Porticor™ Virtual Private Data™

DATA ENCRYPTION AND KEY MANAGEMENT

YARON SHEFFER, APRIL 2011

There are many benefits in moving your IT operations to the cloud. Cloud Computing is attractive because of its operational and economic advantages. Cloud computing is flexible, allowing you to spin up (or down) servers as needed, and to use seemingly unlimited amounts of storage. You pay only for what you use and only for the time that you use it.

But cloud computing requires data security and privacy: you may need to comply with regulations, such as PCI DSS or HIPAA, or you may find that your reputation, brand or competitive edge depends on keeping your data to yourself. These issues should be top priority when moving to the Cloud, and they are under your *responsibility*. In fact, a typical cloud provider agreement explicitly states that "you bear sole responsibility for adequate security, protection and backup of your Content and Applications…"

The Porticor Virtual Private Data™ (VPD™) solution provides your sensitive data with strong security and privacy guarantees; it offers the flexibility you expect in the Cloud, and a short time-to-solution; wrapped in an affordable, pay-as-you-go and "cloud-friendly" price.

Porticor VPD™ encrypts the data and protects it from unauthorized modification, using a unique technology and an easy to manage cloud-based appliance. Porticor VPD™ allows you, the customer, to retain complete ownership of your most important business data, by using an innovative key management system. This breakthrough technology ensures that nobody but yourself – not even Porticor – knows your keys. Not only is your data protected from outside access, the Porticor™ key management system ensures that the data is never accidentally lost.

THE CLOUD AND ITS RISKS

When an IT application is moved to a public cloud, all of the old security risks associated with it in the past still exist. In addition, there are new risks vectors: where previously your servers along with your data were physically protected within your server room, now the “virtual servers” and “virtual storage devices" are potentially accessible to anybody able to breach the protections enacted by the cloud provider.

The green data storage (e.g. disk volume) in Figure 1 is being threatened from three new directions:

1. The first attacker is someone who was able to breach the access control provided by the cloud provider, possibly by stealing your cloud access credentials or exploiting vulnerabilities in the cloud access control infrastructure.
2. Attacker #2 is coming from another server in the same customer account within the cloud; this may be a server which belongs to a different project of the same customer and that should not receive access to the data. This attacker might have legitimate access to Virtual Server 2, or may have breached it using, for example, one of the thousands of known Web application vulnerabilities.
3. Another potential threat is coming from an insider (attacker #3) within the cloud provider’s network.

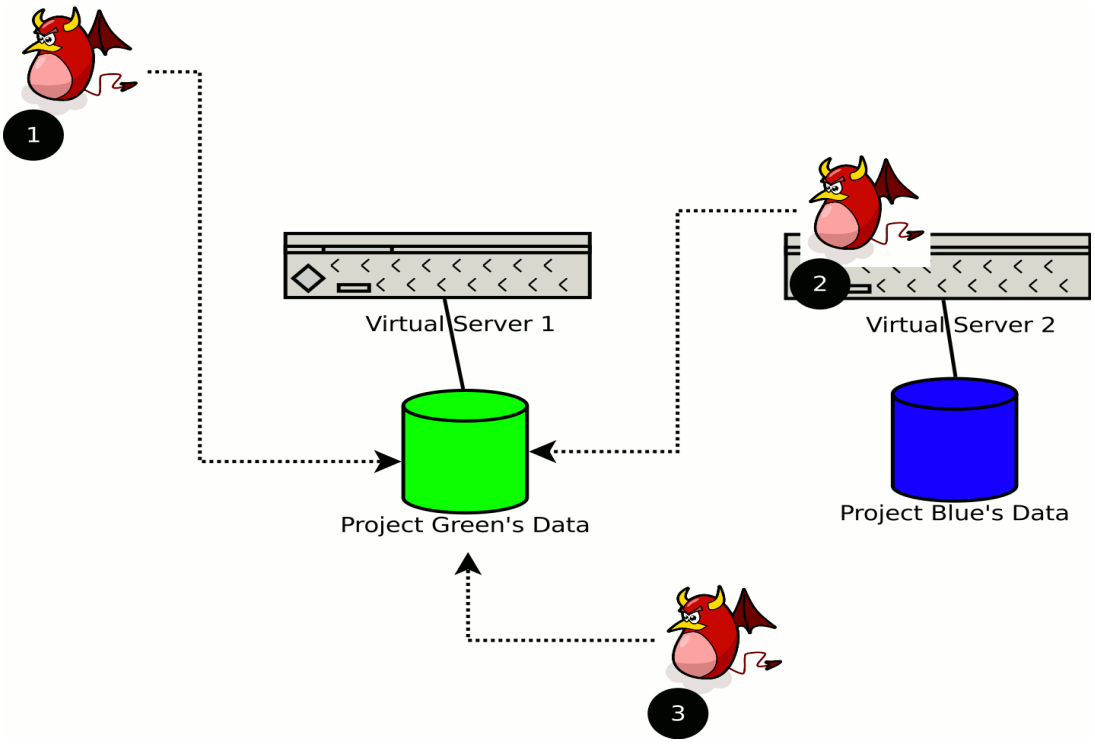

FIGURE 1 NEW THREATS TO DATA IN THE CLOUD

These new threat vectors are, of course, added to all the "old" threat vectors that were relevant when the application was in a physical server room. (Note that Porticor also offers solutions to many of these "traditional" security issues; these however are beyond the scope of this paper).

DATA ENCRYPTION TO THE RESCUE

For the last few years, encryption has had an ever increasing role in data protection. The most secured solutions, utilized full disk encryption, and decrypted only the relevant parts for reading.

Porticor™ applies the same encryption technology to virtual disk volumes, and distributed storage (e.g. Amazon® S3) in the cloud

Each disk block written by your application (e.g. by a database server) goes through the Porticor™ virtual appliance, where it is encrypted and sent to the disk volume. At no point is the plaintext data written to persistent storage. All requests to read data from the disk similarly go to the Porticor™ appliance, which reads the encrypted data blocks, decrypts them and sends the plaintext data back to the requesting application.

Porticor™ technology includes a unique ability to "hook" the Porticor™ solution between the customer's storage and the customer's servers in the cloud (i.e. applications, databases). This "hooking" technology is transparent to the customer, though of course it requires the customer's permission, and allows the Porticor™ solution to be injected without any changes to the customer's project code: quickly, automatically and transparently.

Porticor™ uses the industry-standard high grade Advanced Encryption Standard (AES) encryption algorithm, with a 256-bit key. Multiple blocks are chained using Cipher-Block Chaining (CBC), and the Encrypted Salt-Sector Initialization Vector (ESSIV) scheme is used to counter so-called fingerprinting attacks[1].

The Porticor™ solution can encrypt on-the-fly several different types of data:

- Disk volumes, which can be exposed to applications as Network File System (NFS) disks, or as Windows shares (CIFS volumes).
- Disk volumes configured as a Storage Area Network (SAN). Porticor™ supports the iSCSI protocol for exposing such volumes. This is a common way to configure storage for database servers.
- Distributed storage, where applications normally write the whole file into a Web Service, and benefit from an extremely high durability. Porticor™ supports the most popular of these storage methods, Amazon's Simple Storage Service (S3).

1 This is the default *encryption* algorithm. Others can be used, by configuring the product.

BEYOND ENCRYPTION

Porticor implements several additional technologies, including

- Digital Signing (to ensure data has not been tampered with)
- Data dispersion and deconstruction™ (patented), to ensure S3 data objects are difficult to find in the cloud
- Logging of Data-related events and alerts, to ensure audit-ability and compliance with regulations (such as PCI DSS or HIPAA).

AND WHAT ABOUT THE KEYS?

Any data encryption consists of running the Encryption algorithm on the plaintext and the secret key, to obtain the ciphertext: $C = E_K(P)$. So, where does one get the secret key from?

The best common practice is to generate as many different random keys as practical, e.g. one key per disk volume or one per S3 object, and to store them securely. Needles to mention, you cannot store the key next to the encrypted data, as it would become vulnerable to the same attacks as the data, which creates a dilemma unique to the cloud: you do not wish to store all your keys in the Cloud, but you need them in the Cloud since your project's Application Servers and Database Servers are in the cloud.

While other vendors require you to either install a physical server in your data center for the key management, or to "trust them" and use their SaaS key storage for your keys, Porticor™ uses a highly innovative and patented approach to store your keys securely in <u>your</u> cloud account ; The Porticor Virtual Key Management™ (PVKM™) technology.

More than just key storage, PVKM™ provides you with three additional industry unique guarantees:

1. <u>Your keys are never exposed to anyone else. Not even to Porticor itself.</u>
2. For the first time, you can use encryption keys in the Cloud while maintaining strong security
3. You enjoy a simple automated system,; while the protected objects (disks, S3 objects) are protected using the strongest security: a key for each object

THE "SWISS BANKER APPROACH"

A metaphor: banks everywhere store millions of (real, physical) safe-deposit boxes in their cellars. To provide their customers with the best security guarantees, Swiss bankers invented a technique that is today used by everyone; each safe-deposit box has two (physical) keys: one is given to the customer, and the other is kept by the bank for safekeeping. Neither the customer nor the banker can open the safe on their own. Both keys are needed to be used at the same time for the safe to yield.

Porticor™ uses a similar approach in its key management solution: whenever you create a new Porticor-protected project, you generate a Master Key. This Master Key must be backed up securely by the customer, because Porticor™ never sees it. The Master Key is kept on the Porticor™ virtual appliance which lives within your own cloud account, but it is never transferred into Porticor's central key management servers. If the virtual appliance is ever terminated, a new one can be rebuilt using the information stored by Porticor™, combined with your backed-up Master Key.

When you encrypt a disk volume or an S3 object, its newly created key is a mathematical combination of the Master Key and a unique key created by PVKM™. Thus the Master key is "one half" of the full key, and the PVKM™ generated key is the "second half" of the full key.

In greater detail: the Porticor™ virtual appliance generates the "second half" of the key for each new object. This "second half" is then used together with the Master key (the "first half") to create the full key.

The "second half" is stored and protected in the PVKM™ system, allowing access only to the approved end user. These is achieved by first encrypting the "Second Half" key by the Master Key and only then store it in the central PVKM™ store. Keys are stored in the PVKM™ system only after further encryption with an RSA private key occurs. This means even Porticor never actually has your keys; Porticor does not even have half of your keys! In tat sense, we do the "Swiss Banker" one better…

To retrieve the data encryption key (e.g. when the virtual appliance has been restarted), the appliance identifies itself to the central PVKM™ system, and receives the *encrypted* data encryption key. This key is decrypted automatically using the Master Key before it is used for any purpose.

When you no longer require ongoing access to a disk volume, you can use the Porticor™ management interface (or the Porticor™ suite of APIs) to "lock" the volume. The key is erased from the virtual appliance, and only retained in the central PVKM™. The volume is still protected by both Master Key and the RSA private key, and the key will be fetched from the PVKM™ system when it is needed again for the reactivation of the volume

PROBLEM SOLVED

Going back to Figure 1, Porticor™ protects your all-important business data by encrypting and digitally signing it, as well as by using a unique data deconstruction technique. Porticor™ also ensures logging, auditing and compliance.

Outsider attackers and insider staff at the cloud provider cannot access the data because they do not have access to the secret keys. They cannot view any of the data, and neither can they change it without the change being detected.

Even attackers coming from unrelated servers of the same customer are thwarted, because keys are protected using *per-project secrets*.

SECURITY DEPLOYED THE CLOUD WAY

Porticor VPD™ is designed from the ground up for cloud applications. Security is achieved in minutes with 3 simple steps:

1. Launch the Porticor™ Virtual appliance in your cloud account
2. Data is copied to the Porticor™ Virtual appliance
3. Configure your application to use the Porticor™ Virtual appliance

WHAT'S NEXT?

You can try the Porticor VPD™ solution with no long-term obligations, and perhaps most importantly, your data will be protected within minutes of starting the trial. Give it a try! Register at https://www.porticor.com/register and apply security to your cloud applications within minutes. Need further help? Contact us at contact@porticor.com