In Cloud Computing We Trust—But Should We?

While many presentations on cloud computing still start with a definition, it won't be long before cloud computing just becomes another type of computing as we know it. Cloud computing is gaining significant market traction because companies from startups to large enterprises alike can quickly leverage an infinite supply of compute power to scale to customer demand while paying only for the resources they consume.

Anup Ghosh
Invincea

Iván Arce
Core Security Technologies

One effect of this move to cloud computing is the breaking down of entry barriers to competition. Small and even startup firms no longer need significant capital (CapEx) to purchase racks of servers and their associated maintenance costs in order to start offering services online. Instead, they can instantly provision a server image online with Amazon Web Services, for example, or lease an off-the-shelf Web server from a company like RackSpace. Even better, if the offering catches fire on the Internet or commercial market, a robust cloud computing service can scale to demand instantaneously instead of risking the demand outstripping server capacity.

Even large firms are quickly adopting cloud computing to take advantage of the decreased costs that result when dropping multimillion-dollar operating expense (OpEx) obligations that go hand-in-hand with managing server farms. Instead, they're adopting public cloud computing services to achieve economies of scale in a shared infrastructure, thereby enabling them to cut costs while focusing on their core business. In other words, the economic value cloud computing brings is compelling and driving adoption forward at a rapid pace.

While the CapEx and OpEx numbers are propelling cloud computing adoption from a business case perspective, the most significant barrier to full adoption across enterprise services is trust. We deliberately use the term "trust" instead of "security" because it isn't yet clear that security is deficient or sufficient in the cloud computing offerings on the market today. Rather, the uncertainty associated with security and privacy of cloud computing services is contributing to a sense of unease when moving valuable corporate IP, sensitive corporate documents, and customer and personnel information to public cloud-based services. Until the industry can provide evidence of trustworthiness either through meaningful standards or a consistent historical record of protection and robustness of service, security and privacy concerns will continue to provide significant friction against cloud computing adoption.

Centralizing Management and Risk

A strong motivation to move to a cloud computing service provider is to centralize server management, and, potentially, even desktops, to a professional management service. In a very large organization with several different business units spread geographically, this can give the corporate CIO the ability to apply corporate policy or industry governance, compliance, and regulation uniformly across the enterprise. Centralizing the management of computing resources in a cloud computing environment, whether private or public, can provide

uniform and consistent quality and compliance for all business unit services.

The flip side of centralizing computing resources is concentration of risk. By putting all your eggs in one basket, so to speak, you're also providing a fairly attractive target for an adversary. In addition, uniform management of computing resources tend to dictate a homogeneous computing infrastructure in practice. The result is that a single vulnerability—for example, in a Windows server—becomes a risk for all enterprise services for all business units. Cyber miscreants and industrial spies understand this well and favor homogeneous infrastructure implementations for this reason.

An interesting case study of this effect is virtual desktop infrastructure (VDI). Virtual desktop implementations move to a cloud computing service model in which desktops are cloud hosted—initially in private clouds—and thin clients are used on "dumb," perhaps even diskless, PCs to connect to the VDI. A cloud service provider now manages the desktop rather than either the individual user or the local IT shop in a business unit. From a governance, compliance, and regulatory standpoint, the centralized management of the desktop in the cloud is attractive because software patches can be applied uniformly and in a timely manner.

On the other hand, by centralizing the desktop, including data storage, in a cloud infrastructure, an adversary no longer has to search for interesting data by hopping from desktop to desktop within an enterprise, while dealing with the friction points of different OS implementations. In fact, the cloud-hosted desktop ensures homogeneity in infrastructure down to the service pack and patch level. Now, for instance, a single user's ill-advised click on a link from a Facebook friend may result in a kernel-level rootkit in a Windows server that's hosting his virtual desktop. Once the server is owned, the 100-plus employees that share this server are now compromised, reducing the work factor for the adversary considerably. Because this user's privileges are now owned as well as the server's administrator account, data for all users—which is also centralized in the cloud—is now potentially susceptible to exploitation. In other words, while management has been centralized and the benefits that accrue with that transition are realized, risk is also centralized—along with additional risks that are immediately inherited with this regime.

Finally, while diskless "dumb" PCs might seem to be the future, it's worth noting that in practice, we'll continue to see standard desktop machines on every desktop in an organization, even as cloud computing initiatives increase. In the case of VDI, the short-term impact will be management of twice the infrastructure—one for desktop machines on the desktop, and another for virtual desktops in the cloud. As VDI and other cloud-related initiatives are spun up and out, consideration for transitioning from current practices to future cloud implementations will require planning, resources, and a risk management strategy.

The Cloud Opportunity: A Clean Sheet

While the opportunity to centrally manage cloud computing assets is a business driver for cloud computing, we in the security community would be remiss if we didn't highlight another unique opportunity cloud computing provides—a clean sheet. Cloud computing is largely implemented as an abstraction layer with a well-defined interface. In other words, the service implementation is a black box to the clients requesting the service because they have no need to know or understand the implementation. This is a clean sheet opportunity for the security community to innovate in the space of this black box, to provide secure and private cloud computing services—albeit with transparency for those paying for the implementation. The opportunity is to inject security innovations in a computing infrastructure at its nascent stage before the infrastructure becomes locked, as it is on the desktop.

The opportunity hasn't been lost on the US government. The federal CIO, Vivek Kundra, has spoken on the government's initiatives to modernize existing stove-piped IT systems in agencies with cloud computing initiatives to cut costs and redundancy. Second, under the auspices of the White House's Office of Science and Technology Policy (OSTP), a Cyber Leap Year Summit was held in August 2009 to develop game-changing approaches to cybersecurity. The results of this effort were three areas released by the Networking and Information Technology and Research and Development (NITRD) office: Moving Target Defense, Tailored Trustworthy Spaces, and Cyber Economic Incentives. These initiatives were given significant backing when the director of the Office of Management and Budget (OMB) sent a memo in July 2010 directing all federal department and agency heads to include these initiatives in their fiscal budget planning for 2012.

We in the security community would be remiss if we didn't highlight another unique opportunity cloud computing provides—a clean sheet.

In the context of cloud computing, all three of these game-changing themes have a role to play. Moving Target Defense strategies enable a cloud computing infrastructure to continually change its

attack surface to create uncertainty for adversaries targeting cloud computing services. By making the attack surface of a cloud implementation dynamic and uncertain, the risk of concentrating your assets in the cloud as described earlier can be substantially mitigated.

Likewise, a cloud computing service is an ideal mechanism for implementing a tailored trustworthy space for a collaborative environment between multiple parties. In such a space, the computing environment and security mechanisms such as identity, authentication, and computing infrastructure are prenegotiated and then provisioned on demand for the service or for a trusted transaction between known parties. In fact, development of tailored trustworthy clouds on demand can be exemplars for the study of cyber economic incentives. As uncertainty is reduced and trust is built around a tailored trustworthy cloud service, an economic model for pricing in security might emerge and encourage full enterprise adoption. Cloud computing provides opportunities for innovation in cybersecurity that may spur adoption in return.

Addressing the Inherent and Inherited Risks in Cloud Computing

Clearly, moving to a cloud-based computing paradigm presents new security and privacy challenges. While it might not be immediately evident what those challenges are, some of them will be inherent to the cloud-based model, while others will be inherited from existing computing models that are either used in cloud computing or interconnected with it. For example, security practitioners have traditionally mapped intangible assets such as proprietary data, algorithms, and other intellectual property to tangible, physical ones such as specific computer hardware, IP addresses, storage systems, or network equipment. In a cloud-based service, this mapping, which previously was used to "secure" fixed assets later in order to manage the risks of intangible assets, no longer applies because the mapping is dynamic.

In this context, pooling data storage resources and their use through APIs that abstract the actual physical medium pose threats at the data deduplication, location, retrieval, and processing layers that can't be easily mapped to any particular group of tangible assets in a cloud computing environment. This forces security practitioners to rethink their data security practices and solutions in light of a risk scenario previously unaccounted for that is inherent to the cloud model.

On the other hand, cloud-based computing will also inherit risk from standard desktop, server, and mobile computing models and from a large menu of other known components that cloud computing providers combine to build their infrastructure and to deliver services. For instance, a PHP Web application running on cloud-located servers with a standard COTS operating system and globally accessible via Wi-Fi or 3G networking using Web browsers on desktop computers and smart mobile devices will be vulnerable to all the known threats of each of the component technologies, plus have the additional risk resultant from combining them together in a service.

To the security practitioner, identifying and understanding the inherent risks of cloud computing while grappling with the inherited risks from an interconnected infrastructure and common vulnerable components may seem academic to some and daunting to others. Regardless, adopting cloud-based computing services will require knowledge of these risks and a risk management strategy to address them appropriately.

While we won't prognosticate what challenges lie ahead in security and privacy for cloud computing, we can be certain that many will emerge. It will be imperative for cloud service providers to be as transparent as possible about these challenges and risks as they develop for the industry to mature. As in every other market and industry that adopts inter-networked computing, security challenges always emerge, and almost always security is "bolted on" after the fact, rather than designed in from the start. The opportunity to build security in from a clean sheet should not be lost on the technical security community.

In this issue of *IEEE Security & Privacy*, we're proud to bring industry thought leadership and innovative approaches to cloud computing security. We are fortunate to present a virtual roundtable of thought leaders from the Cloud Computing Security Alliance and leading cloud service providers including Google, Microsoft, Amazon, and Cisco. We also present five articles on cloud computing security that lay out challenges and potential approaches to address them. Our goal with this special issue of *S&P* is to stimulate thoughtful discourse, convey knowledge, and encourage innovation in cloud computing security. □

Anup Ghosh *is founder and chief scientist of Invincea, a venture-backed security company developing next generation Internet security products to protect desktops and computer networks. Ghosh is also a research professor in George Mason University's Volgenau School of Information Technology and Engineering. He has a PhD in electrical engineering from the University of Virginia. Contact him at akghos@gmail.com.*

Iván Arce's *biography can be found on p. 10.*