DEFENSESYSTEMS
KNOWLEDGE TECHNOLOGIES AND NET-ENABLED WARFARE

DOD's move to the cloud keeps security experts up at night

- **By John Edwards**
- **Aug 22, 2011**

The high-profile security breaches the Defense Department has suffered in the past couple of years highlight the wide range of threats it faces — from the disgruntled soldier who gave secret documents to WikiLeaks to the state-sponsored hackers suspected in the recent theft of 24,000 files related to new weapons systems.

The fact that those breaches occurred on supposedly secure systems that DOD and its industry partners have operated for years shows just how challenging cybersecurity can be, even under the best of circumstances.

Related coverage:

DARPA to help shield cloud networks from cyberattack

Now DOD officials have a new set of risks to worry about as they push forward with plans to overhaul the way the military uses IT. They want to move to a cloud-computing model in which computer, network and software resources are standardized and shared among many parties, thereby reaping cost and operational benefits that the old approach of duplicative but incompatible IT systems could never deliver.

Of all the emerging technologies — including mobile devices, wireless networks and social media platforms — cloud computing is widely viewed as the one that most often keeps DOD's information assurance experts from getting a good night's sleep.

DOD's cloud central

A lot of that worry now falls to Richard Hale, chief information assurance executive at the Defense Information Systems Agency. DISA is the staging area for much of DOD's IT centralization efforts and has been building the cloud infrastructure and services used by a broad and growing set of DOD customers. DISA offers software-as-a-service tools, such as e-mail and Web conferencing; platform as a service, or on-demand computing; and data storage.

Hale and his team are responsible for making those services as secure as possible, but given the still-developing nature of the cloud, they are venturing into uncharted territory.
One decision has been easy: DISA has so far steered clear of commercial cloud services. "Given the large number of information assurance questions, we're approaching the use of shared, commercial clouds in a cautious way," Hale said.

Instead, DISA is building an internal cloud environment using hardened servers. The agency is also relying on the Defense Advanced Research Projects Agency to seek out and deliver innovative new technologies and approaches to cloud network security.

As they build their cloud infrastructure, DISA officials are paying special attention to the mechanisms that grant authorized access to IT resources.

"In this private cloud, we're focusing strongly on driving out anonymity through the use of the cyber identity credentials issued by a [National Security Agency]/DISA service called the DOD Public Key Infrastructure," Hale said.

The PKI credentials are being deployed on the Secret IP Router Network this year and next, Hale said. SIPRnet is cleared to transmit information classified up to and including the secret level. Hale said he expects that everyone on that network will be using the credentials by the end of fiscal 2012.

DISA is also helping DOD re-engineer the way it controls user access to information resources, particularly data that resides in the cloud. “We believe that direct authentication from a client device to a server via the use of a PKI credential is the right model,” Hale said. “This means no middle layers — for instance, portals — are involved in the actual authentication.”

DOD would also like to eliminate individual user accounts, which are clumsy to use and prone to negligence, theft and misuse. “The account-based access model inhibits sharing in a place as large as DOD [and] with as many different information services as we have,” Hale said. “Access should be granted using…attribute-based access control.”

Such systems grant authenticated users access to specific resources based on set policies and the permission level assigned to the user or group. Access control also often includes authenticating the identity of the user who is trying to log in.

The benefits of automation

Clouds present other security challenges. They can be more dynamic and complex than traditional IT environments because services are constantly turned on and off to meet changing user needs, and workloads are shifted across the infrastructure to optimize the use of processing and storage resources.

DOD wants to automate many of those activities to remove the human element from the systems administration tasks as much as possible. “Automation is the only way to do some of these things fast enough and without the vulnerabilities introduced by human error,” Hale said.

To that end, DOD’s cyber experts are turning to the Security Content Automation Protocol (SCAP), a standard developed by the National Institute of Standards and Technology to enable automated vulnerability management and measurement and policy compliance evaluation.

DISA buys many enterprise security and measurement tools for DOD. “We require SCAP compliance in all of these so we can better connect these different tools into a more automated security ecosystem,” Hale said.

The makeup of DOD’s IT infrastructure might be in transition, but its ultimate purpose is not. "DOD's information infrastructure exists to support better, faster, cheaper mission execution,” Hale said. “All of us have to treat [information assurance] as the mission-essential tool it is.”

DARPA imagines a more defensive cloud

Under its new Mission-oriented Resilient Clouds program, the military said it wants to turn the tables on cyberattackers and use the cloud’s distributed nature to act as a “vulnerability damper and a source of resiliency,” according to a recent bid announcement.

The Defense Advanced Research Projects Agency kicked off the MRC program in May by asking commercial and academic researchers to help build stronger cloud networks. DARPA wants MRC bidders to come up with new security approaches to achieve three main goals.

1. Collective immunity, whereby multiple computing hosts working together would give the Defense Department’s cloud networks continuous and automatic backup and cross-checking capabilities.
2. A cloudwide public health infrastructure that quickly recognizes threats, assesses the trustworthiness of network resources, and continuously reallocates those elements so that high-priority tasks are guaranteed access to trustworthy resources.
3. A diverse environment that reduces the possibility that a weakness discovered on one network resource can be successfully exploited on its counterparts.

The program represents a shift in DOD’s thinking about cloud security, said Bryan Ward, director of the cloud computing practice 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.”

But DARPA must be careful that any new technologies it cultivates don’t cause inadvertent harm, said Ron Ritchey, a cloud security

principal at Booz Allen Hamilton.

“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.”

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.

About the Author

John Edwards is a contributing writer for Defense Systems.