DARPA MRC initiative: Security in the cloud

Researchers are working on a proactive system for handling cyberattacks on cloud services and infrastructures

BY JOHN EDWARDS

As the Defense Department begins sending its most sensitive information into the cloud, the Defense Advanced Research Projects Agency is developing a new generation of resilient cloud services that are designed to maintain and support military objectives during a cyberattack.

According to DARPA, a traditional focus on perimeter defense can't sufficiently secure existing network enclaves. The approach is even less likely to provide reliable security in cloud environments, where a massive concentration of homogeneous hosts on high-speed networks lack internal checks and rely on implicit trust among hosts within limited perimeter defenses.

DARPA's Mission-oriented Resilient Clouds (MRC) program aims to bolster cloud security by developing technologies that would detect, diagnose, and respond to attacks on cloud services and infrastructures, effectively building a community health system. DARPA researchers are also working on technologies that would enable cloud applications and infrastructures to continue functioning while under attack.

"In effect, the idea is to enable a cloud-based architecture that provides fault tolerance and mission assurance for widely distributed multi-host systems similar to business-critical online transaction processing systems that tie together a fabric of varied network nodes...into a host architecture that can survive any individual component failure or predicted class of attack," said Mark Cohn, chief technology officer at Unisys Federal Systems, based in Reston, Va.

DARPA researchers are looking for ways to keep cloud services functioning even while under attack.

PROTECT AND PRESERVE

The MRC program's most important aspect is its focus on preserving access to mission-critical resources, said Geoff Webb, director of solution strategy at NetIQ, a Houston-based user access and security systems vendor.

"While cloud computing generally offers a much higher degree of availability due to the inherently distributed nature of clouds, there is a very real threat that monoculture in the cloud might result in a targeted attack against a specific type of host infecting all of the connected systems in a cloud, which could put a mission at risk," he said.

Webb added that the MRC initiative addresses this issue by "introducing manageable diversity and dynamic trust models that could potentially identify and stop an attack or failure before it affects the entire cloud."

Victor Morrison, senior security engineer at Creative Computing Solutions, a Rockville, Md., company that provides IT services to the federal government, said the program indicates an eagerness by DOD to investigate promising new cloud security approaches.

"The DARPA MRC program is focused on creating countermeasures and an evolved architecture to the current approach of perimeter security stance," he said.

Until MRC is ready for deployment, DOD will have to rely on existing government and commercial security technologies and practices, despite the fact that they, too, are undergoing an evolution and have not yet been fully tested in a military cloud environment.

Besides the Federal Risk and Authorization Management Program, the other major guidance and resources for adopting cloud computing are the National Institute of Standards and Technology's cloud computing initiative and 800 series publications, and the Defense Information Systems Agency's Rapid Access Computing Environment and Secure Technology Application Execution programs. DISA also functions as a cloud broker. ■

Additional Online Resources

DARPA's Mission-oriented Resilient Clouds Program
http://www.darpa.mil/Our_Work/I2O/Programs