THE GEORGE WASHINGTON UNIVERSITY
HOMELAND SECURITY POLICY INSTITUTE

HSPI Issue Brief Series

CLOUD COMPUTING RISKS AND NATIONAL SECURITY
KEEPING PACE WITH EXPANDING TECHNOLOGY

HSPI Issue Brief 07
September 9, 2010
Frank Cilluffo, Ron Ritchey, and Timothy Tinker

While cloud computing* offers limitless possibilities in terms of collaboration and access to data, the indefinable structure of this advanced technology raises several security concerns. The George Washington Policy University Homeland Security Policy Institute hosted a recent forum sponsored by Booz Allen Hamilton and Cisco Systems to address the myriad security concerns that arise as cloud computing deployments expand.

It is imperative that security issues be addressed up-front to meet the policy implications and derive full benefits of the cloud computing deployments.

During the forum, panelists spoke of the need to include security into the very design of cloud computing as the technology advances. The panelists also emphasized the need for unprecedented cooperation and a unified front when addressing the security challenges associated with the cloud computing technology.

Protecting Data

When helping people adopt the concepts of cloud computing, Ronald Ritchey of Booz Allen Hamilton said security is one of the top issues that always surfaces. As new and technologically advanced concepts are created, security cannot be ignored. Ritchey said that data is the "golden egg" we want to protect in our systems, and there are many ways to accomplish this.

Depending upon where the actual data exists, privacy concerns change, as does the regulatory framework governing privacy. Simple things like generating keys depend on where the data is. While there might not be a need to encrypt data that flows between two different servers, encryption would be a necessity for data moving between two virtual systems in the Amazon cloud.

* Cloud Computing is a fundamentally new approach that allows Internet users (including companies and individuals) to tap almost instantly all the data, software, storage, and computing power the user needs.

Not only are security controls important, Ritchey said, but the transparency of the implementation of those controls — for people relying on someone else's infrastructure — is a key consideration. Ritchey believes sharing infrastructure will only strengthen the cloud in terms of capacity as well as security.

The fact that cloud computing allows data providers to offer self-service models to individuals and organizations has both positive and negative implications. Since many different systems may be running in a single environment, with different levels of security controls, the weakest link may create security issues.

Sharing is Key

The concepts of sharing and security are traditionally at odds with each other, Tim Grance, Program Manager of Cyber & Network Security Program for the National Institute of Standards and Technology (NIST), said sharing is the key to cloud computing's success. Resource pooling reduces costs. When data is shared freely, it facilitates innovations and limitless social benefits can be derived from it. Are there security risks associated with cloud computing? Sure, but Grance espouses optimism about cloud computing, saying "We can do this. We can get there."

Grance described a future with seamlessly moving work flows and economics and other demands that would lead to optimizing efficiency, all facilitated by and through the cloud. His agency, NIST, uses a definition framework that breaks the system down into three deployment models: the private cloud; the community cloud; and the public cloud. There also are three service models: software as a service; platform as a service; and infrastructure as a service. All share the essential characteristic of on-demand self-service.

The advantages of cloud computing, Grance said, are cost reduction, scalability and, agility. That agility allows cloud users to facilitate quick innovation, which is the model's key benefit. For example, consider gene sequencing. The value of large-scale data analytics cannot be overstated for this type of project. And as for workforce capacity, or simply tapping into great minds thinking along the same lines, cloud computing technology could make it possible in the not too distant future to send email to an endless list of agencies within a single government cloud.

Innovation, Grance said, is the big win. He cautioned cloud users not to be paralyzed by security and privacy issues and advises users to steer orderly migration where appropriate and negotiate service level agreements carefully.

High Expectations

Now may be one of the most challenging times in terms of navigating security concerns in the cloud, said Henry Sienkiewicz, Technical Program Director of Computing Services for the Defense Information Systems Agency (DISA). He pointed out that "we are at the peak of inflated expectations" for cloud computing.

As someone who works with an organization that helps the Department of Defense with combat support computing (everything from providing command and control to managing parts and replenishing supplies to providing troops with medical care, paying war fighters and coordinating transportation), Sienkiewicz has a unique view of cloud computing. He sees one key challenge as finding a way to take platform-centric worlds and change to a service methodology. This requires a shift from purely platform delivery to a holistic system.

Enter the cloud, a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources — networks, servers, storage, applications and services — that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Web 2.0 technologies have allowed companies that support the Department of Defense to incredibly streamline the military decision-making process, something cloud computing can continue to benefit, Sienkiewicz said. What used to be an 18–24-month timeframe for procuring supplies, for example, has been shaved down to 3–6 months. While he also grapples with the safe, secure use of social media and understands concerns with security in the cloud, he agreed with other panelists that such concerns shouldn't hamper progress.

Cloud computing's "rapid elasticity" that allows for broad access, on-demand self-service, and resource pooling lends well to four models. The acquisition model is based on purchasing of services. The technical model is scalable, elastic, multi-tenant and sharable. The access model brings data over the network to any device. And the business model is based on pay for use. An example of that might be the music subscription services such as Rhapsody and Thumbplay that charge $10 per month for access to virtually any song or album.

Software-as-a-service is now available via the cloud. Platform/infrastructure-as-a-service might not be immediately available, but it's a much quicker process due to the cloud computing capabilities.

Public Opinion Matters

Michael Nelson, visiting professor at Georgetown University and a long-time Internet scholar said convincing people that the cloud will be secure is equally important as actually securing the cloud. And that's important, he believes, because while about 2 billion people now access the Internet through computers, laptops or smartphones, there will be hundreds of billions of

Internet access devices in the future. And the devices that allow for connections will do so cheaply.

Nelson believes that in the next five years, 80 percent of all computing worldwide will be done in the cloud because of the economics and advancing technology. For that enormous shift to occur, though, there must not only be an agreement on standards, which practically exists today, but people must actually use the standards.

The security in a cloud must be tight. The cloud's incredibly flexible platform of course brings up security concerns because people can misuse it, they can find vulnerabilities, and the most maleficent can do real damage.

In the area of security, culture becomes a challenge, Nelson said, because people generally are resistant to change. The old idea of a "fortress with a firewall" doesn't work in the cloud. Breaking through the old mindsets highlights the need to track data movement and usage and show customers can track access to data.

Nelson said that when faced with management opposition to adopting cloud computing, remember this is not a migration to outsourcing data to another organization. The cloud computing model makes it easier to access more data.

No one, including Nelson, would argue that cloud will have perfect security, just as none of today's systems have such perfect security. Yet every day, a lot of exciting work is in play to make the cloud work for everyone. Inevitably, what might stymie the effort will be culture — including acceptance by the masses — and management hesitation to jump into what can be seen as a great abyss, security-wise.

Money Talks

While countless students have been using the cloud for years by accessing such services as Gmail, Dan Kent, Federal Systems Engineering Director for Cisco Systems, said he deals with many federal agencies that struggle with cloud computing. The dichotomy springs from issues with control and trust. These agencies, for example, have much more at risk than a grade-schooler or even a small start-up company. Still, Kent tells agency officials about the benefits of cloud computing.

Kent ties this technology to cost savings and flexibility. The benefit of time to delivery means organizations can quickly meet their mission requirements without spending six months setting up servers. The data platform already exists.

Kent stated that for the three cloud models: software-as-service, infrastructure-as-service and platform-as-service, each comes with different levels of responsibility. These responsibilities

apply to virtual private cloud, public cloud or community cloud, all of which need to pay attention to maintain security boundaries for the user.

Migrating to cloud technology does not have to be a light-switch move. Kent advises agencies to evolve from consolidation to virtualization to automation to utility to market. He also believes cloud access is possible before security outside an organization by taking a "pragmatic, evolutionary approach." That might include a cloud security architecture built on a cloud service security layer, a cloud edge protecting the cloud provider network, an enterprise and data center edge and a security services layer, topped by a secure virtual access layer. Above all, Kent said, users must first "get your own house in order" with security and then expand to the cloud.

Strong Coalitions

Nils Puhlmann co-founded the Cloud Security Alliance, which started as a handful of interested computer professionals and has rapidly expanded to 8,000 members worldwide. Five hundred of the alliance's members put together a guide on cloud computing because the issue is undeniably global.

For example, the Japanese government has a large cloud initiative, and the European Union is exploring ways to use the cloud for e-health efforts.

Yet while security principles and philosophies haven't changed, the computing culture certainly has changed because of a shift in the model of how to use technology to get things done. Social media including wikis, which can change moment by moment, devices such as iPhones and the like mean agility knows no bounds.

Puhlmann said the lack of transparency about security models is understandable — who wants to post their security infrastructure on the Internet and be pummeled with attacks? So the challenge is to share risk-based security without compromising anyone's proprietary information.

Security, Puhlmann said, has not kept pace with the culture shift. By and large there's still the promotion of anti-virus technologies, even though they have been shown to be largely ineffective. There's still a focus on finding the attacker, even though that's becoming an increasingly difficult goal to accomplish.

Puhlmann suggested the answer lies in offering services that allow individuals to have access to the same data, the same transparency, so they can continue to serve their companies by providing risk-based security information and trends. Cloud computing, by its very design, could potentially solve some traditional security problems, not the least of which is storing data in one, vulnerable place — a static target.

By moving away from the concept of that static target, or sitting duck, data moves around the cloud. Thus, attackers don't know where the data is at any given time.

Looming Questions, Possible Solutions

When it comes to security in cloud computing, concerns include the multi-tenancy aspect. In other words, can you trust an infrastructure provider to keep data separate if you and your competitor share that infrastructure? There's an absolute need for security governance to protect weak links from security breeches. Another concern is network access, or how to keep data available without compromising proprietary information.

The answer to some of those concerns lies in standards, in which the National Institute of Standards and Technology plans to play a leading role, service level agreements with built-in security clauses, and legal language that translates across national boundaries because the cloud certainly knows no home country.

Who will actually drive security in the cloud? Forum participants touched on the role the government, the market, and even academia might play. What's certain is that security problems will only be solved through collaboration, the very strength of the cloud computing model.

The cloud is still in its infancy, and its strengths — including speed and agility — point to encouraging possibilities on the security front. That is, if the computing community works together to ensure security is woven into the fabric of future versions of the cloud.

RESOURCES

www.gwu.edu/hspi/policy/issue_cyber.cfm: HSPI's Hot Topic--Cyber webpage
http://www.cloudsecurityalliance.org/: Cloud Security Alliance (includes downloadable guidance document)
www.sourceforge.net*:* For downloading and developing free open source software

"Reading Assignments" given by Michael Nelson and Tim Grance at the event:
(2008) Let IT Rise. The Economist (subscriber/registration only. Available here from a third party)
Carr, Nicolas. (2008) The Big Switch. W.W.Norton
Christensen, Clayton. (2003) The Innovator's Dilemma. HarperCollins
Various OECD papers on Cloud Computing. Organization for Economic Cooperation & Development

Introduction to Cloud Computing:

Geelan, Jeremy. (2009) Twenty-One Experts Define Cloud Computing. Cloud Computing Journal
Cheng, Roger. (2010) Cloud Computing: What Exactly is it Anyway? Wall Street Journal
Federal Cloud Computing Services. US General Services Administration
Hanna, Steve. (2009) Cloud Computing: Finding the Silver Lining Juniper Networks
Gardner, Dana. (2010) Executives Experimenting With Mostly 'Private' Cloud Architectures Cloud Computing Journal

Technical Cloud Computing Reports:

(2009) Private Cloud Computing for Enterprises: Meet the Demands of High Utilization and Rapid Change. Cisco Systems
Rayport, Jeffrey F. (2009) Envisioning the Cloud: The Next Computing Paradigm. Marketspace
Grance, Tim. Mell, Peter. (2009) Effectively and Securely Using the Cloud Computing Paradigm. National Institute of Standards and Technology

Security and Cloud Computing:

(2009) Security and Cloud Computing. Booz Allen Hamilton
(2009) Cisco 2009 Midyear Security Report. Cisco Systems
(2009) ENISA Clears the Fog on Cloud Computing Security. European Network and Information Security Agency
Hanna, Steve. (2009) A Security Analysis of Cloud Computing. Web Security Journal
(2009) Security Guidance for Critical Areas of Focus in Cloud Computing. Cloud Security Alliance
Brodkin, Jon. (2008) Gartner: Seven Cloud Computing Risks InfoWorld
Binning, David. (2008) Top Five Cloud Computing Security Issues. Computer Weekly
(2009) Security Issues Hobble Cloud Computing. Homeland Security Newswire
(2009) Building Customer Trust in Cloud Computing With Transparent Security Sun Microsystems

Cloud Computing in the Government Sector

(2009) The Government's Effective Migration to a Cloud Computing Environment. Booz Allen Hamilton
Arthur, Charles. (2010) Government to Set up Own Cloud Computing System. The Guardian
(2009) Cloud Computing in Government. IBM Center for the Business of Government
Foley, John. (2010) Air Force Seeks Secure Cloud Computing. Information Week
Claburn, Thomas. (2009) Google Plans Private Government Cloud. Information Week
(2009) Industry Perspectives of Federal Cloud Computing at FOSE. Booz Allen Hamilton
Beizer, Doug. (2010) Cloud Computing success depends on knowing what to ask. Federal Computer Week
Calabresi, Massimo. (2009) Wikipedia for Spies: The CIA Discovers Web 2.0. Time Magazine
Hoover, J. Nicholas. (2009) Department of Defense Pursues Private Cloud. Information Week
Roth, Bill. (2009) CIA Falls for Cloud Computing in a Big Way. Web Security Journal

Frank J. Cilluffo *is Director of The George Washington University Homeland Security Policy Institute (HSPI).* ***Ron Ritchey*** *is a Principal at Booz Allen Hamilton, Inc.* ***Timothy Tinker*** *is Director of the Center for Risk and Crisis Communications at Booz Allen Hamilton, Inc.*

Founded in 2003, The George Washington University Homeland Security Policy Institute (HSPI) is a nonpartisan "think and do" tank whose mission is to build bridges between theory and practice to advance homeland security through an interdisciplinary approach. By convening domestic and international policymakers and practitioners at all levels of government, the private and non-profit sectors, and academia, HSPI creates innovative strategies and solutions to current and future threats to the nation. The opinions expressed in this Issue Brief are those of the authors alone. Comments should be directed to hspi@gwu.edu.