

CALGARY CHAPTER HIGHLIGHTS

President's Message	1
Luncheon Dates	1
Fall Conference	2
Congrats to Exam Writers	3
Article: Securing Virtualized Data	4
ISACA Global News	6

CHAPTER OFFICERS & DIRECTORS

Sanjeev Saha,
President

Shahid Qureshi,
Vice President

Greg Winters,
Past President

Jagruti Sampat,
Secretary

Satish Chavali,
Treasurer

Jarka Winters,
Communications
Director

Diego Tabares,
Membership Director

Maria Hession,
Program Director

Ray Mingle,
Education Director

'Biyi Adeniran,
Technology Director

Louis Fernandes,
CISA/CISM Coordinator

Alvaro Janikian,
Webmaster

Linda Chan,
Newsletter Editor

ISACA INSIDER

www.isaca-calgary.org

A newsletter for Calgary Chapter members about ISACA news updates, events and articles of interest

Volume 4, 2008



November 2008

President's Message

Dear Members,

I hope you all had a great summer and are looking forward to another productive winter. Your ISACA chapter has reconvened after a summer break and we have planned another exciting conference for you to fulfill your learning needs and also satisfy your professional development requirements. We are continuing to follow the short format of a one day conference that is available at a convenient location downtown and is also cost effective. I encourage all of you to register and support the event. Details will be sent out soon.

The ISACA Board has included a new member 'Biyi Adeniran who has assumed the role of the Technology Director. 'Biyi will make an effort to keep our members informed of new technological developments through newsletter articles, luncheons, and

conferences. If you have any specific ideas about new technology that you would like to share with members or need information about new technology please get in touch with 'Biyi. We will do our best to bring an expert to share knowledge.

The ISACA Board is going to invite comments from members through an electronic survey to align our services with members' expectations from the chapter. The Board is always open to suggestions and ideas from members to improve our services, so please do not hesitate to get in touch with any of the Board members to share your ideas. We will make every effort to make your association with the local chapter useful.

The ISACA Board is always looking for volunteers to raise the bar in terms of

the ISACA experience we are able to provide our members. If you would like to volunteer some of your time to give back to your professional community and also develop your leadership skills please come forward and help the Board. The ISACA Board sent two delegates to the International Leadership Conference in Toronto and two delegates to the Western Region Leadership Conference in Victoria this year. The chapter is committed to developing leadership among the volunteers on the board and will continue to support such participation.

I look forward to meeting many of you at our Fall conference and other future events.

Sanjeev Saha

Monthly ISACA Luncheon Dates

Upcoming Dates: December 17, January 20, February 17, March 17

- Please note that the November luncheon has been cancelled, due to the Chapter's focus on bringing to you the Fall Conference.
- The December luncheon will be held jointly with the IIA Calgary luncheon.

Time: 11:30 AM to 1:00 PM

Location: Fairmont Palliser Hotel, 133 - 9th Avenue SW, Calgary

Important
DATE!

2008 Fall Conference

Tuesday, November 18, 2008

LOCATION: Fairmont Palliser Hotel, 133 – 9th Avenue
SW, Calgary

TIME: 8:00 a.m. to 5:00 p.m. (Registration & breakfast
begins at 8:00 a.m.)

REGISTRATION: ISACA members: \$250; Non-members: \$300

***** Package rate for a group of 5 members: \$1,000 *****

**A light breakfast, lunch and break refreshments are included in
registration fee**

9 CPE hours will be awarded

Attend an interactive day of presentations focusing on strategies and techniques in IT, security, and internal audit. The latest in thought leadership will be presented by leading experts from professional services and industry. You will have a unique opportunity to network with other IT and internal audit, security, privacy and finance peers from the Calgary Area to glean new strategies and develop new relationships. Please plan on joining us at the Fairmont Palliser Hotel. Conference information will be updated at: <http://www.isaca-calgary.ca/events/education-conferences/calgary-conference.html>

How to Register

Registration cost includes participation in all sessions, breakfast and lunch.

To register for this event, go to the ISACA Calgary website at

www.isaca-calgary.org

Click on: Events > Education & Conferences

Visa, MasterCard and AMEX accepted. For further details,
please phone Sanjeev@ 403-509-7512.

Session details and speaker bios are also posted on the website.

Congratulations to the Following Successful CISA® Exam Writers from June 2008

Amiran Alavidze
 Jean-Herbert Kouassi Allali
 Arlene Dawn Chamulak
 Tom Ginn
 Asad Gul
 Vipul Punamchand Jasani
 Maul Lars
 Jonathan Lin
 John Mustoe
 Richard Niewinski
 Frank M. Pados
 Witold Strzelecki

Congratulations to the Following Successful CISM® Exam Writers from June 2008

Wylie Shanks
 Kelly Lee Grant

The preceding does not necessarily represent a complete list of all individuals who were successful in passing the CISA or CISM exam. This list may not include individuals who did not grant permission to have their name published, who have not paid their exam related fees, who have not signed the exam registration form, or who are not members of the Calgary chapter.

Chapter Announcement: The Chapter would like to welcome 'Biyi Adeniran to the Board of Directors. He is the Manager of IT Audit at Westjet and he has joined the Board as the new Technology Director. We would also like to thank Grace Rengifo for her past service to the Board and we wish her all the best.

About ISACA

With more than 75,000 members in more than 160 countries, ISACA® (www.isaca.org) is a recognized worldwide leader in IT governance, control, security and assurance. Founded in 1969, ISACA sponsors international conferences, publishes the Information Systems Control Journal®, and develops international information systems auditing and control standards. It also administers the globally respected Certified Information Systems Auditor™ (CISA®) designation, earned by more than 60,000 professionals since 1978; the Certified Information Security Manager® (CISM®) designation, earned by more than 9,000 professionals since 2002; and the new Certified in the Governance of Enterprise IT™ (CGEIT™) designation.

To contact ISACA International...

Voice.....+1.847.253.1545
 Fax.....+1.847.253.1443
 Webwww.isaca.org
 E-mail ...info@isaca.org



Article: Securing Virtualized Data

By Robert Beggs, CISSP CISA

Virtualization is frequently used in the IT world; however, we'll focus on using this technology to describe the process of creating an abstraction layer (sometimes call the "hypervisor") that separates guest operating systems from the underlying hardware, enabling multiple virtual machines to be hosted on a single physical device.

Nearly everyone has become familiar with virtualization over the past couple of years as vendors such as VMWare and Microsoft compete against open-source solutions like XEN to gain ownership of an expanding market. Customers are obtaining real costs savings by reducing the number of management personnel and consolidating hardware, power, and space costs – savings in excess of 25% are frequently reported. Virtualizing multiple systems also improves operational flexibility, simplifies application delivery, and enhances business continuity and disaster recovery.

At the same time, virtualization can enable several security benefits. Resource consolidation and ease of management can reduce misconfigurations that lead to system exploits. Isolating operating systems and applications (to create test environments, or as "virtual appliances") expands the functionality of a network. In fact, if you go to www.vmware.com, you will see literally hundreds of virtualized applications – each one a machine that comes fully pre-installed and pre-configured, significantly reducing costs. Virtualized systems also support forensic analysis and make vulnerability research easier.

Unfortunately, the new technologies come with security risks that must be addressed before they can be fully deployed.

One can start by considering the technical risks of virtualization as a new technology. Although the host operating system and the guest operating systems are STILL being targeted by attackers, there is also a new target – the hypervisor layer. Some have argued that the mere presence of the hypervisor increases the "attack surface" of the network; its mere presence is enough to make a network more vulnerable to attack. Others have argued that hypervisors are small and well-written constructs of code, and do not introduce a significant risk into the network once they are deployed. However, both parties agree that it is possible that a compromise of the hypervisor could potentially allow an attacker to move from one guest operating system to another.

Thus far, there have been no practical attacks in the wild that have exploited this risk; however, the attackers are continuing to target the hypervisor.

On the other hand, compromises that affect guest operating systems (the virtual machines) are known to affect the host and other guest systems. A search of the Common Vulnerabilities and Exposures list (<http://cve.mitre.org/>) has identified weaknesses in VMWARE, Microsoft, and XEN products that can cause denial of services conditions in the host operating system or the hypervisor that would negatively impact other virtual machines.

Other guest-to-guest or guest-to-host attacks that have occurred include a vulnerability identified by CORE that allowed attackers to access files of the host system using shared folders. In addition, several proof-of-concept attacks have been described that allow attackers from one virtual machine to see into another virtual machines using memory space on the video card, which is shared between the two VMs.

Perhaps the greatest technical risk is the management of backup files and archives. Because a virtual machine is stored as several files, an attacker can steal a VM by copying the files from a storage folder or while they are moving from one location to another across the wire, and they're not encrypted. Once the virtual machine is in the attacker's possession, they can inspect it for hardwired user IDs, passwords, and data that could have value on its own, or be used to further a data breach.

One of the more interesting attacks would be to compromise the integrity of a stored virtual machine, perhaps by injecting a keylogger to steal user passwords into it. The attacker would then place it back in a business's storage repository. The next person who retrieved the virtual machine and entered a password would unknowingly supply it to the attacker via the keylogger software.

The greatest technical risk is that of controlling rouge virtual machines. The major virtualization vendors make it easy for anyone to obtain the software to use virtualization. This makes it relatively easy for employees to employ virtualized software whenever and wherever they wish (one of the touted advantages of virtualization). Unfortunately, if those VMs have not been hardened to reduce vulnerabilities, they can be easily compromised by attackers. And once compromised, they give attackers a foothold on your network, making further compromise easier.

The last point highlights of management issues around virtualization security – how do you control configuration, changes, and the implementation of security patches on virtual machines that can literally be installed, or moved, or taken down in a matter of minutes?

There are some security measures that can be taken to lessen the risks that come with virtualization. DigitalDefence recommends that companies start by NOT forgetting the security basics: continue to employ a defence-in-depth strategy, with multiple layers of security controls that reinforce each other. Validate that the controls work – remember: "trust, but verify (and document!)". Overall, model virtual security on the same practices you employ for your physical network.

Some specific points:

- Most standards and "industry best practices" (e.g.: PCI DSS, ISO 27001:2005) don't acknowledge virtualization as separate issue; you'll have to identify the overall IT and security strategies and goals for your own specific organization
- Conduct a risk assessment before you start. Use threat models – know 'what's the worst thing that could happen'
- Harden the host and guest operating systems to a documented standard. There are operating-specific documents available from most OS vendors, and there are some guidelines for the virtualization applications themselves. DISA has released the "Virtual Machine Checklist" (<http://iase.disa.mil/stigs/checklist>), and VMWare's Infrastructure 3 Security Hardening Guide also contains useful information (<http://www.vmware.com/resources/techresources/726>)
- Take advantage of virtualization-enabling hardware, such as the AMD-V and Intel VT CPUs. These specialized processors not

only make virtualization easier, but they can put controls on how shared hardware, such as NIC cards, can interact with each virtual machines. Limit and reduce the sharing of hardware resources such as CPUs, RAM, hard drive space, and NIC cards

- Isolate virtual machines; put systems with similar sensitivity (e.g.: confidential data types) into the same security zone. Control access into and out of that security zone. In cases where the sensitivity of the data is high, control access among guest virtual machines in that zones.
- Manage the creation and alteration of virtual machines. Segregate roles and administrative functions. This may be difficult, as the questions that emerge include: should an administrator on the host system have access to all guest virtual machines? What VM users should be allowed access to the host to assist in rebooting or administrative tasks? Who will be allowed to perform sensitive operations such as powering on or off a virtual machine? Organizations may need to consider creating new roles, such as VM administrators, VM authors, VM users, etc
- Control access to the virtualization service console and the management utilities
- Turn off un-utilized VMs and ensure that VMs that are centrally stored cannot be altered
- Control the implementation of rogue VMs using Active Directory, or scripts such as VHDAudit (<http://downloads.chriswolf.com>)
- Take advantage of specialized 3rd party tools, such as Tripwire's free utility to assess the security of VMWare ESX 3.0|3.5 against the documented VMWare security guidelines
- Consider using and IDS/IPS for virtual systems. For example, Third Brigade (www.thirdbrigade.com) offers deep packet inspection, a stateful firewall, and intrusion detection and prevention that reside directly in the guest virtual machines – ensuring that the security is always employed, no matter where the VM is moved to on the network
- When your network is virtualized, validate it with a full security audit by an objective third party – make sure it's provably secure

Robert Beggs is the President of DigitalDefence. He can be contacted at robert.beggs@digitaldefence.ca.

Reproduced by permission of DigitalDefence Inc.

Opinions expressed in the newsletter represent the views of the authors and advertisers and may differ from policies and official statements of the Information Systems Audit and Control Association and/or the IT Governance Institute® and their committees, and from opinions endorsed by authors' employers, or the editors of this newsletter. This newsletter does not attest to the originality of authors' content.

CGEIT Grandfathering Application Deadline Extension

Demand for CGEIT (Certified in the Governance of Enterprise IT) has been impressive. During 2008 ISACA has certified more than 1,000 CGEITs!

Due to overwhelming response, the application deadline for certification under the grandfathering provision has been extended to December 31,

2008. CGEIT certification is available to a wide range of IT governance related professionals. If you perform any of the activities below, you may be eligible for certification:

- * Audit/Assurance -- Advise on industry accepted practices and frameworks to improve IT Governance
- * IT Management -- Manage the enterprise architecture, including infrastructure and applications
- * Project Management -- Manage IT-enabled investment portfolios through their useful asset life cycle
- * Consultancy -- Develop IT and IS strategic plans and control frameworks
- * Information Security -- Integrate information security into enterprise IT governance
- * Risk Management -- Oversee the development and consistent application of the risk management framework
- * Executive Management -- Oversee the development and maintenance of the IT strategic plan

For more information on grandfathering requirements or to obtain an application, please visit www.isaca.org/cgeitapp. Act today before the grandfathering opportunity expires. Should you find that you do not meet the grandfathering work experience requirements, consider the CGEIT exam. Achieving certification by passing the CGEIT examination and submitting an application for approval, requires fewer years of work experience than under the grandfathering provision. The next exam offering is June 2009 and corresponding updates will be posted in December at www.isaca.org/cgeit.

If you have any questions, please send an e-mail to ISACA's Certification Department at certification@isaca.org.



We Welcome Your Feedback!

Please send your feedback on this newsletter to newsletter@isaca-calgary.org

ISACA Global News

Reminder of CPE Hours

Please remember that there are only two months remaining to earn your required continuing professional education (CPE) hours for the 2008 reporting year. To view the CPE policies, please visit

- www.isaca.org/cisacpepolicy
- www.isaca.org/cismcpepolicy or
- www.isaca.org/cgeitcpepolicy.

Certifications to Date

Since their inception, 61,908 CISA, 9,724 CISM and 664 Certified in the Governance of Enterprise IT™ (CGEIT™) certifications have been awarded.

e-Symposia Archive

Date	Topic	CPE Hours
Oct 28, 2008	Improve the Audit, Minimize the Risk	3
Sept 30, 2008	Risk and Compliance - Audit Fatigue	3
Aug 26, 2008	Application Security: Attack and Response	3
July 28, 2008	Security and Compliance Unite	3

The ISACA® e-Symposium on November 18 is called, "PCI Compliance – What do the Guidelines Mean to Me?" To register for the November e-symposium and take the first step toward earning three free CPE credits, please visit isaca.brighttalk.com. E-symposia recorded and archived for viewing on demand.

ISACA e-Learning Campus

The CISA® Online Review Course is now available on the ISACA e-Learning Campus, www.isaca.org/elearning. This interactive, web-based course was developed to provide CISA exam candidates and ISACA members with an efficient and cost-effective tool for preparing for the exam or performing information systems audits and reviews.

Nomination Process to Begin Earlier

The nomination process for positions on the 2009-2010 ISACA Board of Directors will begin earlier than usual to allow members more time to consider nominating someone or securing someone to nominate them. This year, the nomination form will be mailed in early November with volume 6, 2008, of the *Information Systems Control Journal*. At the same time, it will be posted to the web site at www.isaca.org/nominate. The deadline for submitting nominations is March 22, 2009.

The nomination form is for Board of Directors nominations only. Positions on key boards and committees are filled via the Invitation to Participate application, which will be mailed at the usual time: with the volume 1, 2009, issue of the *Journal*. It will be posted to www.isaca.org/participate at the same time.

Call for Articles

We are always looking for interesting technical articles from members of the Calgary Chapter. Interested individuals should contact the editor at newsletter@isaca-calgary.org.

Did You Know...

ISACA has completed an enterprise glossary, available at www.isaca.org/glossary. The purpose of the glossary is to bring consistency, where possible, to how terms within the assurance, security and IT governance professions are defined. Key CISA, CISM and CGEIT terms, as well as the entire glossary, are available for complimentary download.