The NSA Scandal's Impact on the Future of Cloud Security

Data Security and Protection in the Wake of the Spying Scandal

Contents

Introduction to Cloud Security vs. Big Brother

Pity Cloud Providers: they worked hard to gain public trust in the security of their platforms, and they seemed to be making progress; but then Edward Snowden, a computer consultant for the NSA, came along. Snowden leaked classified information about top-secret government surveillance programs that snoop on cloud users, and called cloud-based information security into question.

Then, news broke that federal agencies attempted to obtain the master encryption keys that Internet companies use to shield millions of users' private communications from spying and eavesdropping.

The ensuing paranoia in the wake of the PRISM scandal may be excessive, but it is opening up interesting conversations with questions that must be addressed:

- How secure is the corporate information residing in Infrastructure as a Service and Platform as a Service clouds?
- Can the government – or indeed anyone with a court order - lay its hands on that information without anyone knowing about it?
- Does encrypting your cloud data protect you, or is that an illusion?
- What measures do you need to take to guarantee security and maintain compliance in the cloud?

Though this scandal brings to mind the Orwellian ethics of Big Brother, we will leave the more philosophical (or legal) debate of whether the government has a right to spy on its citizens for others. Instead, we will address the practicalities and explain how you can **keep your data private and secure**.

Cloud Economics

Though the NSA scandal has shined a light on surveillance in the cloud, the reality is that this is not the only way a government can access your data. The headlines love a scandal, but the NSA news is only an example subset of a bigger, more important question: can anyone with a court order (not necessarily a government entity with a court order) have access to your private cloud data?

The government can indeed have backdoors in your cloud provider's hypervisor. However, they can also have backdoors in your operating system (maybe on your laptop) or your network (perhaps on your router), using the same laws to demand cooperation from the vendors. So the cloud is not uniquely vulnerable in this respect.

The cloud is “special” because it allows any snooper (including, but not limited to the government) to scan massive amounts of cloud-based information, without regard to who owns it, and WITHOUT needing to open specific backdoors to specific resources.

Remember, even for the government, there is a question of cost-effectiveness. Scanning all the data from a cloud provider is relatively easy, because massive amounts of data from multiple owners is all available in one virtual place. In fact, many of the cloud providers scan it regularly themselves (for advertising purposes, or even security scans).

Though possible, scanning your laptop through a backdoor is less likely, because it requires a specific decision to chase after YOU. In other words; the “economics” of PRISM are simple: it is a huge net that catches all fish, rather than a fishhook that targets one fish.

So how can law-abiding companies avoid getting caught in the fisherman’s net?

A Two-Part Solution

The juxtaposition of information security best practices, compliance with regulations like PCI DSS and HIPAA that require you to protect your data, and now the government trying to access encryption keys – all brings us to the question of control.

The obvious answer to privacy concerns is to keep control of your private things. If you do not want anyone reading your data, keep it at home under lock and key. But in today’s modern lifestyle, where the web – in both private life and commerce – has become ubiquitous, locking up your data takes on a whole new meaning.

Ideally, you want to use the cloud freely and at the same time, maintain your privacy. The perfect solution would be to use all the solutions from cloud providers, encrypt your data, but keep the master cloud encryption keys for yourself.

Think about it: the PRISM scandal would not be possible if not for the fact that Cloud Providers – commercial entities – own the master encryption keys to much of the internet. The NSA went after the Cloud Providers because they own these keys. And cloud providers do obey the law, which means that if the law is on the government’s side – they must comply and hand over your private information.

The only entity that has your own best cloud privacy interests at heart – is you. And yours is the only entity that should control your master cloud encryption keys. Not the cloud providers, or a third party security vendor. Only you.

Which means that the only logical solution must have two parts: strong encryption of the data and secured management of encryption keys.

Part One: Encryption

Indeed, when looking at cloud security, cloud encryption is often one of the first solutions that come to mind. Encryption enables an organization to build "mathematical walls" around the data and therefore, keep prying eyes away from the sensitive data.

The most secure data encryption solutions must support all of the major business use cases: full disk encryption, database encryption, file system encryption, distributed storage encryption and even row or column encryption.

To get technical, a good encryption solution must also:

- Use strong data encryption; for example, the Advanced Encryption Standard (AES) encryption algorithm with a 256-bit key.
- Understand how to use encryption correctly; for example by correctly choosing your block encryption techniques, countering fingerprinting attacks correctly, or correctly generating random values for keys.

Part Two: Key Management

High-quality encryption is very important but many tend to forget that encryption is only one part of the cloud security solution. The second and more complicated part is key management. Think about the following scenario: your information resides in cloud infrastructure, you encrypt your data, but the encryption key resides unencrypted in your virtual server or with hardware owned by the cloud provider. In such a scenario – data encryption achieves very little.

To effectively encrypt and secure your cloud data, there's a need for a different key management approach. One that is designed specifically for the cloud rather than "welded" to it. An example for such technology is split-key encryption.

Split-key (as the name insinuates) splits an encryption key in two (or more) "parts." One "part" is known only to the end user, while the second is known to an automated, secure key-management system. The two half keys are joined inside the customer's IaaS account.

A related technology, Homomorphic Key Management, can be used to ensure these key "parts" are always encrypted – even while in use inside the customer's IaaS account – so the cloud provider never knows the keys. Even the automated key management system itself - actually never knows the keys – since they are *always* encrypted!

These techniques enable true cloud security by guaranteeing, for the first time, that the encryption keys are not visible to the IaaS provider, nor even to the security provider, while running as a 100% cloud solution (to read more – download the white paper **here**).

Conclusion: Securing the Cloud

Cloud security can be achieved. Your data can be safe. You can trust cloud solutions.

To do so, there's a need for a new perspective and new tools designed for the cloud. Implementing traditional security systems, or trusting the cloud provider to secure your information for you, simply won't cut it anymore.

You must be sure that you, and only you, own your keys.

That means that you cannot opt for a solution that is controlled by anyone other than yourself. Specifically, avoid a solution that is owned by your cloud provider, since such an approach is open to subpoena.

This brings up a contradiction. How on earth can you use the cloud's full potential, yet defend yourself from your cloud provider and keep key ownership to yourself?

Our advice: try split-key encryption, a technology in which you keep control even in the cloud; and homomorphic key management, a technology that encrypts your encryption keys, even at the time when they are being used by you. The combination of these two technologies gives you an enterprise-worthy assurance that only you control your encryption keys.

What level of paranoia is justified in the wake of PRISM? The truth is, no paranoia is necessary if you take proper steps to understand your exposure to risk and to properly protect yourself. These technologies change the economics of surveillance – making you the fish that swims its own path, rather than with the school of fish that gets caught by the Big Brother fishnet.

About Porticor

Porticor Virtual Private Data (VPD) is a comprehensive solution that combines strong encryption with patented key management so you can both protect information and maintain privacy and security in the cloud. Porticor VPD encrypts the entire data layer including virtual disks, databases, files, object storage and more. It also addresses the processes necessary for managing your encryption environment and encryption keys. It provides the strong security needed for security and compliance in a convenient, cost-effective, fully cloud-based solution.

Like a Swiss banker offering a traditional safety deposit box, Porticor requires two keys to encrypt or decrypt an object. Each key is encrypted to protect it while it is resident in your cloud account using patent-pending homomorphic key management technology.

With Porticor, you hold a Master Key which is never present in the cloud in a plain, unencrypted form. Therefore you retain control of your encrypted data – without having to install and maintain expensive key management servers on premise. Porticor VPD is the only pure cloud solution where you – and only you – hold the key to your data.