

DARPA to help shield cloud networks from cyberattack

Mission-oriented Resilient Clouds program would boost security and reliability

- By John Edwards
- Aug 17, 2011

With cloud computing rapidly emerging as a critical Defense Department mission support platform, the Defense Advanced Research Projects Agency is asking commercial and academic computer researchers to help build stronger cloud networks.

DARPA's Mission-oriented Resilient Clouds program, introduced in May, aims to help DOD protect its mission-focused cloud infrastructures from external threats and provide continued mission effectiveness during any type of cyberattack. Upon completion, the MRC program will run alongside DOD's Clean-slate design of Resilient, Adaptive, Secure Hosts program for limiting host vulnerabilities. According to DARPA's MRC program announcement release, the agency would like bidders to turn the tables on attackers and develop security approaches that take advantage of a distributed network's ability to rapidly amplify and propagate attacks and "use the network as a vulnerability damper and a source of resiliency."

Multiple approaches

To achieve its target, DARPA is urging bidders to consider several possible design approaches, including using redundant hosts, correlating attack information between hosts and creating network-wide resource diversity. To this end, DARPA is asking project bidders to not only address known cloud system security technologies and processes but also pursue new approaches to the design of networked computations and cloud computing infrastructures.

Related coverage:

[DARPA's satellite cluster project enters design phase](#)

The program indicates a shift in the way DOD is approaching cloud security, said Bryan Ward, cloud computing practice director at Serco, a military technical services provider that's considering an MRC bid.

"Most of the cloud tools that are out there are one-off manifestations of traditional tools that focus on the physical infrastructure," he said. "Standards bodies and research organizations...are all recognizing that a lot of these tools need to be revamped to look at the virtual network that's created by the cloud." Ward said he thinks that MRC's approach is designed to get researchers thinking about cloud security in different and novel ways. "They want people to think out of the box," he said.

But Ron Ritchey, a cloud security principal at Booz Allen Hamilton, a firm based in McLean, Va., that provides technology consulting services to DOD and other government agencies, noted that as DARPA explores the thin forward edge of cloud security, it needs to be careful that any new technologies it cultivates don't cause inadvertent harm.

"One of the things we have to worry about in information security in general is that the controls that are put in place aren't more onerous than the attacks," Ritchey said. "When we are introducing something that has the potential of dramatically increasing the complexity and understanding of operations, we really need to think that through very carefully."

3 major goals

DARPA wants the MRC project to achieve three major goals: collective immunity, a cloud-wide public health infrastructure and a diverse moving target environment.

A collective immunity situation, created by several hosts working together in unison, would give DOD cloud networks continuous and automatic backup and cross-checking capabilities. Meanwhile, a robust public health infrastructure would enable DOD cloud networks to protect themselves against external attacks by quickly recognizing threats; assessing the trustworthiness of network resources, such as servers, network bandwidth and storage; and continuously reallocating these network elements so that higher priority tasks are guaranteed access to trustworthy resources.

By creating a diverse cloud environment, DARPA hopes to turn DOD network resources into moving targets with servers, storage systems and other major elements all featuring unique attributes. The approach is designed to lessen the possibility that a weakness discovered on one network resource can be successfully exploited on its counterparts. Ritchey said that although he likes this approach in theory, he feels that project researchers will likely struggle to create a constantly shifting network environment that also provides complete reliability.

"You're basically causing minute performance or behavioral changes in the system to disrupt attacks," he said. "You have to be really confident that those changes you're making aren't causing subtle or gross impact to the defined purpose of the system."

The payoff

DARPA's MRC project timeline calls for work to begin in early 2012. System design and development will run through the end of 2014, with integration and testing wrapped up by the end of 2015.

If, at the end of the process, DARPA manages to create a new and safer cloud environment, Ward said he believes that the MRC program will deliver a twofold benefit to DOD. "Many of the techniques the DARPA plan describes will benefit not only security but reliability as well," he said. "It's a program that seems likely to get the most value for the buck."

About the Author

John Edwards is a contributing writer for Defense Systems.



© 1996-2011 1105 Media, Inc. All Rights Reserved.