Special Notice

Cyber Grand Challenge (CGC) Architecture Proposers' Day

DARPA-SN-14-20

February 2014

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

DARPA-SN-14-20
Cyber Grand Challenge (CGC) Architecture
Proposers' Day – February 18, 2014

The Defense Advanced Research Projects Agency (DARPA) Information Innovation Office (I2O) will host the Cyber Grand Challenge (CGC), an unmanned cyber defense tournament.[1] In support of the CGC Architecture, DARPA anticipates publishing a Broad Agency Announcement (BAA) soliciting innovative proposals for efforts which will enable DARPA to test and evaluate fully automated systems that perform software security reasoning and analysis. When released, the BAA will be posted on the Federal Business Opportunities (FBO) website, http://www.fedbizopps.gov. On behalf of parties interested in the anticipated BAA for the Cyber Grand Challenge Architecture, DARPA/I2O will conduct a briefing on February 18, 2014. This Proposers' Day is unclassified.

Attendance at the CGC Architecture Proposers' Day is voluntary and is not required to propose to subsequent solicitations (if any) on this topic. The Proposers' Day does not constitute a formal solicitation for proposals or abstracts. This announcement is issued solely for information and program planning purposes and is not a Request for Information (RFI). Since this is not an RFI, no submissions against this notice will be accepted by the Government. DARPA will not provide reimbursement for costs incurred to participate in this Proposers' Day. Interested parties to this notice are cautioned that nothing herein obligates the Government to issue a solicitation.

PROGRAM OVERVIEW

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 DARPA Cyber Grand Challenge 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.

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.

[1] See the CGC Rules document at www.darpa.mil/cybergrandchallenge for a detailed description of the CGC.

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.

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 the CGC program is to identify effective, integrated automation of cyber reasoning tasks. This objective will be accomplished through competitions held on a closed, monitored network ("Competition Framework") which is currently being constructed by a Competition Framework Team. To support the framework and the competition events, DARPA anticipates the CGC Architecture BAA will include two technical areas. The first will focus on developing network services that accept remote network connections, perform processing on network-supplied data, and interact with remote hosts over network connections; the second will focus on developing novel techniques to develop integrity mechanisms to protect against human interference and other potential obstacles to fully automated competition.

PURPOSE

The purpose of the CGC Architecture Proposers' Day is threefold:

1. To familiarize participants with the Cyber Grand Challenge and its structure.

2. To identify potential proposers and promote understanding of the anticipated CGC Architecture BAA proposal requirements.
3. To promote discussion of synergistic capabilities among potential program participants.

Additional information regarding the CGC is available at http://www.darpa.mil/cybergrandchallenge/. It is anticipated that the CGC Architecture BAA will be published at http://www.fbo.gov by mid-late February 2014.

TENTATIVE AGENDA

Registration: 8:00-9:00
Presentations/Discussions: 9:00-12:00

REGISTRATION INFORMATION

The Proposers' Day will be held on February 18, 2014, at the DARPA Conference Center, 675 N. Randolph Street, Arlington, VA, from approximately 8:00 a.m. to 12:00 noon (Eastern). Availability is on a first-come-first-served basis.

Registration for the Proposers' Day must be completed online at www.sa-meetings.com/CGCArchitectureProposersDay no later than 12:00 noon (Eastern) on February 14, 2014.

Non-US citizens must submit a DARPA Form 60 "Foreign National Visit Request" no later than 12:00 noon (Eastern) on February 12, 2014. DARPA Form 60s may be obtained at the registration site and should be faxed to 703-797-4505 or emailed to CGC-ArchitectureBAA@darpa.mil.

Registration confirmations will be emailed to the address provided. All attendees will be required to present Government-issued photo identification upon entry to the event.

POINT OF CONTACT

All questions regarding the Proposers' Day should be sent to CGC-ArchitectureBAA@darpa.mil.