Top Teams' Automated Cybersecurity Systems Preparing for Final Face-off

DARPA's Cyber Grand Challenge Final Event Aims to Usher In New Era of Scalable, Machine-speed Software Search and Repair

OUTREACH@DARPA.MIL
7/13/2016

The Heartbleed security bug existed in many of the world's computer systems for nearly two-and-a-half years before it was discovered and a fix circulated in the spring of 2014, by which time it had rendered an estimated half a million of the internet's secure servers vulnerable to theft and other mischief. And while Heartbleed was in some respects an outlier, long-lived critical flaws in widely deployed bedrock internet infrastructure are not rare. Analysts have estimated that, on average, such flaws go unremediated for 10 months before being discovered and patched, giving nefarious actors ample opportunity to wreak havoc in affected systems before they move on to exploit new terrain.

The reason for these time lags? In contrast to the sophistication and automation that characterize so much of today's computer systems, the process of finding and countering bugs, hacks and other cyber infection vectors is still effectively artisanal. Professional bughunters, security coders, and other security pros work tremendous hours, searching millions of lines of code to find and fix vulnerabilities that could be taken advantage of by users with ulterior motives.

But what if that system of finding and fixing flaws were just as fast and automated as the computer systems they are trying to protect? What if cyber defense were as seamless, sophisticated, and scalable as the internet itself?

Those are questions at the heart of DARPA's Cyber Grand Challenge, a multiyear program that is set to culminate in Las Vegas next month at a unprecedented, open-to-the-public cyber defense competition to be held in collaboration with DEF CON, one of the world's largest and most venerable annual hacker conferences. During the one-day event, computer programs developed by seven remarkable teams will vie for millions of dollars in prizes as they compete in the world's first automated game of Capture the Flag (CTF)—the same game played by top hackers in their annual displays of cyber intrusion and defense acumen.

Playing in a specially created computer testbed laden with an array of bugs hidden inside custom, never-before-analyzed software, the machines will be challenged to find and patch within seconds—not months—flawed code that is vulnerable to being hacked, and find their opponents' weaknesses before the defending systems do. The entire event will be elaborately visualized on giant monitors in the Paris Las Vegas Hotel's 5,000-person-capacity auditorium while expert "sportscasters" document the historic competition.

And it may not end there. The organizers of DEF CON CTF have boldly invited the winning automated system to compete against the world's best human hackers in their Capture the Flag competition the following day, Aug. 5. That would be the first-ever inclusion of a mechanical contestant in that event, and could presage the day when, as eventually happened with chess and Jeopardy!, a computer proves to be the Grand Master of cyber defense.

But let's not get a head of ourselves, said Mike Walker, the DARPA program manager who launched the Cyber Grand Challenge in 2013 and who, for the past year, has been increasingly consumed with leading the elaborate preparations for the final event as separate infrastructure teams test and monitor the synthetic operating system on which the event will play and oversee the installation of gigantic chillers to keep the racks of high-performance computers from overheating on game day.

"Unlike the case with self-driving cars, where the path to full autonomy, while challenging, is now just a matter of technological advances, we still don't know if autonomy involving the kind of reasoning that's required for cyber defense makes conceptual sense," Walker said. "We certainly don't expect any machine to win against humans at DEF CON this year. But at a minimum we'll learn a lot from seeing how the systems fare against each other, and if we can even provide a clear proof of concept for autonomous cyber defense, that would be revolutionary," he said. "In the same way that the Wright brothers' first flight didn't go very far but launched a chain of events that quickly made the world a much smaller place, a convincing demonstration that automated cyber defense is truly doable would be a major paradigm shift, and would speed the day when networked attackers no longer have the inherent advantage they enjoy today."

The Cyber Grand Challenge Final Event is free and open to the press, with media opportunities to be scheduled before, during, and after the day's event. For registration and other information, including details and videos about the seven competing teams, please visit www.cybergrandchallenge.com and http://www.darpa.mil/news-events/2015-07-08.

###

Media with inquiries should contact DARPA Public Affairs at outreach@darpa.mil

---

TAGS

| Automation | Countermeasures | Cyber | Events |

SIMILARLY TAGGED CONTENT

Cyber Grand Challenge (CGC) Final Event
Cyber Grand Challenge Announces 1st Group of Teams, Final Event at DEF CON
DARPA Announces Cyber Grand Challenge
Cyber Grand Challenge
DARPA Exploring Ways to Protect Nation's Electrical Grid from Cyber Attack

IMAGES

CGC