Top Threats
to
Cloud Computing V1.0

Prepared by the
Cloud Security Alliance
March 2010

Introduction

The permanent and official location for the Cloud Security Alliance Top Threats research is:

http://www.cloudsecurityalliance.org/topthreats

Table of Contents

Foreword

Welcome to the Cloud Security Alliance's "Top Threats to Cloud Computing", Version 1.0. This is one of many research deliverables CSA will release in 2010.

Also, we encourage you to download and review our flagship research, "Security Guidance for Critical Areas of Focus in Cloud Computing", which you can download at:

http://www.cloudsecurityalliance.org/guidance

The Cloud Security Alliance would like to thank HP for their assistance in underwriting this research effort.

Best Regards,

Jerry Archer
Alan Boehme
Dave Cullinane
Paul Kurtz
Nils Puhlmann
Jim Reavis

The Cloud Security Alliance Board of Directors

Underwritten by HP

Acknowledgments

Working Group Leaders

Dan Hubbard, Websence
Michael Sutton, Zscaler

Contributors
Amer Deeba, Qualys
Andy Dancer, Trend Micro
Brian Shea, Bank of America
Craig Balding, CloudSecurity.org
Dennis Hurst, HP
Glenn Brunette, Oracle
Jake Lee, Bank of America
Jason Witty, Bank of America
Jim Reavis, Cloud Security Alliance
John Howie, Microsoft
Josh Zachry, Rackspace
Ken Biery, Verizon Business
Martin Roesler, Trend Micro
Matthew Becker, Bank of America
Mike Geide, Zscaler
Scott Matsumoto, Cigital
Scott Morrison, Layer 7 Technologies
William Thornhill, Bank of America
Wolfgang Kandek, Qualys

Advisory Committee
Archie Reed, HP
Daniele Catteddu, ENISA – European Network and Information Security Agency
Dave Cullinane, eBay
Giles Hogben, ENISA – European Network and Information Security Agency
Gunter Ollmann, Damballa
Jens Jensen, Open Grid Forum
Joshua Pennell, IOActive
Nils Puhlmann, Zynga
Rick Howard, VeriSign

Executive Summary

Cloud Computing represents one of the most significant shifts in information technology many of us are likely to see in our lifetimes. Reaching the point where computing functions as a utility has great potential, promising innovations we cannot yet imagine.

Customers are both excited and nervous at the prospects of Cloud Computing. They are excited by the opportunities to reduce capital costs. They are excited for a chance to divest themselves of infrastructure management, and focus on core competencies. Most of all, they are excited by the agility offered by the on-demand provisioning of computing and the ability to align information technology with business strategies and needs more readily. However, customers are also very concerned about the risks of Cloud Computing if not properly secured, and the loss of direct control over systems for which they are nonetheless accountable.

To aid both cloud customers and cloud providers, CSA developed "Security Guidance for Critical Areas in Cloud Computing", initially released in April 2009, and revised in December 2009. This guidance has quickly become the industry standard catalogue of best practices to secure Cloud Computing, consistently lauded for its comprehensive approach to the problem, across 13 domains of concern. Numerous organizations around the world are incorporating the guidance to manage their cloud strategies. The guidance document can be downloaded at www.cloudsecurityalliance.org/guidance.

The great breadth of recommendations provided by CSA guidance creates an implied responsibility for the reader. Not all recommendations are applicable to all uses of Cloud Computing. Some cloud services host customer information of very low sensitivity, while others represent mission critical business functions. Some cloud applications contain regulated personal information, while others instead provide cloud-based protection against external threats. It is incumbent upon the cloud customer to understand the organizational value of the system they seek to move into the cloud. Ultimately, CSA guidance must be applied within the context of the business mission, risks, rewards, and cloud threat environment — using sound risk management practices.

The purpose of this document, "Top Threats to Cloud Computing", is to provide needed context to assist organizations in making educated risk management decisions regarding their cloud adoption strategies. In essence, this threat research document should be seen as a companion to "Security Guidance for Critical Areas in Cloud Computing". As the first deliverable in the CSA's Cloud Threat Initiative, the "Top Threats" document will be updated regularly to reflect expert consensus on the probable threats which customers should be concerned about.

There has been much debate about what is "in scope" for this research. We expect this debate to continue and for future versions of "Top Threats to Cloud Computing" to reflect the consensus emerging from those debates. While many issues, such as provider financial stability, create significant risks to customers, we have tried to focus on issues we feel are either unique to or greatly amplified by the key characteristics of Cloud Computing and its shared, on-demand nature. We identify the following threats in our initial document:

- Abuse and Nefarious Use of Cloud Computing
- Insecure Application Programming Interfaces
- Malicious Insiders
- Shared Technology Vulnerabilities
- Data Loss/Leakage
- Account, Service & Traffic Hijacking

- Unknown Risk Profile

The threats are not listed in any order of severity. Our advisory committee did evaluate the threats and each committee member provided a subjective ranking of the threats. The exercise helped validate that our threat listing reflected the critical threat concerns of the industry, however the cumulative ranking did not create a compelling case for a published ordered ranking, and it is our feeling that greater industry participation is required to take this step. The only threat receiving a consistently lower ranking was Unknown Risk Profile, however the commentary indicated that this is an important issue that is simply more difficult to articulate, so we decided to retain this threat and seek to further clarify it in future editions of the report.

Selecting appropriate security controls and otherwise deploying scarce security resources optimally require a correct reading of the threat environment. For example, to the extent Insecure APIs (Application Programming Interfaces) is seen as a top threat, a customer's project to deploy custom line-of-business applications using PaaS (Platform as a Service) will dictate careful attention to application security domain guidance, such as robust software development lifecycle (SDLC) practices. By the same token, to the extent Shared Technology Vulnerabilities is seen as a top threat, customers must pay careful attention to the virtualization domain best practices, in order to protect assets commingled in shared environments.

In addition to the flagship CSA guidance and other research in our roadmap, this research should be seen as complimentary to the high quality November 2009 research document produced by ENISA (European Network and Information Security Agency), "Cloud Computing: Benefits, Risks and Recommendations for Information Security". ENISA's research provides a comprehensive risk management view of Cloud Computing and contains numerous solid recommendations. The ENISA document has been a key inspiration, and we have leveraged the ENISA risk assessment process to analyze our taxonomy of threats. We encourage readers of this document to also read the ENISA document: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

Our goal is to provide a threat identification deliverable that can be quickly updated to reflect the dynamics of Cloud Computing and its rapidly evolving threat environment. We look forward to your participation on subsequent versions of "Top Threats to Cloud Computing", as we continue to refine our list of threats, and to your input as we all figure out how to secure Cloud Computing.

Threat #1: Abuse and Nefarious Use of Cloud Computing

Description

IaaS providers offer their customers the illusion of unlimited compute, network, and storage capacity — often coupled with a 'frictionless' registration process where anyone with a valid credit card can register and immediately begin using cloud services. Some providers even offer free limited trial periods. By abusing the relative anonymity behind these registration and usage models, spammers, malicious code authors, and other criminals have been able to conduct their activities with relative impunity. PaaS providers have traditionally suffered most from this kind of attacks; however, recent evidence shows that hackers have begun to target IaaS vendors as well. Future areas of concern include password and key cracking, DDOS, launching dynamic attack points, hosting malicious data, botnet command and control, building rainbow tables, and CAPTCHA solving farms.

Examples

IaaS offerings have hosted the Zeus botnet, InfoStealer trojan horses, and downloads for Microsoft Office and Adobe PDF exploits. Additionally, botnets have used IaaS servers for command and control functions. Spam continues to be a problem — as a defensive measure, entire blocks of IaaS network addresses have been publicly blacklist.

Remediation

- Stricter initial registration and validation processes.
- Enhanced credit card fraud monitoring and coordination.
- Comprehensive introspection of customer network traffic.
- Monitoring public blacklists for one's own network blocks.

References

- http://www.malwaredomainlist.com/
- http://blogs.zdnet.com/security/?p=5110
- http://voices.washingtonpost.com/securityfix/2008/07/amazon_hey_spammers_get_off_my.html

Impact

Criminals continue to leverage new technologies to improve their reach, avoid detection, and improve the effectiveness of their activities. Cloud Computing providers are actively being targeted, partially because their relatively weak registration systems facilitate anonymity, and providers' fraud detection capabilities are limited.

CSA Guidance Reference

Domain 8: Data Center Operations
Domain 9: Incident Response, Notification and Remediation

Service Models

IaaS	PaaS	SaaS

Threat #2: Insecure Interfaces and APIs

Description

Cloud Computing providers expose a set of software interfaces or APIs that customers use to manage and interact with cloud services. Provisioning, management, orchestration, and monitoring are all performed using these interfaces. The security and availability of general cloud services is dependent upon the security of these basic APIs. From authentication and access control to encryption and activity monitoring, these interfaces must be designed to protect against both accidental and malicious attempts to circumvent policy. Furthermore, organizations and third parties often build upon these interfaces to offer value-added services to their customers. This introduces the complexity of the new layered API; it also increases risk, as organizations may be required to relinquish their credentials to third-parties in order to enable their agency.

Examples

Anonymous access and/or reusable tokens or passwords, clear-text authentication or transmission of content, inflexible access controls or improper authorizations, limited monitoring and logging capabilities, unknown service or API dependencies.

Remediation

- Analyze the security model of cloud provider interfaces.
- Ensure strong authentication and access controls are implemented in concert with encrypted transmission.
- Understand the dependency chain associated with the API.

References

- http://www.programmableweb.com
- http://securitylabs.websense.com/content/Blogs/3402.aspx

Impact

While most providers strive to ensure security is well integrated into their service models, it is critical for consumers of those services to understand the security implications associated with the usage, management, orchestration and monitoring of cloud services. Reliance on a weak set of interfaces and APIs exposes organizations to a variety of security issues related to confidentiality, integrity, availability and accountability.

CSA Guidance Reference

Domain 10: Application Security

Service Models

IaaS	PaaS	SaaS

Threat #3: Malicious Insiders

Description

The threat of a malicious insider is well-known to most organizations. This threat is amplified for consumers of cloud services by the convergence of IT services and customers under a single management domain, combined with a general lack of transparency into provider process and procedure. For example, a provider may not reveal how it grants employees access to physical and virtual assets, how it monitors these employees, or how it analyzes and reports on policy compliance.

To complicate matters, there is often little or no visibility into the hiring standards and practices for cloud employees. This kind of situation clearly creates an attractive opportunity for an adversary — ranging from the hobbyist hacker, to organized crime, to corporate espionage, or even nation-state sponsored intrusion. The level of access granted could enable such an adversary to harvest confidential data or gain complete control over the cloud services with little or no risk of detection.

Examples

No public examples are available at this time.

Remediation

- Enforce strict supply chain management and conduct a comprehensive supplier assessment.
- Specify human resource requirements as part of legal contracts.
- Require transparency into overall information security and management practices, as well as compliance reporting.
- Determine security breach notification processes.

References

- http://blogs.bankinfosecurity.com/posts.php?postID=140
- http://technicalinfodotnet.blogspot.com/2010/01/tethered-espionage.html

Impact

The impact that malicious insiders can have on an organization is considerable, given their level of access and ability to infiltrate organizations and assets. Brand damage, financial impact, and productivity losses are just some of the ways a malicious insider can affect an operation. As organizations adopt cloud services, the human element takes on an even more profound importance. It is critical therefore that consumers of cloud services understand what providers are doing to detect and defend against the malicious insider threat.

CSA Guidance Reference

Domain 2: Governance and Enterprise Risk Management
Domain 7: Traditional Security, Business Continuity, and Disaster Recovery

Service Models

IaaS	PaaS	SaaS

Threat #4: Shared Technology Issues

Description

IaaS vendors deliver their services in a scalable way by sharing infrastructure. Often, the underlying components that make up this infrastructure (*e.g.*, CPU caches, GPUs, etc.) were not designed to offer strong isolation properties for a multi-tenant architecture. To address this gap, a virtualization hypervisor mediates access between guest operating systems and the physical compute resources. Still, even hypervisors have exhibited flaws that have enabled guest operating systems to gain inappropriate levels of control or influence on the underlying platform. A defense in depth strategy is recommended, and should include compute, storage, and network security enforcement and monitoring. Strong compartmentalization should be employed to ensure that individual customers do not impact the operations of other tenants running on the same cloud provider. Customers should not have access to any other tenant's actual or residual data, network traffic, etc.

Examples

- Joanna Rutkowska's Red and Blue Pill exploits
- Kortchinksy's CloudBurst presentations.

Remediation

- Implement security best practices for installation/configuration.
- Monitor environment for unauthorized changes/activity.
- Promote strong authentication and access control for administrative access and operations.
- Enforce service level agreements for patching and vulnerability remediation.
- Conduct vulnerability scanning and configuration audits.

References

- http://theinvisiblethings.blogspot.com/2008/07/0wning-xen-in-vegas.html
- http://www.blackhat.com/presentations/bh-usa-09/KORTCHINSKY/BHUSA09-Kortchinsky-Cloudburst-PAPER.pdf
- http://www.microsoft.com/technet/security/Bulletin/MS10-010.mspx
- http://blogs.vmware.com/security/2010/01/announcing-vsphere-40-hardening-guide-public-draft-release.html

Impact

Attacks have surfaced in recent years that target the shared technology inside Cloud Computing environments. Disk partitions, CPU caches, GPUs, and other shared elements were never designed for strong compartmentalization. As a result, attackers focus on how to impact the operations of other cloud customers, and how to gain unauthorized access to data.

CSA Guidance Reference

Domain 8: Data Center Operations
Domain 13: Virtualization

Service Models

IaaS	PaaS	SaaS

Threat #5: Data Loss or Leakage

Description

There are many ways to compromise data. Deletion or alteration of records without a backup of the original content is an obvious example. Unlinking a record from a larger context may render it unrecoverable, as can storage on unreliable media. Loss of an encoding key may result in effective destruction. Finally, unauthorized parties must be prevented from gaining access to sensitive data.

The threat of data compromise increases in the cloud, due to the number of and interactions between risks and challenges which are either unique to cloud, or more dangerous because of the architectural or operational characteristics of the cloud environment.

Examples

Insufficient authentication, authorization, and audit (AAA) controls; inconsistent use of encryption and software keys; operational failures; persistence and remanence challenges: disposal challenges; risk of association; jurisdiction and political issues; data center reliability; and disaster recovery.

Remediation

- Implement strong API access control.
- Encrypt and protect integrity of data in transit.
- Analyzes data protection at both design and run time.
- Implement strong key generation, storage and management, and destruction practices.
- Contractually demand providers wipe persistent media before it is released into the pool.
- Contractually specify provider backup and retention strategies.

References

- http://en.wikipedia.org/wiki/Microsoft_data_loss_2009
- http://news.cnet.com/8301-13846_3-10029707-62.html
- http://nylawblog.typepad.com/suigeneris/2009/11/does-cloud-computing-compromise-clients.html

Impact

Data loss or leakage can have a devastating impact on a business. Beyond the damage to one's brand and reputation, a loss could significantly impact employee, partner, and customer morale and trust. Loss of core intellectual property could have competitive and financial implications. Worse still, depending upon the data that is lost or leaked, there might be compliance violations and legal ramifications.

CSA Guidance Reference

Domain 5: Information Lifecycle Management
Domain 11: Encryption and Key Management
Domain 12: Identity and Access Management

Service Models

IaaS	PaaS	SaaS

Threat #6: Account or Service Hijacking

Description

Account or service hijacking is not new. Attack methods such as phishing, fraud, and exploitation of software vulnerabilities still achieve results. Credentials and passwords are often reused, which amplifies the impact of such attacks.

Cloud solutions add a new threat to the landscape. If an attacker gains access to your credentials, they can eavesdrop on your activities and transactions, manipulate data, return falsified information, and redirect your clients to illegitimate sites. Your account or service instances may become a new base for the attacker. From here, they may leverage the power of your reputation to launch subsequent attacks.

Examples

No public examples are available at this time.

Remediation

- Prohibit the sharing of account credentials between users and services.
- Leverage strong two-factor authentication techniques where possible.
- Employ proactive monitoring to detect unauthorized activity.
- Understand cloud provider security policies and SLAs.

References

- http://www.infoworld.com/d/cloud-computing/hackers-find-home-in-amazons-ec2-cloud-742
- http://vmetc.com/2009/03/12/virtual-machine-sniffer-on-esx-hosts/

Impact

Account and service hijacking, usually with stolen credentials, remains a top threat. With stolen credentials, attackers can often access critical areas of deployed cloud computing services, allowing them to compromise the confidentiality, integrity and availability of those services. Organizations should be aware of these techniques as well as common defense in depth protection strategies to contain the damage (and possible litigation) resulting from a breach.

CSA Guidance Reference

Domain 2: Governance and Enterprise Risk Management
Domain 9: Incident Response, Notification and Remediation
Domain 12: Identity and Access Management

Service Models

IaaS	PaaS	SaaS

Threat #7: Unknown Risk Profile

Description

One of the tenets of Cloud Computing is the reduction of hardware and software ownership and maintenance to allow companies to focus on their core business strengths. This has clear financial and operational benefits, which must be weighed carefully against the contradictory security concerns — complicated by the fact that cloud deployments are driven by anticipated benefits, by groups who may lose track of the security ramifications.

Versions of software, code updates, security practices, vulnerability profiles, intrusion attempts, and security design, are all important factors for estimating your company's security posture. Information about who is sharing your infrastructure may be pertinent, in addition to network intrusion logs, redirection attempts and/or successes, and other logs.

Security by obscurity may be low effort, but it can result in unknown exposures. It may also impair the in-depth analysis required highly controlled or regulated operational areas.

Examples

- IRS asked Amazon EC2 to perform a C&A; Amazon refused. http://news.qualys.com/newsblog/forrester-cloud-computing-qa.html
- Heartland Data Breach: Heartland's payment processing systems were using known-vulnerable software and actually infected, but Heartland was "willing to do only the bare minimum and comply with state laws instead of taking the extra effort to notify every single customer, regardless of law, about whether their data has been stolen." http://www.pcworld.com/article/158038/heartland_has_no_heart_for_violated_customers.html

Remediation

- Disclosure of applicable logs and data.
- Partial/full disclosure of infrastructure details (*e.g.*, patch levels, firewalls, etc.).
- Monitoring and alerting on necessary information.

References

- http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1349670,00.html
- http://chenxiwang.wordpress.com/2009/11/24/follow-up-cloud-security/
- http://www.forrester.com/cloudsecuritywebinar
- http://www.cerias.purdue.edu/site/blog/post/symposium_summary_security_in_the_cloud_panel/

Impact

When adopting a cloud service, the features and functionality may be well advertised, but what about details or compliance of the internal security procedures, configuration hardening, patching, auditing, and logging? How are your data and related logs stored and who has access to them? What information if any will the vendor disclose in the event of a security incident? Often such questions are not clearly answered or are overlooked, leaving customers with an unknown risk profile that may include serious threats.

CSA Guidance Reference

Domain 2: Governance and Enterprise Risk Management
Domain 3: Legal and Electronic Discovery
Domain 8: Data Center Operations
Domain 9: Incident Response, Notification and Remediation

Service Models

IaaS	PaaS	SaaS

