Imagine if your computer could heal itself when attacked

August 8 2016, by Tim Johnson, Mcclatchy Washington Bureau

Computer, heal thyself! With menacing bugs and viruses floating around the internet, such a command would be useful. In fact, it may be moving toward reality.

A glimpse of "self-healing" computers unfolded in a massive Las Vegas ballroom Thursday night, and the moment evoked crucial leaps in computer development, such as when IBM's Deep Blue beat a reigning world master at chess in 1997 and more recent experiments with computerized self-driving cars.

The challenge on the stage was for seven competing teams to set their supercomputers loose against one another, protecting their own systems and attacking others. They faced some of the most daunting digital viruses known to humans, and the computers acted autonomously to find, diagnose and fix software flaws.

Judges announced Friday morning that a team of academics and hackers once affiliated with Carnegie Mellon University in Pittsburgh had snatched the $2 million top prize.

"I can say with certainty that a spark was lit today, and we have proven that this autonomy is possible," said Mike Walker, program manager for the Defense Advanced Research Projects Agency, the Pentagon's visionary "mad science" agency, which hosted the Cyber Grand Challenge.

The implications could be far-reaching as the world moves into the "internet of things," in which automobiles, lighting systems, medical devices and even coffeepots become subject to virus attacks. As it is now, computer vulnerabilities can remain undetected for months, and require tedious work of searching through complex computer programs to patch the problems. A successful "self-healing" prototype could transform the way cybersecurity is conducted.

Touted as the world's first all-machine hacking tournament, the challenge drew more than 100 teams in qualifying rounds, leading to Thursday night's seven-team faceoff. For some 5,000 techies in attendance at Bally's Paris Las Vegas Conference Center, it was geek nirvana.

Rival computers faced an escalating array of attacks, starting with the Morris worm, which appeared in 1988, moving to the SQL Slammer, which infected 75,000 computers in 10 minutes in 2003, on to the .lnk bug from 2010 and facing onslaughts from other nasty fresh digital critters.

Most teams were coding nonstop in the days leading to the tournament, and exhaustion marked the final chapter as much as excitement.

"I'm going to sleep," said Dr. David Melski, a leader of Team TechX, which took the $1 million second prize as the tournament closed. Melski's day job is vice president of research at GrammaTech Inc., a tech spinoff from Cornell University in Ithaca, New York.

Competitors said they had no doubt that teaching computers to heal themselves would be a major step.

"Every day, we trust more and more parts of our lives to computers, to software. ... We want this to be safe," said Thanassis Avgerinos, a leader

of the winning ForAllSecure team.

Another member, Ryan Goulden, said computers operated at far greater speeds than human hackers and that computers would outwit them if autonomous cybersecurity became viable.

"If you can patch faster than humans can exploit, then you've solved hacking, right?" Goulden said.

Designing the software for the competing teams was arduous.

"We're talking about dozens of thousands of lines of code, maybe 60,000 lines," said Giovanni Vigna, an Italian professor of computer science at the University of California at Santa Barbara, who led the third-place finisher, Team ShellPhish.

At his lab, Vigna recruited researchers from Russia, India, China, Germany and Italy - "14 people, I would say 60 hours a week for at least three months. We put it together, fueled by sushi."

While computers are fast at examining all mathematical possibilities, programmers still struggle to emulate coding akin to human intuition to find problems and speed solutions.

The supercomputers were lit up in pastel colors on a stage in the ballroom. They bore names like Galactica, Xandra, Mech-Phish, Crspy, Jima, Mayhem and Rubeus. Some 180 tons of water flowed through pipes under the racks holding the supercomputers to keep them cool.

Organizers cautioned that it may take years of development before ordinary smaller computers can fend off attacks by themselves.

"There's still a huge gap between (achievements at the event) and being

able to roll it out across enterprise networks tomorrow," said John Launchbury, the director of the information innovation office at DARPA.

Nonetheless, the Pentagon agency has a track record of stimulating breakthrough technologies, including GPS navigation systems, stealth technology and the internet itself.

It has periodically offered prize money for challenges as a way to draw innovators, researchers and dreamers across disciplines to hunt for novel, risky approaches without knowing whether a solution can be found. Other prizes have been offered in robotics development and self-driving cars.

"This is the magic of challenges. Challenges are not the right solution to every problem," said Walker, a former computer vulnerability researcher. "They're a great solution when a technology is on the horizon at the edge of feasibility and needs integration with a bunch of existing cutting-edge technologies."

Like many such breakthroughs, usage can toggle between benign and aggressive aims. Walker acknowledged that self-healing computers could be used for offensive purposes.

"But the difference between offensive use and defensive use is the difference between secrecy and openness," Walker said.

Vigna of Team ShellPhish said his group would make its software public, and other teams in the challenge were expected to do the same.