Cloud Computing and Cyber Defense

A White Paper provided to the National Security Council and Homeland Security Council as input to the White House Review of Communications and Information Infrastructure.

Bob Gourley
Chief Technology Officer, Crucial Point LLC
bob@bobgourley.com
21 Mar 2009

Advancing technology has the potential of dramatically changing the security posture of the federal enterprise and, if engineered correctly, the entire IT fabric of the globe. Potential security enhancements in the communications infrastructure, the software codebase, and cloud computing all hold great potential for dramatic positive change. This paper provides an overview of the cloud computing components relevant to security and proposes items for both awareness and action by the Federal IT team.

What is cloud computing? The term is used two different ways in the IT community. To most users, cloud computing is any capability delivered over the network. If it is not local computing it is from the cloud. To these users, almost all enterprise IT is cloud computing. Technologists and enterprise architects use the term in a different way. To them, cloud computing implies new ways of providing capability on demand by use of virtualized resources. It involves pools of storage, network, processing and other computational resources that can be efficiently allocated on demand. It also implies far more agility in support of operational missions. Technologists view cloud computing as a means to most efficiently deliver computer power via an application program interface (API).

What follows is a snapshot of the current glideslope of technology in this area, an update on relevant activities in the private sector which can further federal enablement of cloud computing security, and a new look at key principles for federal implementation of cloud computing.

Industry Visions: Major IT powerhouses, including Microsoft, Sun Microsystems, IBM, Google, and Oracle are all addressing the major shift to Cloud Computing in slightly different ways, but all capture the essence similarly. All pay great attention to industry thought leaders like Tim O'Reilly, CEO of O'Reilly Media, and writer Nicholas Carr.

- **Tim O'Reilly**'s position as a leader of technology publishing and as facilitator of Silicon Valley's greatest technology expositions informs his continuing assessments on the state of computing. He considers Cloud Computing as the foundation for the next generation of computing, which he has been calling Web2.0. Cloud computing has long been a vision industry was building towards, with a network of networks seen as the platform for all significant computing (in 1982 Sun Microsystems established its company with the vision that "The Network Is The Computer"). O'Reilly articulates the ideal goal of cloud computing being that every device we think of as a computer today is really just a device that connects into the grid of connected computers to deliver required services. To O'Reilly, cloud computing is about increasing functionality using the power of the entire grid and all the people it connects to.

- **Nicholas Carr** is one of the most popular and most controversial writers on IT today. His books and articles have forced strategic discussions for years by examining concepts like the true strategic value of IT to an organization. In 2003 he penned a Harvard Business Review article "IT Doesn't Matter" in which he argued that the strategic importance of IT has diminished in inverse proportion to the use of IT, since it is now so commonplace. In 2004 he published another controversial piece on "The End of Corporate Computing" in the MIT Sloan Management Review where he argued that increasingly companies will purchase IT as a utility service from outside suppliers. Carr is now documenting the move to Cloud Computing is a book titled "The Big Switch" where he draws parallels to the shift to the use of electricity as a utility. A hundred years

ago, companies stopped generating their own power and plugged into the newly built electric grid. The cheap power provided by utilities didn't just change how businesses operate. It set off a chain reaction of economic and social transformations that brought the modern world into existence. Carr writes that today a similar revolution is under way. Hooked up to the Internet's global computing grid, information-processing plants have begun pumping data and software into our homes and businesses. So now computing is turning into a utility.[1]

Commercially available cloud services: Every company that provides IT hardware, software or services now contributes to cloud computing. We can measure the state of Cloud Computing by a survey of capabilities available right now from Google, Amazon, Microsoft, Salesforce.com and VMware.

- **Google:** The core of Google's business is all in Cloud Computing. Services delivered over network connections include search, e-mail, online mapping, office productivity (including documents, spreadsheets, presentations, databases), collaboration, social networking and voice, video, data services. Users can subscribe to these services for free or pay for increased levels of service and support. As an example of the types of cloud services provided, this paper is being written in the Google cloud. As it was written it was securely saved and backed up in a way that only the author could access, then when the draft was near complete it was shared with a small number of reviewers. When it was finalized the paper was stored as a PDF file for distribution. All this was done in a cloud with better security and privacy features than home PCs. Privacy and security on Google cloud services have many weaknesses, including the fact that data on Google's servers is not protected with strong encryption. However, the dramatic improvement over security of content when left on PC hard drives is a very positive trend and as Google continues to enhance security of its cloud services protection will only increase.

- **Amazon:** As the world's largest online retailer, the core of Amazon's business is ecommerce. While ecommerce itself can be considered Cloud Computing, Amazon has also been providing capabilities which give IT departments direct access to Amazon compute power. Key examples include S3 and EC2. S3 stands for Simple Storage Services. Any internet user can access storage in S3 and access stored objects from anywhere on the Internet. EC2 is the Elastic Compute Cloud, a virtual computing infrastructure able to run diverse applications ranging from web hosts to simulations or anywhere in between. This is all available for a very low cost per user. Amazon invests highly in security, however, current criticisms of its cloud approach including issues with availability (outages of even a moment can be costly for cloud services consumers). Another key concern is the ability of malicous attackers to leverage Amazon and the power of their processors in ways that Amazon can not detect or monitor. For example, attackers who might want to leverage the power of a super computer to crack encryption keys could lease large numbers of servers from Amazon and cut down the processing time required for brut-force attacks, and Amazon might only know that processors are being used.

- **Microsoft:** Traditionally Microsoft's core business has been in device operating systems and device office automation software. However, Microsoft has also always been in the server business and is in almost every data center today. Since the early days of the Internet Microsoft has also provided web hosting, online e-mail and many other cloud services. Microsoft now also provides office automation capabilities via a cloud ("Office Live") in an approach referred to as "Software Plus Services" vice "Software as a Service" to allow synchronous/asyncrhonous integration of online Cloud documents with their traditional offline desktop-resident versions. The next evolution of Microsoft's offerings are built on a foundation they call "Azure" but this foundation is still in a development release and is not a reliable offering yet. A criticism of Microsoft's approach has been that weaknesses in their desktop products and operating systems might be replicated into their cloud environment, however, the strength of cloud computing security models will eventually mitigate these weaknesses.

- **Salesforce.com:** The core mission of Salesforce.com has been in delivery of capabilities centered around customer relationship management. However, in pursuit of this core Salesforce.com has established themselves as thought leaders in the area of Software as a

Service and is delivering an extensive suite of capabilities via the Internet. A key capability provided is the site Force.com, which enables external developers to create add-on applications that integrate into the main Salesforce.com application and are hosted on Salesforce.com's infrastructure. Salesforce.com is critical to track since they are functionality leaders in the delivery of cloud computing power.

- **VMware:** Provides several technologies of critical importance to enabling cloud computing, and has also started offering its own cloud computing on demand capability called vCloud. This type of capability allows enterprises to leverage virtualized clouds inside their own IT infrastructure or hosted with external service providers.

- **Cisco:** Has long provided the switch fabric of the Internet and the interconnect inside datacenters and is now offering enhanced collaborative tools and unified computing capabilities that bring the foundation of cloud computing to any datacenter.

- **Sun Microsystems:** With almost 100% of Sun's R&D budget being focused on data center enhancements the company has positioned itself to be the primary provider of large scale compute power and it forms the foundational elements of most cloud offerings today. Sun enables secure access to clouds via identity management approaches and also offers delivery of cloud compute power via thin clients.

There are many other companies contributing to cloud capabilities, but the survey above captures the direction of the industry. All major players are onboard and clear mega trends have emerged.

Industry Trends Relevant to the Federal Approach: Industry cloud computing designs provide reliable services delivered through data centers that make extensive use of virtualization to deliver services. These services are available anywhere in the world, with connection to a network giving access to compute power as if it were local. Commercial offerings are increasingly based on quality of service agreements which spell out expected levels of performance and availability. Open source software and open standards are foundations for most cloud computing today (even Microsoft has announced its own increased commitment to open standards and full publication of standards and interfaces in support of its cloud computing).

Consumers of cloud computing capabilities are not budgeting or paying for infrastructure, they pay for capability, frequently on a subscription basis. Utilization of computing resources is optimized though capabilities like virutalization, since virtualization allows for hardware to be used more than it is when left idle. Consumers do not have to engineer for peak load, the IT providers must engineer for that.

Industry experience with cloud computing has resulted in extensive documentation on key characteristics that users should expect from cloud computing. Key characteristics include[2]:

- Customer **capital expenditure** is minimized which lowers barriers to entry, as infrastructure is owned by the provider and does not need to be purchased for one-time or infrequent intensive computing tasks.
- **Device and location independence** enables users to access systems regardless of their location or what device they are using, e.g., PC, mobile.
- **Multi-tenancy** enables sharing of resources, and costs, among a large pool of users, allowing for:
    - **Centralization** of infrastructure in areas with lower costs, e.g., real estate, electricity, etc.
    - **Peak-load capacity** increases (users need not engineer for highest possible load levels)
    - **Utilization and efficiency** improvements for systems that are often only 10-20% utilised.
- **On-demand allocation** and de-allocation of CPU, storage and network bandwidth
- **Performance** is monitored and consistent
- **Reliability** is enhanced by way of multiple redundant sites, which makes it suitable for business continuity and disaster recovery
- **Scalability** meets changing user demands quickly without users having to engineer for peak loads. Massive scalability and large user bases are common, but not an absolute requirement.

- **Sustainability** is achieved through improved resource utilisation, more efficient systems, and carbon neutrality. Nonetheless, computers and associated infrastructure are major consumers of energy.
- **Security** typically improves due to centralization of data, increased security-focused resources, increased ability to patch and upgrade, increased ability to monitor, increased ability to encrypt and many other reasons. However, there are concerns about loss of control over certain sensitive data. When designed in at the beginning, security of cloud architectures is significantly higher than non-cloud approaches. Enterprises requiring significantly enhanced security should consider private clouds, where the data center is controlled by the enterprise vice outsourced.

Industry experiences in cloud computing are underscoring that all these characteristics are achievable and can be optimized by well engineered, central planning activities that focus on organizational mission.

A new look at key principles for Federal implementation of cloud computing: The security of the federal enterprise, as well as its functionality, can be significantly enhanced by smartly implementing cloud computing. The following are some key principles that can facilitate this:

- The importance of mission-focused engineering. Private clouds inside the federal enterprise can enhance mission support, but mission-focused engineering should be a first step in this pursuit.
- The continual need for security, including data confidentiality, integrity and availability. All federal computing approaches must be engineered to be in total consonance with IA guidelines to assure federal information, information systems and information infrastructure. Cloud Computing, when engineered right, makes dramatic, positive changes to the mission assurance posture of the federal enterprise. Cloud computing enables stronger end point security and better data protection. It also enables the use of thin clients and the many security benefits they provide. Identity management and encryption remain of critical importance.
- The need for always instantaneously available backup of data in the cloud. Ensured availability under all circumstances is a key benefit of smart cloud computing approaches.
- The continual need for open source and open standards. Most cloud infrastructure today is based on open source (Linux, Solaris, MySQL, Glassfish, Hadoop) and this positive trend will help in net centric approaches. According to the IDC Group, open source software (OSS) is "the most significant, all-encompassing and long-term trend that the software industry has seen since the early 1980's" Gartner projects that by 2012, 90 percent of the world's companies will be using open source software. This all indicates open source and open standards should be a key principle for federal cloud computing and other net centric approaches.
- The continual need to evaluate both low barrier to entry and low barrier to exit. As approaches to cloud computing are evaluated, too frequently the cost of exiting an approach is not considered, resulting in lock-in into a capability that may soon be inefficient. Cloud computing capabilities should be adopted that do not result in lock-in.
- The need for open standards. Cloud computing contributions to enhanced functionality for the federal workforce and increase intereoperability as the code, API's and interfaces for cloud computing are secure but are widely published for all participants to interface with. Federal involvement in open source and open standards communities should continue and be accelerated, since increasingly cloud computing open standards are being discussed and designed by open standards bodies like W3C, OASIS, IETF and the Liberty Alliance. Document and other formats used by federal cloud computing activities will be open and available for all authorized users on all devices.
- The need to understand the cost of "private clouds". For at least the near term, the federal government will remain a provider of "private cloud" capabilities where security dictates ownership levels of control over compute power. This fact means the federal enterprise must continually engineer for change and technology insertion, which underscores the need for low barriers to exist in design criteria.

Regarding security, cloud computing holds the potential to dramatically change the continuous loosing game of continual workstation patching and IT device remediation by reducing the amount of applications

on desktops and changing the nature of the desktop device from fat client to thin client. Devices can now have their entire memory and operating system flashed out to the device from private clouds and can have the power of the cloud presented to users as if the user is on an old fashioned desktop. This can be done in a way that never requires IT departments to visit the workstation to patch and configure it. And since all data is stored on private clouds it can be encrypted and access only provided to authorized users. No data can ever be lost when laptops are stolen and no data can ever be lost when desktops are attacked by unauthorized users. Security by well engineered use or cloud computing and thin clients or cloud computing and smart fat clients is dramatically enhanced.

This all leads to a key conclusion for the federal enterprise: as we move forward in cloud computing for support to the mission, the federal enterprise should continue to strengthen formal processes to ensure that lessons learned from both industry and the governments's own successful cloud computing initiatives are continually examined and broadly adopted across the enterprise.

Bob Gourley is the former CTO of the Defense Intelligence Agency and is a recipient of Infoworld's Top 25 CTO award for 2007. He won AFCEAs award for meritorious service to the intelligence community in 2008 and is now the lead writer at http://ctovision.com and is the CTO of Crucial Point LLC, an IT consultancy. Contact Bob at bob@bobgourley.com

---

1. See http://www.youtube.com/watch?v=6PNuQHUiV3Q for a video of Cloud Computing context featuring interviews with luminaries like Tim O'Reilly.
2. See http://en.wikipedia.org/wiki/Cloud_computing for more info.