Topics

1. What is Cloud Computing?
2. The Same Old Security Problems
3. Virtualization Security
4. New Security Issues and Threat Model
5. Data Security
What is Cloud Computing?
What is Cloud Computing?

“Cloud computing is 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.”

NIST definition of Cloud Computing
Cloud Service Architectures as Layers

Application

OS + App Server Stack

Infrastructure

Platform

Software Application
Cloud Service Models Abstraction Layers
Multi-Tenancy

1. Tenant 1
   - Instance 1

2. Tenant 1
   - Instance
   - Same application but distinct instance/customer

3. Tenant 1
   - Instance
   - (+): Efficient use of server resources without apparent differences to end users
   - (-): Scalability limits

4. Tenant Load Balancer
   - Tenant 1
   - Tenant 2
   - Instance
   - Instance
Cloud Deployment Architectures

Cloud Computing Types

- Hybrid
  - Private/Internal
  - Public/External

- The Cloud
  - On Premises/Internal
  - Off Premises/Third Party
- Data Loss
- Downtimes
- Phishing
- Password Cracking
- Botnets and Other Malware

Same Old Security Issues
"Regrettably, based on Microsoft/Danger's latest recovery assessment of their systems, we must now inform you that personal information stored on your device—such as contacts, calendar entries, to-do lists or photos—that is no longer on your Sidekick almost certainly has been lost as a result of a server failure at Microsoft/Danger."
Rackspace to issue as much as $3.5M in customer credits after outage

Power failures in Dallas facility took customer servers offline last week.

By Jon Bıldıç, Network World
July 06, 2009 03:15 PM ET


UPDATE [11/07/09 12:43PM PDT]: This issue is resolved. Windows Azure is in the process of being restored.

UPDATE [11/07/09 9:36PM PDT]: We've identified and verified a recovery patch for this issue. We hope to have everything back to normal.

UPDATE [11/07/09 3:36PM PDT]: Recovery is underway. Windows Azure is experiencing an outage. We are in the process of restoring service.

What is affected: Applications may be impacted for some time.

Windows Azure is currently experiencing an outage. We are working on a recovery plan.

UPDATE [11/07/09 1:36PM PDT]: Windows Azure is currently experiencing an outage. We are working on a recovery plan.

What is affected: Applications may be impacted for some time.

When the outage began: About 10:30pm PST last night.

Who is affected: Potentially anyone currently running an application.

We will post updates to this thread throughout the day as we investigate the issue. There is currently no ETA for a fix.

Related Content
- 10 cloud computing companies to watch
- Rackspace launches cloud storage
- Rackspace challenges Amazon with new cloud server services
- China blocks microblogs for ‘Jasmine Revolution’

Amazon S3 Availability Event: July 20, 2008

We wanted to provide some additional detail about the problem we experienced on Sunday, July 20th.

At 8:40am PDT, we determined that servers within Amazon S3 were having problems communicating with each other. As a result of the outage, Amazon S3 uses a gossip protocol to quickly spread server state information throughout the system. This allows Amazon S3 to quickly route around failed or unreachable servers, among other things. When one server connects to another as part of processing a customer request, it starts by gossiping about the system state. Only after gossip is completed will the server send along the information related to the customer request. On Sunday, we saw a large number of servers that were spending almost all of their time gossiping and a disproportionate amount of servers that had failed while gossiping. With a number of servers gossiping and failing while gossiping, Amazon S3 wasn’t able to successfully process many customer requests.

At 1:32am PST, after exploring several options, we determined that we needed to shut down all communication between Amazon S3 servers, shut down all components used for request processing, clear the system state, and then reactivate the request processing components. By 11:05am PST, all server-to-server communication was stopped, request processing components shut down, and the system state cleared. By 2:20pm PST, we restored internal communication between all Amazon S3 servers and began reactivating request processing components concurrently in both the US and EU.

At 2:57PM PDT, Amazon S3’s EU location began successfully completing customer requests. The EU location began successfully completing customer requests and request rates and error rates in the EU had returned to normal. At 4:02PM PDT, Amazon S3’s US location began successfully completing customer requests, and request rates and error rates had returned to normal by 4:18PM PDT.

We have now determined that message corruption was the cause of the server-to-server communication problems. More specifically, we found that there were a handful of messages on Sunday morning that had a single bit corrupted such that the message was still intelligible, but the system state information was incorrect. We use MD5 checksums throughout the system, for example, to prevent, detect, and recover from corruption...
Phishing

“hey! check out this funny blog about you...”

---

Microsoft has confirmed that the publication of thousands of Hotmail passwords was the result of a phishing attack against users of the popular email service.

Precise details of the strike, which was first uncovered on Monday, remain unclear. But in a statement, the American software company said...
Cloud Computing Used to Hack Wireless Passwords

German security researcher Thomas Roth has found an innovative use for cloud computing: cracking wireless networks that rely on pre-shared key passphrases, such as those found in homes and smaller businesses.

Roth has created a program that runs on Amazon’s Elastic Cloud Computing (EC2) system. It uses the massive computing power of EC2 to run through 400,000 possible passwords per second, a staggering amount, millions of rounds of brute force calculations. As a result, it’s able to efficiently process large amounts of data and solve complex problems.

In other words, this isn’t a clever or elegant hack, and it doesn’t rely on any flaw in wireless networking technology. Roth’s software merely generates millions of passphrases, encrypts them, and sees if they allow access to the network.

However, employing the theoretically infinite resources of cloud computing to brute force a password is the clever part.

Purchasing the computers to run such a crack would cost tens of thousands of dollars, but Roth claims that a typical wireless password can be guessed by EC2 and his software in about six minutes. He proved this by hacking networks in the area where he lives. The type of EC2 computers used in the attack costs 25 cents per minute, so $1.68 is all it could take to lay open a wireless network.

As of today, Amazon EC2 is providing what they call “Cluster GPU Instances”: An instance in the Amazon cloud that provides you with the power of two NVIDIA Tesla “Fermi” M2050 GPUs. The exact specifications look like this:

- 22 GB of memory
- 33.5 EC2 Compute Units (2 x Intel Xeon X5570, quad-core “ Nehalem” architecture)
- 2 x NVIDIA Tesla “Fermi” M2050 GPUs
- 1690 GB of instance storage
- 64-bit platform
- I/O Performance: Very High (10 Gigabit Ethernet)
- API name: cg1.4xlarge

GPUs are known to be the best hardware accelerator for cracking passwords, so I decided to give it a try: How fast can this instance type be used to crack SHA1 hashes?

Using the CUDA-Multipass, I was able to crack all hashes from this file with a password length from 1-6 in only 49 minutes (1 hour costs 2.10$ by the way.).

This just shows you one more time that SHA1 for password hashing is deprecated – You really don’t want to use it anymore! Instead, use something like scrypt or PBKDF2! Just imagine
Botnets and Malware

Treasury Dept. has cloud hacked

Mon, 2010-05-10 02:20 PM
By: Melissa Jane hyperfield

The Treasury Department was hacked last week, leaving the Web site for its Bureau of Engraving and Printing - the agency responsible for printing U.S. dollars - down from May 3 to May 7.

The Treasury had moved to a cloud platform last year and the department blamed its cloud computing provider (the Treasury's Web site is hosted by Network Solutions) for the incident.

In a statement released May 4, the Treasury Department said, "The Bureau of Engraving and Printing (BEP) entered the cloud computing arena last year. The hosting company used by BEP had an intrusion and as a result of that intrusion, numerous websites (BEP and non-BEP) were affected. On May 3, the Treasury Government Security Operations Center was made aware of the problem and subsequently notified BEP.

"BEP has four Internet address URLs all pointing to one public website. Those URLs are BEP.gov, BEP.treas.gov, Moneyfactory.gov and Moneyfactory.com. BEP has since suspended the website. Through discussions with the provider, BEP is aware of the remediation steps required to restore the site and is currently working toward resolution."

Roger Thompson, chief research officer for IT security software vendor AVG Technologies USA, Inc. of Chelmsford, MA, was the first to notice the hack, and reported it to the FBI. Thompson revealed that the hackers had added a tiny snippet of a virtually undetectable frame HTML code that redirected visitors to a Ukrainian Web site. From there, a variety of Web-based attacks were launched using an easy-to-purchase malicious toolkit, called the Elcomray Exploit Pack. Only first-time users were affected; returning to the site a second time did not lead to more attacks, making it difficult for law enforcement to track the perpetrators.

For less $1,000 - the Elcomray Exploit Pack costs only $700 - even the most minimally talented hacker can exploit flaws in Microsoft Internet Explorer, Firefox and Adobe Acrobat Reader. The widespread problem of low-cost hacking that takes advantage of this commonly used software was highlighted in the 2010 Symantec report.

Despite the inherent risks involved in cloud platforms, IT experts tend to agree that the government would reap more benefits from using them, rather than not, and have encouraged government agencies to move towards the cloud in recent months.

"I am not going to say this will scare users away from cloud computing," says Thomas Krafft. "But it definitely brings into clear focus the issues.

Zeus "in-the-cloud"

Published: December 28, 2009, 04:38 AM by Methusela Cebrian Ferrer

A new wave of a Zeus bot (Zbot) variant was spotted taking advantage of Amazon EC2's cloud-based services for its C&C (command and control) functionalities.

This notable scheme is a highlight from the latest spammed executable "amasz.exe" (63.498 bytes), for which we have recently published blog titled "Christmas is knocking on the door, so does the malware!"

Evil greeting card arrives to users' mailbox

Entices users to click a malicious URL which links to a hacked legitimate website perpetrated for criminal activity such as serving Zeus bot variant.

Once executed, the Zeus bot variant will communicate to its C&C server, which in this case is controlled using "in-the-cloud" based services.

[Figure 01 - Zeus displays cyber-criminal activities]

<table>
<thead>
<tr>
<th>Action</th>
<th>URL</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>POST</td>
<td><a href="http://kw-270.com/p001.amazonaws.com/zeus/gate.php">http://kw-270.com/p001.amazonaws.com/zeus/gate.php</a></td>
<td>svchot.eve (ar)</td>
</tr>
<tr>
<td>POST</td>
<td><a href="http://kw-270.com/p001.amazonaws.com/zeus/gate.php">http://kw-270.com/p001.amazonaws.com/zeus/gate.php</a></td>
<td>svchot.eve (ar)</td>
</tr>
<tr>
<td>POST</td>
<td><a href="http://kw-270.com/p001.amazonaws.com/zeus/gate.php">http://kw-270.com/p001.amazonaws.com/zeus/gate.php</a></td>
<td>svchot.eve (ar)</td>
</tr>
<tr>
<td>POST</td>
<td><a href="http://kw-270.com/p001.amazonaws.com/zeus/gate.php">http://kw-270.com/p001.amazonaws.com/zeus/gate.php</a></td>
<td>svchot.eve (ar)</td>
</tr>
</tbody>
</table>

[Figure 02 - Zeus bot variant communication]

As shown in Figure 03, the Zeus bot variant injects code into the system processes (such as svchot.eve) and connects to its cloud server [Figure 02] for configuration (config.bin) of the master for its criminal activity.
Features
- Isolation
- Snapshots

Issues
- State Restore
- Complexity
- Scaling
- Transience
- Data Lifetime

Virtualization Security
Virtualization Security Features: Isolation

Using a VM for each application provides isolation

- More than running 2 apps on the same server.
- Less than running on 2 physical servers.

![Virtualization Diagram]

- VM$_1$ Guest
- VM$_2$ Guest
- VM$_n$ Guest

Host Applications

- Hypervisor

Host Operating System

Hardware Layer (CPU, RAM, etc.)
Virtualization Security Features: Snapshot

- VMs can record state.
- In event of security incident, revert VM back to an uncompromised state.
- Must be sure to patch VM to avoid recurrence of compromise.
State Restore

- VMs can be restored to an infected or vulnerable state using snapshots.
- Patching becomes undone.
- Worms persist at low level forever due to reappearance of infected and vulnerable VMs.
Complexity

- Hypervisor may be simple or not, but
- It is often another layer on top of host OS, adding complexity and vulnerabilities.
Hypervisor Security

Vulnerability consequences

- Guest code execution with privilege
- VM Escape (Host code execution)

---

<table>
<thead>
<tr>
<th>Vendor</th>
<th>CVEs</th>
</tr>
</thead>
<tbody>
<tr>
<td>KVM</td>
<td>32</td>
</tr>
<tr>
<td>QEMU</td>
<td>23</td>
</tr>
<tr>
<td>VirtualBox</td>
<td>9</td>
</tr>
<tr>
<td>VMware</td>
<td>126</td>
</tr>
<tr>
<td>Xen</td>
<td>86</td>
</tr>
</tbody>
</table>
Inter-VM Attacks

- Attack via shared clipboard
  - http://www.securiteam.com/securitynews/5GP021FKKO.html
- Use shared folder to alter other VM’s disk image
  - CVE-2007-1744
Scaling

- Growth in physical machines limited by budget and setup time.
- Adding a VM is easy as copying a file, leading to explosive growth in VMs.
- Rapid scaling can exceed capacity of organization’s security systems.
Transience

Users often have specialized VMs.
- Testing
- Different app versions
- Demos
- Sandbox

that are not always up, preventing network from converging to a known state.

- Infected machines appear, attack, then disappear from the network before can be detected.
- Vulnerable systems likewise appear too briefly to be detected and patched.
Data Lifetime

Although data was correctly sanitized from VM disk and/or memory, snapshots can retain multiple copies of both VM memory and disk data.
- Accountability
- No Security Perimeter
- Larger Attack Surface
- New Side Channels
- Lack of Auditability
- Regulatory Compliance
- Data Security

New Security Issues
Accountability

SaaS

PaaS

IaaS

* Few exceptions

Cloud Provider

Cloud Consumer

Application
Web/App/DB server
Computing
Network
Storage
No Security Perimeter

- Little control over physical or network location of cloud instance VMs
- Network access must be controlled on a host by host basis.
Larger Attack Surface

Cloud Provider

Your Network

Attacker

VM₁
Guest

VM₂
Guest

VM₃
Guest

VM₄
Guest

... VMₙ
Guest

Hypervisor
New Side Channels

- You don’t know whose VMs are sharing the physical machine with you.
  - Attackers can place their VMs on your machine.
  - See “Hey, You, Get Off of My Cloud” paper for how.

- Shared physical resources include
  - CPU data cache: Bernstein 2005
  - CPU branch prediction: Onur Acııçmez 2007
  - CPU instruction cache: Onur Acııçmez 2007

- In single OS environment, people can extract cryptographic keys with these attacks.
Lack of Auditability

- Only cloud provider has access to full network traffic, hypervisor logs, physical machine data.
- Need mutual auditability
  - Ability of cloud provider to audit potentially malicious or infected client VMs.
  - Ability of cloud customer to audit cloud provider environment.
Regulatory Compliance
Certifications

Is AWS now PCI certified?

The AWS core infrastructure and services listed below are PCI D by an authorized independent Qualified Security Assessor.

PCI “certification” is a term reserved for those merchants who AWS, as a service provider, does not directly manage cardholders not require certification). AWS provides a secure environment to establish a secure cardholder environment and to achieve their underlying technology infrastructure is compliant. Achieving PCI helps our customers obtain their own PCI certification.

Service provider levels are defined as:

- Level 1: Any service provider that stores, processes and
- Level 2: Any service provider that stores, processes and annually

What Amazon Web Services product offering transmission of credit card data?

Services that support the processing, storage, and transmission have been validated as being compliant with PCI standards. The

- Amazon Elastic Compute Cloud (EC2)
- Amazon Simple Storage Service (S3)
- Amazon Elastic Block Storage (EBS)
- and Amazon Virtual Private Cloud (VPC)

ISO 27001 Certification

The following information will help you understand in greater detail why ISO 27001 certification is important and how it helps to demonstrate our commitment to providing a secure infrastructure for your business-critical applications and data.

What is ISO 27001 certification?

ISO 27001 is a security management standard that specifies security management best practices and comprehensive security controls following the ISO 27002 best practice guidance. This is a widely-recognized international security standard in which our customers showed significant interest. Certification in the standard requires us to:

- Systematically evaluate our information security risks, taking into account the impact of company threats and vulnerabilities
- Design and implement a comprehensive suite of information security controls and other forms of risk management to address company and architecture security risks
- Adopt an overarching management process to ensure that the information security controls meet the our information security needs on an ongoing basis

The key to the ongoing certification under this standard is the effective management of a rigorous security program. The Information Security Management System (ISMS) required under this standard defines how we perpetually manage security in a holistic, comprehensive way. The ISO 27001 certification is specifically focused on the AWS ISMS and measures how our internal processes follow the ISO standard. Certification means a third-party accredited independent auditor has performed an assessment of our processes and controls and confirms they are operating in alignment with the comprehensive ISO 27001 certification standard.

How does this certification impact AWS?

AWS welcomes the ISO 27001 standard and best practices into our organization. The certification confirms our longstanding commitment to the security of our services to our customers. Going through the certification process confirms that we are addressing each element of the ISO standard and that our management practices follow internationally-recognized best practices.

What does this mean to you as a customer?

Our ISO 27001 certification demonstrates our commitment to information security at every level. Compliance with this internationally-recognized standard, validated by an independent third-party audit, confirms that our security management program is comprehensive and follows leading practices. This certification provides more clarity and assurance for customers evaluating the breadth and strength of our security practices.
Data in Transit
Data at Rest
Data in Processing
Data Remanence
Homomorphic Encryption
## Data Security

<table>
<thead>
<tr>
<th>Confidentiality</th>
<th>Symmetric Encryption</th>
<th>Homomorphic Encryption</th>
<th>SSL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrity</td>
<td>MAC</td>
<td>Homomorphic Encryption</td>
<td>SSL</td>
</tr>
<tr>
<td>Availability</td>
<td>Redundancy</td>
<td>Redundancy</td>
<td>Redundancy</td>
</tr>
</tbody>
</table>

- Storage
- Processing
- Transmission

Plus data remanence.
Public Key Cryptography

Alice

Key Generation Program

01111011001
Large Random Number

Public
Private

Bob

Encrypt

6EB6957008E03CE4
Alice's public key

Decrypt
Alice's private key

Hello Alice!

Hello Alice!
Homomorphic Public-key Encryption

Public-key Crypto with additional procedure: \textbf{Eval}

\[ c^* \leftarrow \textbf{Eval}_{pk}(\Pi, c_1,\ldots,c_n) \]

\( \Pi \) a Boolean circuit with \textsc{ADD}, \textsc{MULT} mod 2

Encryption of inputs \( m_1,\ldots,m_n \) to \( \Pi \)

Encryption of output value \( m^*=\Pi(m_1,\ldots,m_n) \)

Homomorphic encryption slides borrowed from people.csail.mit.edu/shaih/pubs/IHE-S-and-P-day.ppt
An Analogy: Alice’s Jewelry Store

- Alice’s workers need to assemble raw materials into jewelry
- But Alice is worried about theft

How can the workers process the raw materials without having access to them?
An Analogy: Alice’s Jewelry Store

- Alice puts materials in locked glove box
  - For which only she has the key
- Workers assemble jewelry in the box
- Alice unlocks box to get “results”
The Analogy

- **Enc**: putting things inside the box
  - Anyone can do this (imagine a mail-drop)
  - \( c_i \leftarrow \text{Enc}_{pk}(m_i) \)

- **Dec**: Taking things out of the box
  - Only Alice can do it, requires the key
  - \( m^* \leftarrow \text{Dec}_{sk}(c^*) \)

- **Eval**: Assembling the jewelry
  - Anyone can do it, computing on ciphertext
  - \( c^* \leftarrow \text{Eval}_{pk}(\Pi, c_1, \ldots, c_n) \)

- \( m^* = \Pi(m_1, \ldots, m_n) \) is “the ring”, made from “raw materials” \( m_1, \ldots, m_n \)
References


