ITL BULLETIN FOR MARCH 2012

GUIDELINES FOR IMPROVING SECURITY AND PRIVACY IN PUBLIC CLOUD COMPUTING

Shirley Radack, Editor
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Cloud computing is an emerging technology that can help organizations become more efficient and agile, and respond more quickly and reliably to their customers' needs. Many government and private sector organizations are currently using or considering the use of cloud computing to increase the performance and efficiency of their information system operations, and to improve the delivery of services.

Cloud computing is a form of distributed computing that provides information technology (IT) services as a commodity and enables users to benefit from the efficient use of computer resources. Users are able to control the computing services they access, while sharing the investment in the underlying IT resources with other consumers. When computing resources are provided by another organization over a wide-area network, cloud computing is similar to an electric power utility. The providers benefit from economies of scale, which in turn enables them to lower individual usage costs and to centralize infrastructure costs. Users pay for what they consume, can increase or decrease their usage, and leverage the shared underlying resources. Organizations using cloud computing can spend less time managing complex IT resources and more time focusing on their core mission work.

The U.S. Office of Management and Budget (OMB) highlighted the potential importance of cloud computing in improving the federal government's management and use of information technology in a statement entitled *Federal Cloud Computing Strategy* (February 2011). The Chief Information Officer (CIO) cited the federal government's IT environment as "characterized by low asset utilization, a fragmented demand for resources, duplicative systems, environments which are difficult to manage, and long procurement lead times…" OMB stated that these inefficiencies negatively impact the government's ability to serve the American public, and identified cloud computing as a model for helping agencies provide reliable, innovative, and timely services, especially when resources are constrained.

Defining Cloud Computing

The National Institute of Standards and Technology (NIST) has defined cloud computing as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or

service provider interaction." See NIST Special Publication (SP) 800-145, *A NIST Definition of Cloud Computing*, listed in the For More Information section below.

NIST has been working in collaboration with government, industry, and standards bodies to accelerate the federal government's secure adoption of cloud computing. NIST's goal is to foster cloud computing systems and practices; support interoperability, portability, and security requirements; and cooperate in the development of needed standards and guidelines.

Security Challenges

Many of the features that make cloud computing attractive can also introduce significant security challenges that cannot be addressed with traditional security models and controls. While cloud computing can be implemented exclusively for an organization as an internal private cloud, its main thrust has been to provide a vehicle for outsourcing parts of the organizational computing environment to an outside party via a public cloud. As with any outsourcing of information technology services, concerns exist about the implications for computer security and privacy. The main issue centers on the risks associated with moving important applications or data from within the confines of the organization's computing center to that of another organization (i.e., a public cloud), which is readily available for use by the general public.

To help organizations realize the benefits of cloud computing while giving appropriate consideration to the security and privacy issues involved, the Information Technology Laboratory (ITL) at NIST recently issued SP 800-144, *Guidelines on Security and Privacy in Public Cloud Computing.* The publication applies the risk-based approach for protecting information and information systems to the complex arrangements for cloud computing services.

NIST SP 800-144, *Guidelines on Security and Privacy in Public Cloud Computing*

These new guidelines, which were written by Wayne Jansen of Booz Allen Hamilton and Tim Grance of NIST, present an overview of public cloud computing, and discuss the benefits and drawbacks of public cloud services with an emphasis on the security and privacy considerations. Users of public cloud computing are advised on effectively dealing with the key security and privacy issues, and the precautions that can be taken to protect the organization's information and systems. Specific guidance is presented on how to protect security and privacy when support for data and applications is outsourced to a cloud provider. The publication provides supplementary material including lists of references, acronyms, and online resources.

NIST's Recommendations for Protecting Security and Privacy in Public Cloud Computing

NIST recommends that federal departments and agencies follow the practices outlined below when planning for and implementing cloud computing:

• Carefully plan the security and privacy aspects of cloud computing solutions before engaging them.

Organizations considering the use of public cloud computing should thoroughly review the sensitivity of their data, which will move from the organization's data center to an infrastructure that is open to use by potential adversaries. Planning helps to ensure that the computing environment is as secure as possible and in compliance with organizational security policies, that privacy is maintained, and that IT resources are spent wisely.

Decisions about outsourcing IT services and about transitioning organizational data, applications, and other resources to a public cloud computing environment should be in accord with the organization's security objectives. Organizations should take a risk-based approach to analyzing available security and privacy options and deciding about placing organizational functions into a cloud environment. The organization's policies, procedures, and standards used for application development and service provisioning, as well as the design, implementation, testing, use, and monitoring of deployed or engaged services, should be applied to cloud computing environments.

Security and privacy must be considered throughout the system life cycle, from the initial planning stage through system disposition. Addressing security and privacy issues after implementation and deployment of the system is much more difficult and expensive, and exposes the organization to unnecessary risk.

• Understand the public cloud computing environment offered by the cloud provider.

Organizations should be aware of the delineation of responsibilities over the cloud computing environment and the implications for security and privacy. Assurances furnished by the cloud provider to support security or privacy claims, or by a certification and compliance review group paid by the cloud provider, should be verified whenever possible through an independent assessment by the organization.

To assess the security and privacy risks, organizations should examine the policies, procedures, and technical controls used by a cloud provider, the technologies used to provide services, and the implications for security and privacy of the system. Details about the system architecture of a cloud can be analyzed and used to evaluate the protection afforded by the security and privacy controls. Continuous monitoring of information systems is an important part of the risk management process, and helps organizations to maintain ongoing awareness of information security, vulnerabilities, and threats in order to support organizational risk management decisions.

• Ensure that a cloud computing solution satisfies organizational security and privacy requirements.

Organizations should require that any public cloud computing solution that they select from a cloud provider is configured, deployed, and managed to meet organizational security, privacy, and other requirements.

While nonnegotiable service agreements in which the terms of service are prescribed completely by the cloud provider are generally the norm in public cloud computing, the organization should consider using negotiated service agreements. Similar to traditional IT outsourcing contracts used by agencies, negotiated agreements can address an organization's concerns about security and privacy details, such as the vetting of employees, data ownership and exit rights, breach notification, isolation of tenant applications, data encryption and segregation, tracking and reporting service effectiveness, compliance with laws and regulations, and the use of validated products that meet federal or national standards. A negotiated agreement can also document the assurances provided by the cloud provider to corroborate that organizational requirements are being met.

The organization's critical data and applications may necessitate the use of a negotiated service agreement in order to use a public cloud, even though the negotiated agreement may be less cost-effective for the organization. Options for addressing the cost considerations include employing compensating controls to work around the identified shortcomings in the public cloud service and using cloud computing environments, such as an internal private cloud. The private cloud can provide greater oversight and authority over security and privacy, limit the types of tenants that share platform resources, and reduce exposure in the event of a failure or configuration error in a control.

When making decisions about selecting services and service arrangements from cloud providers and moving functions to the cloud, organizations should consider the benefits in cost and productivity as well as the risks and liability. While it may not be possible for government organizations to outsource all of their IT services to a public cloud, some services can be outsourced if the risks are carefully considered.

• Ensure that the client-side computing environment meets organizational security and privacy requirements for cloud computing.

Services from different cloud providers, as well as cloud-based applications developed by the organization, can impose exacting demands on the client, and raise security and privacy concerns. Web browsers are a key element for client-side access to cloud computing services. Clients may also include small lightweight applications that run on desktop and mobile devices to access services. The various available plug-ins and extensions for web browsers can cause security problems. Many browser add-ons do not provide automatic updates, allowing the continuation of existing vulnerabilities. Similar problems exist for other types of clients as well.

Maintaining physical and logical security over clients can be difficult, especially with embedded mobile devices such as smart phones. Their size and portability can result in the loss of physical control. Built-in security mechanisms are often not used or can be

circumvented without difficulty by knowledgeable parties who gain control over the device and who receive custom-built native applications directly rather than through a web browser.

Social media, personal webmail, and other publicly available sites are a concern, since they increasingly serve as avenues for social engineering attacks that can negatively impact the security of the client, its underlying platform, and the cloud services accessed. A backdoor Trojan, keystroke logger, or other type of malware running on a client device undermines the security and privacy of public cloud services as well as other Internet-facing public services accessed. Organizations should review existing security and privacy measures as part of their overall cloud computing security architecture and employ additional measures, if needed, to secure the client side.

• Maintain accountability over the privacy and security of data and applications implemented and deployed in public cloud computing environments.

Organizations should employ appropriate security management practices and controls over cloud computing to assure a secure environment. Organizations should monitor their information system assets and assess the implementation of policies, standards, procedures, controls, and guidelines that establish and protect the confidentiality, integrity, and availability of information system resources.

Organizations should collect and analyze available data about the state of the system regularly and as often as needed to manage security and privacy risks for each level of the organization: governance level, mission or business process level, and information systems level. The continuous monitoring of information security involves maintaining ongoing awareness of privacy and security controls, vulnerabilities, and threats to support risk management decisions. Organizations that conduct ongoing monitoring of the security of networks, information, and systems can respond by accepting, avoiding, or mitigating risk as situations change.

Since significant portions of the computing environment are under the control of the cloud provider and may be beyond the organization's purview, both qualitative and quantitative factors should be applied in a risk analysis. Risks must be carefully weighed against the available technical, management, and operational safeguards and the necessary steps must be taken to reduce risk to an acceptable level. The organization must also ensure that security and privacy controls are implemented correctly, operate as intended, and meet organizational requirements.

Organizations need a level of confidence about a cloud service environment based on the ability of the cloud provider to provide the security controls necessary to protect the organization's data and applications, and information about the effectiveness of the controls. It may not be feasible to verify the correct functioning of a subsystem and the effectiveness of security controls as extensively as with an internal organizational system. Third-party audits may be used to establish a level of trust. If the level of confidence in

the service falls below expectations and the organization is unable to employ compensating controls, it must either reject the service or accept a greater degree of risk.

Cloud computing depends on the security of many individual components, including components for general computing, and management components, such as for self-service, resource metering, quota management, data replication and recovery, service level monitoring, and workload management. The complexities among these many components can affect security. Organizations should ensure to the maximum extent practicable that all cloud computing elements are secure, and that security and privacy are maintained based on sound computing practices.

For More Information

The NIST publications listed below provide information to help organizations implement the recommendations for the secure implementation of cloud computing and the integration of cloud computing into the system development life cycle. For information about these and other security-related publications, see here.

Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*
FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*
NIST SP 800-18 Rev.1, *Guide for Developing Security Plans for Federal Information Systems*
NIST SP 800-34 Rev.1, *Contingency Planning Guide for Federal Information Systems*
NIST SP 800-37 Rev.1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*
NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*
NIST SP 800-53 Rev.3, *Recommended Security Controls for Federal Information Systems and Organizations*
NIST SP 800-53A Rev.1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans*
NIST SP 800-60 Rev.1, *Guide for Mapping Types of Information and Information Systems to Security Categories: (2 Volumes) - Volume 1: Guide Volume 2: Appendices*
NIST SP 800-61 Rev.1, *Computer Security Incident Handling Guide*
NIST SP 800-64 Rev 2, *Security Considerations in the System Development Life Cycle*
NIST SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response*
NIST SP 800-88, *Guidelines for Media Sanitization*
NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment*
NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*
NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*
NIST SP 800-145, *A NIST Definition of Cloud Computing*

The NIST Cloud Computing Program supports the federal government's efforts to incorporate cloud computing as a replacement for, or enhancement to, traditional information system and application models where appropriate. General information about NIST's cloud computing program is available here.

For information about the risk-based approach to system development, and the Risk Management Framework (RMF) that helps organizations develop a disciplined and structured process for integrating information security and risk management activities into the life cycle of an information system, see the NIST web page here.

Information about NIST's information security programs is available from the Computer Security Resource Center here.

ITL Bulletin Publisher: Elizabeth Lennon
Writer/Editor
Information Technology Laboratory
National Institute of Standards and Technology
Email here.