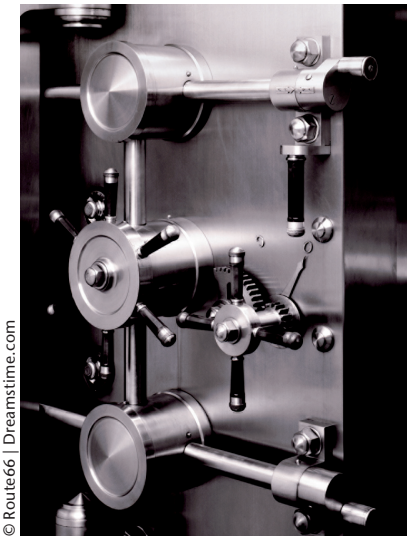

What's Special about Cloud Security?

Peter Mell, *US National Institute of Standards and Technology*

Although cloud security concerns have consistently ranked as one of the top challenges to cloud adoption,[1] it's not clear what security issues are particular to cloud computing. To approach this question, I attempt to derive cloud security issues from various cloud definitions and a reference architecture.

Defining Cloud Computing

The European Network and Information Security Agency (ENISA) defines cloud computing as "an on-demand service model for IT provision, often based on virtualization and distributed computing technologies."[2] It says that cloud computing architectures have highly abstracted resources, near-instant scalability and flexibility, nearly instantaneous provisioning, shared resources, service on demand, and programmatic management.

The US National Institute of Standards and Technology (NIST) has also published a cloud definition, which it has submitted as the US contribution for an international standard.[3] According to NIST,

> Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (for example, networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

The NIST definition lists five essential characteristics of cloud computing: on-demand self-service, broad network access, resource pooling, rapid elasticity or expansion, and measured service. It also lists three service models—software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS)—and four deployment models—private, community, public and hybrid—that, together, categorize ways to deliver cloud services.

NIST has also published a cloud computing reference architecture.[4] As Figure 1 shows, this architecture outlines the five major roles of cloud consumer, provider, broker, auditor, and carrier.

These definitions and reference architecture provide a foundation from which we can begin to analyze cloud security issues.

Cloud Security Controls

Let's first look at cloud security controls documented within the Cloud Security Alliance (CSA) security control framework, which was informed by both the ENISA and NIST definitions. The CSA guidance, version 2.1, contains 98 different cloud security controls from 13 domains, which aim to "help evaluate initial cloud risks and inform security decisions."[5]

This body of work would seem to indicate that, based on published cloud definitions, we can identify 98 cloud-specific security controls. However, all 98 controls have been mapped to existing implementation-independent security control frameworks.[6] This includes NIST Special Publication 800-53 and the International Organization for Standardization 27001-2005. Based on this evaluation, these security controls don't seem unique to cloud computing—US government and internationally standardized general-purpose security controls cover all known CSA cloud security controls.

The US government's Federal Risk and Authorization Management Program (FedRAMP, www.fedramp.gov) for cloud computing

Published by the IEEE Computer Society
1520-9202/12/$31.00 © 2012 IEEE

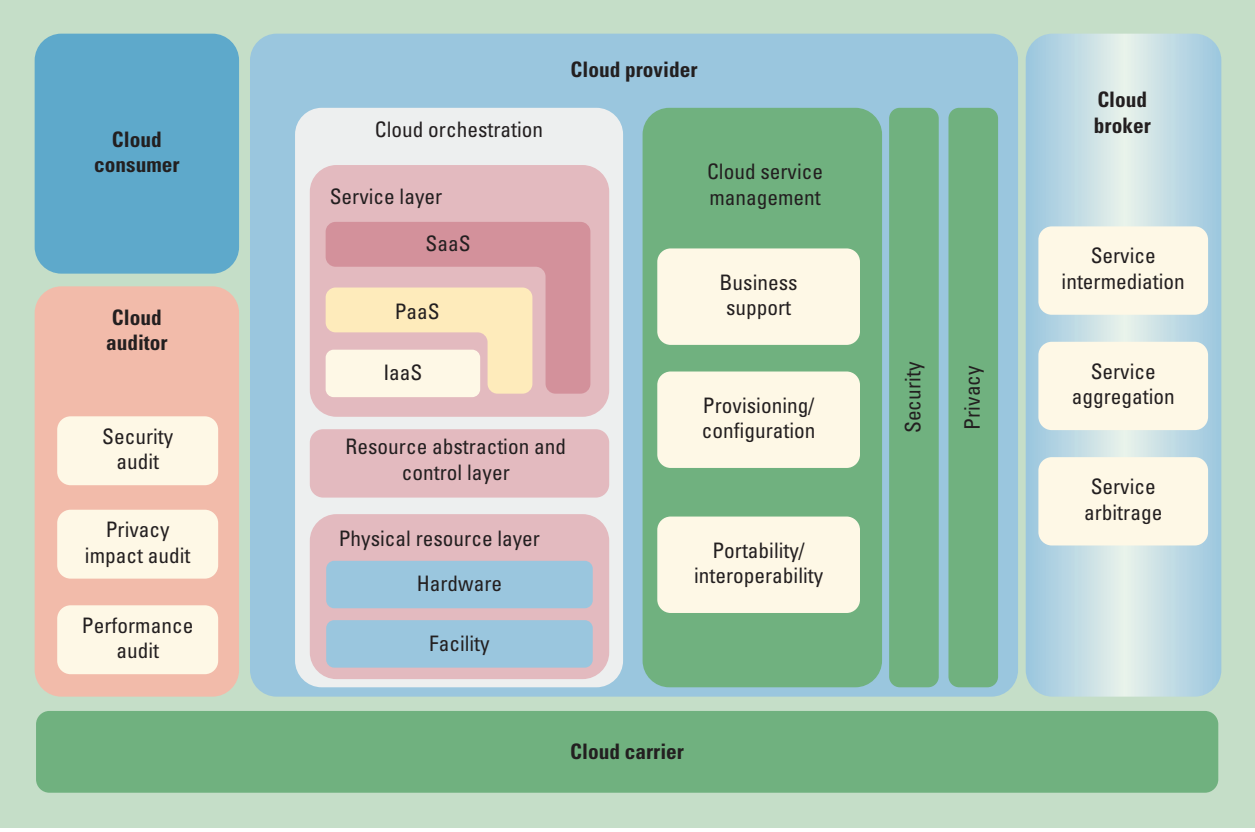

Figure 1. NIST cloud computing reference architecture. It outlines five major roles: cloud consumer, provider, broker, auditor, and carrier.

also uses the NIST cloud definition.[7] Instead of creating new cloud security controls, FedRAMP published a selection of existing general-purpose controls from the NIST Special Publication 800-53 security control catalog (www.gsa.gov/graphics/staffoffices/FedRAMP_Security_Controls_Final.zip). Thus, the FedRAMP controls are also generically applicable.

This lack of novel security controls for the cloud might arise from the fact that cloud computing is the convergence of many different technology areas, including broadband networks, virtualization, grid computing, service orientation, autonomic systems, and Web 2.0. Each of these underlying technology areas has been independently addressed by existing general-purpose security controls, so it seems logical to assume we can address the composition of these technology areas using these same general-purpose security controls.

However, the cloud paradigm might still present security issues that require a novel application of the set of existing general-purpose security controls. Evidence for this argument lies in the fact that each CSA cloud security control was mapped to multiple controls from the general-purpose control frameworks.

Derivation of Cloud Security Issues

To show the existence of these security issues, I list a sampling derived from the initial cloud definitions and reference architecture. Many of the essential cloud characteristics, definitional models, and architectural components suggest cloud security issues.

Cloud Brokers

This reference architecture actor implies security composition challenges within composed clouds, such as a SaaS built on an IaaS.

On-Demand Delivery

This cloud characteristic suggests security challenges associated with the business user being able to easily and instantly obtain new computing resources that must be pre-secured on delivery.

Resource Pooling

This cloud characteristic guides customers toward a "put all your eggs in one basket" approach that might let users concentrate security resources on a single basket but that also heightens the need for backup and resiliency solutions. From a cloud customer perspective, this characteristic

reveals the possibility that attacks against one customer could inadvertently affect another customer using the same shared resources.

Service Models

The cloud definition service models reveal challenges with multitenancy in a resource pooled environment. All service models have data multitenancy, while PaaS and IaaS additionally have processing multitenancy in which user processes might attack each other and the cloud itself.

Infrastructure as a Service

This service model reveals challenges with using virtualization as a frontline security defense perimeter to protect against malicious cloud users.

Broad Network Access

This cloud characteristic shifts the security model to account for possibly untrustworthy client devices that are fully reliant on the network for service.

Measured Service

This cloud characteristic reveals the need to measure cloud usage to promote overall cloud availability.

The cloud computing paradigm appears to present special security issues that will require research and careful consideration. At this point, however, these issues don't appear to require completely new security controls but instead the creative application of existing security techniques.

Acknowledgments

Certain products or organizations are identified in this document, but such identification does not imply recommendation by the US National Institute of Standards and Technology (NIST) or other agencies of the US government, nor does it imply that the products or organizations identified are necessarily the best available for the purpose. This article reflects the author's personal opinions—not the opinions of the Department of Commerce or NIST.

References

1. "IT Cloud Services User Survey, Part 2," IDC Enterprise Panel, Aug. 2008 www.clavister.com/documents/resources/white-papers/clavister-whp-security-in-the-cloud-gb.pdf.
2. "Cloud Computing: Benefits, Risks, and Recommendations for information Security," European Network and Information Security Agency, Nov. 2009; www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport.
3. "Final Version of NIST Cloud Computing Definition Published," *NIST Tech Beat*, 25 Oct. 2011; www.nist.gov/itl/csd/cloud-102511.cfm.
4. F. Liu et al., *NIST Cloud Computing Reference Architecture*, NIST recommendation, Sept. 2011; http://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/ReferenceArchitectureTaxonomy/NIST_SP_500-292_-_090611.pdf.
5. "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1," Cloud Security Alliance, Dec. 2009; https://cloudsecurityalliance.org/wp-content/uploads/2011/07/csaguide.v2.1.pdf.
6. "CloudControlsMatrix,Version1.2" Cloud Security Alliance, Aug. 2011; https://cloudsecurityalliance.org/research/initiatives/ccm.
7. S. VanRoekel, "Memorandum for Chief Information Officers," Executive Office of the President, 8 Dec. 2011, footnotes 5 and 6; www.cio.gov/fedrampmemo.pdf.

Peter Mell *is a computer scientist at the US National Institute of Standards and Technology. His research interests include big data technology, cloud computing, vulnerability databases, and intrusion detection. Contact him at mell@nist.gov.*