Information Systems Audit and Control Association

SAN FRANCISCO CHAPTER LOCAL AREA NETWORK

WINTER 2001-2: DOUBLE ISSUE

Winner of the 2000 Wayne K. Snipes Award – Best ISACA Chapter in the USA and the World

Winner of the 1999 and 2000 Newsletter Contest – Best Newsletter for Large Chapters in North America

PRESIDENT'S MESSAGE

Todd Weinman
President

Contents

We are just over half way through the 2001-2 Chapter year and fortunately, my hair is still more brown than gray. In fact, as I look both backwards and forward it is turning out to be a remarkable year for our Chapter.

Fall eXciting seminar a big success!

On September 19-21, the San Francisco ISACA Chapter hosted our first annual three day multi-track conference. By all accounts this education event was a huge success. Certainly there are any number of things that can go wrong in hosting an event of this size. Remarkably, while we faced a number of challenges, there were no major glitches.

One of the challenges we faced involved the fact that a number of our speakers were flying into San Francisco from other parts of the country. That caused quite a bit of concern, when, less than a week before the event, airports across the country were closed. Fortunately, all of our speakers arrived for their sessions. While we are grateful to all those who presented, in particular I would like to thank Richard Prendergast, Bill Hancock, Rodney Kocot, Mike Villegas, Rhonda Tubertina and Mark Larripa, all of whom had to fly in to San Francisco. All of these individuals demonstrated a real commitment, as they all had a ready-made excuse and yet they all followed through. Edmund Lam, our former President, also deserves special mention for stepping in at the last minute (when another speaker cancelled) to present on auditing Cisco Routers.

Over 60 individuals attended part or all of the event, which featured tracks in Fundamentals, Security, and Hot Topics. At our September luncheon, which was held on the last day of the Seminar, we honored our Chapter members who passed the CISA exam this past June.

Thanks and recognition must also be extended to our fabulous Education Committee, led by Steven Hudoba. Other members of the Education Committee who contributed to the success of this event are Rick Beckman, Stuart White, Deb Frazer, William Luk and Mary Laude. Planning has already begun for next year's seminar. If you would like to get involved with the planning efforts, or, if you are interested in presenting, please contact me at todd_weinman@yahoo.com.

Thanks and recognition must also be given to those who sponsored the event. Sponsorship is critical to the success of an event such as this as it allows us to achieve our primary objective: keeping costs down to deliver a high quality, reasonably priced, education event for our members. Special thanks to PricewaterhouseCoopers, Captus Networks, iSecure Privacy and Lander International.

Joint SF ISACA/SF IIA meeting draws huge crowd!

On October 16th, we held our second annual SF ISACA/SF IIA joint luncheon. Approximately 140 people attended presentations by audit groups from The Gap (with co-source partners KPMG) and Bank of America. The presenters explored scenarios in which IS audit and financial/operational auditors work together. Presenters from The Gap/KPMG focused on audit issues relating to the relocation of a shared-services center, while the Bank of America presentation focused on that organization's approach to change initiatives, with the example of a new high-powered check processing system.

Excellent full day seminar at Bank of America

On Thursday, November 15th, the SF ISACA Chapter held a full day seminar at the Bank of America facility in Concord. The seminar was divided into two half-day sessions with the morning session focusing on auditing networks and the afternoon session addressing call centers. The two sessions paired BofA IT professionals with their respective audit partners, and also included a tour of their call center. The preparation by the nine Bank of America professionals was outstanding, and the feedback on the event was excellent.

December luncheon addresses timely topic

Our December luncheon meeting featured a panel discussion on how companies are responding to the events of 9-11. The panel was moderated by Neville Morcom and included valuable insights from Karen Dye, Deb Frazer, Esther Silver, and Amitabh Sharma. Attendees received gift boxes of See's Chocolates; and several lucky attendees were recipients of prizes from our first Holiday raffle – carrying cases compliments of Arthur Andersen. Much to my chagrin, Board members were not eligible for the raffle.

January education event draws big crowd

Our January education event addressed the very timely topic of Auditing Web Applications. The event featured presentations by Ihzar Bar-Gad, Terry Bezdek, Goran Kovacevic, Steve Madeiros and Bob Grill. (A more detailed review of this event can be found elsewhere in this newsletter).

Newsletter changes

One of my goals as Chapter President was to improve the technical content of our newsletter. This Winter Double Issue features half a dozen articles of relevance to IT audit practitioners (special thanks to Dave Lufkin and Bank of America for their many contributions to this newsletter.) We hope this is just a start. I encourage each of you to consider contributing articles for the newsletter. Keep in mind that the articles don't have to be the length of Ph.D. dissertations; the important thing is that they convey information of use to your colleagues in the profession. If you are interested in writing articles, please feel free to contact me at todd_weinman@yahoo.com.

Web site problems resolved

As some of you may have noticed, we recently experienced some difficulties with our Web site. The origin of the problem was a system conversion gone bad at our Web hosting company (talk about a company that could use a good IS auditor or two.) The end result was that our Web site was frozen for several weeks. Any changes we tried to make to the site during that time would corrupt the site. Fortunately, our former President and trusted Webmaster, Lance Turcato, worked us through the situation, which involved migrating to a new Web host. In the process, Lance also put his artistic flair to the test and redesigned our site. Check it out at www.sfisaca.org.

Key changes to the Board of Directors

The SF ISACA Chapter recently lost two key Board members and Officers. 1st Vice President (and Communications Chair) Justin Gibson recently relocated to San Antonio, Texas; and 2nd VP (and Education Chair) Steven Hudoba recently returned to Southern California. Both individuals have served the organization with the utmost dedication and commitment. Fortunately, we have some very competent replacements waiting in the wings. The 1st VP role will be assumed by Beverly Davis (who is also the Chair of our CACS 2002 committee, while the 2nd VP position was filled by our current Education Chair, Rick Beckman. In addition, we'd like to welcome Anne Woodbury to the Board as our new Treasurer. Anne is taking over for Christina Cheng who is taking off several months on maternity leave (she will continue on the Board as a Director).

CISA exam and review course

It's that time of year again – time to start preparing for the 2002 CISA exam in June. The SF ISACA Chapter offers a review course to assist in preparing for the exam. The CISA certification continues to be highly valued by companies that hire IS auditors. It is a sign of commitment and dedication to your professionalism. More detailed information on the CISA Review Course can be found elsewhere in this newsletter.

CACS

Our Chapter is gearing up for hosting the 2002 North American CACS conference in early May. Those interested in being involved with the preparation and hosting may contact Beverly Davis at 415-616-2766, or by e-mail at davisb@fhlbsf.com. We look forward to seeing you at CACS.

As you can see, we are in the midst of an action-packed year of Chapter events. I would like to thank again the many individuals and companies who have volunteered their time and resources to help make our events a success. I also encourage each of you to consider becoming involved in your Chapter.

Sincerely,

Todd Weinman
President

SAN FRANCISCO ISACA FULL-DAY SEMINAR

Auditing and Managing 3rd Party Relationships • Thursday, March 21, 2002 • 7 hours of CPE credit

Session description

The current economic downturn has presented many challenges for business. One of the most significant to IT auditors and business process owners alike is the increase in reliance on third-party service providers, i.e., outsourcing. Outsourcing is increasing, not just in IT, but in other areas of operations. Certainly we are seeing outsourcing on the rise in such IT areas as data center management, desktop support, systems maintenance, and telecommunications management. In addition, more and more businesses are looking to third parties to manage such functions as treasury, documentation, procurement, and customer service, to name only a few. Generally, all outsourced functions impact the IT environment, as it is virtually impossible to find a business process that does not involve information technology systems of some variety.

Outsourced services change the fabric of an organization and increase risk. Business process owners and auditors both face new considerations in examining controls around managing the third-party relationships. From the selection process, through managing service level agreements, to gaining assurance over the vendor's own control environment, outsourcing can be a veritable nightmare for the ill prepared. In the sessions presented on March 21, you will hear from practitioners as well as vendors about how you can proactively assist your organization in mitigating the risk brought on by outsourcing. During the final session of the day, attendees will be able to pose questions to a panel of all of the day's speakers.

Register

To see a detailed outline of the presentation, to read biographies of the speakers, and to find other important details about the seminar, visit our chapter Web site: www.sfisaca.org

Schedule

Time	Description
8:00-8:30 am	Registration and Breakfast
8:30-10:00 am	Auditing Vendor Selection and Due Diligence *Dan Bertuleit, IT Audit Consultant, Barclays Global Investor*
10:00-11:30 am	Planning and Executing a Review of your Vendor's IT Security and Controls *Nancy Wiesbrook, IT Audit Manager, APL Ltd.*
11:30-12:30 pm	Lunch
12:30-2:00 pm	Managing the Relationship – The Vendor's Perspective *Becky Schultz, Senior Account Representative, Affiliated Computer Services*
2:00-3:30 pm	Independent Vendor Reviews – Which Attestation is Best? *Kai Wong, Senior Manager, Deloitte & Touche*
3:30-5:00 pm	Open Panel Discussion

This schedule is subject to change and revision.

Pricing (including SaverPass info if applicable)

$110 Members (or 3 Saverpasses)
$135 Non-members (or 4 Saverpasses)
$ 75 Full-time students

Location

The Palace Hotel, in San Francisco's Financial District at the corner of Market and New Montgomery Streets
2 New Montgomery Street, San Francisco, CA 94105, 415-243-8062

Cancellation Policy: If after submitting your reservation you determine that you need to cancel, please do so at least 72 hours prior to the event by contacting the registration coordinator, Helen Winters, at either helen@landerint.com or at 510-232-4264 x10.

Please do not be a 'no show'. Our Chapter is billed for reservations made with our facilities provider, and we will have to pass the charges on to you. Thank you for your cooperation.

FBI LISTS 20 MOST DANGEROUS INTERNET SECURITY WEAKNESSES

by Maria Shaw

Maria Shaw is a Senior Manager with Deloitte & Touche's Enterprise Risk Services group in San Francisco.

Originally from the UK, Maria graduated from Cambridge University and is a chartered accountant as well as a CISA. Maria has moved to California as she loves the weather, the lifestyle and the people.

The SANS Institute and the National Infrastructure Protection Center (NIPC) released a document summarizing the Twenty Most Critical Internet Security Vulnerabilities. This list has been used by thousands of organizations to prioritize their efforts so they could close the most dangerous holes first. It also serves as a great tool for auditors, allowing the auditor to focus their resources on these top security risks.

The SANS/FBI Top Twenty list is valuable because the majority of successful attacks on computer systems via the Internet can be traced to exploitation of security flaws on this list. For instance, system compromises in the Solar Sunrise Pentagon hacking incident and the easy and rapid spread of the Code Red and NIMDA worms can be traced to exploitation of unpatched vulnerabilities on this list.

These few software vulnerabilities account for the majority of successful attacks, simply because attackers are opportunistic – taking the easiest and most convenient route. They exploit the best-known flaws with the most effective and widely available attack tools. They count on organizations not fixing the problems, and they often attack indiscriminately, scanning the Internet for any vulnerable systems.

In the past, system administrators reported that they had not corrected many of these flaws because they simply did not know which vulnerabilities were most dangerous and were too busy to correct them all. Some vulnerability scanners search for 300 or 500 or even 800 vulnerabilities, thus blunting the focus your system administrators need to ensure that all systems are protected against the most common attacks. The Top Twenty list is designed to help alleviate that problem by combining the knowledge of dozens of leading security experts from the most security-conscious federal agencies, the leading security software vendors and consulting firms, the top university-based security programs, the SANS Institute and CERT/CC.

The Top Twenty list is segmented into three categories: General vulnerabilities, Windows vulnerabilities and Unix vulnerabilities.

Top general vulnerabilities

- Default installs of operating systems and applications
- Accounts with no passwords or weak passwords
- Non-existent or incomplete backups
- Large number of open ports
- Not filtering packets for correct incoming and outgoing addresses
- Non-existent or incomplete logging
- Vulnerable CGI programs

Top Windows vulnerabilities

- Unicode vulnerability (Web Server folder traversal)
- ISAPI extension buffer overflows
- IIS RDS exploit (Microsoft Remote Data Services)
- NETBIOS – unprotected Windows networking shares
- Information leakage via null session connections
- Weak hashing in SAM (LAN Manager hash)

Top Unix system vulnerabilities

- Buffer overflows in RPC services
- Sendmail vulnerabilities
- BIND weaknesses
- Remote commands
- LPD (remote print protocol daemon)
- sadmind and mountd
- Default Simple Network Management Protocol (SNMP) strings

Full details of the Top Twenty vulnerabilities including a detailed description, systems impacted, vulnerability notifications, how to determine if you are vulnerable, and how to protect against them, can be found on the SANS site at http://www.sans.org/top20.htm

WINDOWS 2000 SECURITY ENHANCEMENTS: KERBEROS

One criticism of Windows NT has been the out-of-the-box openness and lack of security features. Windows 2000 offers many improvements in both security features available and in the increased granularity of the security options. One of these improvements is the default authentication method, Kerberos version 5. This article gives an overview of how Kerberos works and looks at some of the benefits of this authentication method.

How does it work?

Using a password or smartcard, the user authenticates to a Key Distribution Center (KDC) which runs on each Domain Controller as a part of the Active Directory. The KDC issues a ticket-granting ticket (TGT) to the client, which is used to access the ticket-granting service (TGS). When the user wants to access a file or other resource, the TGS is presented to the resource to prove the user's identity and access capabilities.

Benefits

There are many benefits to using the Kerberos authentication. First, it is a more efficient authentication method than NT Lan Manager (NTLM). NTLM requires the application server to contact the Domain Controller to authenticate each client. Kerberos supplies the credentials directly to the client eliminating the need for the application server to contact the Domain Controller.

Another benefit is mutual authentication. The Kerberos ticket contains an encrypted session key. A valid application server will be able to decrypt the session key and sign a response back to the client, proving the identification of the server to the client. That way the client knows the server they access is actually the one they intended to access, preventing a man-in-the-middle or server impersonation attack.

Kerberos also supports delegation of authentication. This support allows authentication information to be forwarded to back-end servers. For example, the client requests access to an application that must in turn access information on a database server. The application server will pass the client's authentication credential to the database server without requiring a separate client authentication to the second server. This efficiency is an important benefit in today's 3-tier application architecture. Since Kerberos is also a mature Internet standard, it allows for interoperability with other systems using Kerberos version 5 authentication.

Conclusion

The use of Kerberos authentication method demonstrates not only some of the improvements in the Windows 2000 operating system, but also illustrates many differences between NT and 2000. These differences, when understood and implemented properly, will increase the overall security of the operating environment. If, however, administrators are not trained in and given time to plan for these changes, enterprises run the risk of creating security holes that could compromise the security of their entire network. The need for training also holds true for the auditors planing to review a Windows 2000 system. Unless you understand the complexities of this operating environment and the changes in the security features, you run the risk of overlooking potential areas of concern.

by Ronda Tubertini

Ronda Tubertini is currently a Vice President and Senior IT Audit Manager at Bank of America. Her experience in Audit and Project Management at companies including EDS and The Associates have allowed her to perform a wide variety of work from data center reviews to NT audits to Control Self Assessment.

Recent projects include leading the risk assessment and review of a technology process optimization initiative within the Bank of America Technology Group, and working to develop Windows 2000 training for the entire IT Audit Group.

Ronda has a BBA in Accounting from Abilene Christian University and is a CISA and CBA. Prior training experience include presentations for both the Dallas IIA and the North Texas chapter of ISACA.

The short story

VPNs perform as relatively inexpensive WANs. Because they contend/coexist with the Internet for performance and with PPTP, L2TP, IPsec, and SOCKS for security, they require significant planning and preparation. That's the short "techie" version. If you want the Paul Harvey "rest of the story" then read on.

What is a VPN?

A Virtual Private Network (VPN) supplies network connectivity over a possibly long physical distance. In this respect, VPNs are a form of a Wide Area Network (WAN). A VPN's key feature is its ability to use public networks like the Internet or private networks that act like the Internet, rather than private leased lines. VPN authentication (verifying your identity) and encryption (scrambling information) technologies create restricted-access networks that use the same cabling as a public network.

VPNs are typically used in 3 different ways:

- Remote access client connections (e.g., connecting to your work's Intranet from home),
- LAN-to-LAN internetworking (e.g., connecting two or more Local Area Networks (LAN) such as branch offices)
- Controlled access within an intranet (e.g., a secure connection within an internal Intranet)

Traditional leased lines

Traditionally, an organization building a WAN procured expensive, dedicated lines to connect their offices together. Only large companies could afford to purchase these lines outright, so most organizations "leased" their lines, paying a monthly charge for the privilege of using cables that no one else could.

An organization typically installs a leased-line WAN to support a long-distance Intranet. Besides file sharing and e-mail, these WANs provide access to intranet Web sites and videoconferencing systems.

Advantages of a VPN

VPNs promise two main advantages over competing approaches – cost savings and scalability (really just a different form of cost savings).

The low cost of a VPN

One way a VPN lowers costs is by eliminating the need for expensive long-distance leased lines. With VPNs, an organization needs only a relatively short dedicated connection to the service provider. This connection could be a local leased line (much less expensive than a long-distance one), or a local broadband connection such as a Digital Subscriber Line.

Another way VPNs reduce costs is by lessening the need for long-distance telephone charges for remote access. VPN clients only need to call their closest service provider's access point. In some cases this may require a long distance call, but it is usually a local call.

A third, subtler way that VPNs may lower costs is by offloading the support burden; with VPNs, the service provider rather than the organization must support dial-up access. Service providers can in theory charge much less for their support than it costs a company internally because the public provider's cost is shared among potentially thousands of customers.

Scalability and VPNs

The cost to an organization of traditional leased lines may be reasonable at first but can increase exponentially as the organization grows. A company with two branch offices, for example, can use just one dedicated line to connect the two locations. If a third branch office needs to be connected, only two more lines are required.

However, as an organization grows and more offices must be added to the network, the number of leased lines required increases dramatically. Four branch offices require six lines for full connectivity, five offices require ten lines, and so on. The mathematical phenomenon that describes this growth is called a combinatorial explosion and in a traditional WAN this explosion limits the flexibility for growth. VPNs that utilize the Internet avoid this problem by simply tapping into the geographically distributed access that is already available.

Disadvantages of VPNs

With the hype that has surrounded VPNs historically, the potential pitfalls or "weak spots" in the VPN model can be easy to forget. The following four concerns with VPN solutions are often raised.

1. VPNs require an in-depth understanding of public network security issues and proper deployment of precautions.

2. The availability and performance of an organization's wide-area VPN (over the Internet in particular) depends on factors largely outside of its control.

3. VPN technologies from different vendors may not work well together due to immature standards.

4. VPNs need to accommodate protocols other than Internet Protocol (IP) and existing (i.e., legacy) network technology.

Generally speaking, these four factors comprise the "hidden costs" of a VPN solution. Whereas VPN advocates tout cost savings as the primary advantage of this technology, detractors cite hidden costs as the primary disadvantage of VPNs.

(Warning! The next two sections are mostly in English, but are by nature very technical.)

VPN technology

VPN technology is based on a tunneling strategy. When a file or other information is sent through a network, it is broken down into small chunks of information called packets. Tunneling involves encapsulating the packets from a base communication protocol format within some other communication protocol thus creating encrypted packets. In the case of VPNs run over the Internet, packets in

one of several VPN protocol formats are encapsulated within IP packets. Information sent through the Internet thereby can be sent securely instead of in clear text.

VPN security

VPNs work hard to ensure that their data remains secure, but its security mechanisms can still be breached. Particularly on the Internet, sophisticated hackers with ample amounts of free time will work equally hard to "steal" VPN data if they believe it contains valuable information such as credit card numbers.

Most VPN technologies implement strong encryption so that data cannot be directly viewed using network sniffers (capturing information on the network). VPNs may be susceptible to "man in the middle" attacks, however, that intercept the session and impersonate either the client or server. In addition, some private data may not be encrypted by the VPN before it is transmitted on the public wire. IP headers, for example, will contain the IP addresses of both the client and the server. Hackers may capture these addresses and choose to target these devices for future attacks.

VPN protocols

Several major network protocols have been implemented for use with VPNs. These protocols attempt to close some of the security holes inherent in VPNs. These protocols continue to compete with each other for acceptance in the industry.

Point-to-Point Tunneling Protocol (PPTP)

PPTP is a protocol specification developed by several companies. People generally associate PPTP with Microsoft because nearly all flavors of Windows include built-in support for the protocol. The initial releases of PPTP for Windows by Microsoft contained security features that some experts claimed were too weak for serious use. Microsoft continues to improve its PPTP support, though.

PPTP's primary strength is its ability to support non-IP protocols. The primary drawback of PPTP is its failure to choose a single standard for encryption and authentication. Two products that both fully comply with the PPTP specification may be totally incompatible with each other if they encrypt data differently, for example.

Layer Two Tunneling Protocol (L2TP)

The original competitor to PPTP in VPN solutions was Layer 2 Forwarding (L2F) – a protocol implemented primarily in Cisco products. In an attempt to improve on L2F, the best features of it and PPTP were combined to create new standard called L2TP. L2TP exists at the data link layer (layer two) in the Open System Interconnection (OSI) Model – thus the origin of its name.

Like PPTP, L2TP supports non-IP clients. It also fails to define an encryption standard. However, L2TP supports non-Internet based VPNs including frame relay, Asynchronous Transfer Mode (ATM), and Synchronous Optical NETwork (SONET).

Internet Protocol Security (IPsec)

IPsec is actually a collection of related protocols. It can be used as a complete VPN protocol solution, or it can be used simply as the encryption scheme within L2TP or PPTP. IPsec exists at the network layer (layer three) in the OSI model.

IPsec extends standard IP for the purpose of supporting more secure Internet-based services (including but not limited to VPNs). IPsec specifically protects against "man in the middle attacks" by hiding IP addresses that would otherwise appear on the wire.

Socket Secure (SOCKS) network security protocol

The SOCKS system provides a unique alternative to other protocols for VPNs. SOCKS functions at the session layer (layer five) in the OSI model, compared to all of the other VPN protocols that work at layer two or three. This implementation offers advantages and disadvantages over the other protocol choices. Functioning at this higher level, SOCKS allows administrators to limit VPN traffic to certain applications. To use SOCKS, however, administrators must configure SOCKS proxy servers within the client environments as well as SOCKS software on the clients themselves.

(Now leaving the technical zone and returning to English.)

VPN hardware and software

Literally dozens of vendors offer VPN related products. These products sometimes do not work with each other because of the choice of incompatible protocols (as described above) or simply because of lack of standardized testing.

Some VPN products are hardware devices. Most VPN devices are effectively routers that integrate encryption functionality. Other types of VPN products are software packages. VPN software installs on top of a host operating system and can require significant customizing for the local environment. Many vendor solutions comprise both server-side hardware and client-side software designed for use with the hardware.

Conclusion

VPNs offer cost reduction benefits versus the traditional leased line solution for deploying large networks. Large-scale development efforts in VPN technology solutions are proceeding but incompatibilities among the products are expected to continue. The task of choosing and deploying a VPN solution remains far from simple. The most common public network used with VPNs is the Internet, but traffic congestion and router failures on the Internet can adversely impact the performance of these VPNs. When building a Net-based VPN, it will be important to choose a high-quality service provider.

by Robert J. Boesewetter
Robert J. Boesewetter is the VP and Technology Audit Consultant for the Bank of America.

NEW DEVELOPMENTS IMPACTING AUDIT

by Todd Weinman

Todd Weinman is the current President of the San Francisco Chapter of ISACA. He is an executive recruiter and Western Regional Director for Lander International, the world's largest recruiting firm specializing in IT Audit.

Todd enjoys visiting audit, information security and consulting departments all over Northern California, and he is in contact on a daily basis with scores of directors, managers and staff level professionals from around the region.

A frequent speaker for ISACA, the IIA and local universities, Todd is a graduate of UC Berkeley and worked for a large CPA firm prior to joining Lander International. Todd was selected as the 1999 CAPC Consultant of the Year for the state of California.

The beginning of 2002 has brought several developments of relevance to internal auditors and their employers.

New insurance industry developments

New insurance industry developments could add up to significantly increased risk and exposure to corporations. The January 2, 2002 edition of Information Week Daily reports that the insurance industry is considering a variety of changes in the way they cover damages related to cyber-crime.

One of those changes is the exclusion of online assets from standard commercial insurance policies. In the past these losses would have been covered, but many insurance companies are now looking at providing such coverage only through more expensive supplemental policies.

Perhaps even more significant, some insurance companies are apparently contemplating excluding coverage for any loss that would result from terrorist-related activities. Given the increased threat of cyber-terrorism, this presents a potentially large exposure which could in the end justify increased spending and resources to mitigate these risks.

The rationale for these changes stems from the increasing array of potential claims that were not taken into account in the original pricing of these policies.

Accounting industry developments

In response to the increasing fallout over the Enron debacle, the AICPA is recommending a number of significant changes that could impact how internal audit departments are staffed. In a February 14, 2002 statement to a House subcommittee (http://ftp.aicpa.org/public/download/news/stmt_jgc_021402.pdf), AICPA Chair, James G. Castellano outlined a number of recommendations.

Castellano cited a 1994 AICPA special committee report, noting that the way in which companies report financial information has not kept pace with changes in business. He expressed that improvements must be made both in the scope and frequency with which this information is reported. The 1994 report favored the term "business reporting," noting that, "business reporting is wider than financial statements," and that it should incorporate a variety of factors outside of financial statements.

One of the more interesting developments for IT auditors is an increasing emphasis on preventative controls and on information systems in general. The memo notes that, "the transition is going to demand personnel of the highest caliber." The report also calls for increased detection of fraud and focus on the risk of management override of key internal controls. Also of interest to IT auditors is a recommendation for increased use of continuous auditing, SysTrust reviews and more sophisticated reporting measures and metrics which will require more technically savvy auditors.

Perhaps the most significant development is the AICPA's stance on non-audit consulting services and internal audit outsourcing. The AICPA will not "oppose prohibitions on auditors of public companies from providing financial systems design and implementation and internal audit outsourcing."

The common theme of these developments is an increased emphasis on the improvement of internal reporting and controls. These developments could result in increased staffing for internal audit departments as well as an increased emphasis on more technically saavy internal auditors.

CALENDAR OF UPCOMING EVENTS

Date	Event	Place	More information
March 6-7, 2002	Fundamentals of IS Auditing, Sacramento ISACA Spring Seminar	CALPERS – Sacramento	http://www.isaca-sacramento.org/
March 21, 2002	**SF ISACA Full Day Seminar Auditing & Managing 3rd Party Vendors**	**The Palace Hotel, San Francisco**	**http://www.sfisaca.org/events/glance.htm**
March 25-27, 2002	Los Angeles ISACA Spring Conference	Universal City Hilton & Towers	http://www.isaca-la.org/2002_Spring_Conference
April 6, 2002 - June 1, 2002	**CISA Review Course**	**425 Market Street, San Francisco**	**http://www.sfisaca.org/cisa/review.htm**
April 18, 2002	**Networking Event**	**The Palace Hotel, San Francisco**	**http://www.sfisaca.org/events/glance.htm**
May 5-10, 2002	**North American CACS Full Week Conference**	**The Fairmont, San Francisco**	**http://www.isaca.org/nacacs2002.htm**
July 7-10, 2002	ISACA International Conference	Mariott Marquis, New York	http://www.isaca.org/international2002.htm
October 2002	**SF ISACA Fall Seminar**	**The Palace Hotel, San Francisco**	**details to be posted at www.sfisaca.org**

MEMBER MILESTONES

Members for over 25 Years

Robert Abbott
Paul J. Ghelev
Douglas Webb

Members for over 20 Years

Richard J. Tuck
Doug Feil
Charles A. Dormann
Gary W. Riske
David L. Lowe
Hector L. Massa
Charles C. Wood
Arnold Dito
David R. Durst
Robert C. Kimball
William Z. Davidson
John R. Wise
Joel L. Lesser
William G. Martin
Kathleen W. Williams
Bruce L. Reid

Members for over 15 Years

Kathryn M. Dodds
Allen H. Martin
Kerry G. Elms
Leslie D. Fondy
Katherine M. Ullman
Jerry K. Hill
Martin W. Taylor
David A. Gilliam
Nancy D. Wiesbrook
Marcus A. Jung
Mary J. Bean
Steven Hudoba
Eugene W. Menning Jr.
Vickie P. Smith
Paley Y. Pang

Members for over 10 Years

Louis R. Walker
Guy T. Anderson
Robert C. Mott
Sharon Tatehara
Jeffrey P. Mazik
Adam F. Levine
Ralph G. Nefdt
Roy B. Cage Jr.
James H. Tanner IV
Todd E. Fenner
Kathleen E. Arnold
Jack B. Cooper Jr.
William Grant
Melody Jean Pereira
Wing K. Yeung
Beatrice K. Ashburn
Lawrence A. Jewik
Juan I. Lorenzo
John F. Harper
Keith D. Scott
Lawrence B. deBerry
Douglas K. Walsch
Lynne A. Trestrail

WEB APPLICATION VULNERABILITIES

by Izhar Bar-Gad

Izhar Bar-Gad is the Chief Technology Officer for Sanctum. Prior to joining the Sanctum team, he was a project leader for Amdocs in Israel for both the Infrastructure and AdvancedResearch groups.

During his military service in the Israeli Defense Forces, Mr. Bar-Gad led the development of a large software project involving communications and information security.

Mr. Bar-Gad holds a Bachelor of Science degree from Tel-Aviv University, and a Masters degree from the Hebrew University, Jerusalem. He is currently a Ph.D. candidate in "Neural Computation" at Hebrew University.

Web site application hacking is quite simple, especially compared to the difficulty of securing such applications. A hacker typically only needs a few hours to study a Web application. By thinking like a programmer, he can identify exploitable shortcuts built into the application. Then, the hacker will interact with the application and its surrounding infrastructure using his Web browser and/or any number of publicly available automated tools. While most Web sites are heavily secured at the network level (e.g., firewalls and encryption), sites generally allow hackers complete access to the enterprise's Web applications. In fact, Gartner Group estimates that 75 percent of Web site intrusions today happen at the application level. Furthermore, they expect this number to increase.

As an information technology auditor, understanding the potential vulnerabilities of Web applications is critical to an effective audit effort.

Web applications

To understand Web application vulnerabilities, one must first define the meaning of a Web application. Although most people have an intuitive notion of the meaning, we rarely define its scope and complexity. Web applications are usually multi-layered systems that include code and data residing in multiple locations within the enterprise (see Figure 1). All of the components of the application can be accessed directly or indirectly from the Internet. Application components can be developed internally by multiple departments with code unique to the enterprise or purchased from external vendor (e.g., Web servers and databases). Vulnerabilities in *any* of the layers of the Web application will ultimately lead to a security breach of the *whole* application.

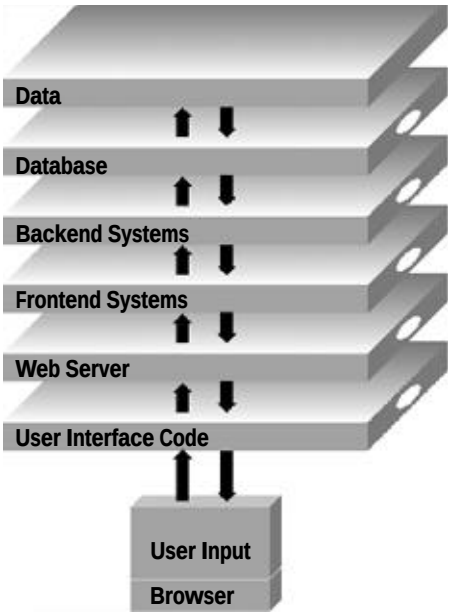

Figure 1

Web application vulnerabilities

Sanctum's auditors have performed over 300 audits and proof of concepts over the last 3 years and have found that 97 percent of the assessed sites had substantial vulnerabilities. The vulnerabilities shown below describe the ten most common vulnerabilities found in Web site.

Most examples are presented in PHP for simplicity but apply equally to all languages used for both the front end (e.g., Java and Perl) and the backend (e.g., C, C++ and even Cobol) of an application.

1. **Cookie poisoning** – Cookies are small pieces of information passed between the server and the browser to maintain client information and/or memory (either short or long term) of the session. The Web application typically maintains this information on the client's machine. Many of these cookies are not cryptographically strong and can be enumerated or manipulated to achieve different valid but unauthorized values. If, for instance, the cookie contains values that represent the identity of the application user, modifying the value would permit a hacker to assume another user's identity in the application. Manipulation of the values contained in cookies is referred to as cookie "poisoning."

2. **Hidden field manipulation** – Hidden fields are embedded within HTML forms to maintain values that will be sent back to the server. They serve as a mean for the Web application to pass information between different parts of an application or between different applications. Using this method, an application may pass data without saving it to a common backend system (most likely a database). Application developers who rely on hidden fields for critical data usually assume that since the field is not visible , application users cannot view or change their values. Contrary to this belief, users can view these fields by examining the HTML code of the page. A malicious user can change this data by using a POST request sent directly to the server. By changing the value the entire logic between the different parts of the application is damaged and manipulated.

3. **Application buffer overflow** – Web applications that accept input should limit the number of characters in the input as well as the input variable name. By sending long strings for input values or their names, a malicious person potentially can corrupt application memory resulting in the application shutting down or the granting of elevated privileges on the server.

4. **Cross-site scripting** – A link to a valid Web site can be manipulated so that one of the parameters of the URL or maybe even the referrer will hold a script. This script will then be implanted by the server into a dynamic Web page and will run on the client side. The script can then perform a "virtual hijacking" of the user's session and activity and can capture information transferred between the user and the legitimate Web application. The user activates the malicious link when he crawls through a third party site or by receiving an e-mail with the link in a Web enabled e-mail client.

5. **Parameter logic tampering** – The basic interaction of the user's browser with the Web application is fundamentally a passing of values to the different programs that make up the application. The application uses these values to compute functions. If the application fails to check the validity of these values and their compliance with the original intent of the function, then by manipulating these values, the output of the function can be compromised.

6. **Backdoor and debug options** – Many sites have additional entryways into the application logic. Debug options that enable easy debugging of the Web application may be left active by developers either intentionally or by mistake. Backdoors in the system that can be activated to bypass authentication mechanisms and achieve control over the server and the application may be installed by developers or administrators (e.g., leaving a root command shell somewhere in the Web site).

7. **Forceful browsing** – If access controls are not properly configured, by directly typing addresses into the Web browser, files and applications may be accessed outside the normal flow of the application. Files that contain crucial information such as logs and databases and backup source files can be viewed. Directory structures can be retrieved and their contents exposed. Even worse, administrator files can be accessed that provide means to take control of the Web host.

8. **Stealth commanding** – If Web applications do not examine all input, a malicious user could embed a script that the Web server will run. Such scripts will run under the Web administrator permissions. Likely results are full control over the Web application and, in most cases, full control over the hosting server.

9. **Known vulnerabilities** – Web applications usually depend largely on standard software provided by third party vendors. This software may be for the Web server, application server, database or any other number of standard packages customized to specific vertical markets. Vulnerabilities are found on a regular basis in all such application due to how common these applications are. The vulnerabilities and automated tools to exploit them are then published on the Internet for hackers' use.

10. **Insecure third party software configuration** – The applications supplied by third party vendors may be configured in different and complex ways to address the needs of the specific site. However, a wrong configuration may compromise the site's security. Examples include default accounts open to outside access and insecure sample and demo files.

Conclusion

Looking at the above vulnerabilities, two questions arise: why do such vulnerabilities exist and what can be done to address them? The answer to the first question lies in factors such as dependence on multiple people during the development process, quality assurance, complexity of applications due to a large number of components, and fast deployment cycles. A partial answer to the second question is found in the audit process; while virtually all sites today attempt to achieve application-level security through a manual audit processes and ultimately fail, new automated tools have recently become available that either perform an automatic vulnerability assessment on the Web application or perform automatic protection on the Web application.

Additional resources

CERT® Coordination Center
http://www.cert.org/

System Administration, Networking, and Security Institute
http://www.sans.org/

Open Web Application Security Project
http://www.owasp.org/

Contains the BUGTRAQ mailing list of vulnerabilities
http://www.securityfocus.org/

Automatic tools for Web application security
http://www.sanctuminc.com/

MEMBERSHIP

Hector Massa
Committee Chairperson

Please join me and the SF ISACA Board in welcoming these new Chapter members.

Brian J. Alfaro
Arthur Andersen LLP

Erina R. Buckley
Levi Strauss & Co.

Anna H. Chan, CPA
SBC Communications, Inc.

Chris Chi-Ian Lou
Actuate Corporation

James A. Cowing, CPA
Certicom Corporation

Kai Cui CPA,CIA
Blue Shield of California

Robert W. Hiday, CISA
Comptroller of the Currency

Lloyd R. Lantz
AMC Consulting

Sandra E. Lee, CMA
PG&E Corporation

Jairo R. Leiva
CSAA

Gloria Lievano, CISA,PMI
Pacific Exchange

Deborah L. Marrs
Hall Kinion

Andrew K. Ng, CISA,CPA
Control Solutions Intl

Kristen A. Ricker
Federal Reserve Bank of S.F.

Erin M. Schuyler Bilvado, CIA
Blue Shield of California

Valerie A. Volkar
Chevron Texaco

Bill T. Vourthis
Fireman's Fund Insurance Co.

Martin D. Westfall
Bank of the West

Mary B. Wolverton
State Compensation Ins. Fund

Coleena Wong, CIA
Bank of Canton of California

Conny M. Cheng
Arthur Andersen
Transferred from the Los Angeles Chapter

Douglas P. Feil, CISA, CFE,CDRP
Comp. Security & Control Svcs.
Transferred from Hawaii Chapter

Heidi Matta Gabor
Kaiser Fdn. Health Plan, Inc.
Transferred from the Los Angeles Chapter

Mark A. Lundin, CISA,CPA
KPMG LLP
Transferred from New England Chapter

Julie A. Odlaug-Dulski, MCSE
eSecurity OnLine
Transferred from the Minnesota Chapter

Olugbemisola O. Oniyinde
JP Morgan Chase
Transferred from Silicon Valley Chapter

Sujatha Prabhakaran, CA,ACA
AHP Manufacturing B.V.
Transfer from Madras Chapter

Yanping Tang, CISA
Providian Financial Corp.
Transferred from the Utah Chapter

32nd ANNUAL NORTH AMERICA CONFERENCE – CACS

May 5-9 2002, Fairmont Hotel, San Francisco

Register now at www.isaca.org/nacacs2002.htm

The 32nd Annual North America Conference – CACS, the world's leading conference for IS Audit, Control and Security, will be hosted by the San Francisco chapter. For over 31 years, this conference has been the choice for all IS Audit, Control and Security professionals seeking to expand their proficiency in state-of-the-art technologies. At the same time, it meets their technical training needs (up to 44 CPE hours can be earned.)

This year's conference will be very exciting! In seven tracks and two Workshops, the conference presents a combination of theoretic and pragmatic points of view and highlights the corresponding challenges for the IS Audit, Control and Security professional. Following is a description of each track.

TRACK DESCRIPTIONS

Track 1

Core Competencies that every IT Audit professional must know and understand to competently perform the job, such as Risk Assessment; Change Management; Business Continuity Planning; IT Security Overview; etc.

Track 2

E-business concepts and challenges such as Risk Assessment; Systems Development; Legal and Web-enabled Risks; Open Standards; Peer-to-peer networks; E-tailing and E-marketplaces; etc.

Track 3

Highly technical sessions in Information Security such as International Standards; Computer Forensics; Cisco Routers; Intrusion Detection; Incident Response; Encryption; Wireless Security; etc.

Track 4

Enterprise Resource Program concepts such as ERP Fundamentals of Security and Control; Data Integrity; Best Practices; Data Warehousing; etc.

Track 5

Latest and most critical issues facing our community such as Call Center Auditing; Overview of Wireless Technologies; Security of Windows 2000 and Unix; Privacy Issues; IT Outsourcing and Co-sourcing; etc.

Track 6

Specific topics for the advanced practitioner such as Internet Policy; Windows 2000 Client/Server Migration Strategies; Security and Control Issues for Web-based Access System Development, LDAP Deployment, Firewalls, etc.

Track 7

Topics pertinent to IS audit directors and executive-level management such as IT Governance; Risk-Based Auditing; Infrastructure Capacity Management, IT Balanced Score Card; CIO Perspective on IT Audit Issues; etc.

Pre-conference workshops

- CISA Review Weekend
- Audit, Control and Security of Operating Systems

Post-conference workshops

- Cryptography, PKIs, CA, Digital Signatures and Trusted Third Parties
- Defining and Building an Information Security Architecture
- Real-world Implementation of CobiT…and the Payback
- A Systematic Approach to Attack and Penetration Testing and Vulnerability Assessment

Contacts

For more detailed information:
Gloria Lievano at glievano@pacificex.com

To assist during the conference:
Marcus Jung, marauditor@juno.com
(only for members of the San Francisco Chapter)

See you at the conference!

ACADEMIC RELATIONS

Brian Alfaro
Committee Chairperson

Does your company need interns?

SF ISACA internship program

The San Francisco ISACA Chapter is developing a project to expose motivated, prospective students to the career of IT assurance and security. This program is a platform where both organizations and students alike can benefit. Organizations offering student internships benefit from choosing to hire bright, enthusiastic students to work on department projects, as students obtain crucial experience necessary for pursuing a career in IT assurance and security.

In light of recent economic conditions, unfortunately, employment has been reduced. However, the need for IT assurance, coupled with the increased threats to IT security from recent events and the shortage of resources necessary to address these needs and risks, can create an opportunity for organizations to use internships to help mitigate these risks.

About the program

This program is designed to identify college students who are members of the student chapters of ISACA in the Bay Area and present them the opportunity to intern in IT assurance and security departments at various organizations throughout the Bay Area. The Academic Relations Committee is respectfully asking San Francisco ISACA members to please submit possible internship opportunities. There is no timeframe for when these opportunities for students should begin or end and opportunities are independently defined by each organization. Likewise, the requirements and wages for hiring students who apply through the Internship Program are defined independently by each organization.

Contact information

Please submit any job descriptions and requirements, or any questions regarding the Internship Program to Brian.Alfaro@us.andersen.com. 415-281-8059.

RECOMMENDED WEB SITES

Provided by
Cliff Nalls, Bank of America

This quarter's featured Network Auditing Web sites are listed below. Access these and other sites from our Chapter Web site at: http://www.sfisaca.org/resources/index.htm.

Network Management Tool RFC 1470

FYI on a Network Management Tool Catalog: Tools for Monitoring and Debugging TCP/IP Internets and Interconnected Devices.
http://rfc.x42.com/

The New Generation of Network Monitoring Systems

http://www.techguide.com/titles/newgen.shtml

Model for Well-Run Information Technology (WRIT)

Telcordia Technologies, Inc.
www.bellcore.com/products_services/conseng/enterprise/expert

Element Management Systems

International Engineering Consortium, WebForum, On-line Tutorials
http://www.iec.org/online/tutorials/

Refer a new member – receive a free gift

Take advantage of the Chapter's *New Member Referral Program.* Chapter members who refer an individual who joins ISACA-San Francisco Chapter will receive a free gift (gift will be delivered to the referring member after payment for the new membership has been received and processed by ISACA International). Don't miss an opportunity to help your colleagues keep abreast of developments in IS audit, security and control. Encourage your colleagues and friends to join ISACA today! For more information or to submit your referral to the *New Member Referral Program*, please send our Membership Committee Chairperson, Hector Massa (hlmsa@aol.com), the name, address, phone number, and e-mail address for the individual being referred.

Your e-mail address

If you have not sent your current e-mail address to ISACA International, then please send your address to hlmsa@aol.com to ensure that you receive important information electronically.

You may also access our Web site at www.sfisaca.org to update your contact information.

ISACA international

847-253-1545 voice
847-253-1443 fax
www.isaca.org

membership@isaca.org
certification@isaca.org
education@isaca.org
bookstore@isaca.org
conference@isaca.org
research@isaca.org
marketing@isaca.org

CISA item writing program

In order to continue to offer an examination that measures a candidate's knowledge of current audit, security and control practices, new questions are regularly required for the CISA Examination. Questions are sought from experienced practitioners who can develop items that relate to the application of sound audit principles and practices. Continuing education hours and cash payments are offered as participating in the CISA Item Writing Program, please request information about the program from ISACA International, Certification Department (certification@isaca.org).

Contribute to this newsletter

To submit an article or to contribute other items of interest for inclusion in future newsletters, please contact our Interim Communications Committee Chair, Todd Weinman at 510-232-4264, or todd_weinman@yahoo.com.

Learn about the San Francisco Chapter

Learn about the CISA certification

Test your skills with our CISA sample test questions

Complete our member survey

Access information regarding ISACA international

Access information regarding our Student Chapters

Register for monthly meetings

Register for seminars

Access information regarding ISACA conferences

Register for the CISA review course

Access our Chapter newsletters and monthly bulletins

Update your membership information (address, phone, E-mail)

Access IS audit, control and security resources

Research employment opportunities

Join a Chapter committee

Learn how you can join ISACA – understand the benefits

Contact Chapter Officers and Directors

JANUARY SF ISACA EDUCATION EVENT REVISITED by Jacki Rivero

Web Application Security
ISACA Meeting, January 17, 2002

Having spent most of my life as a pretty hard-core tech-type, I wasn't really sure what to expect when an organization of auditors announced they were holding a seminar on auditing Web applications. I'm happy to say I was pleasantly surprised by the day's presentations.

First up was Izhar Bar-Gad, CTO of Sanctum, a producer of Web Application Security software. While he did demo his company's products, most of his talk was focused on the types of exposures inherent in Web Applications. General Network security, in terms of firewalls, encryption, authentication, and such, is usually pretty well addressed in most companies. However, even the best laid plans of mice and Network Engineers can be completely undone by any number of application coding exposures. Contrary to popular perception, most hacks are done not with the intent of inflicting some type of mass destruction, but rather for personal gain. Some examples:

- Altering "hidden field" data. The coder may include some key piece of information, such as price per unit in a field embedded in the code, but not displayed on the page. The hacker can pull up the code using any edit tool, and alter the hidden field to his advantage, say, changing the price from $195 per unit to $1.95 per unit.
- Cookie poisoning. The hacker identifies the unique portion of each cookie, and alters it to suit his objective, such as transferring funds from someone else's bank accounts into his own.
- Leaving Debug on. Leaving the "debug" option on in a program makes it much easier for the coder to respond to problems. However, debug also leaves the code – and any data it comes in contact with – completely exposed to inquiring minds.

Of course, plenty of opportunities abound for anyone wishing to commit malicious mischief just for the fun of it, such as:

- Buffer Overflow. Increasing the number of characters allowed in a field beyond what the system will handle, thus forcing a crash.
- Stealth Commanding. Inserting an executable command into a field where data is expected to give the hacker the ability to gain control of the server.
- Cross-site Scripting. This is a bit more elaborate than other hacks, since it involves allowing client(s) to establish legitimate connections, then "listening in," like on an old telephone "party line." The hacker can collect all the data exchanged between the client(s) and the server.

Next up were Steve Madeiros and Robert Grill of CalFed. The gist of their presentation was that network security is more than firewalls and encryption. Using the OSI 7-layer network model as a basis, they demonstrated that there are a lot of other factors to consider, such as:

- The physical security of the equipment.
- Whether there were any "single point of failure" points in the network configuration, such as a firewall with no backup failover solution.
- Whether any device was at risk because of being overburdened by network traffic, demanding some type of load balancing solution.
- The types of Internet protocols being made available, such as Telnet, http, or FTP, and the ports on which they run.
- The security or lack thereof inherent in the Operating Systems software, be it NT, UNIX, or even OS/390.

Terry Bezdek of BofA gave a very interesting presentation on Web Application security from a completely different angle: application usability. His program for reviewing applications includes valuable tests not only for in-house developed Web applications, but also for any third-party applications and services being considered.

Application usability is more than determining whether the screens are easy to walk through. Other factors to consider include:

- The robustness of the supporting infrastructure. There are a couple of angles to consider here:
  - Nothing deters customers from using a Web site like not being able to get out to it, or experiencing abysmal response time.
  - Underestimating infrastructure requirements may lower the installation price, but it could result in performance problems that undermine any benefits the system had to offer to begin with. (NOTE: This is a particularly good thing to be mindful of when considering third-party outsourcer offerings.)
- Whether there are controls in place to ensure on-going customer satisfaction. In order to remain viable, the Web site has to continually evolve, offering new services and better performance. The biggest part of the "controls" piece is the Change Management process, ensuring that any changes to the application are adequately thought-out and tested, and don't blind-side the customer.

The last speaker was Goran Kovacevic, of PricewaterhouseCoopers. The focus of his presentation was the importance of developing and implementing an overall strategy for performing on-going assessments of Web application security. There are two different approaches, and they are not mutually exclusive:

- "White Hat" methodology – taking a pro-active approach to identifying exposures and correcting them before the application goes live. A "white hat" approach will include identifying not only code vulnerabilities, but also the reasons why someone might want to hack into the system to begin with.
- "Black Hat" methodology – periodically attempting to hack your own applications and network from the outside. There are legitimate security companies who can be retained to do just this, reporting on the effectiveness of the security.

Tools are available, including some free ones available for download from the Internet. It is wise, however, not to rely exclusively on the tools to find the exposures. The best methodology is one which incorporates the best of both – tools to pre-empt any exposures before the code goes live, and continual checks after the fact to make sure no new opportunities have been discovered.

All in all, attending the seminar was a very worthwhile experience. You can't go wrong with San Francisco's Plaza hotel, (although, for a while there, someone got a little crazy with the air conditioning).

Many exposures inherent in Web applications today are left over from the days when getting a Web presence up ASAP took precedence over quality controls. Application developers were often long on coding skills, but short on awareness of change management and application security best practices. Software installers were not aware of the dangers in leaving "default" files or demo versions active. Of course, for as long as Microsoft remains in business, it's a good bet there will be successive generations of hackers devoted to finding security holes in the software. All of this makes Web application security a most timely topic.

UNDERSTANDING THE ANATOMY OF A WEB SITE: N-TIER ARCHITECTURE

by Alex Stephens

Ph.D, VP and Technology Audit Consultant, Bank of America

In order to effectively audit Web applications, one must have an understanding of how Web sites are constructed. This article will provide you with a basic understanding of N-Tier Architectures of which Web sites are constructed.

The phrase "N-Tier Architecture" does not refer to Bauhaus styles or ziggurats; rather, it is a simple blueprint for the construction of Web sites. An "N-Tier Architecture" outlines a "division of labor" for the digital age – a means of distributing the work of an application (e.g., a Web site) across several network-connected computers. The "N" in N-tier simply represents the number of logical "building blocks" (or tiers) that go into the construction of a distributed application. Such modular design schemes (or "architectures") are popular as servers can be dedicated to specific logical tasks and additional functionality can be inserted into the architecture without completely revamping the site.

As an example, consider a common manifestation of an N-Tier Architecture: the e-commerce Web site. While there are varying degrees of complexity, the design of these sites boils down to three fundamental components: a user-interface tier, a "business logic" (or application) tier, and a database tier. As you might expect, such a design is called a "3-Tier Architecture".

As Web surfers, we are familiar with the "user-interface" tier. This is a Web site's facade – the server we connect to when we point our browsers to a page of interest. Since it is critical that the Web server present data as quickly as possible, the user-interface tier is unencumbered by any other processing. The Web server simply manages connections and presents content. All other work – such as the processing of forms or the archiving of customer data – is relegated to different tiers.

The term "business logic" is hopelessly vague, which is why many people call the second tier the "application layer". This layer is the workhorse of an e-commerce site. Simple actions (e.g., formatting data entered on a form) can result in a fair amount of processing. To prevent the slow down of the user-interface tier, the application layer takes on these processing duties and acts as an intermediary for the front-end Web servers and back-end database. At a minimum, application servers take data entered by a user, reformat it and pass a proper query to a back-end server. The application server also receives the back-end server's response, dynamically generates content and ships this content to the Web server for presentation to the user.

The back-end of an e-commerce site typically involves some flavor of database. The database is the equivalent of an information warehouse. This back-end layer keeps a record of the site's inventory and it can be used to archive customer and transaction data.

To understand how these individual tiers combine to form a functioning Web site, let's follow a simple search query at a hypothetical on-line bookstore. When we point our browser to the bookstore's main page, we are connected to the site's user-interface tier. Since there is a search function on this site, we enter a topic of interest (e.g., "Frank Lloyd Wright") and submit a search request. The Web server takes this input and passes it along to the application server. The application server has no idea if a book on Frank Lloyd Wright is in inventory, as the database houses that information. So, the application server reformats the search request and passes it to the database server in a language that the database software can comprehend. The database checks its index for any reference to Frank Lloyd Wright. If there is a match, the database returns info associated with that subject back to the application server which reformats the data into a browser-readable table of titles, prices and any other relevant information. This page is forwarded to the Web server, which passes the result of our query, full-circle, back to our browser.

While e-commerce Web sites aren't as visually spectacular as Bauhaus skyscrapers or a Mesopotamian temple, the functionality of sites based on the N-Tier Architecture is nonetheless impressive.

2002 CISA Review Course – ISACA San Francisco Chapter

Review course objectives

This review course is designed to assist candidates in preparing for the CISA Examination to be held on Saturday, June 8, 2002.

The Eight, four-hour review sessions will be taught by professional IS Auditors and will include lectures, practice questions and exams, and classroom discussions. The instructors for this year's course include professionals from Charles Schwab & Co., Inc., Coopers & Lybrand, KPMG, Deloitte & Touche, VISA, Bank of America, and Lander International.

CISA coordination committee

Questions regarding the review course or the CISA examination should be directed to the CISA Coordination Committee:

Sumit Kalra, skalra99@yahoo.com
Brian Alfaro, brian_alfaro@yahoo.com

CISA exam registration

The International office of the I.S. Audit & Control Association administers registration for the CISA examination. To register for the exam contact the International office to obtain registration materials at www.isaca.org, certification@isaca.org, or 847-253-1545.

NOTE: Exam registration forms sent by mail must be postmarked by April 3, 2002. Registration forms sent by fax must be received by April 3, 2002.

Review course fees

ISACA Members: $250
Non-members: $435 (includes 1 year ISACA membership)
$250 Review course fees
$110 Int'l + $30 processing fee (Int'l dues for the year)
$45 Chapter (SF Chapter dues for the year)

Repeat Students: No Fee (It is our policy to permit any CISA Review Course participants who do not pass the CISA exam to attend the following year's CISA Review Course at no cost, other than the cost of books and study materials)

Review course schedule

Domain 1: The IS Audit Process
April 6, 2002 (8:00am - 12:30pm)

Domain 1: Management, Planning, and Organization
April 13, 2002 (8:00am - 12:30pm)

Domain 2: Technical Infrastructure and Operation Practices
April 20, 2002 (8:00am - 12:30pm)

Domain 3: Protection of Information Assets
April 27, 2002 (8:00am - 12:30pm)

Domain 4: Disaster Recovery and Business Continuity
May 4, 2002 (8:00am - 12:30pm)

Domain 5: Business Application System Development, Acquisition, and Maintenance
May 11, 2002 (8:00am - 12:30pm)

Domain 6: Business Process Evaluation and Risk Management
May 18, 2002 (8:00am - 12:30pm)

No Class (Holiday)
May 25, 2002

Practice Exam
June 1, 2002 (8:00am - 12:00pm)

Review course information

Location: 425 Market Street (@ Fremont), room 2605, Downtown San Francisco

Transportation: The nearest BART station is the Embarcadero station. Parking is available in lot located on Fremont between Howard and Folsom ($2/day). Garage located at 50 Fremont ($6/day).

Course materials (recommended)

Review manuals available from International ISACA (order directly from www.isaca.org):

- Auditing & Systems: Exam Questions and Explanations, 9th edition
- Candidate's Guide to the CISA Examination, 2002
- CISA Bulletin of Information (BOI), 2002
- CISA Review Manual, 2002
- CISA Review Questions, Answers and Explanations CD-ROM, 2002
- CISA Review Questions, Answers & Explanations Manual, 2002 Supplement

Review course registration form

Complete and send this form along with payment to:

San Francisco ISACA Chapter
ATTN: CISA Review Registration
P.O. Box 26675
San Francisco, CA 94126

Fee enclosed (Check one):
Member rate, $250 _____
Non-member rate, $435 _____

Name: _____
Company: _____
Address: _____
City: _____
State: _____
Zip code: _____
Phone: _____
Fax: _____
E-mail: _____

The SF ISACA Chapter recognizes candidates who successfully pass the CISA examination by hosting a recognition luncheon following the announcement of the CISA exam results. We offer successful candidates the opportunity to invite their immediate supervisor or audit director, gratis, to the luncheon. If you would like your supervisor to be invited to the recognition luncheon when you pass the CISA exam, please indicate so below and supply the requested information. NOTE: Supervisors will only be contacted if you pass the exam.

Invite my supervisor to the Recognition Luncheon (circle choice): YES NO

If 'YES', supply the following information for your supervisor:

Name: _____
Title: _____
Company: _____
Address: _____
City: _____
State: _____
Zip code: _____
Phone: _____
Fax: _____
E-mail: _____

YOU TOO CAN BECOME A ROCK STAR!

Become an ISACA volunteer

Of the many worthwhile reasons to become a volunteer for the San Francisco Chapter of ISACA, becoming a Rock Star is only one of them. Some of the other benefits of volunteering include:

- The opportunity to network with influential people in the profession
- Gain visibility among your peers
- Develop leadership and management skills you might not have an opportunity to acquire on your job.
- Work with great people and have fun!

SF board members attend PCM conference in Seattle

This past October, three members of the San Francisco chapter of ISACA attended the President's Council Meeting (PCM) in Seattle. The PCM is an annual meeting in which Chapter leaders from the Western part of the United States and Canada gather to share best practices. The picture below is from a social expedition to the Experience Music Project, an interactive rock and roll museum.

Performing in the above picture is the Grunge Rock band Kalra. Members (pictured from left to right), on keyboards – former SF ISACA 1st VP Justin Gibson, on drums – Chapter President, Todd Weinman, on vocals – CISA Review Chair, Sumit Kalra (also pictured, Debbie Lew, former President of Los Angeles ISACA and several groupies). With great regret, the group disbanded when it was revealed that they only know one song.

SAN FRANCISCO CHAPTER BOARD ROSTER 2001/2002

Executive Board

President
Todd Weinman
Lander International
510-232-4264, ext. 17
todd_weinman@yahoo.com

1st Vice President
Beverly Davis
Federal Home Loan Bank
415-616-2766
davisb@fhlbsf.com

2nd Vice President
Rick Beckman
Bank of America
925-675-5282
rick.beckman@bankofamerica.com

Treasurer
Anne Woodbury
925-944-5982
annewoodbu@aol.com

Secretary
Bill Davidson
Bay Area Rapid Transit – IAD
510-464-6954
wdavids@bart.gov

Directors

Directors
Kathleen Arnold
Sun Microsystems, Inc.
650-336-0028
kathleen.arnold@sun.com

Christina Cheng
Safeway, Inc.
925-467-3563
christina.cheng@safeway.com

Sumit Kalra
Charles Schwab
415-636-7686
sumit.kalra@schwab.com

Edmund Lam

Hector Massa
Office of Thrift Supervision
650-746-7138
hector.massa@ots.treas.gov

Stuart R. White
Visa International
650-432-4320
srwhite@visa.com

Committees

CACS 2002
Beverly Davis, Chair
Kathleen Arnold
Swee Fuller
Steven Hudoba
Marcus Jung
James Kastle
Edmund Lam
Gloriea Lievano
Eva Paiva
Todd Weinman

CISA Review
Sumit Kalra, Chair
Brian Alfaro
Helen Sun

Communications
Todd Weinman, Interim Chair
Brian Alfaro
Doug Feil
David Lufkin
Maria Shaw
Aron Thomas
Lance Turcato

Education
Rick Beckman, Chair
Carey Carpenter
Anne Cole
Deb Frazer
Steven Hudoba
Jim Kastle
William Luk
Todd Weinman
Stuart White

Membership
Hector Massa, Chair

Advisory Board

Advisory Board
Robert Abbott
Arnold Dito
Kathryn Dodds
Chuck Dormann
Doug Feil
Carol Hopkins
Roberta Hunter
Marcus Jung
Susan Snell
Lance Turcato
Richard Tuck

ISACA – San Francisco Chapter
Communications Committee
PO Box 26675
San Francisco, CA 94126