TRUSTED COMPUTING GROUP™

Cloud Computing and Security – A Natural Match

April 2010

Trusted Computing Group
3855 SW 153rd Drive, Beaverton, OR 97006
Tel (503) 619-0562 | Fax (503) 644-6708
admin@trustedcomputinggroup.org
www.trustedcomputinggroup.org

CLOUD COMPUTING AND SECURITY – A NATURAL MATCH

Cloud computing provides Internet-based services, computing, and storage for users in all markets including financial, healthcare, and government. This new approach to computing allows users to avoid upfront hardware and software investments, gain flexibility, collaborate with others, and take advantage of the sophisticated services that cloud providers offer. However, security is a huge concern for cloud users.

Cloud providers have recognized the cloud security concern and are working hard to address it. In fact, cloud security is becoming a key differentiator and competitive edge between cloud providers. By applying the strongest security techniques and practices, cloud security may soon be raised far above the level that IT departments achieve using their own hardware and software.

To recognize the latest approaches to cloud security, you must first understand the fundamental Trusted Computing technologies on which these approaches are based. Then you'll learn how to apply them in the cloud.

TRUSTED COMPUTING: STANDARDS FOR STRONG SECURITY

A key hurdle to moving IT systems to the cloud is the lack of trust on the cloud provider. The cloud provider, in turn, also needs to enforce strict security policies, requiring additional trust in the clients. To improve the mutual trust between consumer and cloud provider, a well-understood trust foundation needs to be in place. Military-grade security systems use special-purpose security hardware as a firm foundation. Now this same technology (known as "Trusted Computing") is available for civilian purposes. The Trusted Computing Group [1], an industry consortium, has developed standards for using Trusted Computing techniques in laptop and desktop computers, networking, and storage.

TCG's member companies, 100-plus major suppliers that cover the enterprise with connectivity and computing technology, also provide technology for cloud computing. As a result, TCG standards have been rapidly adapted to address cloud security. Let's learn more about these powerful standards.

Trusted Platform Module. To provide stronger computer security than software alone can provide, TCG has defined the specification for the widely implemented Trusted Platform Module (TPM). The TPM is an international standard, hardware security component built into many computers and computer-based products. The TPM includes capabilities such as machine authentication, hardware encryption, signing, secure key storage, and attestation. Encryption and signing are well-known techniques, but the TPM makes them stronger by storing keys in protected hardware storage. Machine authentication is a core principle that allows clouds to authenticate to a known machine to provide this machine and user a higher level of service as the machine is known and authenticated.

Attestation requires a bit more explanation. When this feature is used, the TPM monitors software as it is loaded and provides secure reports on exactly what is running on the machine. This monitoring and reporting are especially important in the virtualized environment of cloud computing where viruses and worms can hide in many places.

With more than 300 million TPMs embedded in enterprise computers, the TPM provides a strong security foundation for other TCG specifications including Trusted Network Connect (TNC) and Trusted Storage. However, these other TCG specifications can work without a TPM at a lower security level by using a software-only approach.

Trusted Network Connect. TCG's Trusted Network Connect (TNC) architecture provides an industry standard approach to network security and network access control (NAC) that works with leading providers such as Microsoft and Cisco. The TNC standards enable administrators to control network access based on user identity and device health while monitoring behavior on the network and responding immediately to problems as they occur.

The Trusted Network Connect (TNC) architecture:

- has strong user authentication
- allows guest access
- blocks the access of unsafe endpoints
- extends access control to clientless endpoints such as IP phones and printers
- coordinates security devices across the enterprise.

Trusted Storage. TCG's Trusted Storage specification provides a manageable, enterprise-wide means for implementing full-disk encryption using hardware included right in the drive. These drives, known as self-encrypting drives, simplify the enterprise encryption process for handling sensitive data, since all data, applications, and drivers are encrypted internal to the drive and key management is an integral part of the design. The hardware-based encryption can take advantage of the TPM if desired and does not require user intervention or impact system performance, unlike traditional software-only encryption schemes that require cycle time from the main processor. With a self-encrypting drive, when a drive is removed for any reason (maintenance, end of life or even theft), the data is completely useless to criminals since they don't know the encryption key.

CRITICAL AREAS FOR CLOUD COMPUTING

The Cloud Security Alliance (CSA) [2] has developed a 76-page security guide (Security Guidance for Critical Areas of Focus in Cloud Computing V2.1) that identifies many areas for concern in cloud computing [3]. This environment is a new model which cannot be well protected by traditional "perimeter" security approaches. From this exhaustive document, we have selected six specific areas of the cloud computing environment where equipment and software implementing TCG specifications can provide substantial security improvements [4]. Figure 1 shows the relationship of these areas in the cloud.

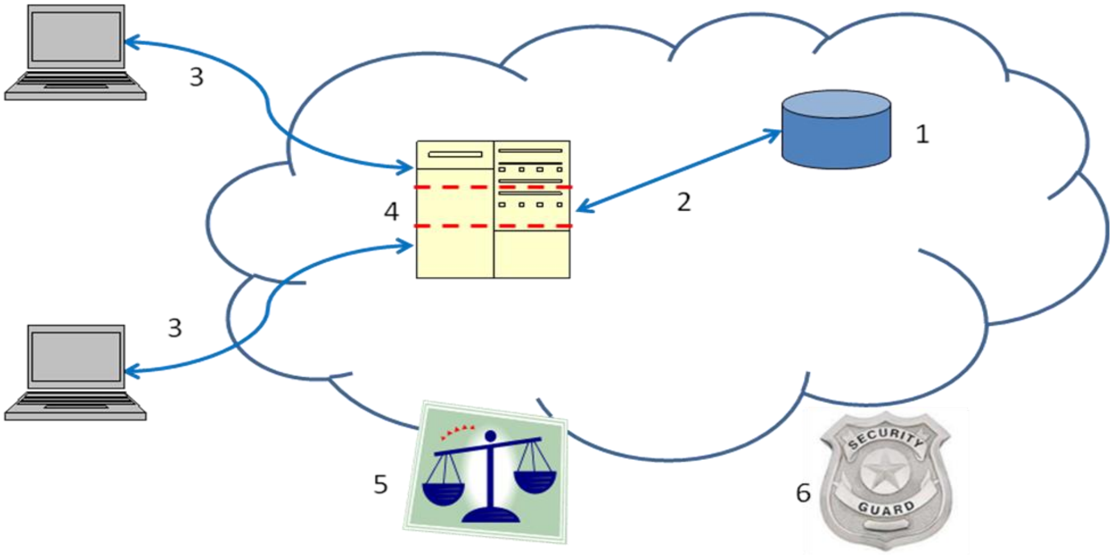

Figure 1. Areas for security concerns in cloud computing: (1) data at rest, (2) data in transit, (3) authentication, (4) separation between customers, (5) cloud legal and regulatory issues and (6) incident response.

1 - Securing data at rest.

Cryptographic encryption is certainly the best practice and in many U.S. states and countries worldwide, it's the law for securing data at rest at the cloud provider. Fortunately, hard drive manufacturers are now shipping self-encrypting drives that implement the TCG's Trusted Storage standards. Self-encrypting drives build encryption hardware into the drive, providing automated encryption with minimal cost or performance impact. Software encryption can also be used, but it is slower and less secure since the encryption key can be copied off the machine without detection.

2 - Securing data in transit.

Encryption techniques should also be used for data in transit. In addition, authentication and integrity protection ensure that data only goes where the customer wants it to go and is not modified in transit. Well-established protocols such as SSL/TLS should be used here. The tricky part is strong authentication, as described next.

3 - Authentication.

User authentication is often the primary basis for access control, keeping the bad guys out while allowing authorized users in with a minimum of fuss. In the cloud environment, authentication and access control are more important than ever since the cloud and all of its data are accessible to anyone over the Internet. The TPM can easily provide stronger authentication than username and passwords. TCG's IF-MAP standard allows for real-time communication between the cloud provider and the customer about authorized users and other security issues. When a user is fired or reassigned, the customer's identity management system can notify the cloud provider in real-time so that the user's cloud access can be modified or revoked within seconds. If the fired user is logged into the cloud, they can be immediately disconnected. Trusted Computing enables authentication of client PCs and other devices, which also is critical to ensuring security in cloud computing.

4 - Separation between customers.

One of the more obvious cloud concerns is separation between a cloud provider's users (who may be competing companies or even hackers) to avoid inadvertent or intentional access to sensitive information. Typically a cloud provider would use virtual machines (VMs) and a hypervisor to separate customers. TCG technologies can provide significant security improvements for VM and virtual network separation. In addition, the TPM can provide hardware-based verification of hypervisor and VM integrity. The TNC architecture and standards can provide strong network separation and security.

5 - Cloud legal and regulatory issues.

To verify that a cloud provider has strong policies and practices that address legal and regulatory issues, each customer must have its legal and regulatory experts inspect cloud provider policies and practices to ensure their adequacy. The issues to be considered include data security and export, compliance, auditing, data retention and destruction, and legal discovery. In the areas of data retention and deletion, Trusted Storage and TPM access techniques can play a key role in limiting access to data.

6 - Incident response.

As part of expecting the unexpected, customers need to plan for the possibility of cloud provider security breaches or user misbehavior. An automated response or at least automated notification is the best solution. TCG's IF-MAP (Metadata Access Protocol) specification enables the integration of different security systems and provides real-time notification of incidents and of user misbehavior.

GETTING EVEN BETTER CLOUD SECURITY

In cloud computing, end-to-end security is critical. Building blocks from TCG and commercial products built on these principles will help make the cloud environment more secure. Ongoing research from TCG and operating system or device security vendors will take advantage of the TPM using additional software to enhance its capability for cloud computing. Other research on cloud computing security is under way at several companies [5]. Today, the good news is that most cloud security issues can be addressed with well-known, existing techniques.

The TPM can be an independent entity that works on behalf of cloud computing customers. Inside every server in the cloud, the TPM and associated software can check what is installed on each machine and verify the machine's health and proper performance. When it detects a problem, TNC technology can immediately restrict access to a device or server. For securing data at rest in the cloud or in clients that access cloud data, self-encrypting drives based on Trusted Storage provide the ultimately secure solution.

Organizations that have already implemented TCG-based solutions can leverage their corporate investment in hardware, software and policies and re-use them for cloud computing. If cloud computing represents an organization's initial implementation of TCG-based technology (used by the cloud provider), the rest of the organization should be re-evaluated for areas where TCG technology can provide improved internal security, including: activating TPMs, use of self-encrypting drives and network access control through TNC.

REFERENCES:

[1.] Trusted Computing Group (TCG): http://www.trustedcomputinggroup.org/
[2.] Cloud Security Alliance (CSA): http://cloudsecurityalliance.org/
[3.] A Security Analysis of Cloud Computing: (http://cloudcomputing.sys-con.com/node/1203943
[4.] Cloud Security Questions? Here are some answers (http://cloudcomputing.sys-con.com/node/1330353)
[5.] Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control:
http://www.parc.com/content/attachments/ControllingDataInTheCloud-CCSW-09.pdf