The Future of Secure Data in the Cloud

David Saer – Foresight Researcher

Given the expected growth in adoption of cloud computing, what new security challenges arise and how can we address them?

Cloud Computing – An Infrastructure Solution for a Changing World?

As organisations prepare for an uncertain and potentially turbulent decade ahead, greater emphasis is being placed on increasing flexibility and agility, reducing asset ownership and controlling costs. In response, a growing number are turning to cloud computing for the provision of many ICT infrastructure and data management services. As a consequence, a variety of interesting questions have emerged surrounding the opportunities and challenges posed by adopting cloud based solutions.

Cloud Computing – Promise and Payoff

A simple definition of cloud computing is the use and availability of virtual servers over the internet, in effect the outsourcing of ICT infrastructure, data management and application hosting to an external provider. Turning to outsourcing partners can bring potentially significant cost savings to businesses. For example, users of cloud based services no longer need to invest in purchasing costly servers to hold data and run their ICT services, or employ the personnel needed to manage them.

A key attraction of cloud computing is the promise of greater flexibility and agility. This is especially attractive to start-ups, as businesses can expand or contract their ICT capacity on demand at a comparatively low cost. This can be seen to reflect a broader trend in business towards rental over ownership in an attempt to manage costs and assets – shifting the expense from a capital to expenditure model.

Security Panacea or Pain?

The implications of this move towards storing data remotely in the cloud could be transformational in terms of security. For example, having the vast majority of ICT infrastructure located and run externally could resolve many traditional security problems related to poor ‘cyber hygiene’. Cloud based solutions also reduce the risk of insider threats, where internal staff are the conduits of threat through incompetence or malicious intent.

A major fear is that, as companies outsource their ICT to cloud based infrastructure providers, they are creating large targets full of the valuable data of multiple companies. There are also the issues of the trustworthiness and reliability of the external providers and the risks posed by ‘multi-tenancy’, where different potentially competing companies occupy the same cloud infrastructure. Can businesses trust the data content and intentions of those

they share the cloud with as well as the administrators in control? Similarly, to what extent should cloud providers trust the data content and intentions of their customers? How much access should these 'hosts' be allowed to verify the quality, legality and reliability of customer data and applications stored on their servers?

Rethinking the Security Paradigm

As companies look to secure the cost savings promised by cloud computing, the burden of responsibility for security has shifted to the cloud infrastructure providers to help protect their customers from malicious actors within and outside the cloud. As a result pre-emptive security and verification are becoming a priority for the vendors of cloud services. For example, HP has focused its research and development efforts on providing a safety-net for their customers. HP's approach is to attempt to build in a comprehensive level of security into their cloud services from the outset of hosting a new customer. The aim is to prevent the theft of data, limit the damage caused by any successful break-ins, and protect end users from failures of the system or any accidental or malicious actions of an administrator.

Pre-emptive security represents a crucial departure from the more traditional approach where systems have had to have security retro-fitted because it was never an issue when they came into being. The new approach emphasises designing security in from conception of the hosting arrangement. For example, the HP model features built in sensors which monitor for unusual activity, and immediately shut down servers that are reporting and inflicting attacks. On top of this, Businesses will increasingly be able to customise the level of security from their cloud infrastructure provider in relation to need by paying for more sensors and security features as required.

The Future of Cloud Computing

This growing focus on infrastructure security is a positive trend given the growing number of businesses moving towards cloud computing models. Security will remain a top concern and is expected to be a lucrative business for those who provide it. IDC estimates the cloud security market could be worth $6 billion annually by 2015.[1] However, many questions still remain in relation to the future of secure cloud computing:

- *What further security considerations does the move to cloud computing present, and what future problems could it create?*
- *What different models of security will evolve around cloud computing?*
- *How can we assess and verify the quality and robustness of the ICT infrastructure security offerings of infrastructure providers?*
- *Will the trust issues surrounding multi-tenancy dissuade some businesses from switching to the cloud?*
- *Could a hybrid model emerge where firms retain their own servers for key data but are willing to outsource other functions and services?*
- *Would a massive security incident derail or just delay uptake of cloud computing?*
- *On the issue of legality, where does responsibility lie, with the data owners or infrastructure providers?*

[1] Cloud Pro, 20/07/2011, http://www.cloudpro.co.uk/cloud-essentials/cloud-security/1321/cloud-security-market-set-hit-6-billion-2015

About Fast Future

Fast Future is a research and consulting firm that works with clients around the world to help them understand, anticipate and respond to the trends, forces and ideas that could shape the competitive landscape over the next 5-20 years. Our work draws on a range of proven foresight, strategy and creative processes to help clients develop deep insight into a changing world. These insights are used to help clients define innovative strategies and practical actions to implement them. Clients include 3M, Astra Zeneca, E&Y, GSK, IBM, Intel, KPMG, Nokia, Novartis, O2, Orange, PwC, SAP, Sara Lee, twofour54 and the OECD. We also work with a range of city and national level government entities around the world.

david@fastfuture.com