenge Binaries (CBs) will be incompatible with any known OS architecture. CBs will run in an environment custom built for the competition. Knowledge of the operating system will not be in scope for the competition; rather,

¹ <http://cwe.mitre.org/>

CGC requires a competition system to reason about the function of compiled binaries receiving inputs from the network. CBs will not conform to any currently known application layer protocols. CB protocol knowledge must be generated automatically by competition systems during CGC events through a process of automated reasoning about software. These constraints will ensure that all knowledge in use by competition systems during CGC events is generated via automatic processes.

Q7: What CPU architecture will CGC run on?

A7: For the purpose of maximizing accessibility and participation: Intel x86, 32-bit.

Q6: What compiler will be used to build the binaries?

A6: CGC will distribute a reference compiler toolchain prior to challenge kickoff. However, challenge binaries may be produced by any compiler including the reference compiler.

Q5: During the final event, what happens when my Competition System fields a new Challenge Binary?

A5: During CFE, in order to enact defenses, a CRS may choose to replace a CB with a newly secured version. To field a replacement CB, a CRS must submit the replacement through an automated API operated by the competition framework. The competition framework will deploy the replacement binary on behalf of the CRS to its networked host. Additionally, the competition framework will make a copy of the replacement CB available to all competitor systems for the purposes of consensus evaluation (Shannon's Maxim). Once deployed, replacement CBs will be required to function as self-contained replacements without custom dependencies, libraries, etc.

Q4: I'm interested in advanced application defenses. Will these be part of CGC?

A4: During CFE, systems will have the ability to deploy network defenses as well as application defenses. To deploy application defenses, competition systems may analyze CBs and field secure replacements. Due to the competitive nature of CGC, DARPA expects that competitors will field many approaches of varying type, advancement, and efficacy.

Q3: What limitations are imposed on replacement CBs during CFE?

A3: During CFE, the competition framework will monitor the availability and correct function of each CB. If a CRS deploys replacement CBs that degrade CB function by impacting performance, correctness of CB responses, or the ability to

service network requests, a negative impact on scoring is expected. Similar constraints will be imposed on replacement CBs during CQE scoring.

Q2: In the CGC Rules, Area of Excellence 2 specifies Autonomous Patching. Does this mean a Cyber Reasoning System (CRS) is required to isolate and remove flaws, or may a CRS field any secure replacement Challenge Binary (CB)?

A2: During the CGC Qualification Event (CQE) and Final Event (CFE), CBs will be evaluated based on availability, correct function, and the mitigation of flaws, as described in the CGC Rules and this FAQ. No specific requirements are imposed on the formulation method for secure replacement CBs.

Q1: Are you planning an Industry Day for competitors?

A1: Two Competitor Day sessions are planned, one on the East Coast, and one on the West Coast.

- The East Coast Competitor Days are currently scheduled for December 3 and 4, 2013 at the DARPA Conference Center, 675 North Randolph Street, Arlington, VA 22203. Note: the second day will be a repeat of the first day to accommodate registered attendees. Availability is on a first-come-first-served basis. All registrations will be for the December 3 session until capacity is reached; at that point, registrations will be for the December 4 session. Please visit <http://www.sa-meetings.com/darpagcccompetitorday> for more information and to register.

- The West Coast Competitor Day is currently scheduled for December 9, 2013 at the Westin St. Francis, 335 Powell St, San Francisco, CA. Availability is on a first-come-first-served basis. Please visit <http://www.sa-meetings.com/darpagcccompetitordaywest> for more information and to register.

Could a purpose built supercomputer play DEF CON Capture the Flag?

Mike Walker
Program Manager

November 14, 2013



Approved for Public Release, Distribution Unlimited

Turing, Rice, & Undecidable Problems:

- Is the software correct & secure?
- If not, how incorrect or insecure is it?

Q: Can we *compete* when the answers required to name a victor are undecidable?



Competitive Programming: TopCoder

1: Construct

2: Challenge

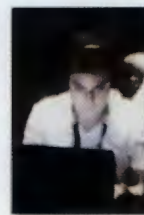
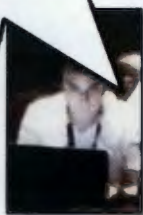
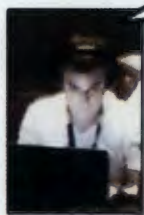
```
bool find( const int x, const int* pBegin, const int* pEnd)
{
    int model = (*pBegin + (*pEnd - 1) - *pBegin) / 2 ;
    if(x == model) return true ;
    else if( x > model)
    { int begin = (model + 1);
      return find( x, &begin, pEnd); }
    else if( x < model)
    { int last = (model - 1);
      return find(x, pBegin, &last); } }
```

```
public static int binarySearch(int[] a, int key) {
    int low = 0;
    int high = a.length - 1;
    while (low <= high) {
        int mid = (low + high) / 2;
        int midVal = a[mid];
        if (midVal < key)
            low = mid + 1;
        else if (midVal > key)
            high = mid - 1;
        else return mid; // key found
    }
    return -(low + 1); // key not found
}
```

```
binary_search(lo, hi, p):
while we choose not to terminate:
    mid = lo + (hi-lo)/2
    if p(mid) == true:
        hi = mid
    else:
        lo = mid
return lo
```

231

int mid = (low + high) / 2;
ArrayIndexOutOfBoundsException *



http://technorazzi.com/wp-content/uploads/2010/08/ctf_denmark2.jpg

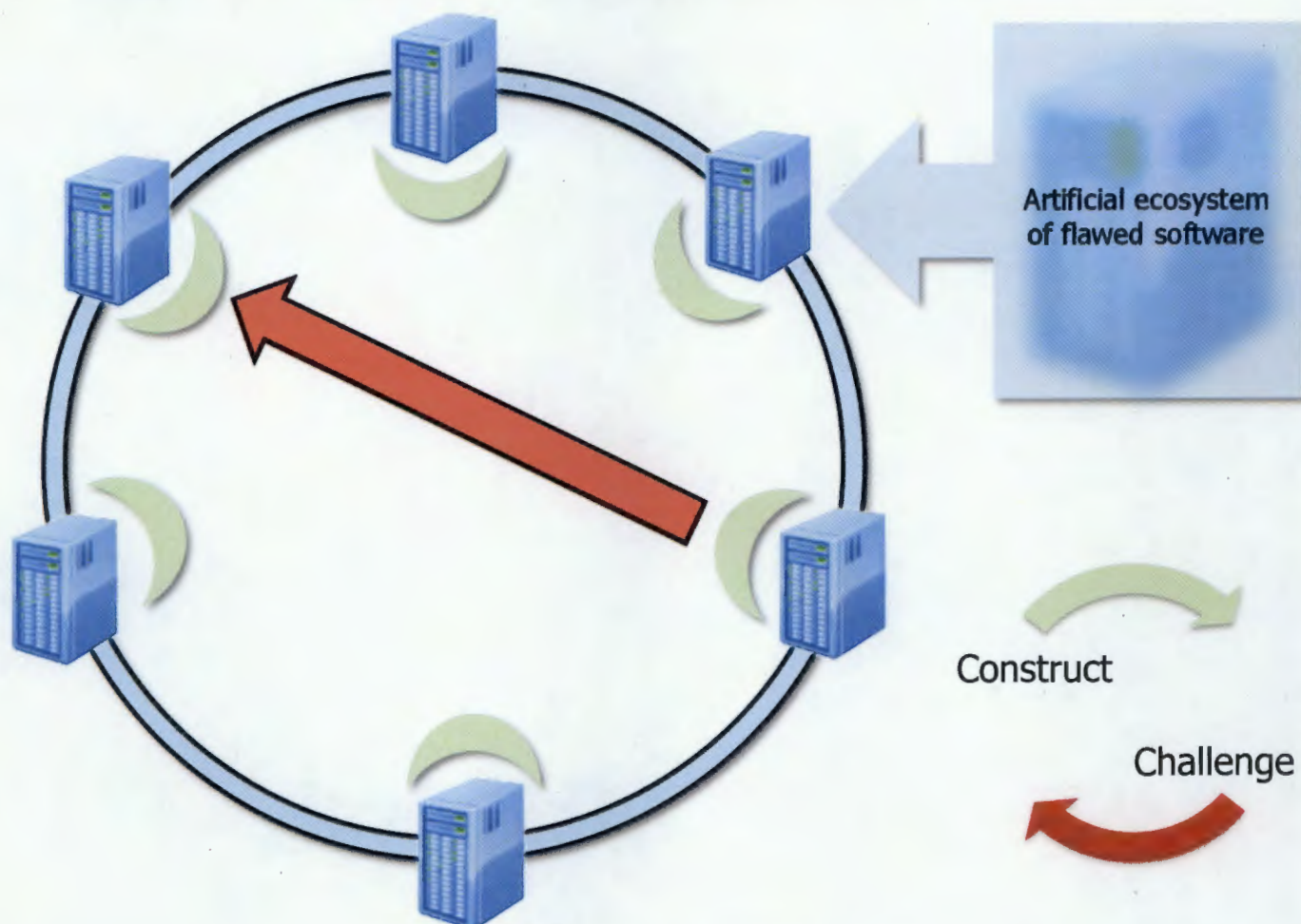
*<http://googleresearch.blogspot.com/2006/06/extra-extra-read-all-about-it-nearly.html>

Approved for Public Release, Distribution Unlimited



Q: Can we *compete* when the answers required to name a victor are undecidable?

A: *consensus evaluation*





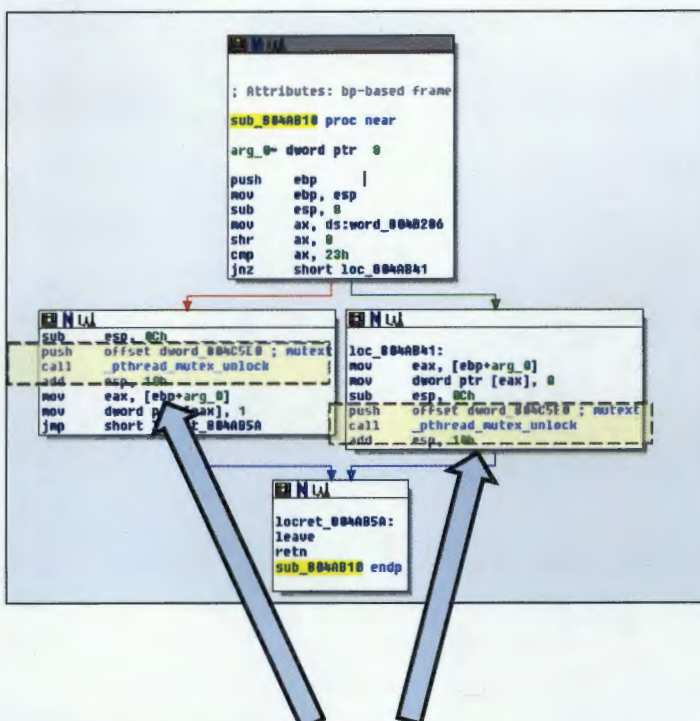
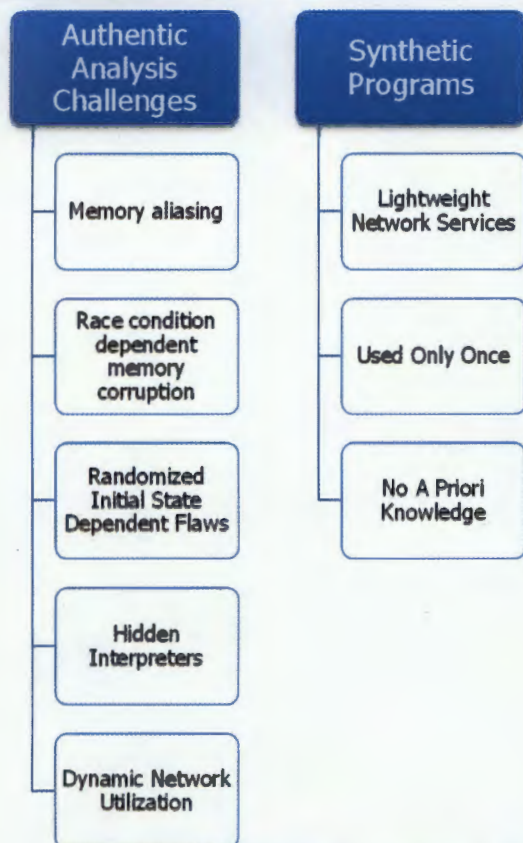
Harness consensus evaluation to identify
breakthrough technology.



CYBER
GRAND_CHALLENGE

A tournament for fully automated network defense

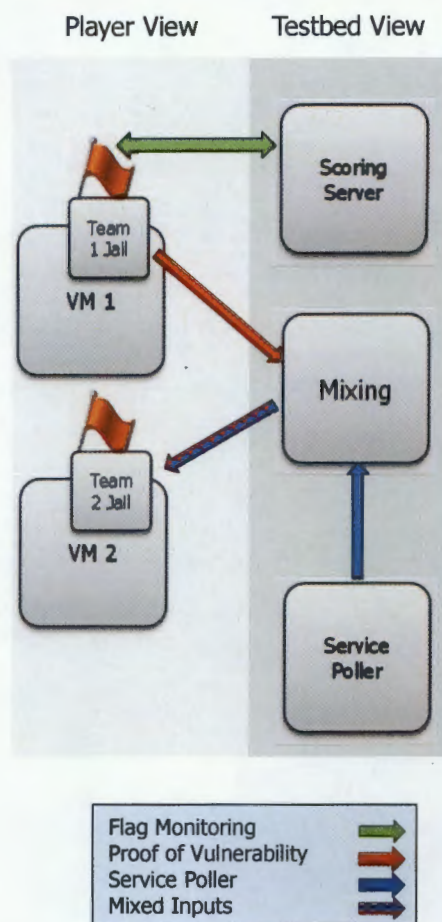
An alternative software ecosystem whose challenges and constraints mirror those imposed on real world network defenders.

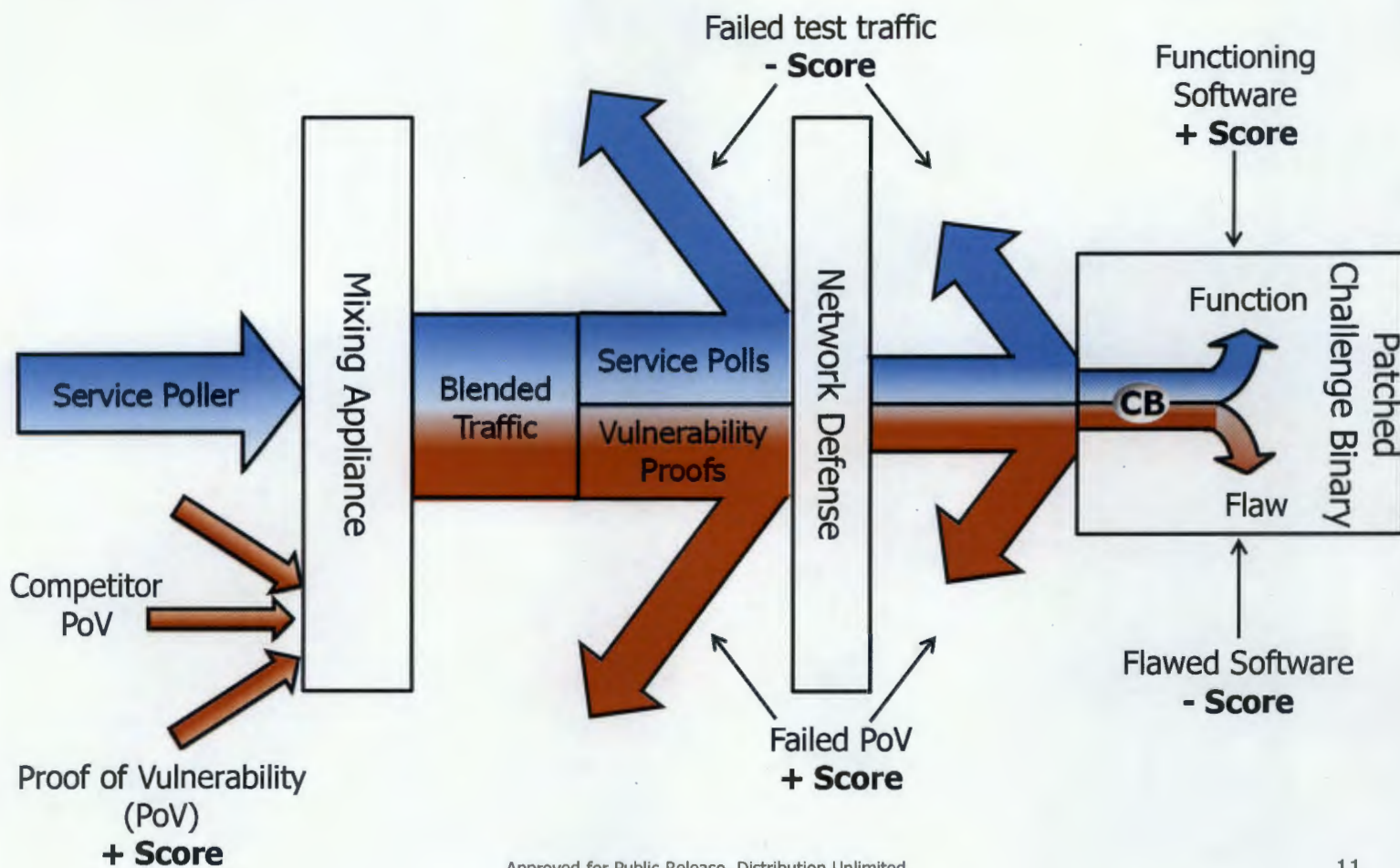


Defcon CTF Qualifiers 2007
 Highest difficulty (500), network application flaw category
 Hidden mutex unlock condition triggers timing specific memory corruption*

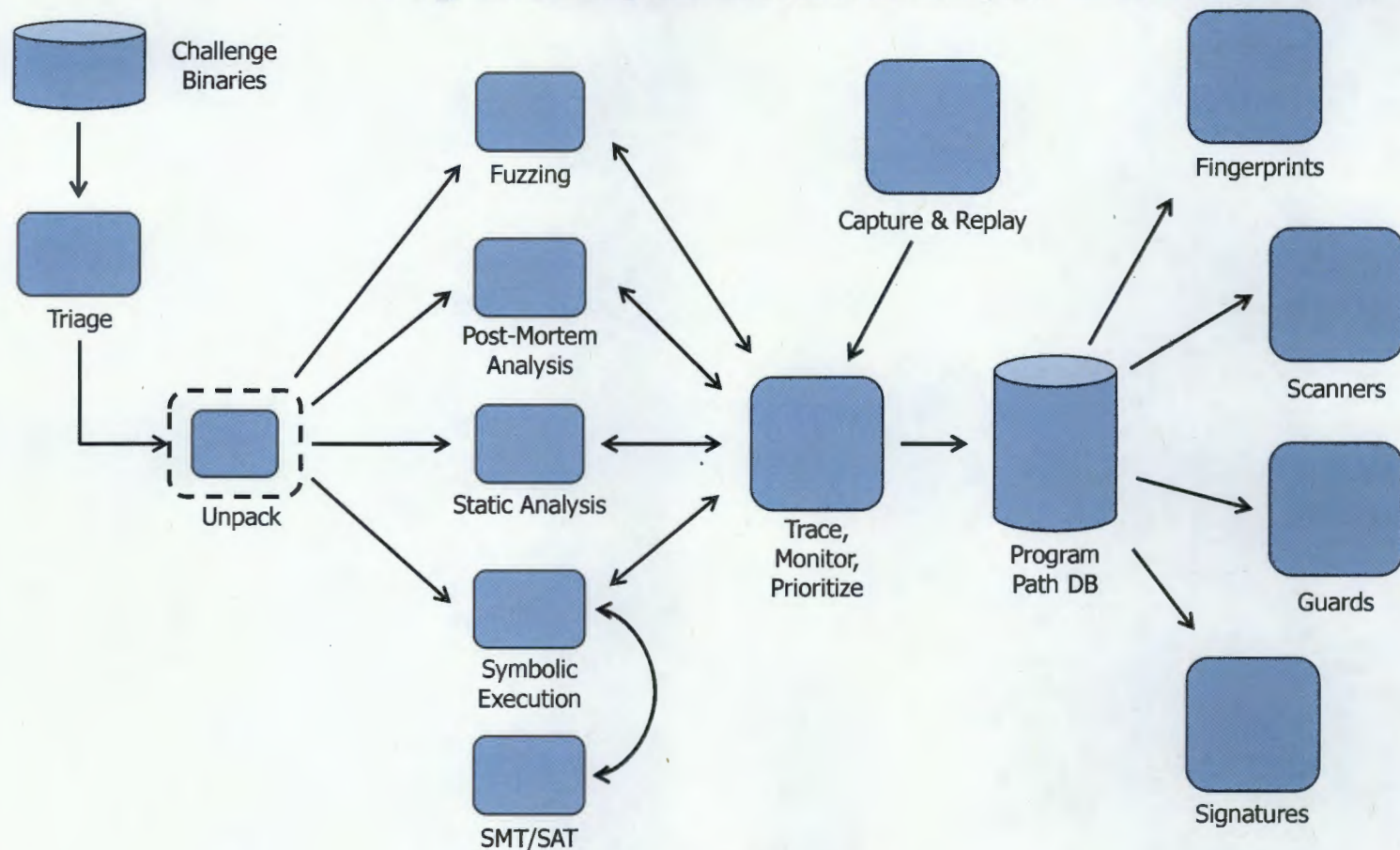
Authentic Skills, Synthetic Software

Challenges	CTF
Attribution & Reputation	Network Mixing
Resilience	New Flags Random Intervals
Availability	Service Poller

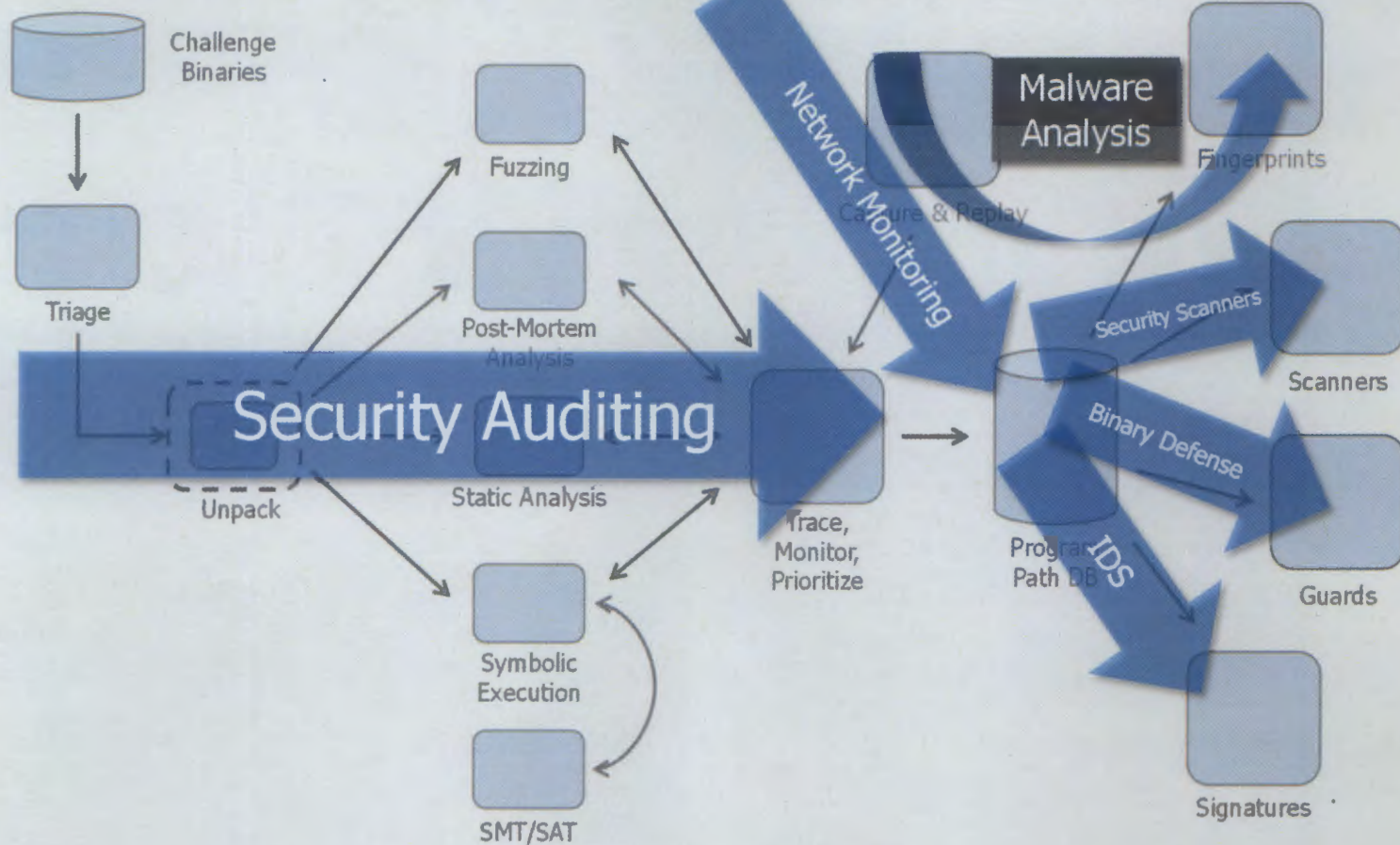




Program Analysis Network Analysis Defense Generation



Program Analysis Network Analysis Defense Generation



Program Analysis Network Analysis Defense Generation

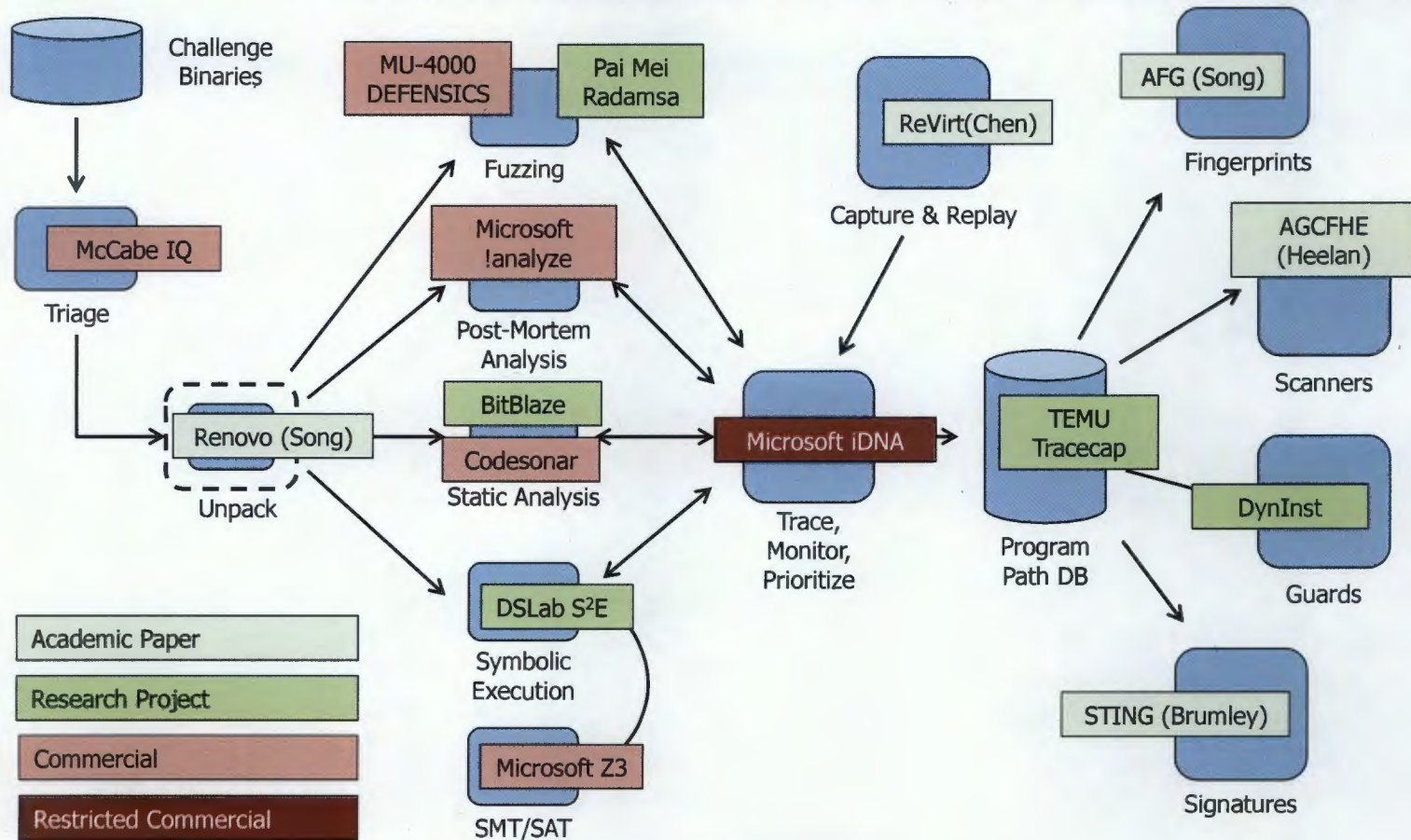
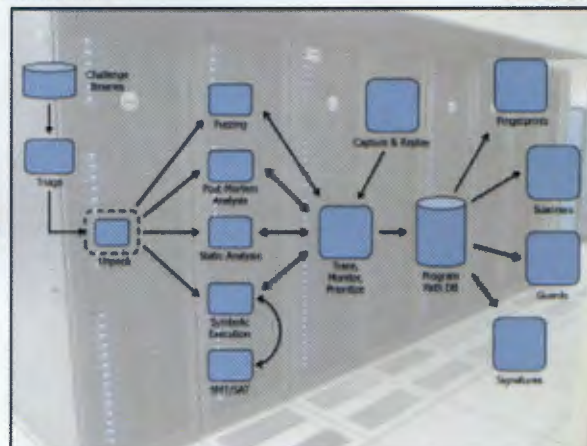




Photo courtesy US Air Force Academy Cyber Competition Club



- Using the competition format which measures analyst cyber reasoning ability...
- A Grand Challenge for *automated defenders*:
- Systems that can detect and repel novel threats from networks



We've Been Here Before



Chess Grandmasters

Dedicated Systems

World Class CS



© IBM Research

Deep Blue



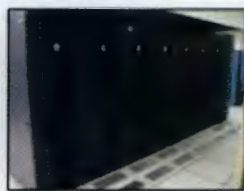
<http://olog.pontiflex.com/2010/05/13/ibm-enters-social-media/>

Can We Do It Again?

Cyber Grandmasters

Dedicated Systems

Program Analysis



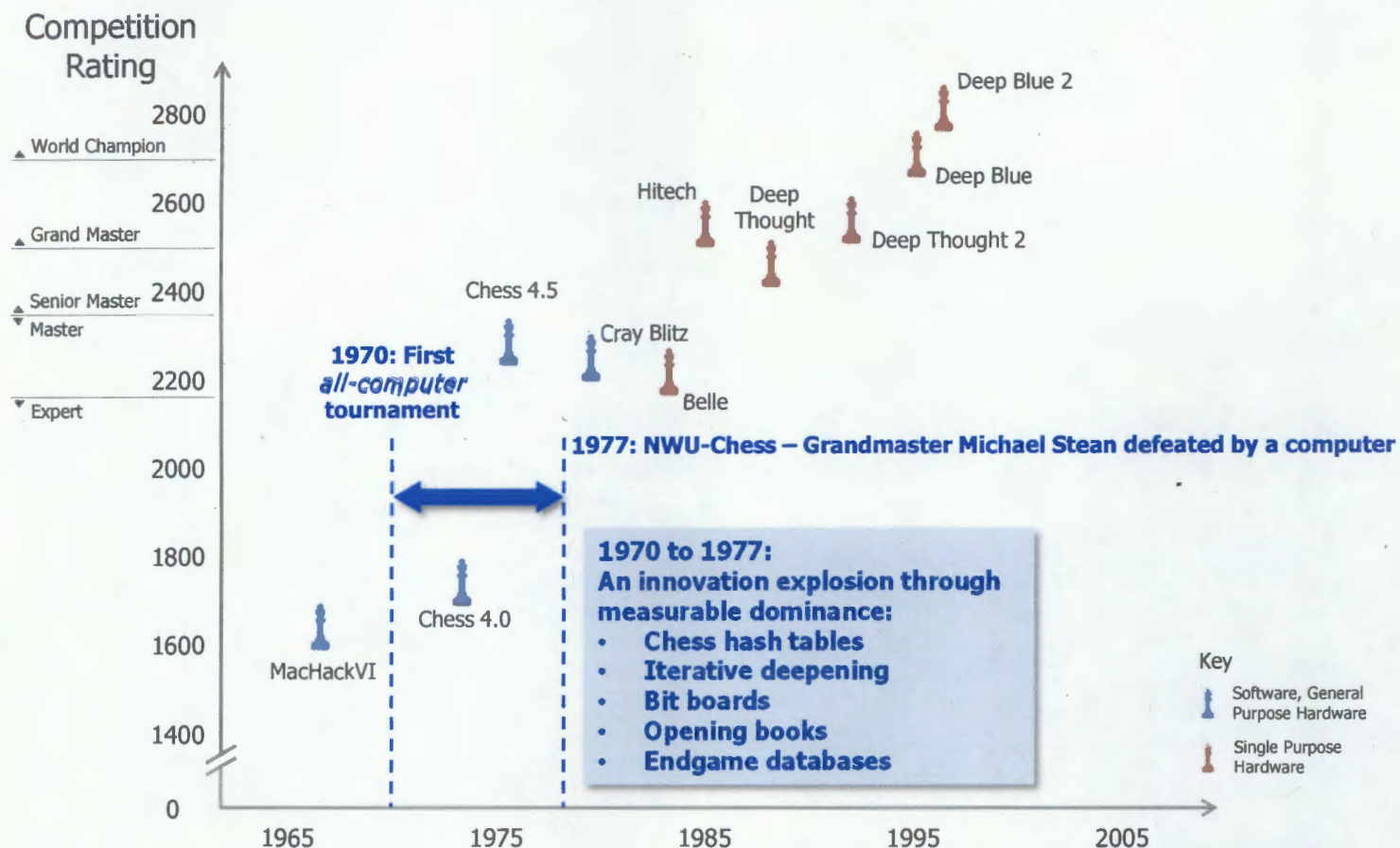
dailynotlines.uark.edu

Deep CTF?



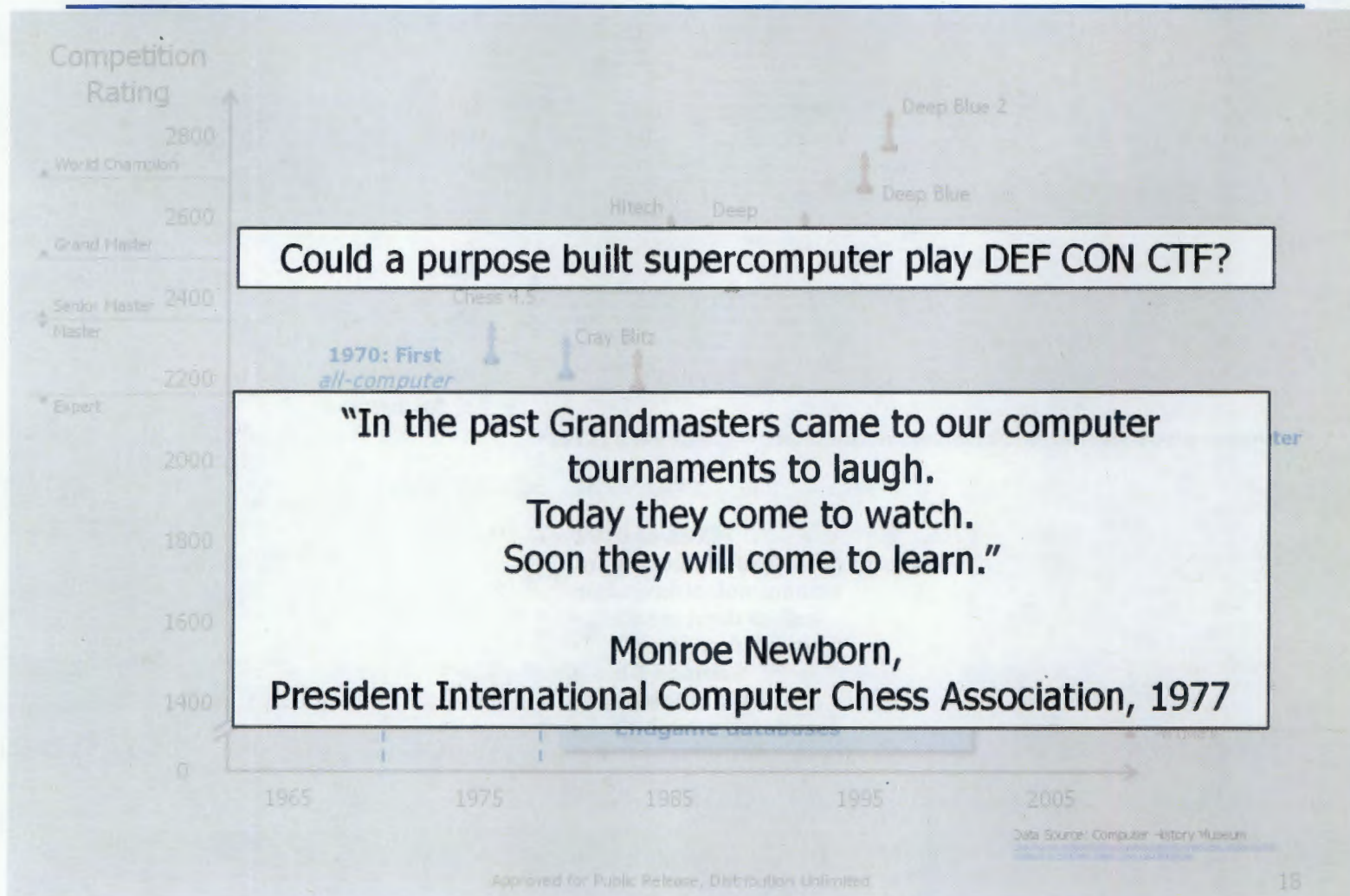
Photo courtesy US Air Force Academy Cyber Competition Club

Approved for Public Release, Distribution Unlimited



Data Source: Computer History Museum
http://archive.computerhistory.org/resources/details/frames/Chess_Inventory/001/00000514/1%20Chess_Inventory_Chess_Inventory/001/00000514.htm

Approved for Public Release, Distribution Unlimited



A new DARPA Challenge...



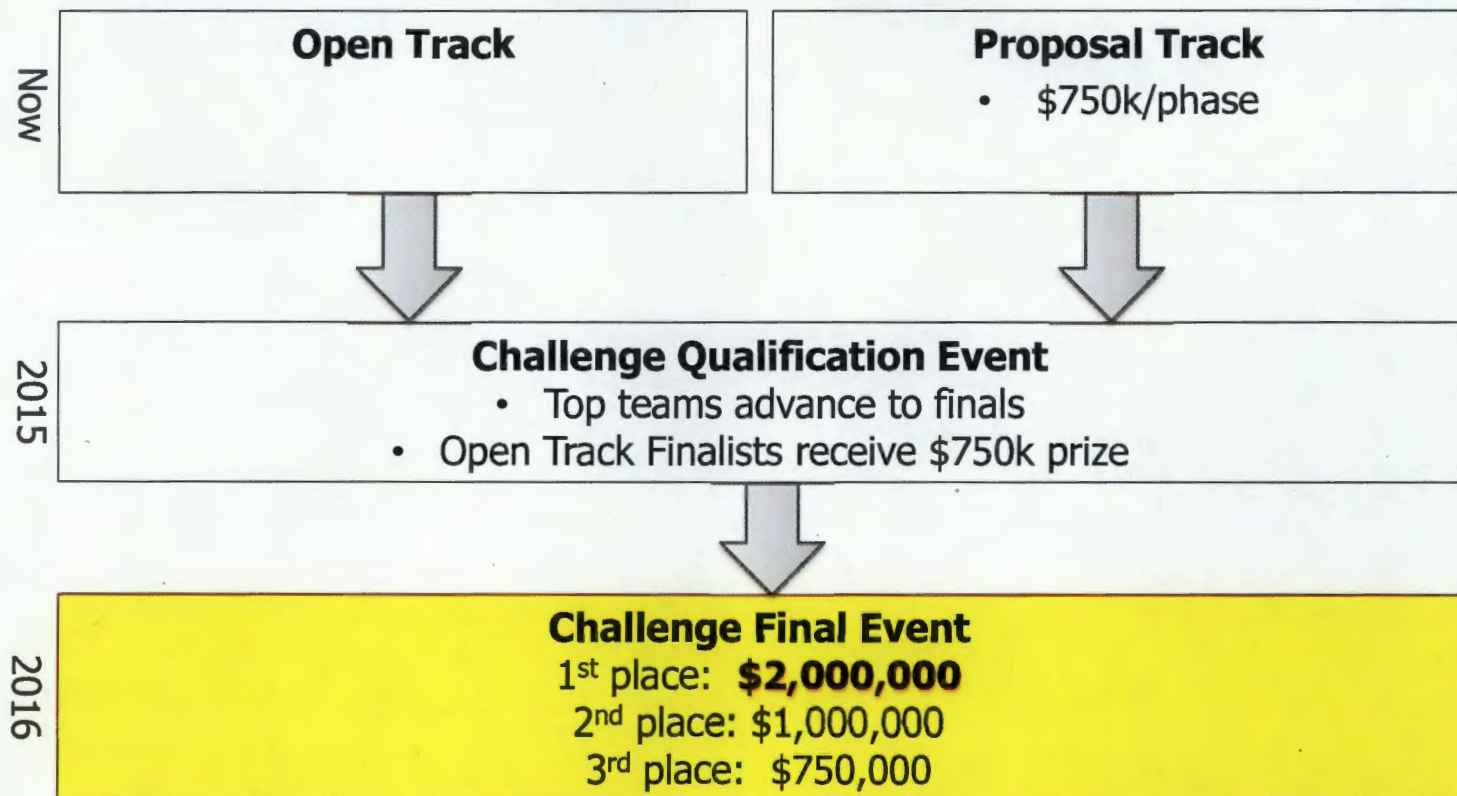
Open Track

- Open to any eligible team
- No IP restrictions on entrant system

Proposal Track

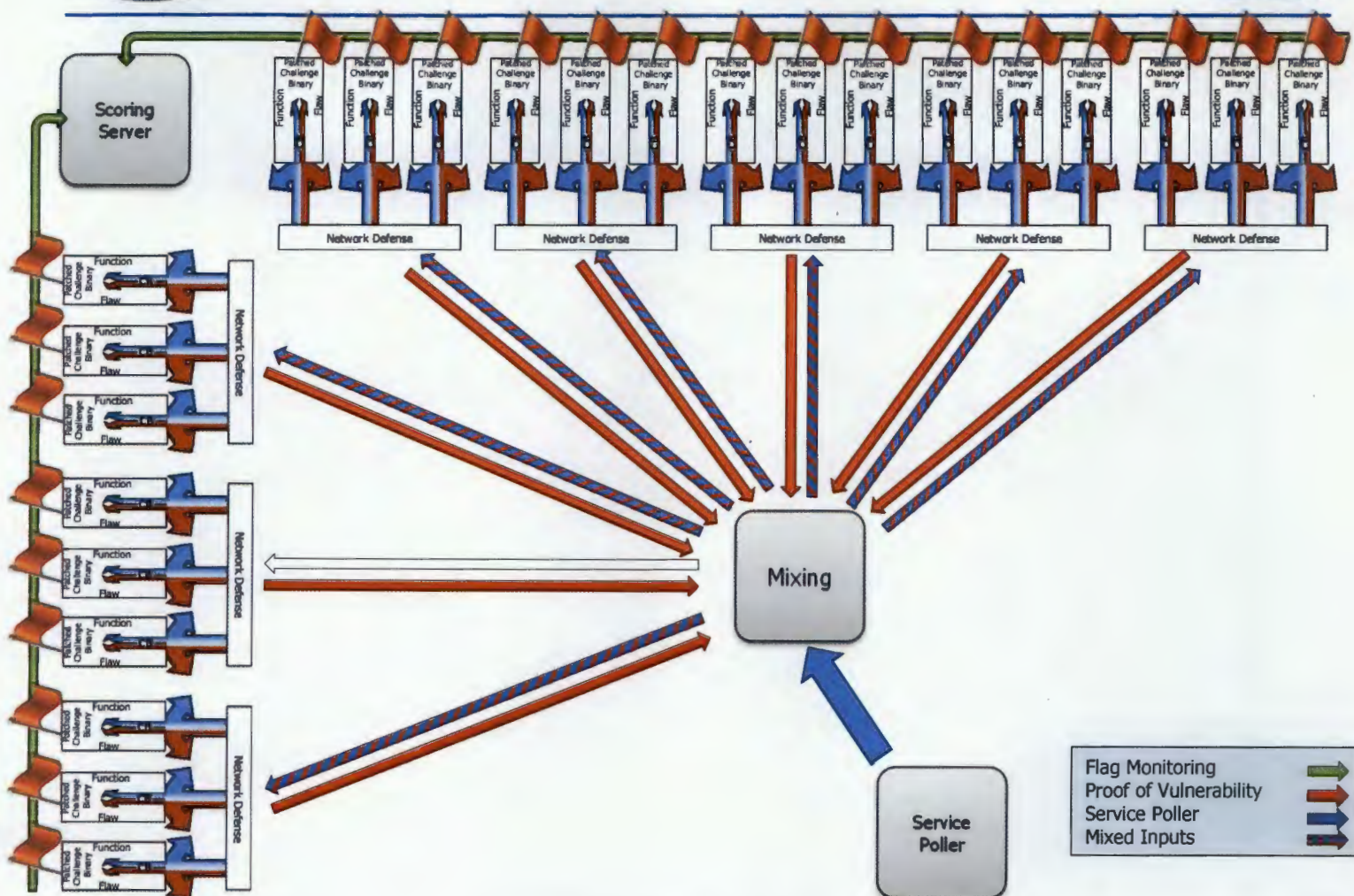
- DARPA Scientific Review Board
- Funded \$750k/phase
- Government Purpose Rights to funded development

See rules at www.darpa.mil/cybergrandchallenge for full details





Scheduled Final Event: Multi-Team Real Time Tournament



Approved for Public Release, Distribution Unlimited



For more information:

www.darpa.mil/cybergrandchallenge

Questions?