



Cloud Computing Security

Cincinnati Chapter Meeting
February 22nd, 2011
James Walden
Northern Kentucky University

OWASP

Copyright © The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document
under the terms of the OWASP License.

The OWASP Foundation
<http://www.owasp.org>

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



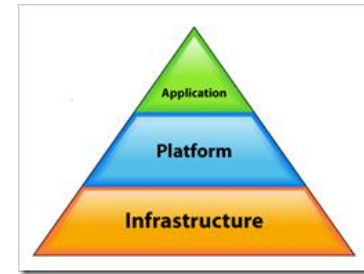
What is Cloud Computing?

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.”

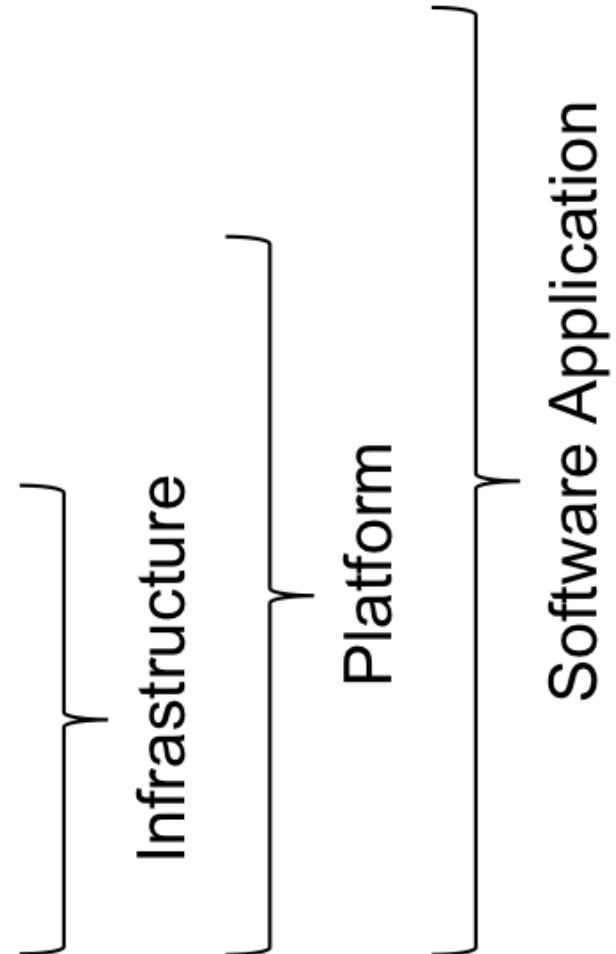
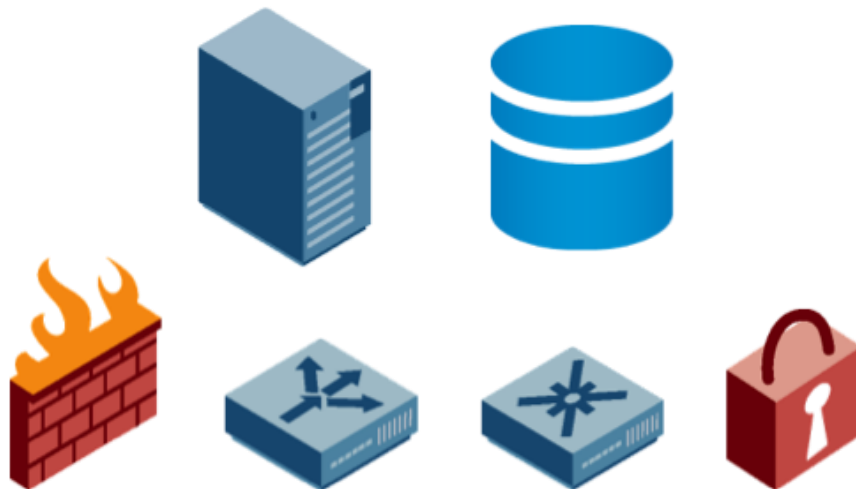
NIST definition of Cloud Computing

Cloud Service Architectures as Layers



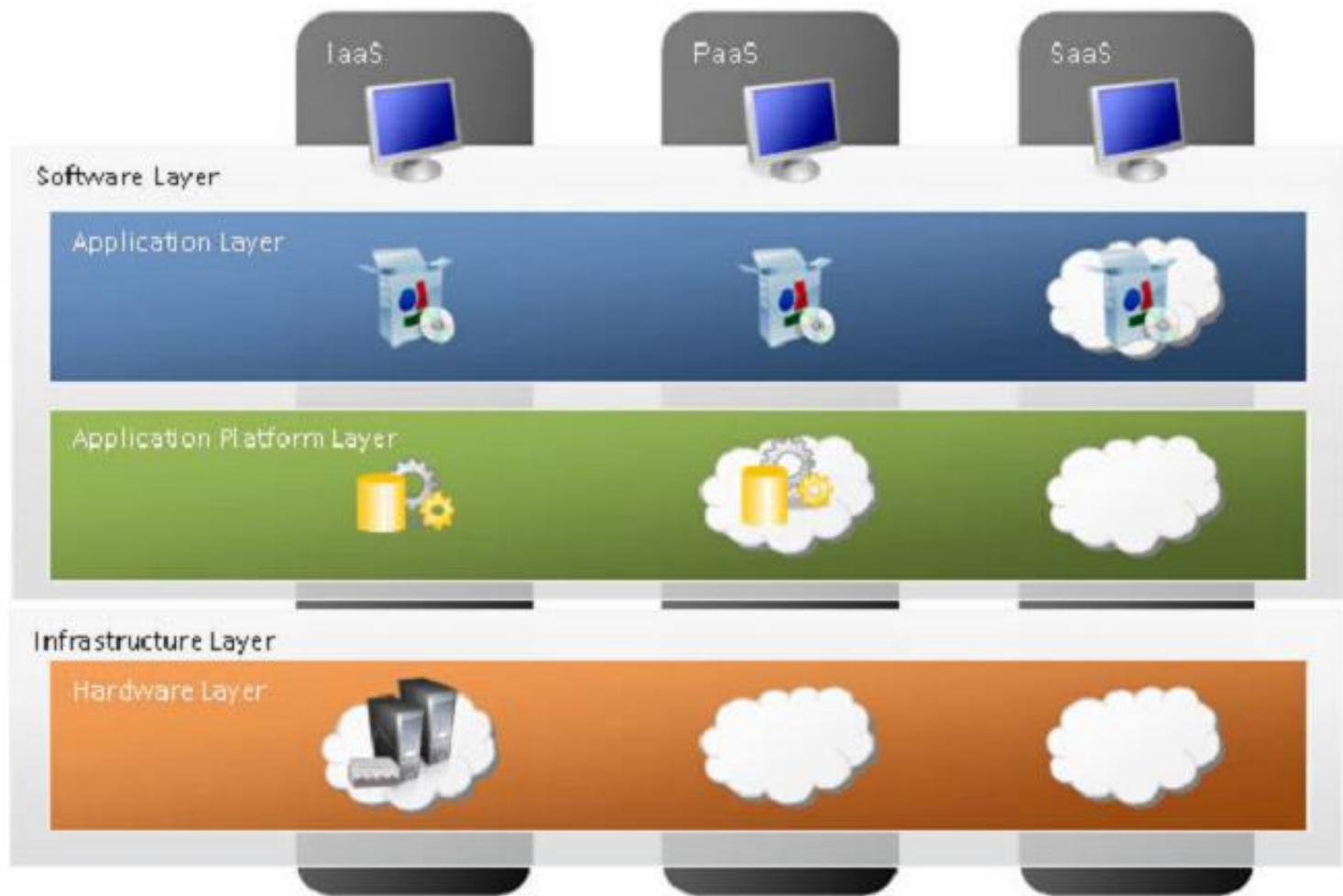
Application

OS + App Server Stack

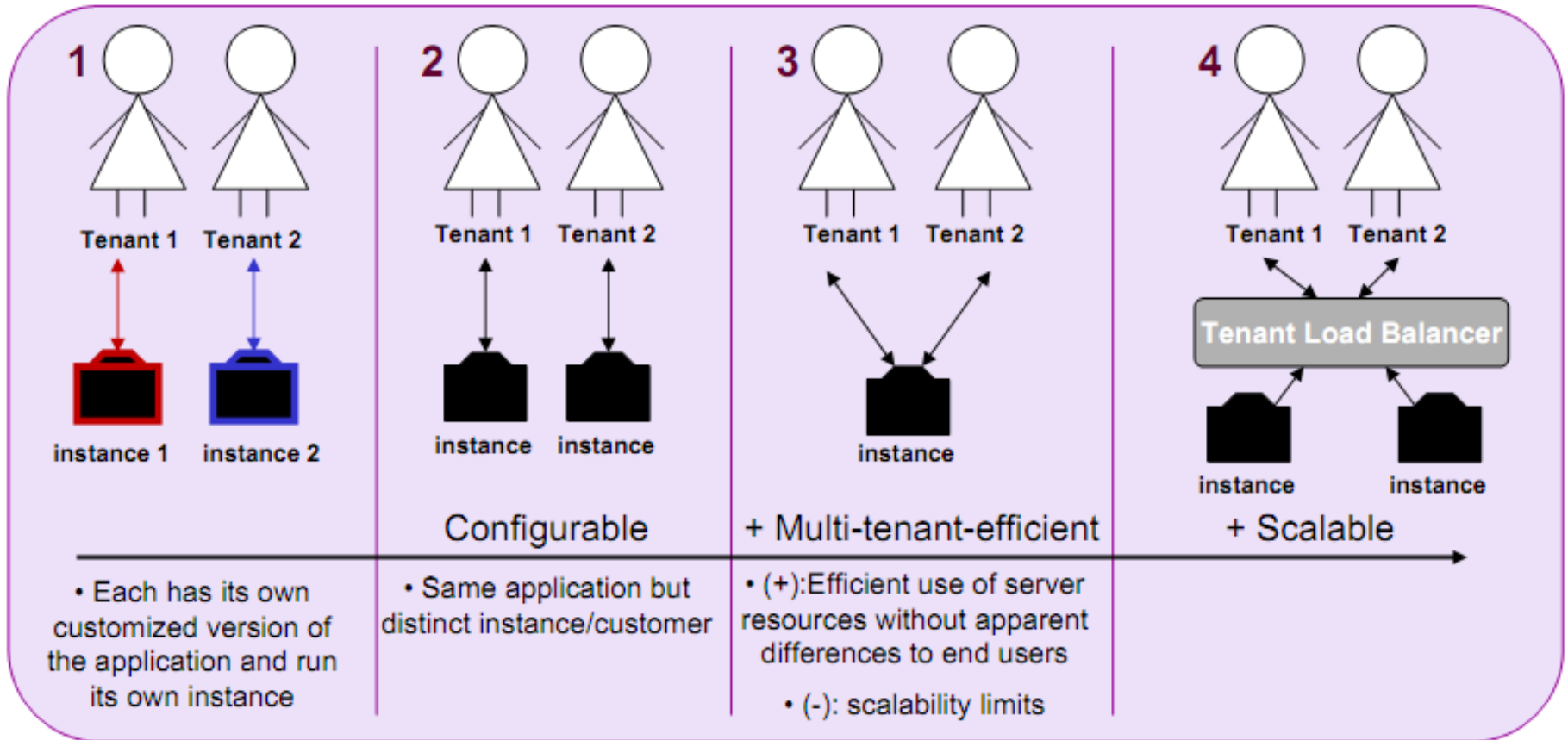


Cloud Service Models Abstraction Layers

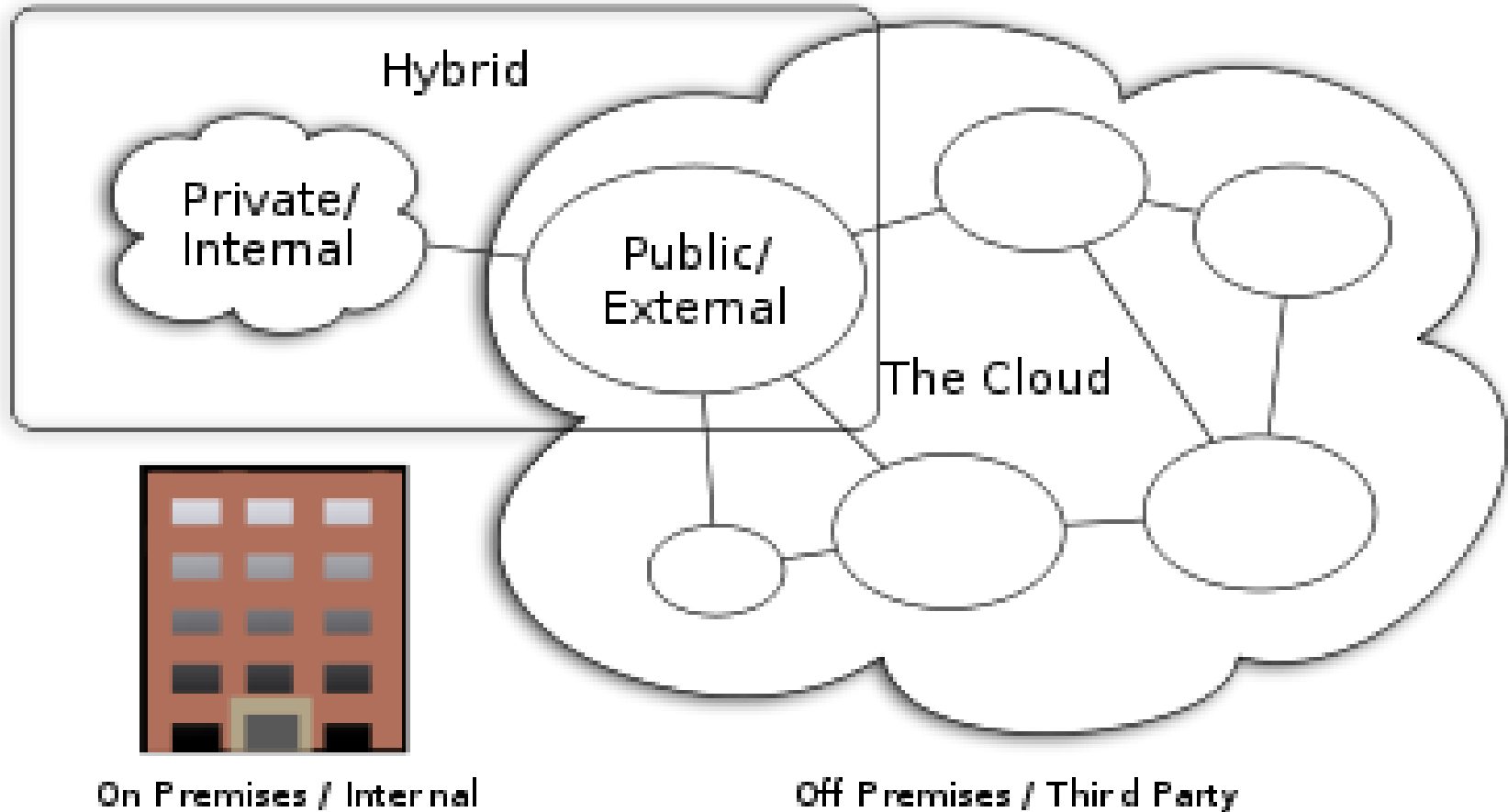
Levels of abstraction in "cloud computing"




Multi-Tenancy



Cloud Deployment Architectures



Cloud Computing Types

- 
- Data Loss
 - Downtimes
 - Phishing
 - Password Cracking
 - Botnets and Other Malware

Same Old Security Issues

Data Loss

"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."



Downtimes

msdn Search MSDN with Bing

Home Library Learn Code Downloads Support Community

Microsoft Developer Network > Forums Home > Developing Applications with Azure - Archive > RESOLVED: Windows Azure Outage

Ask a question

Search Forums: Search Windows

RESOLVED: Windows Azure Outage

Locked



Steve Marx



UPDATE [3/17/09 7:44PM PDT]: Summary of what happened and on the Windows Azure blog: <http://blogs.msdn.com/windowsazure/windows-azure-malfunction-this-week-end.aspx>

Sign In to Vote

UPDATE [8:24PM PDT]: This issue is **resolved**. Windows Azure is

UPDATE [3:36PM PDT]: We've identified and verified a recovery plan applying throughout the cloud. ETA is five hours to complete recovery everything's back to normal.

Windows Azure is currently experiencing an outage. We are investigating ETA for a resolution. A large number of deployments are currently restarted.

What is affected: Applications may be unreachable or in "stopped" periods of 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 outage. There is currently no ETA for a fix.

Edited by [Steve Marx](#) Saturday, March 14, 2009 10:36 PM

Edited by [Steve Marx](#) Sunday, March 15, 2009 3:26 AM

Edited by [Steve Marx](#) Sunday, March 15, 2009 3:25 AM

Edited by [Steve Marx](#) Saturday, March 14, 2009 6:07 PM

Edited by [Steve Marx](#) Wednesday, March 18, 2009 2:45 AM

NETWORKWORLD

News | Blogs & Columns | Subscriptions | Videos | Events | More

Security | LAN & WAN | UC / VoIP | Infrastructure Mgmt | Wireless | Software | Data Center | SM

Cloud Computing | Virtualization | Disaster Recovery | Server | PC | Network Storage | Storage Management | Green

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 Brodtkin](#), Network World
July 06, 2009 03:15 PM ET

16 Comments | Print

UPDATE: Rackspace's Dallas data center was that was caused by the failure of an electrical connectivity to some servers," the company through its [blog](#) and [Twitter](#).

[Rackspace](#) is being forced to pay out between to customers in the wake of a power outage

Rackspace, which offers a variety of hosting services, suffered power generator failures on June 2 part of the day.

Rackspace [reported](#) to the [Securities and Exchange Commission](#) one-time service credits to impacted customers. A number hasn't been determined as Rackspace issues service credits due to these events."

Related Content

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

[View more related content](#)



SERVICE HEALTH DASHBOARD

[Amazon Web Services](#) » [Service Health Dashboard](#) » Amazon S3 Availability Event: July 20, 2008

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, error rates in all Amazon S3 datacenters began to quickly climb and our alarms went off. By 8:50am PDT, error rates were significantly elevated and very few requests were completing successfully. By 8:55am PDT, we had multiple engineers engaged and investigating the issue. Our alarms pointed at problems processing customer requests in multiple places within the system and across multiple data centers. While we began investigating several possible causes, we tried to restore system health by taking several actions to reduce system load. We reduced system load in several stages, but it had no impact on restoring system health.

At 9:41am PDT, we determined that servers within Amazon S3 were having problems communicating with each other. As background information, 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's 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 large number of servers gossiping and failing while gossiping, Amazon S3 wasn't able to successfully process many customer requests.

At 10:32am PDT, 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's state, and then reactivate the request processing components. By 11:05am PDT, all server-to-server communication was stopped, request processing components shut down, and the system's state cleared. By 2:20pm PDT, we'd 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 came back online before the US because there are fewer servers in the EU. By 3:10pm PDT, 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 4:58pm PDT.

We've 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 that occurred while the system was in a "stopped" state. However, we didn't have the same

the power outage was the result of a



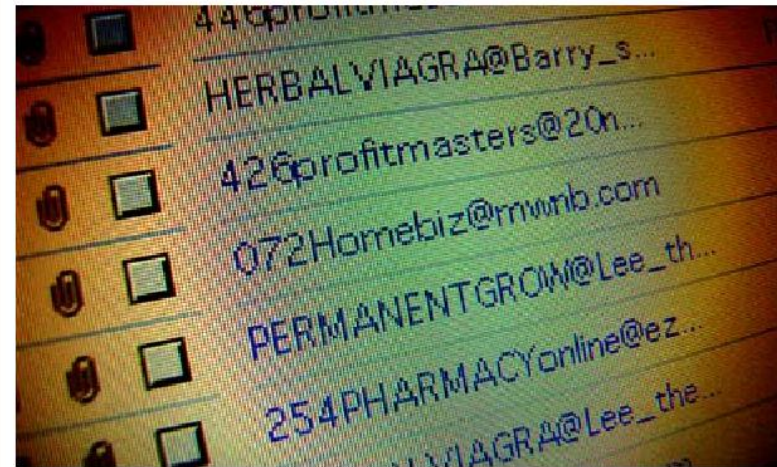
Phishing

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



Hotmail password breach blamed on phishing attack

Bobbie Johnson, San Francisco
guardian.co.uk, Tuesday 6 October 2009 07:58 BST
Article history



Attack: Spam emails may have been responsible. Photograph: Roger Tooth

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



Password Cracking

PCWorld News Reviews How-To's Downloads Shop & Compare Apps Business Center

PCWorld Business Center Discover news, guides, and products for your business

Software & Services Office Hardware Security Servers & Storage Cell Phones & Mobile

Security Alert Practical security advice » More Security Alert » RSS » All Blogs Enter your email to get

Tweet 69 2 Digg Like 40 4 Comments +9 Recommendations Email Print

BUSINESS CENTER Jan 10, 2011 8:31 pm

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.

SIMILAR ARTICLES:

[Gawker Hack Exposes Ridiculous Password Habits](#)

[What Cloud Computing Means For the Real World](#)

[Can 'Encrypted Blobs' Help With Secure Cloud Computing?](#)

[Virtualization is Key to Cloud Security](#)

[7 Ways to Avoid Getting Hacked by Anonymous](#)

[Password Reuse Is All Too Common, Research Shows](#)

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, hitherto unheard of outside supercomputing circles--and very likely made possible because EC2 now allows graphics processing units (GPUs) to be used for computational tasks. Among other things, these are particularly suited to password cracking tasks.

In other words, this isn't a clever or elegant hack, and it doesn't rely on a 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 28 cents per minute, so \$1.68 is all it could take to lay open a wireless network.

Cracking Passwords In The Cloud: Amazon's New EC2 GPU Instances

Posted on 15. November 2010 by Thomas Roth

Update: Great article about this at [Threatpost!](#) This also got [slashdotted](#), featured on [Tech News Today](#) and there's a [ZDNet article](#) about this.

Update: Because of the huge impact I have clarified some things [here](#)

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-Multiforce, 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.):

```
Compute done: Reference time 2950.1 seconds
Stepping rate: 249.2M MD4/s
Search rate: 3488.4M NTLM/s
```

This just shows 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



- Home
- Technology Sectors
- Market Sectors
- Buyer's Guide
- Back Issues
- Videos

Technology Sectors

- [Access Control | Identification](#)
- [CBRNE | Detection](#)
- [Communications](#)
- [Cyber Security](#)
- [Disaster Preparedness | Emergency Response](#)
- [Education | Training](#)
- [IT Security](#)
- [Perimeter Protection](#)
- [Video Surveillance | CCTV](#)

Market Sectors

- [Airport | Aviation Security](#)
- [Border Security](#)
- [Federal | Agencies | Legislative](#)
- [Infrastructure Protection](#)
- [Law Enforcement | First Responders](#)
- [Maritime | Port Security](#)
- [Military | Force Protection](#)
- [State | Local Security](#)
- [Security Services](#)

Treasury Dept. has cloud hacked

Mon, 2010-05-10 02:20 PM

By: [Melissa Jane Kronfeld](#)

[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 iframe 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 Eleonore 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 [Eleonore 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 09 2009, 04:39 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 "xmas2.exe" (63,488 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]

Action	URL	Details
GET	http://ec2-170.compute-1.amazonaws.com/zeus/config.bin	svchost.exe [sr
POST	http://ec2-170.compute-1.amazonaws.com/zeus/gate.php	svchost.exe [sr
POST	http://ec2-170.compute-1.amazonaws.com/zeus/gate.php	svchost.exe [sr
POST	http://ec2-170.compute-1.amazonaws.com/zeus/gate.php	svchost.exe [sr
POST	http://ec2-170.compute-1.amazonaws.com/zeus/gate.php	svchost.exe [sr

[Figure 02 - Zeus bot variant communication]

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

■ Features

- ▶ Isolation
- ▶ Snapshots

■ Issues

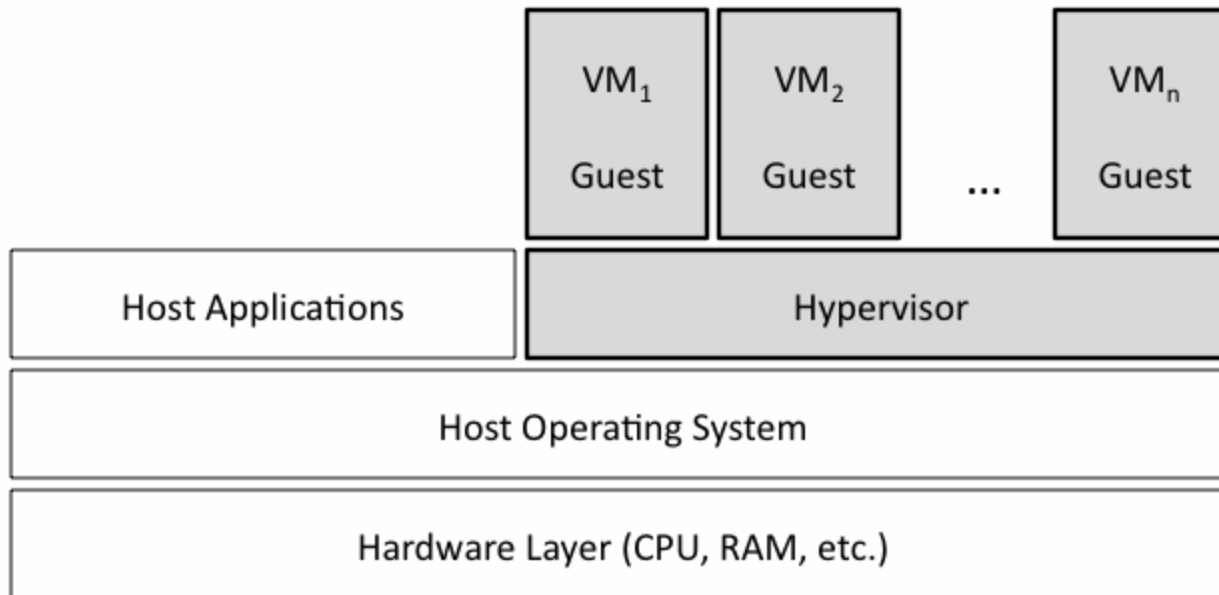
- ▶ State Restore
- ▶ Complexity
- ▶ Scaling
- ▶ Transience
- ▶ Data Lifetime

Virtualization Security

Virtualization Security Features: Isolation

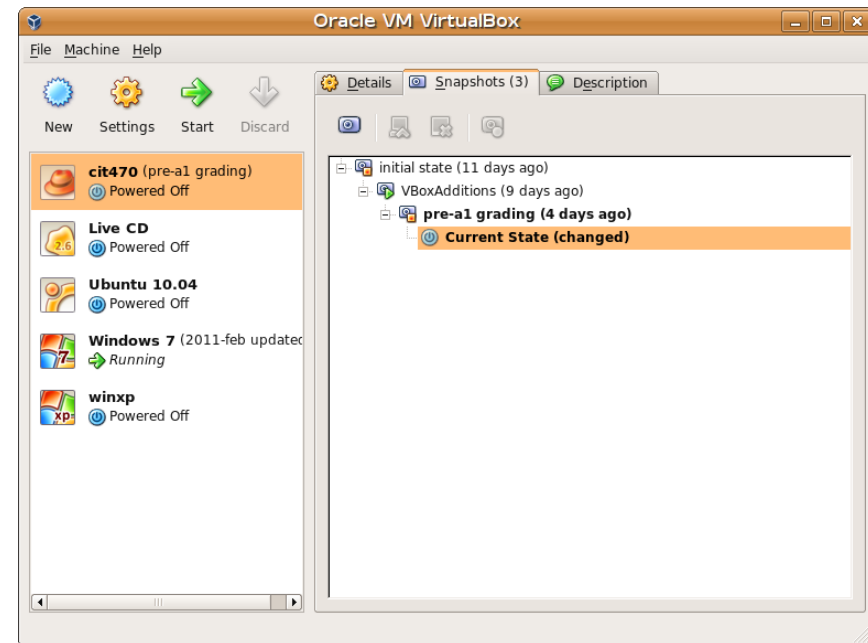
Using a VM for each application provides isolation

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



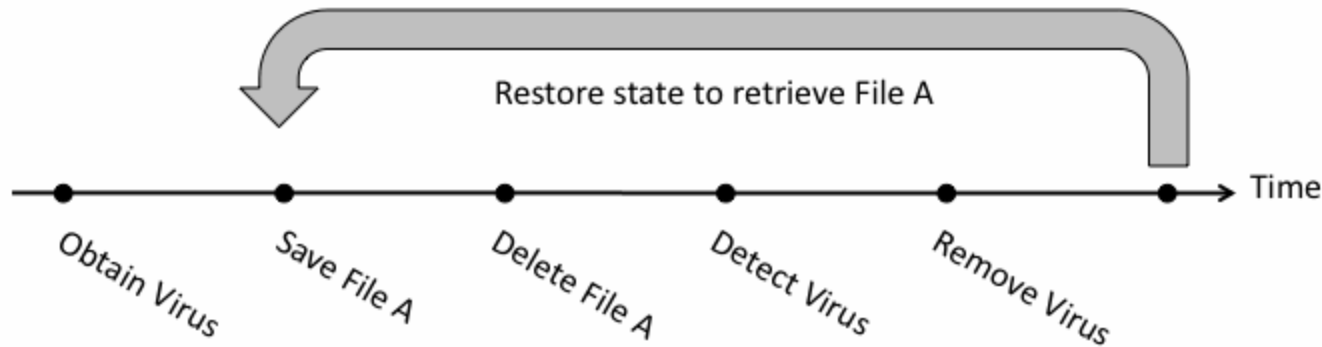
Virtualization Security Features: Snapshot

- 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.



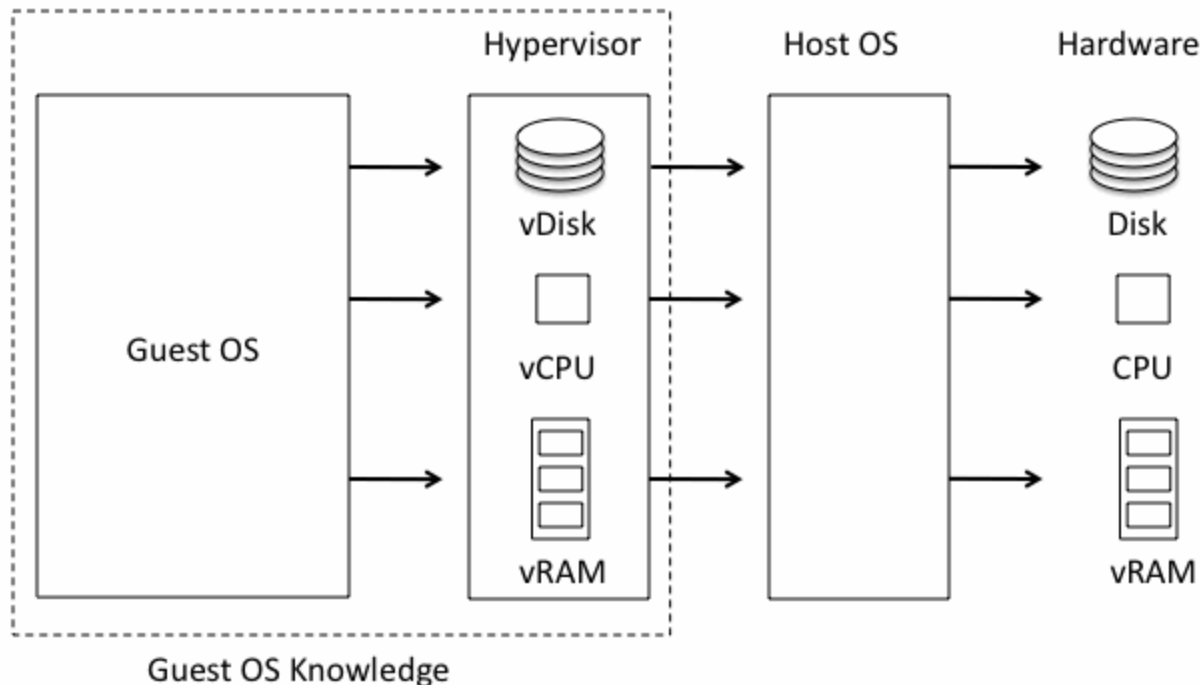
State Restore

- 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.



VMware Security Advisories (VMSAs)

VMSA-2009-0006

VMware Hosted products and patches for ESX and ESXi resolve a critical security vulnerability

VMware Security Advisory

Advisory ID: VMSA-2009-0006
 Synopsis: VMware Hosted products and patches for ESX and ESXi resolve a critical security vulnerability
 Issue date: 2009-04-10
 Updated on: 2009-04-10 (initial release of advisory)
 CVE numbers: CVE-2009-1244

1. Summary

Updated VMware Hosted products and patches for ESX and ESXi resolve a critical security vulnerability.

2. Relevant releases

VMware Workstation 6.5.1 and earlier,
 VMware Player 2.5.1 and earlier,
 VMware ACE 2.5.1 and earlier,
 VMware Server 2.0,
 VMware Server 1.0.8 and earlier,
 VMware Fusion 2.0.3 and earlier,

VMware ESXi 3.5 without patch ESXe350-200904201-0-SG,

VMware ESX 3.5 without patch ESX350-200904201-SG,

VMware ESX 3.0.3 without patch ESX303-200904403-SG,

VMware ESX 3.0.2 without patch ESX-1008421.

NOTE: General Support for Workstation version 5.x ended on 2009-03-19. Users should plan to upgrade to the latest Workstation version 6.x release.

Extended support for ESX 3.0.2 Update 1 ends on 2009-08-08. Users should plan to upgrade to ESX 3.0.3 and preferably to the newest release available.

3. Problem Description

a. Host code execution vulnerability from a guest operating system

A critical vulnerability in the virtual machine display function might allow a guest operating system to run code on the host.

This issue is different from the vulnerability in a guest virtual device driver reported in VMware security advisory VMSA-2009-0005 on 2009-04-03. That vulnerability can cause a potential denial of service and is identified by CVE-2008-4916.

The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CVE-2009-1244 to this issue.

Xen CVE-2008-1943

VBox CVE-2010-3583

Hypervisor Security

Vulnerability consequences

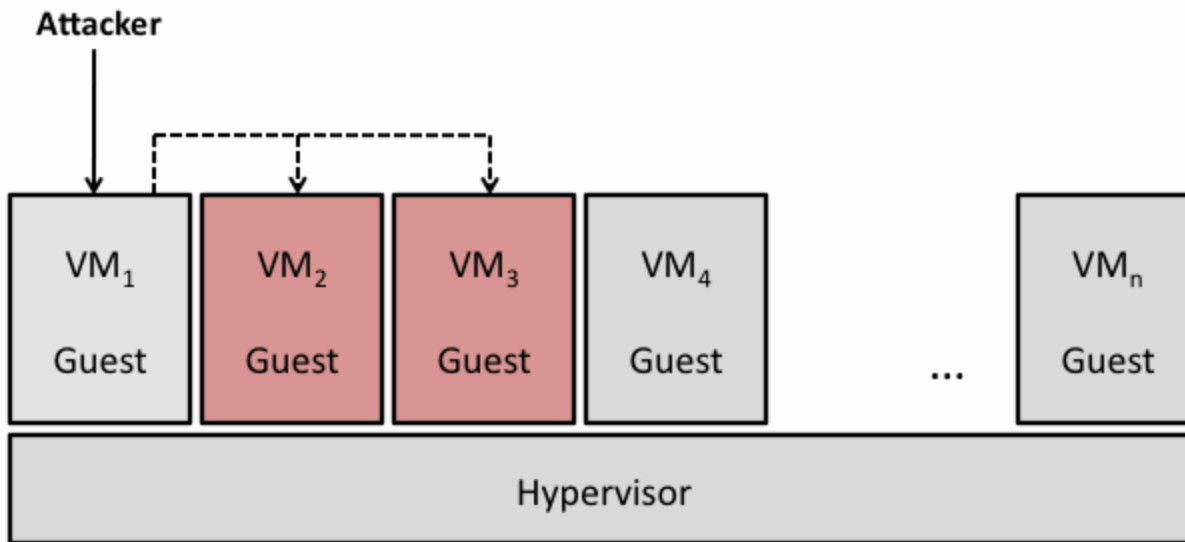
- ▶ Guest code execution with privilege
- ▶ VM Escape (Host code execution)

Vendor	CVEs
KVM	32
QEMU	23
VirtualBox	9
VMware	126
Xen	86



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.

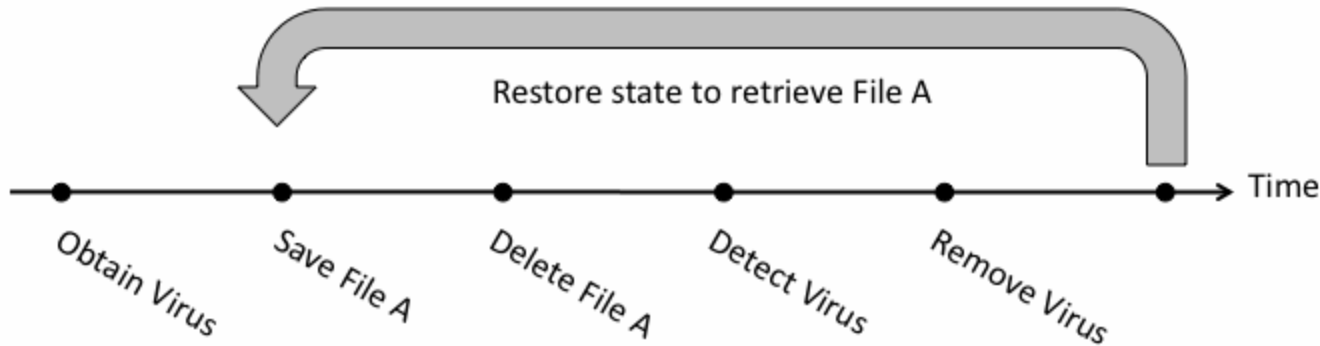
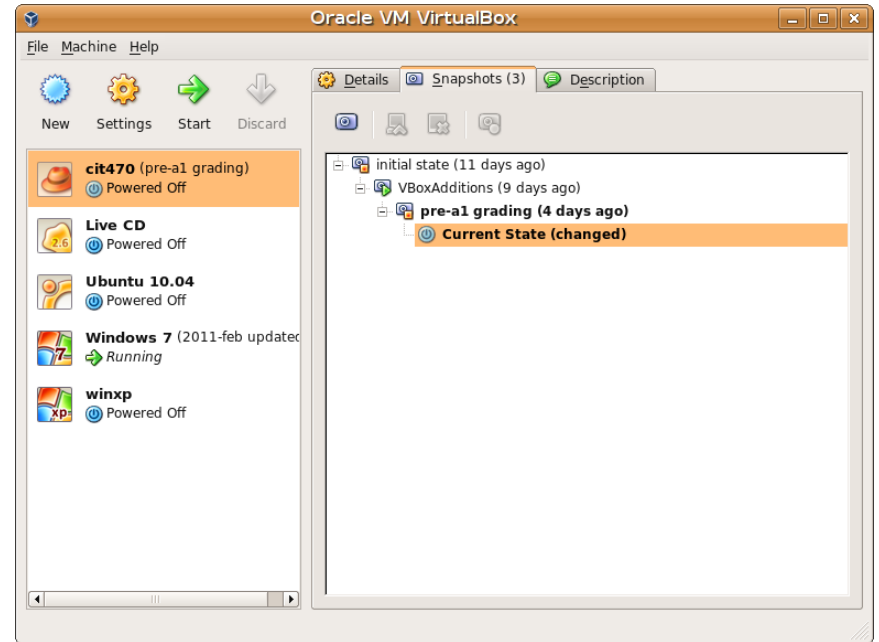
- ▶ Testing
- ▶ Different app versions
- ▶ Demos
- ▶ Sandbox

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

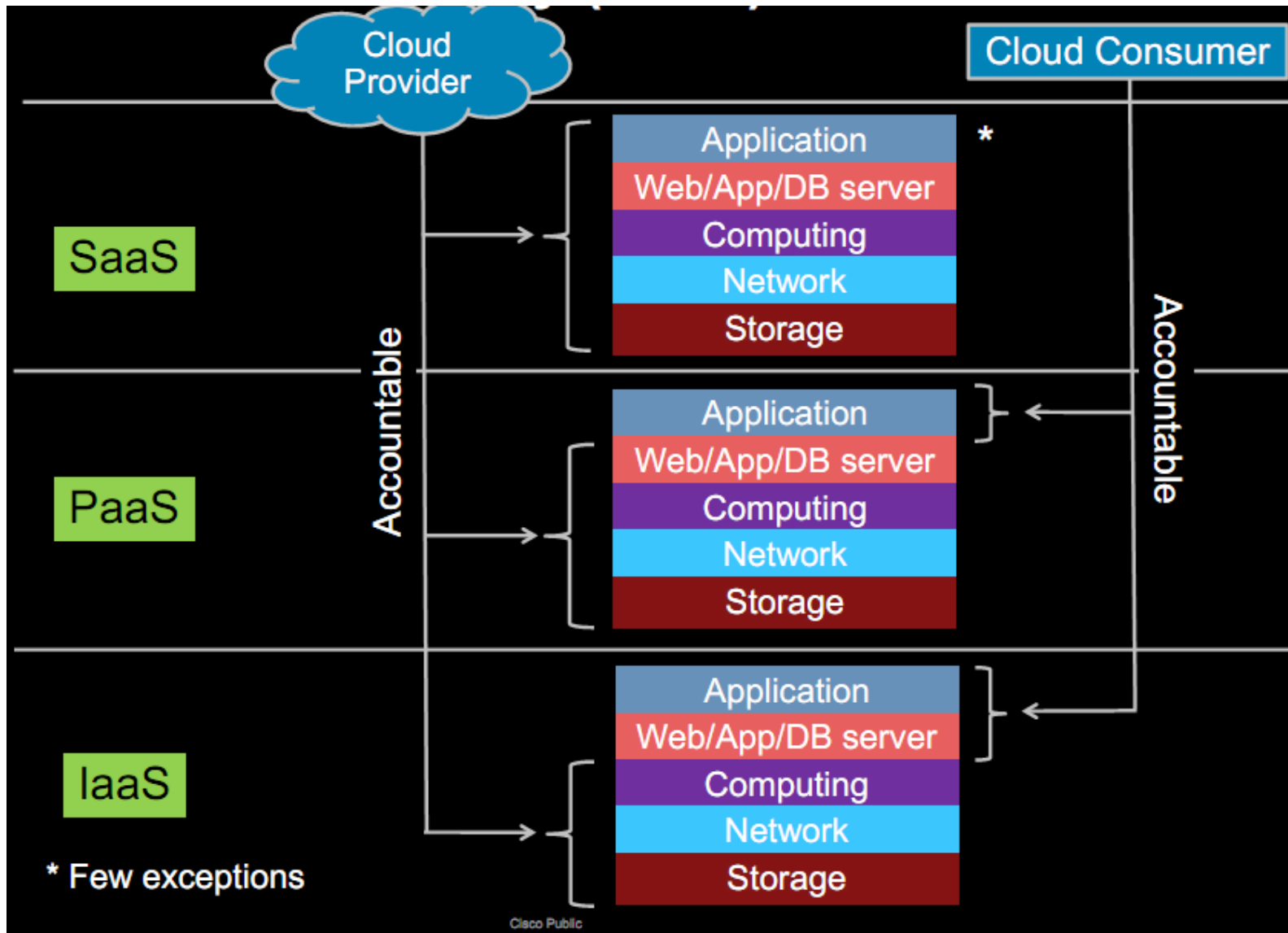
Although data was correctly sanitized from VM disk and/or memory, snapshots can retain multiple copies of both VM memory and disk data.



- 
- Accountability
 - No Security Perimeter
 - Larger Attack Surface
 - New Side Channels
 - Lack of Auditability
 - Regulatory Compliance
 - Data Security

New Security Issues

Accountability

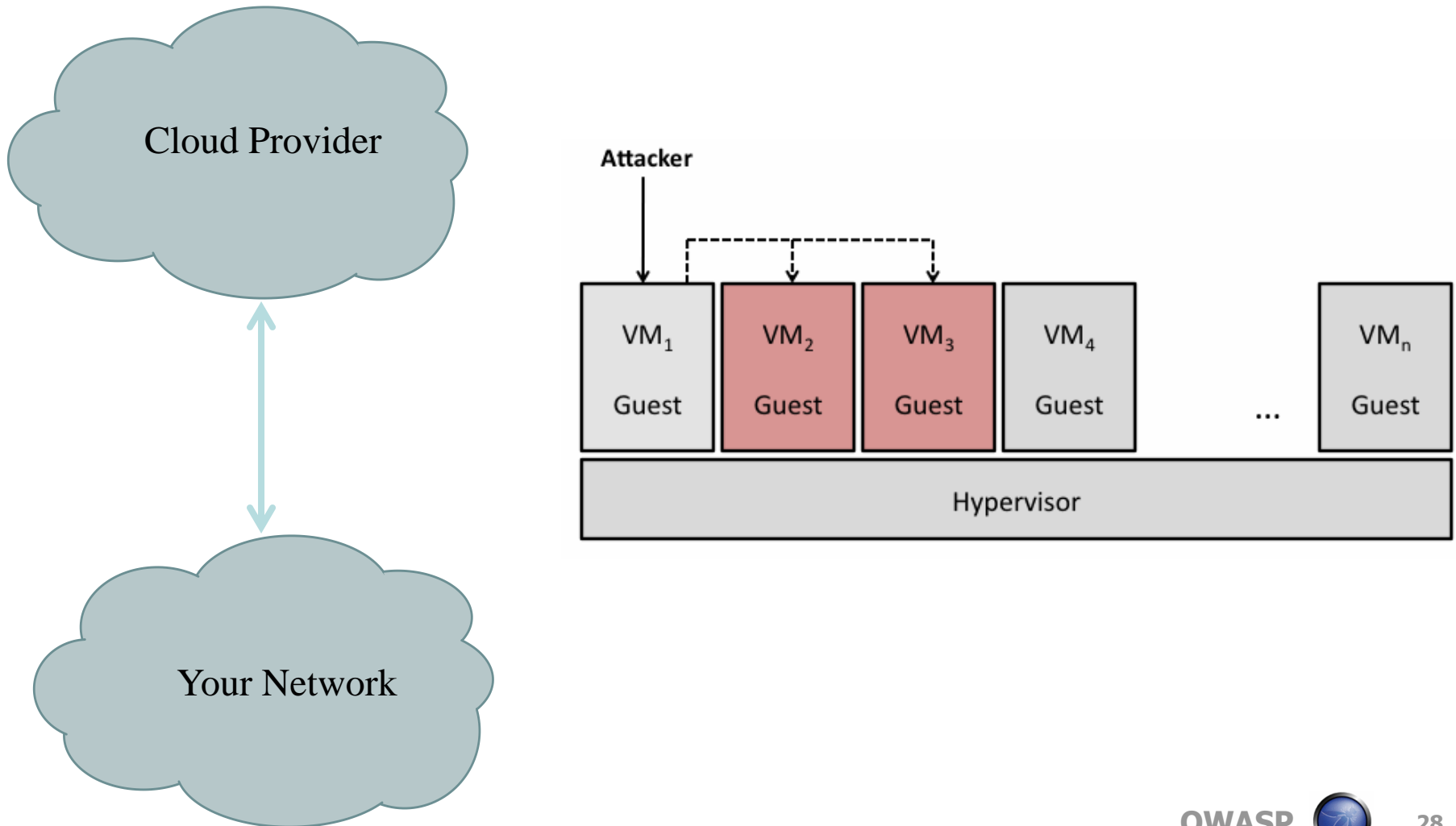


No Security Perimeter

- 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



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 Aciicmez 2007
 - ▶ CPU instruction cache: Onur Aciicmez 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

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.

Is AWS now PCI certified?

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

PCI "certification" is a term reserved for those merchants who process, store, or transmit cardholder data (AWS, as a service provider, does not directly manage cardholder data and therefore does not require certification). AWS provides a secure environment that helps our customers establish a secure cardholder environment and to achieve their underlying technology infrastructure is compliant. Achieving PCI certification helps our customers obtain their own PCI certification.

Service provider levels are defined as:

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

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

Services that support the processing, storage, and transmission of credit card data 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)

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

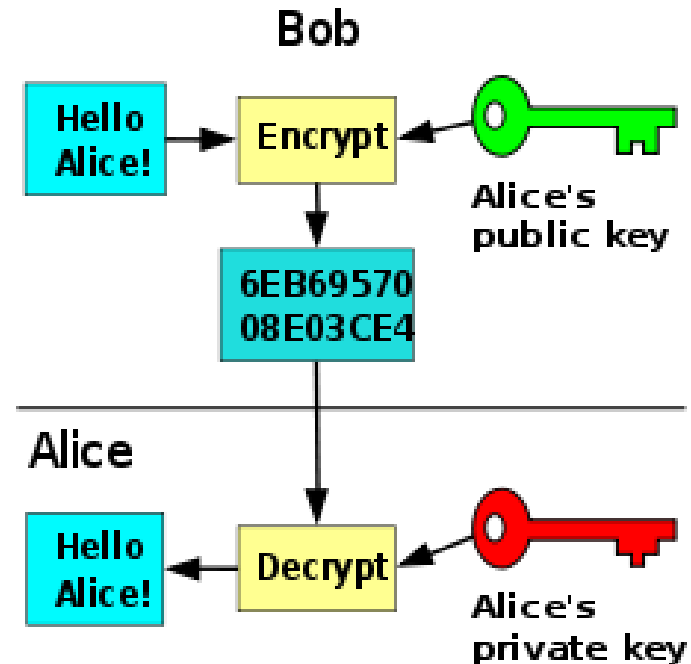
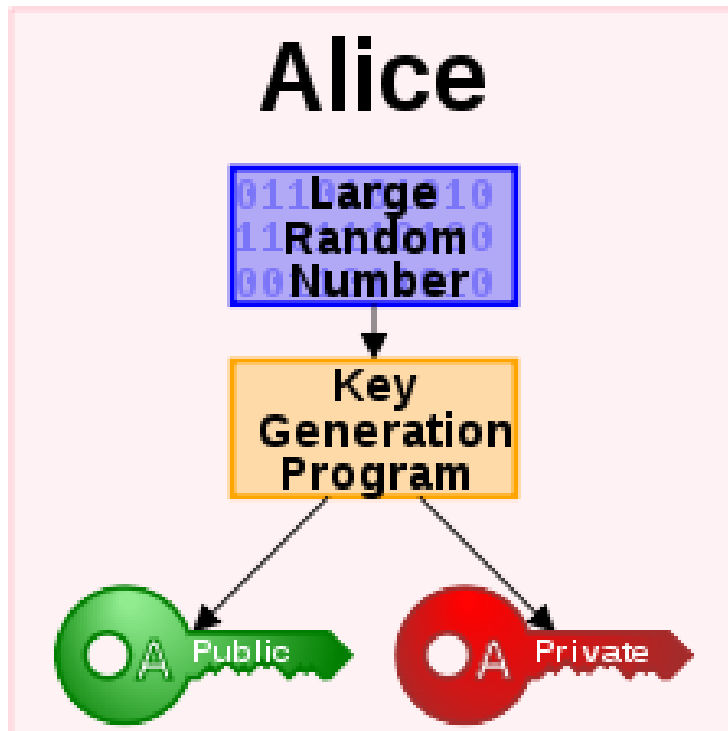
Data Security

Data Security

Confidentiality	Symmetric Encryption	Homomorphic Encryption	SSL
Integrity	MAC	Homomorphic Encryption	SSL
Availability	Redundancy	Redundancy	Redundancy
	Storage	Processing	Transmission

Plus data remanence.

Public Key Cryptography



Homomorphic Public-key Encryption

Public-key Crypto with additional procedure: **Eval**

$$c^* \leftarrow \text{Eval}_{pk}(\Pi, c_1, \dots, c_n)$$

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

Encryption of inputs
 m_1, \dots, m_n to Π

Π a Boolean circuit with ADD, MULT mod 2

*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
- ▶ $c^* \leftarrow \text{Eval}_{pk}(\Pi, c_1, \dots, c_n)$

■ $m^* = \Pi(m_1, \dots, m_n)$ is “the ring”, made from “raw materials” m_1, \dots, m_n

References

1. Yanpei Chen, Vern Paxson and Randy H. Katz, "What's New About Cloud Computing Security?" Technical Report No. UCB/EECS-2010-5, <http://www.eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-5.html>, Jan. 20, 2010.
2. Tal Garfinkel and Mendel Rosenblum. "When virtual is harder than real: security challenges in virtual machine based computing environments." In *Proceedings of the 10th conference on Hot Topics in Operating Systems - Volume 10 (HOTOS'05)*, Vol. 10. USENIX Association.
3. Craig Gentry. "Computing arbitrary functions of encrypted data." In *Commun. ACM* 53, 3 (March 2010), 97-105. DOI=10.1145/1666420.1666444
4. Doug Hyde. "A Survey on the Security of Virtual Machines." <http://www1.cse.wustl.edu/~jain/cse571-09/ftp/vmsec/index.html>, 2007.
5. Tim Mather, Subra Kumaraswamy, and Shahed Latif, *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance*, O'Reilly Media, 2009.
6. T. Ristenpart, E. Tromer, H. Shacham, and S. Savage. "Hey, You, Get Off of My Cloud! Exploring Information Leakage in Third-Party Compute Clouds." In S. Jha and A. Keromytis, eds., *Proceedings of CCS 2009*, pages 199–212. ACM Press, Nov. 2009.
7. NIST, DRAFT A Definition of Cloud Computing, http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf, January 28, 2011.
8. NIST, DRAFT Guidelines on Security and Privacy in Public Cloud Computing, http://csrc.nist.gov/publications/drafts/800-144/Draft-SP-800-144_cloud-computing.pdf, January 28, 2011.