MILITARY & AEROSPACE ELECTRONICS AVIONICS INTELLIGENCE AVIONICS INTERNATIONAL

Military & Aerospace Electronics

SUBSCRIBE | ADVERTISE | ABOUT | CONTACT

Search

HOME TOPICS DEPARTMENTS MAGAZINE WEBCASTS WHITE PAPERS EXECUTIVE BRIEFINGS BUYER'S GUIDE MOBILE

The challenge of a secure military cloud

November 14, 2013

Reliable security and efficient resource allocation are central concerns as the military moves mission-critical information to the cloud.

BY **J.R. Wilson**

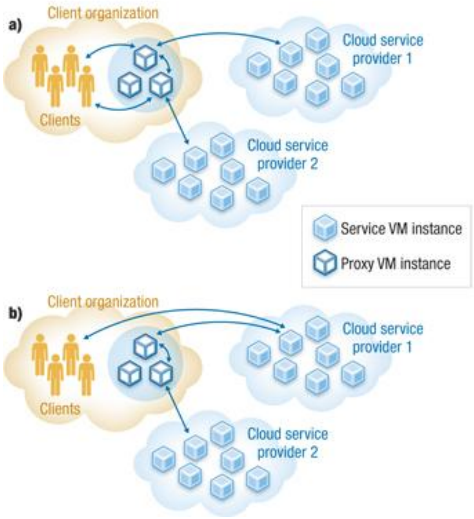
With all the changes brought by a global Internet and the subsequent transition of data to digital formats across all segments of society, security challenges have grown even faster, from cyber espionage and dedicated denial of service (DDoS) to cyber warfare.

In recent years, a new approach to data storage and sharing, generically called "the cloud", has begun to grow faster than security could match. On the positive side, that has brought less expensive operations, faster updates, easier sharing; on the negative, a plethora of new security issues.

While individuals typically use public clouds-such as those provided by Amazon.com, Google, and Apple-large entities with vast amounts of data have turned to private, "secure" clouds. The most concerned users, current and future, are government agencies, especially the military.

"The bulk of military data is just routine business information that is not particularly sensitive and could very easily go into a cloud that is considered commercially secure without a lot of headaches," says John Howie, chief operating officer of the Cloud Security Alliance (CSA) and a member of the IEEE Computer Society and its security-related programs. "That becomes very different when you start talking about highly classified data. There you will find some of the nature of the cloud, such as shared infrastructure, will get in the way of using current commercial cloud offerings.

"So cloud providers are building special environments for the military and others with top secret information, such as the U.S Department of Energy," Howie continues. "Those are more 'community' rather than public clouds. So you will see the government procure regular cloud offerings that meet FISA [Foreign Intelligence Surveillance Act] standards, but more specialized clouds being adopted by the military that meet an entirely different set of standards."



(Figure 1: In the cloud computing paradigm, three layers are stacked, providing on-demand infrastructure, middleware, and software services. The cloud stack sits above the virtualization layer.)

In February 2011, the Obama Administration issued a Federal Cloud Computing Strategy that essentially ordered federal entities-including military and intelligence services-to begin switching to cloud-based data storage and sharing. The strategy implemented a cloud first policy "intended to accelerate the pace at which the government will realize the value of cloud computing by requiring agencies to evaluate safe, secure cloud computing options before making any new investments."

"Cloud computing has the potential to play a major part in addressing...inefficiencies and improving government service delivery. The cloud computing model can help agencies grappling with the need to provide reliable, innovative services despite a lack of resources," the new Strategy proclaimed.

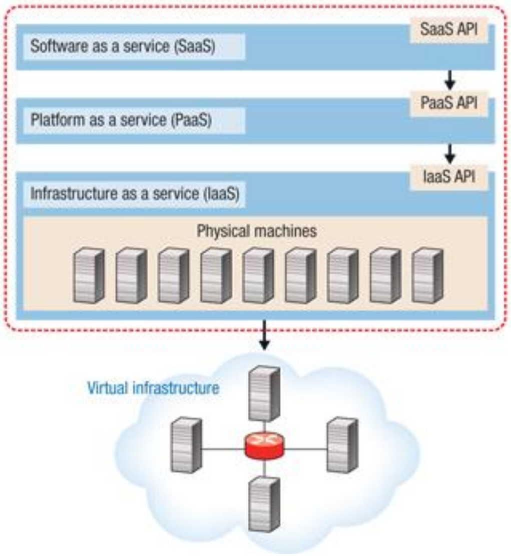
"Cloud computing can be implemented using a variety of deployment models-private, community, public or a hybrid combination. Each agency will re-evaluate its technology sourcing strategy to include consideration and application of cloud computing solutions as part of the budget process."

The directive, released by U.S. Chief Information Officer Vivek Kundra, also predicted a whole-of-government shift to the cloud will accelerate an earlier effort, the Federal Data Center Consolidation Initiative, intended to restructure the government's fragmented data center environment.

"Through the FDCCI, agencies have formulated detailed consolidation plans and technical roadmaps to eliminate a minimum of 800 data centers by 2015," the report noted. "Cloud computing can accelerate [those] efforts by reducing the number of applications hosted within government-owned data centers.

"For those that continue to be owned and operated directly by Federal agencies...environments will be more interoperable and portable, which will decrease data center consolidation and integration costs because it reduces unnecessary heterogeneity and complexity in the IT environment."

The strategy acknowledged such goals must be measured against a wide range of risk assessments, tailored by each agency according to its mission and requirements, no matter which deployment model is used. Of import to the U.S. Department of Defense (DOD) and its partners in industry and academia is adherence to Federal Information Security Management Act (FISMA) requirements, such as compliance with Federal Information Processing Standards, Authorization to Operate requirements, and monitoring and reporting vulnerability and security events.


SaaS API
Software as a service (SaaS)
PaaS API
Platform as a service (PaaS)
IaaS API
Infrastructure as a service (IaaS)
Physical machines
Virtual infrastructure

(Figure 2: Conceptual cloud-based security overlay networks are composed primarily of cloud security and management units in addition to the customer network's protected endpoints. This generic architecture can be used to deploy any cloud-based security solution.)

"It is essential that the decision to apply a specific cloud computing model to support mission capability considers these requirements. Agencies have the responsibility to ensure that a safe, secure cloud solution is available to provide a prospective IT service and should carefully consider agency security needs across a number of dimensions," according to the Strategy. Those include:

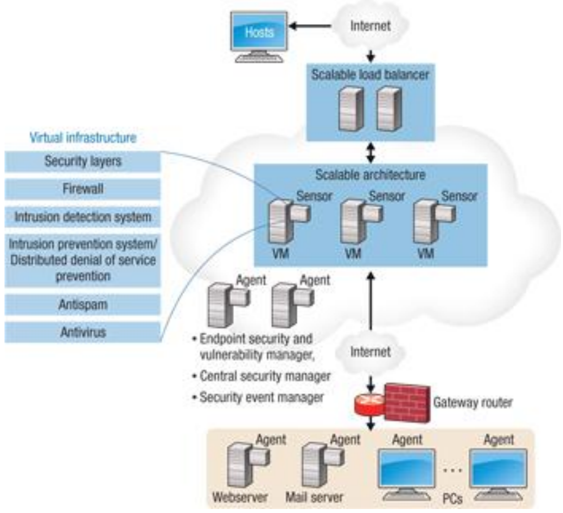
- Data characteristics to assess which fundamental protections an application's data set requires;
- Privacy and confidentiality to protect against accidental and nefarious access to information;
- Integrity to ensure data are authorized, complete and accurate;
- Data controls and access policies to determine where data can be stored and who can access physical locations; and
- Governance to ensure that cloud computing service providers are sufficiently transparent, have adequate security and management controls and provide the information necessary for the agency to appropriately and independently assess and monitor the efficacy of those controls.

Due to the special security needs of many government agencies-and a desire to create a system of cloud governance that will outlast individuals or administrations-the Strategy assigned specific roles and responsibilities to a number of federal agencies and organizations, including:

- National Institute of Standards and Technology (NIST) - Lead and collaborate with federal, state and local government agency CIOs, private sector experts and international bodies to identify and prioritize cloud computing standards and guidance;
- General Service Administration (GSA) - Develop government-wide procurement vehicles and cloud-based application solutions where needed;

- Department of Homeland Security (DHS) - Monitor operational security issues related to the cloud;
- Federal CIO Council - Drive government-wide adoption of clouds, identify next-generation cloud technologies and share best practices and reusable example analyses and templates; and
- Office of Management and Budget (OMB) - Coordinate activities across governance bodies, set overall cloud-related priorities and provide guidance to agencies.

"Cheaper processors, faster networks, and the rise of mobile devices are driving innovation faster than ever before. Cloud computing is a manifestation and core enabler of this transformation," the Strategy concluded.



Despite the widespread and rapid adoption of cloud computing across all sectors of society and government, there remains considerable confusion among new or non-users about what a cloud is and how it differs from traditional methods of data storage and sharing.

(Figure 3: Client sends a request to cloud C1, which dynamically discovers the need to use services from clouds C2 and C3. C1 employs proxies to manage these interactions.)

"A lot of people do tend to think of the cloud as some mythical place-but it really is a way of doing things, not a place. At the bottom of it is physical hardware-computers, hard drives, and so on. So the things that apply today regarding managing our own servers also apply to clouds," says Geoff Webb, director of Solution Strategy at NetIQ in Houston. "It's just as easy and possible for the IT service people handling a cloud to cause problems through mistakes as it is by your own IT department.

"A private cloud requires a fair degree of maturity in how it is managed-it is not for the faint of heart or inexperienced. If you have a lot of resources, but with varying demand on those, and someone with whom you can share those, then you both get more than if you each owned your own systems separately," Webb says. "But it requires knowledge, capability, trust in the people sharing the cloud and accepting the risk you both bring to it. I don't want to share resources-even in a private cloud-for highly critical information."

Stelios Sidiroglou, a research scientist at MIT's Computer Science and Artificial Intelligence Laboratory in Cambridge, Mass., says defining cloud computing, especially a secure cloud, is harder than it should be.

"A lot of people have a very hard time understanding it. The cloud is similar to distributed computing we've had, but has a different name because of the different operations that have emerged in the past few years," he said. "And that is probably the source of a lot of confusion, because so many different services now have been attributed to the same concept-cloud computing.

"That confuses the issue of cloud security-are you just trying to secure one of those services or multiples or all? So first you have to identify what kind of cloud computing you're working on and focus on that," Sidiroglou continues. "You have to think about everything-the underlying hardware and operating systems and types of software being used."

NIST defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

The core of cloud computing centers on three service models: software as a service (SaaS); platform as a service (PaaS); and infrastructure as a service (IaaS).

In addition, NIST has outlined five essential characteristics of cloud computing-on-demand service, broad network access, resource pooling, rapid elasticity and measured service-and four primary deployment models:

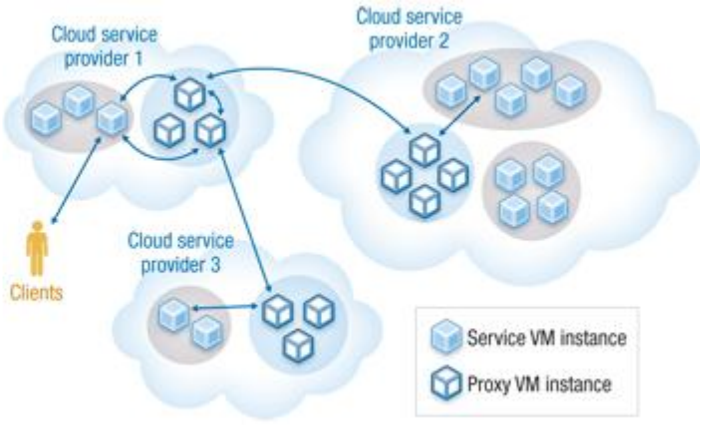
- Private cloud: Infrastructure operated solely for an individual organization, although it may be managed by a third party and exist either on- or off-premise.
- Community cloud: Infrastructure is shared by several organizations within a specific community with shared concerns (such as mission or security requirements); it may be managed by the organizations or a third party and may exist on- or off-premise.
- Public cloud: Infrastructure is available to the general public or a large industry group and is owned by an organization selling cloud services.
- Hybrid cloud: Infrastructure is a composition of two or more clouds (private, community or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

"We look at the cloud as a consumption model of the underlying technologies to support the mission," says Kyle Keller, cloud business director at EMC Corp. in Hopkinton, Mass. "We want to get to a point where we can set model and security at the application level and maintain control and visibility even if that software goes to another user and you don't maintain direct control.

"It's not so much secure cloud computing as secure computing in general. Many of our customers want to move into the cloud, but don't have the best legacy security to begin with; cloud computing is an opportunity to do things differently. In the legacy arena, we looked at how to bolt security around the infrastructure. Now the technology is built in, so security controls in a virtualized space become foundational to the architecture from day one rather than something we build on after the fact."

The 2012 National Defense Authorization Act required the DOD Chief Information Officer to create a strategy for migrating defense data and government-provided services from Department-owned and operated data centers to cloud computing. That includes generally available private sector services that provide better capability at lower cost with the same or greater degree of security.

In July 2012, DOD Chief Information Officer Teresa M. Takai released a Defense Department Cloud Computing Strategy "to enable the Department to increase secure information sharing and collaboration, enhance mission effectiveness and decrease costs using cloud services. Active participation and commitment of all DOD components is critical to ensure consistency, optimize benefits and achieve the goal of this strategy."



“Figure 4: The proxy as a service scenario calls for cloud service providers to deploy proxies as an autonomous cloud systems and offer it as a service to their clients.)

That goal is to use cloud computing to secure information and provide IT services supporting the Department's mission, anywhere, anytime on any authorized device. It expanded beyond the earlier Federal Strategy in emphasizing the increasing danger of both state-sponsored and individual cyber threats, even as increasing budget constraints force transformations in IT structure and management. To that end, DOD created the Joint Information Environment (JIE) to deliver "faster, better informed collaboration and decisions enabled by secure, seamless access to information regardless of computing device or location."

"The DOD Enterprise Cloud Environment is a key component to enable the Department to achieve JIE goals. The DOD Cloud Computing Strategy introduces an approach to move the Department from the current state of a duplicative, cumbersome and costly set of application silos to an end-state which is an agile, secure and cost-effective service environment that can rapidly respond to changing mission needs," according to the report.

That effort is being leveraged with the Federal Risk and Authorization Management Program (FedRAMP) to establish a standard approach to assess and authorize cloud computing services and define requirements for the continuous auditing and monitoring of cloud computing providers.

"The DOD Enterprise Cloud Environment will include separate implementations and data exchanges on Non-secure Internet Protocol Router Network (NIPRNet), Secure Internet Protocol Router Network (SIPRNet) and Top Secret Sensitive Compartmentalized Information (TS SCI) security domains," the DOD Strategy reported.

"This environment will be closely aligned with intelligence community-led initiatives and support information-sharing with DOD traditional and non-traditional partners on the Joint Worldwide Intelligence Communications System (JWICS) and other networks. All cloud services must comply with Department IA [Information Assurance], cyber security, continuity and other policies."

Government-wide and DOD requirements to implement cloud computing as quickly as possible have put even more impetus on aerospace and defense industry and related academia to finalize their own adoption of cloud computing.

Many of the security concepts developed for pre-cloud systems remain viable, albeit with some tweaking. Even secure clouds typically are built with COTS software common to non-cloud systems, according to Howie-and if vulnerabilities exist in that software, they are likely to appear in the cloud, as well. To deal with those and other threats, many clouds now employ multiple levels of security-defense in depth-starting from the host's physical perimeter to the data itself.

"If there is vulnerability in one area, there will be layers elsewhere that will still protect the data and stop attacks or detect them," he said. "You can build a cloud that requires access to a closed network first, such as SIPRNET, then only someone able to access that secure network could access the cloud.

"Typically, if there is an attack, the problem is when the user-not the cloud provider-fails to take advantage of available security mechanisms. Ultimately, the cloud provider-even for private or secure clouds-is not in control of the ultimate security of the user's data. It is up to the customers to understand their responsibilities in using a cloud service. Security is actually a shared responsibility."

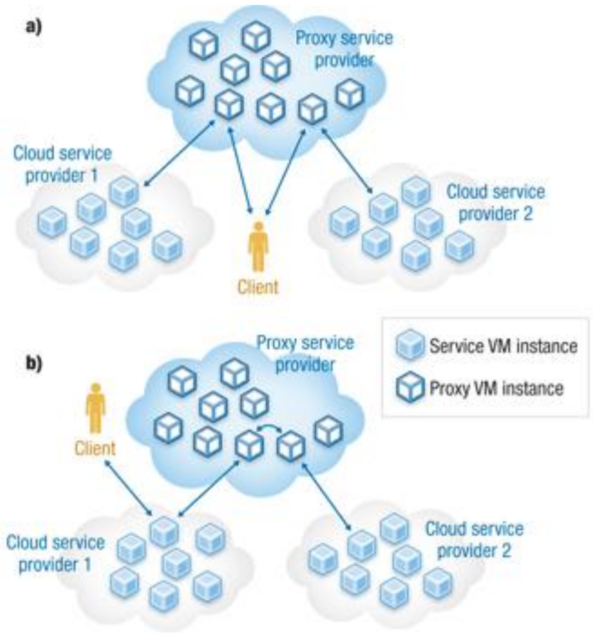
Kevin Haley, director of security response at Symantec Corp. in New York, says there are similarities between the threats facing commercial users and aerospace and defense organizations. "The majority of threats are coming from profit-oriented groups, such as criminals. The real threat to government computing, and industry, involves espionage. If an attacker can steal secrets from a target's traditional systems or a cloud, he no doubt will," he said. "Attacking a cloud really isn't more difficult than attacking a standard data network-in some ways, it could be easier.

"If I can get your log-in details, I don't have to worry about whatever security system the cloud provider has implemented. So if your data is in the cloud, you not only have to worry about vetting your employees who have access, but also the cloud providers' employees."

Clouds also are vulnerable to the Stuxnet approach, a computer worm used in an indirect, but targeted, attack on Iran's nuclear facilities in 2010. "It's a technique we have seen quite a bit in recent years-if I can't directly attack my target, I can attack the people who work for my target or someone who does business with my ultimate target," Haley said. "A lot of the focus tends to be on very high-level vulnerabilities, but as we focus on more high-tech hacking and solutions, we tend to lose sight of the simplest avenues, such as stealing log-in details."

Among efforts to secure DOD cloud computing is DARPA's Mission-oriented Resilient Clouds (MRC) program. "Where compelling incentives to do this exist, security implications of concentrating sensitive data and computation into computing clouds have yet to be fully addressed. The perimeter defense focus of traditional security solutions is not sufficient to secure existing enclaves. It could be further marginalized in cloud environments where there is a huge concentration of homogeneous hosts on high-speed networks without internal checks and with implicit trust among hosts within those limited perimeter defenses," according to DARPA.

"The MRC program aims to address some of these security challenges by developing technologies to detect, diagnose and respond to attacks in the cloud, effectively building a 'community health system' for the cloud. MRC also seeks technologies to enable cloud applications and infrastructure to continue functioning while under attack. To achieve these goals, the program will research development of innate distributed cloud defenses, construction of shared situational awareness and dynamic trust models, and introduction of manageable and taskable diversity into an otherwise homogeneous cloud, as well as development of mission-aware adaptive networking technologies."



(Figure 5: On-premises proxy calls for clients to deploy proxies within the infrastructure of their organization. (a) A client employs two proxies to interact with CSPs C1 and C2. (b) A client initiates a service request with C1, which then discovers the need for a service from C2.)

As with many DARPA programs, MRC, launched in November 2011, involves research by a number of organizations, including MIT's SAIL.

"You can make systems more and more secure, but it's just an ongoing arms race and I don't see an end to that. You can set up systems that guarantee previous methods won't work in the future, but attackers are very versatile and will always come up with some way," says Martin C. Rinard, SAIL's MRC principal investigator. "If you have even a small vulnerability in some piece of hardware, it's hard to see how you could not at least mount a DDoS against it. The state-of-the-art in cloud security tends to evolve very quickly over time in the ongoing arms race. Our goal is to develop ongoing trends in how to analyze those.

There is an enormous amount of creative, high-level research underway to address issues current and future, known and still to be discovered. "You can expect to see very great changes in this environment in the next five years or so," Rinard says.

In the ancient manner of armor versus anti-armor, those seeking to secure the cloud face an endless challenge from ever more aggressive and technically sophisticated attackers.

"The cloud is very seductive, but I guarantee that in five years, we will look back and say there are a lot of good uses for clouds, but it doesn't solve all problems," Webb predicts. "Right now a very sensible discussion is underway as to what should or should not be in clouds and, even then, what should be in a public cloud and what in a private."