Information Systems Audit and Control Association

SAN FRANCISCO CHAPTER LOCAL AREA NETWORK

THIRD QUARTER 2002

*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

Beverly G. Davis
President

Our team has a plan! On behalf of the Board of Directors we would like to extend our sincere appreciation for selecting us as your chapter's leaders. Your votes counted and the new Board has an exciting plan for the upcoming year. The newly elected Board leadership includes the strengths and talents of twelve outstanding individuals.

Christina Cheng, the 1st Vice President, has been extremely active and has contributed to the Board in many roles. She has served as Treasurer, assisted with the CISA Review Course, and above all she has accepted the challenge of coordinating this year's Communications Committee. This year's primary focus is to provide the members with more substantive technical material as part of the newsletter content. Dave Lufkin is our newest Board member and has graciously accepted his role as being our primary source for coordinating the newsletter technical material. As always, if you would like to make a contribution to the newsletter content, feel free to contact Christina.

Carey Carpenter, the 2nd Vice President, became a contributor to an outstanding team of strong leaders (Rick Beckman, Steve Hudoba, Justin Gibson, and Todd Weinman). At mid-year we lost three key members of the Education Committee and Carey, recruited by Todd Weinman, assisted the chapter with completing last year's education schedule. We are pleased that Carey has agreed to accept the leadership role of facilitating the goals established under the tutelage of our previous chapter leadership. Two new Board members, Gloria Lievano and Jennifer Smith, are very strong leaders who have provided the Education Committee with outstanding resources to achieve a sterling commitment level for another year. Look out members, they are planning the 2002 eXciting Fall Conference. It is guaranteed to be outstanding!

Lisa Corpuz, our Secretary and also a part of the Education Committee came on board as a committee member and quietly added support to team. When called upon to serve in a more challenging role, Lisa accepted the leadership torch without reservation. We have been most fortunate to have individuals on the Board who have multiple interests and Lisa is one of them.

Anne Woodbury, our Treasurer, took the helm when Christina was on Maternity Leave. Literally, Christina was on leave for the birth of her daughter in January 2002. Anne has without a doubt done a magnificent job in managing the chapter's financial resources. Since Anne took over she has moved forward with implementing systems to manage the Budget Process while generating up to date financial information to better evaluate event financial outcomes. We are proud of this direction and value Anne's contributions.

Brian Alfaro, started as a volunteer working diligently with the Student Chapter at San Francisco State. His drive and initiative positioned the chapter for recruiting a new resource pool. Brian was instrumental in developing a Student Internship Program and expanding the CISA Review Scholarship Awards. This year Brian will coordinate the CISA Review Program. Congratulations Brian!

Bill Davidson, has been our chapter's historian and guide to implementing effective leadership. For over a decade Bill has contributed substantially to our chapter. He has held many offices and this year Bill

Contents

PRESIDENT’S MESSAGE – continued

will manage the Membership Committee. Thanks Bill for being that solid rock which I can lean on!

Sumit Kalra is another of those individuals who is always there when you need them. This year Sumit has resolved to take the role as the Academic Liaison with the Student Chapters. We are excited about what Sumit has planned, so look forward to seeing more students accepting the role of CISA professional.

Last but not least is me as your President. I am honored and pleased to serve in this capacity and I am hopeful that we as a Board will do an exceptional job in the upcoming year. We have our challenge of providing the membership with “Quality” educational events. Thank you for this opportunity and our team has a plan to make this year’s experience one that will standup to the rest.

Now that you know who the leadership is, I would like to take a few more minutes of your time to update you on Chapter operations. The Chapter is a professional organization that is managed by professional volunteers. Volunteers do all the monthly training events and communications. If you can find time in your schedule to assist the chapter in any way, please send me an e-mail at davisb@fhlbsf.com. Thanks again for your support and welcome to our new fiscal year!

Sincerely,

Beverly G. Davis
President

CALENDAR OF UPCOMING EVENTS

Date	Event	Place	More information
September 19, 2002	Joint IIA / ISACA Luncheon Meeting, Managing Operational Risk – Lessons Learned from the Basel II Capital Framework	Sheraton Palace Hotel, San Francisco	www.sfisaca.org
October 16-18, 2002	Fall Seminar	Sheraton Palace Hotel, San Francisco	www.sfisaca.org
November, 2002	Full Day Seminar	TBD, San Francisco	www.sfisaca.org
December, 2002	Luncheon Meeting	Sheraton Palace Hotel, San Francisco	www.sfisaca.org
National events			
September 16-20, 2002	IS Audit and Control Training Week	St. Louis, MO USA	www.isaca.org

2nd Annual eXciting Fall Seminar • October 16-18

eXtreme Educational Opportunity

In this fast-paced, high-tech world in which we live, racing to keep up with the demands placed on an IS Audit professional is challenging.

The SF ISACA Fall eXciting Seminar offers an eXcellent opportunity to stay on top of change and maintain your competitive edge. Respected instructors from industry and public accounting will provide valuable information on a wide variety of topics affecting our profession.

This year's Fall eXciting Seminar will again be held at the beautiful Palace Hotel in San Francisco's Financial District:

Palace Hotel
2 New Montgomery Street
Corner of Market and New Montgomery Streets
San Francisco, CA

More details and registration forms can be found at our Web site:
http://www.sfisaca.org/events/2002-October.htm

eXceptional Value

Nowhere else can you receive such high quality training at this low price (Prices include breakfast and lunch)

Three-Day Event (including Chapter Luncheon)*	Daily Registration Fee*	Chapter Luncheon Only
$500 Members (or 16 Saverpasses)	$225 Members (or 7 Saverpasses)	$40 Members (or 1 Saverpass)
$600 Non-members (or 20 Saverpasses)	$250 Non-members (or 8 Saverpasses)	$50 Non-members (or 1 Saverpass + $10)
		$20 Student

***Early Registration Discounts**
Participants who register early are entitled to the following discounts. Registrations must be mailed in (*postmarked no later than September 20, 2002*) to the Chapter with payment in full (checks or Saverpasses only).

$50 discount for Three-Day Event
$25 discount for Daily Registration
$5 discount for Chapter Luncheon

The SF Chapter of ISACA is grateful for our Fall eXciting Seminar Sponsors

PRICEWATERHOUSECOOPERS

Deloitte & Touche

KPMG

LANDER INTERNATIONAL
Where talent meets technology

PentaSafe
The safest way to grow your business.

eXciting Fall Seminar • October 16-18 • eXcellent Lineup of Topics and Presenters

Attendees may mix and match tracks; any session is open to any participant.
Please remember that the speaker and topic schedule are subject to change!

	Core Competencies	Information Security	Hot Topics
Wednesday, 10/16/02			
8:00 - 9:45 am	Intro to IS Auditing & General Controls – Level I *Byers/Sheikh, D&T*	Wireless Security *Tony Butts, Wells Fargo*	Understanding Web Application Security *TBD, Sanctum*
10:00 - 11:45 am	General Computer Controls – Level II *Stephen Spalding, D&T*	Information Warfare *Wells Fargo*	Proven Practices for Securing Web Enabled Applications *TBD, Sanctum*
1:00 - 2:45 pm	Application Auditing Systems *Evan Kyono, D&T*	Intrusion Detection *Eugene Schultz, Lawrence Berkeley Nat'l Lab*	Instant Messaging *Julie Kendall, Apple*
3:00 - 4:45 pm	Auditing: Basic Security Auditing *TBD, D&T*	VPN Security *Bruce Bragg, Wells Fargo*	Auditing Unix in a Mainframe Environment *Alan Wong, BofA*
Thursday, 10/17/02			
8:00 - 9:45 am	Change Management Trends & Tools Demo I *Kevin Fried, D&T/ Serena*	Auditing Oracle Database Security I *Deepti Bhatanagar, D&T*	Auditing Linux I *TBD, IBM*
10:00 - 11:45 am	Change Management Trends & Tools Demo II *Kevin Fried, D&T/ Serena*	Auditing Oracle Database Security II *Deepti Bhatanagar, D&T*	Auditing Linux II *TBD, IBM*
1:00 - 2:45 pm	Project Risk Management/ SDLC Reviews I *Byers/Thomas, D&T*	Auditing Cisco Routers & Switches I *Alan Wong, BofA*	Auditing Microsoft Active Directory I *TBD, PwC*
3:00 - 4:45 pm	Project Risk Management/ SDLC Reviews II *Stephen Madler, D&T*	Auditing Cisco Routers & Switches II *Alan Wong, BofA*	Auditing Microsoft Active Directory II *TBD, PwC*
Friday, 10/18/02			
8:00 - 9:45 am	Risk Based Auditing – Incorporating COBIT *D&T*	Auditing UNIX I *Rodney Kocot, Union Bank of California*	Risks and Challenges of Outsourcing *Kendall Tieck, BofA*
10:00 - 11:45 am	Best Practices – CAATs *Sheryl Eberhardt, D&T*	Auditing UNIX II *Rodney Kocot, Union Bank of California*	Ensuring the Effectiveness of PKI Security & Controls *TBD, PwC*
12:00 - 2:30 pm	OCTOBER CHAPTER LUNCHEON Identity Management – PwC		
2:45 - 4:30 pm	Business Continuity Management *Rob Yewell, D&T*	Benchmarking Information Security Practices *TBD, Pentasafe*	Developing Tools for Identifying Key Risk Indicators *Brad Ames, HP*

MEMBER MILESTONES

Members for over 25 Years

Douglas A. Webb, 1976
Charles A. Dormann, 1977

Members for over 20 Years

Gary W. Riske, 1978
David L. Lowe, 1978
Hector L. Massa, 1978
Charles C. Wood, 1979
Arnold Dito, 1979
David R. Durst, 1979
Robert C. Kimball, 1980
William Z. Davidson, 1980
Bob Gligorea, 1980
Carol Muller, 1980
Joel L. Lesser, 1981
William G. Martin, 1981
Kathleen W. Williams, 1981
Bruce L. Reid, 1981
Peter Hsieh, 1982
Judith Wall, 1982

Members for over 15 Years

Kathryn M. Dodds, 1983
Allen H. Martins, 1983
Kerry G. Elms, 1983
Leslie D. Fondys, 1983
Katherine M. Ullman, 1984
Jerry K. Hill, 1984
Martin W. Taylor, 1984
Richard J. Tuck, 1985
David A. Gilliam, 1985
Nancy D. Wiesbrook, 1985
Marcus A. Jung, 1985
Stephen Banks, 1986
Mary J. Bean, 1986
Steven Hudoba, 1986
Eugene W. Menning Jr., 1986
Vickie P. Smith, 1986
Paley Y. Pang, 1986
Kelvin Patterson, 1986
Louis R. Walker, 1987

Members for over 10 Years

Guy T. Anderson, 1988
Robert C. Motts, 1988
Sharon Tatehara, 1988
Jeffrey P. Mazik, 1988
Adam F. Levine, 1988
Ralph G. Nefdt, 1989
Kathleen E. Arnold, 1990
Beatrice K. Ashburn, 1990
Jack B. Cooper Jr., 1990
Todd E. Fenner, 1990
William Grant, 1990
Robert W. Hiday, 1990
Wing K. Yeung, 1990
Lawrence A. Jewik, 1990
Juan I. Lorenzo, 1990
Melody Jean Pereira, 1990
Keith D. Scott, 1990
James H. Tanner IV, 1990
Lawrence B. deBerry, 1991
Lynne A. Trestrail, 1991
Douglas K. Walsch, 1991
Leah J. McKern, 1992
J. Michael Samuel, 1992
Aidan M. Collins, 1992
Neville R. Morcom, 1992
Myoung Andy Kim, 1992
Foong Meng Wong, 1992
Scott W. Van Tyle, 1992
Lance M. Turcato, 1992
Richard M. Buford, 1992
Alec J. DeSimone, 1992
Jeffrey A. Nigh, 1992
Michael J. Cuggino, 1992
Carol A.Tanner, 1992

WIRELESS ACCESS

White paper
Phoenix chapter
ISACA

by Thomas Gleason

Thomas Gleason is an
Information Systems Auditor
with Maricopa Community Colleges

2411 W. 14th Street
Tempe, AZ 85281
Tom.Gleason@domail.maricopa.edu

This technology, officially called 802.11b, is seeing rapid implementation on college campuses and within industry. It serves to network computers without the use of cables and wall jacks and performs very well for home use or in areas where security is not a key concern. The rapid adoption of 802.11b has organizations as diverse as Starbucks and Arizona State University installing wireless networks to serve their clientele.

The technology is cheap. A wireless access point (AP) serves as the transmitting station and can serve from 32-250 wireless users and costs less than $200. Wireless cards cost under $100 and, once installed in a notebook or desktop computer, allow machines to share data with others on the network. They also gain access to the broader wide area network (WAN) and the Internet. The radio frequency used allows data transmissions at a maximum rate of 11mbs and will transmit up to 91 meters indoors and 450 meters outdoors. Obstructions like ceilings and walls can greatly diminish the range [1]. Special antennas can detect wireless networks several city blocks away.

A wireless network piggybacking on the main network would be easy to install and hard for the network administrator to detect. A typical installation consists of plugging a small AP/router into an office RJ45 network wall jack. The router's Ethernet address (MAC) can usually be set to any value. Devices connected by cable or wireless to a router/AP are assigned a new IP address using DHCP and are hidden behind the router's Network Address Translation (NAT) firewall. The packets they transmit have a unique MAC.

The key problem with wireless is the weak default security. The wireless network's password is radio broadcasted in clear text and is subject to being hijacked by hackers driving around with a notebook computer. In fact, this popular drive-by-and-snoop pastime is called "war driving". The hacker Web site www.netstumbler.com provides free software to collect wireless passwords and hosts a database listing many thousands of wireless networks, their passwords, and even popup geographic maps showing the location of the hacked AP. A hacker can connect to a poorly secured wireless network just by knowing the AP's password.

To improve security, it's essential not to rely only on the AP wireless password and to consider activating the optional Wired Equivalency Privacy (WEP) encryption. The WEP encryption algorithm can be hacked [2] but it's time consuming. At the present time about 50% of wireless installations run without WEP as it causes performance to degrade. Implementing wireless with a virtual private network (VPN) [3] or additional encryption like Secure Shell (SSH) will serve to greatly improve security but adds more complexity to the setup.

Knowing the AP password and gaining access to the wireless network means people can use your Internet connection but that doesn't necessarily mean they can compromise individual computers. Common sense dictates that computers sharing the AP should have logon authentication and a good security administration policy. For small networks and where WEP isn't workable, the administrator may want to turn off DHCP, assign static IP addresses, and change the IP subnet from the usual default of 192.168.1.0. Many APs allow you to control access based on the MAC address of the NIC attempting to associate with it. If the MAC address of the NIC isn't in the table of the AP, it can't be associated and the intruder can't get in. And while it's true that there are ways of spoofing a MAC address sniffed out of the air, it takes an additional level of sophistication.

Proposed new standards to the IEEE 802.1X Standard protocol have promised to provide future wireless networks with better security and increased transmission speeds. But, even those standards are now in doubt. A recent research paper [4] stated that wireless sessions using the new security scheme could be stolen by an intruder pretending to be an AP and then either hijacking the connection or stealing information with a "man in the middle" attack. Until a security standard adopts symmetric authentication (proof of identity) between the AP and client it's doubtful that wireless networks will offer adequate security.

In the near future, we can expect a growing base of wireless networks and related devices. Until security measures catch up with the technology, systems connected via 802.1X should be treated as external networks and the AP should be outside the organization's firewall.

[1] The wireless LANs indoor data transfer rate between computers will generally degrade beyond 30 meters from the AP. Internet connections transfer data at only about 1.5mpbs and will retain good performance at a greater distance.

[2] AT&T Labs Technical Report: http://www.cs.rice.edu/~astubble/wep_attack.pdf Approximately 6 million packets are needed to break WEP. This could be collected in a few hours on a moderately used network. In reality, WEP encryption effectively stops all but the most determined intruder.

[3] VPN Explained: http://www.linksys.com/edu/part7.asp

[4] http://zdnet.com.com/2102-1105-839948.html William Arbaugh and Arunesh Mishra, University of Maryland, February 2002

RECOMMENDED WEB SITES

A practical guide to dealing with network security scofflaws – *CrossNodes*

While security tools play a significant role in maintaining information integrity, every organization seems to have its (un)fair share of users who just don't follow the rules. This article gives some practical tips on implementing formal policies with formal penalties for infraction.

http://networking.earthweb.com/netsecur/article/0,,12084_963021,00.html

Keeping corporate information confidential – *SC Magazine*

The chief investment officer of a Washington, DC-based banking and private equity consulting firm, takes a long hard look at the risks to corporate privacy from disgruntled employees, greedy insiders, rogue contractors, and even unethical clients – and what you can do to minimize those risks.

http://www.infosecnews.com/opinion/2002/01/30_03.htm

How hackers can destroy your business: a true story – *InternetWeek*

Anonymous hackers have forced a British firm out of business. CloudNine Communications, one of Britain's oldest Internet Service Providers (ISPs), shut down last week in what computer experts believe is the first instance of a company being hacked out of existence.

http://www.internetweek.com/story/INW20020201S0003

2002: The year of the trojan? – *ZDNet News*

Earlier this month, we entered the year of the black horse, according to the Chinese calendar. Here, Robert Vamosi shares his thoughts on why the major security threats this year are likely to follow the same analogy – and what you can do to prevent trojan horses fooling you into letting them into your PC.

http://zdnet.com.com/2100-1107-830278.html

Just because you're paranoid doesn't mean they aren't out to get you – *searchSecurity.com*

Although it would be great if you could make your networks invisible to the world, the technology, as they say, isn't here yet. But if you follow David Strom's advice – particularly with reference to those 'power users' who believe the rules don't apply to them, you can ensure a reasonable level of enterprise privacy.

http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci802189,00.html

Securing your VPN – *SC Magazine*

As the number of telecommuters grows, so do the risks associated with VPNs to enable remote workers to connect to the corporate network. It's important to know that VPNs don't address the threat posed by pests. If you're using Check Point VPN-1(r), see Section 2 for one step you can take.

http://www.infosecnews.com/opinion/2002/02/20_02.htm

Useful and Informative Links
Here are some links to articles dealing with information security. If any of you have links to sites that you frequently reference, let us know and we'll pass them on to the membership.

ACADEMIC RELATIONS

Brian Alfaro
Former Committee Chairperson

Congratulations to the recent graduates of the Student Chapter of ISACA at San Francisco State University this past Spring! The Student Chapter President, Carrie Li has contributed immensely in the continued development of the SFSU Student Chapter by increasing student membership and organizing career events.

The Student Board of Directors are currently planning the future semester and have voted Jose Ramirez to succeed Carrie as President for the Fall 2002 semester. As for the Academic Relations Committee Chair, Sumit Kalra, will take upon the role and responsibilities of this position. The students will greatly benefit from Sumit, since he is also a San Francisco State University alumnus. In addition, Sumit will fit well in being a mentor because he also helped pioneer the IS Audit curriculum.

Providing key mentoring to the Student Chapter has resulted in many contributions at the Parent Chapter level from past college graduates. Brian Alfaro will move on to take upon the responsibilities of CISA Review Course Coordinator. It is a continued goal to have more students sit for the CISA exam and also contribute to organizations such as ISACA as they continue in their careers.

Sumit Kalra is the Committee Chairperson for Academic Relations for 2002/2003.

MEMBERSHIP

Bill Davidson
Committee Chairperson

The membership count for the San Francisco Chapter as of August 1, 2002, stands at 379 members. Please join me and the San Francisco ISACA Board of Directors in welcoming the following new chapter members.

Maria Brandenburg
Fireman's Fund Insurance Company

Renato Burazer, CISA
Deloitte & Touche LLP
Transferred from the Slovenia Chapter

Jocelyn Chan
PricewaterhouseCoopers LLP
Transferred from the Los Angeles Chapter

Conor S. Crowley, CISSP
Freelance
Transferred from the Chicago Chapter

Cary K. Dare
Samtrans

James Draper, CISA, BA, ACA
KPMG
Transferred from the London, UK Chapter

Francis Ha
San Francisco, CA
Transferred from the Hong Kong Chapter

Julie Kendall, CISA
Apple Computer Inc.
Reinstated Member

Paul M. Kizirian
Wells Fargo Bank

David L. Koon
San Francisco, CA

Kendall D. Tieck
Bank of America

John W. Totulis
Household Credit Services
Reinstated Member

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, William Davidson (wdavids@bart.gov), 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 wdavids@bart.gov 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 Communications Committee Chair, Christina Cheng at (925) 467-3563, or christina.cheng@safeway.com.

www.sfisaca.org

Information Systems Audit & Control Association
San Francisco Chapter

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

HARDENING THE UNIX SYSTEM, PART TWO

PART TWO

by Dan Hilton
Technology Audit Consultant
Bank of America

In the 2nd Quarter newsletter, Part One of Hardening the Unix System was presented. The purpose of this three-part article is to introduce steps auditors can take to ensure the Unix system is properly configured. If your Unix systems are hosting critical applications, you want to ensure they are configured to limit security or reputation risks.

Part One spoke of rhost files, netrc files, the hosts.equiv file, the login banner, password settings, and umask settings. This article will present the following items that should also be reviewed when reviewing the configurations on a Unix system: user IDs, Unix services, and system timeout.

User IDs

Description

A user ID is a unique identifier that a user is assigned to authenticate to a Unix system. When accompanied with a password, the combination of the two allow the user access.

Control

Obtain the list of IDs and cross-reference with the company's personnel list or directory to ensure that access is appropriate and commensurate with job responsibilities. To help with this process, each user ID should have a name, department, and phone number documented next to each user (see below for details). User IDs of terminated or transferred employees can be maliciously used against the system.

Second, each user ID should be reviewed to ensure that each ID has a unique UID number. A UID number is associated with each user and is used by the system to determine what resources that user ID can access. If two or more IDs have the same UID number, then two IDs could share the same system resources. For example, the UID for root is always 0. If another user was assigned a UID of 0, then that user would have unlimited access to data that root should only be able to access.

Finally, there are approximately 12 system user IDs that are shipped with every Unix system. They are outlined in the section below. These user IDs should not be active IDs, unless they are absolutely necessary for normal business operations. If activated, these IDs can permit access to specific system files where user access should be restricted. In addition, these IDs are not associated with a particular user, and a clear audit trail is not recorded when the IDs are used.

File(s) to review

The following command should be executed to obtain a list of the system user IDs:

```
cat /etc/passwd
```

An example of a UID is highlighted below. In addition, the system IDs are listed with several of the functionalities in parenthesis. The remaining functionalities can be found using the resources identified in the final paragraph.

UID example

```
johnd:x:1006:10:John Doe, Unix Support,
555-555-1111:/export/home/danh:/bin/ksh
```

System IDs

```
daemon:x:1:1::/:
```

(used for managing some system utilities)

```
bin:x:2:2::/usr/bin:

sys:x:3:3::/:

adm:x:4:4:Admin:/var/adm:

lp:x:71:8:Line Printer Admin:/usr/spool/l
```

(used for print services)

```
smtp:x:0:0:Mail Daemon User:/:
```

(used for mail services)

```
uucp:x:5:5:uucp Admin:/usr/lib/uucp:
```

(used to maintain UUCP)

```
nuucp:x:9:9:uucp Admin:/var/spool/uucppub

listen:x:37:4:Network Admin:/usr/net/nls:

nobody:x:60000:60001:Nobody:/:
```

(used as a default user with no access privileges)

```
noaccess:x:60002:60002:No Access User:/:

nobody4:x:65534:65534:SunOS 4.x Nobody:/:
```

(used as a default user with no access privileges)

Unix Services

Description

Unix has a multitude of available services that may or may not be used to help operate the system. For example, ftp and telnet are two services on the system, which are typically used by individuals accessing the device. FTP or File Transfer Protocol is often used on a Unix system to transfer files to and from one computer to another, and Telnet is used by the users to connect remotely.

Control

The following are the standard services available on the system: ftp, telnet, shell, login, exec, uucp, finger, tftp, comsat, talk, ntalk, echo, discard, chargen, time, discard, and daytime.

As with many operating systems, the risk of operating certain services is much greater than the benefit received. For example, finger can be used by an individual, without access, to gain further knowledge about a particular system. Such information can then be used to gain unauthorized access. Many of the services listed above have risk factors that must be weighed against their benefit before they are used.

Practical Unix & Internet Security, by Simson Garfinkel, is an excellent source for describing each service and its related risks. An auditor should review each of the services on the system and determine what is needed for standard business operations. It is typically recommended that FTP and Telnet be the only active services in a Unix environment.

File(s) to review

To review the services on the system, execute the following command:

```
cat /etc/inetd.conf
```

Below are two lines of output from such a command.

```
telnet stream tcp nowait root
/usr/sbin/in.telnetd in.telnetd

# finger stream tcp nowait nobody
/usr/sbin/in.fingerd in.fingerd
```

To determine if a service is activated, look for a # sign to the left of each row. If the # sign is present, it indicates that the service is not active. If the # sign is not present, the service is active.

System timeout

Description

A user often walks away from his or her computer while still logged on. System timeout specifies the inactive time that must lapse before the user is automatically logged off.

Control

Review this file to ensure that a reasonable timeframe is established to ensure a user is logged off. If timeout is not set and a user remains active on the system, an unauthorized user could use the authorized person's system to perform malicious acts. A recommended setting for timeout is 300 (this is in seconds). This equates to five minutes of inactivity before a user is logged off.

File(s) to review

Solaris: `cat /etc/default/login`

HP: `cat /etc/profile`

AIX: `cat /etc/security/login.cfg`

The output from Solaris and HP should display, `TIMEOUT = 300`. The output for AIX should display, `LOGINTIMEOUT = 300`

If the setting has a # sign to the left of the line, `TIMEOUT` or `LOGINTIMEOUT` is disabled.

As stated in Part One, these are certainly not all the potential vulnerabilities on a system. New vulnerabilities and security holes are frequently identified which require security patches and new controls. Much like any other technology, you must make an effort to read various periodicals and books that publish new information. The following are a few recommended sources of Unix information:

- Practical Unix & Internet Security, by: Simson, Garfinkel, and Gene Spafford
- http://www.sans.org/
- http://www.geek-girl.com/unix.html
- http://www.unixreview.com/

Part One focused on unsecured files, message banners, passwords, and umask settings. Part Two has now addressed the controls and risks associated with user IDs, Unix services, and system timeout. In the final issue, several more Unix controls and risks will be addressed which will also significantly improve the security on a Unix device. Also, a few additional Web sites will be provided which give additional information on auditing a Unix system. By reviewing the information provided in this series of articles, along with using the recommended resources, it should improve your understanding of how to effectively secure a company's Unix systems.

3rd ANNUAL JOINT SF ISACA/SF IIA LUNCHEON PRESENTATION

Managing Operational Risk – Lessons Learned from the Basel II Capital Framework

Thursday, September 19, 2002 • 1.5 hours of CPE credit

Session description

Operational risk management is an emerging issue in the banking industry. This is due in part to several recent well-publicized events such as large-scale business resumption breakdowns and major trading losses from internal control failures. At the same time, proposed capital charges for operational risk are being deliberated as part of the Basel II capital framework. (Basel II is an effort to revise and modernize international capital requirements for the banking industry.) While the Basel accords are limited to the banking industry, these decisions will impact the market's expectations for sound capital and risk management practices in other industries as well.

Speaker bio

Michael E. Johnson an officer in Banking Supervision and Regulation with the Federal Reserve Bank in San Francisco. Mr. Johnson is responsible for the development, training, and support of examination programs that assess operational risk, including information technology and wealth management, at State member banks, bank holding companies, and regional data processing companies in the 12th Federal Reserve District. He also participates on numerous Federal Reserve System policy groups dealing with operational risk, information technology, and e-banking supervision.

Prior to this assignment, Mr. Johnson served as the officer in charge of internal automation support for his department, and previously had responsibility for approving bank mergers and acquisitions in California and the Western Region of the United States. Before joining the Federal Reserve Bank of San Francisco seven years ago, Mr. Johnson was director of the mergers and acquisitions unit for the Federal Reserve Bank of Dallas.

Register

To register or to find other important details about the program, visit our Web site: www.sfisaca.org

Schedule

Time	Description
11:30-12:00 pm	Registration
11:30-12:30 pm	Lunch
12:30-2:00 pm	Presentation

Pricing

Including Saver Pass info (if applicable)

$40 Members (or 1 Saver Pass)
$50 Non-members (or 1 Saver Pass plus $10)
$20 Students
Payable in cash, check, or Saver Pass only – no credit cards.

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, Tim Sauer, at either tim@landerint.com or at (510) 232-4264 x24.

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.

SAN FRANCISCO CHAPTER BOARD ROSTER 2002/2003

Executive Board

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

1st Vice President
Christina Cheng
Safeway, Inc.
925-467-3563
christina.cheng@safeway.com

2nd Vice President
Carey Carpenter
Deloitte & Touche
415-783-5290
ccarpenter@deloitte.com

Treasurer
Anne Woodbury
Providian Financial
925-738-4849
anne_woodbury@providian.com

Secretary
Lisa Corpus
Providian Financial
415-278-8713
lisa_corpuz@providian.com

Directors

Directors
Brian Alfaro
Andersen LLP
415-546-8200

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

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

Gloria Lievano
Pacific Exchange
415-393-7933
glievano@pacificex.com

Dave Lufkin
Bank of America
925-675-1878
dave.m.lufkin@bankofamerica.com

Jennifer Smith
Wells Fargo
415-396-7955
smithjen@wellsfargo.com

Todd Weinman, past president
Lander International
510-232-4264, ext. 17
todd@landerint.com

Committees

Academic Relations
Sumit Kalra, Chair

CISA Review
Brian Alfaro, Chair
Sumit Kalra
Helen Sun

Communications
Christina Cheng, Chair
Lance Turcato, Web Master
Brian Alfaro
Doug Feil
David Lufkin
Maria Shaw
Aron Thomas

Membership
Bill Davidson, Chair
Hector Massa

Education
Carey Carpenter, Co-chair
Todd Weinman, Co-chair
Lisa Corpuz
Jim Kastle
Helen Leung
Gloria Lievano
William Luk
Maryam Malek
Cliff Nalls
Jennifer Smith
Roy Vaiani
Stuart White

Volunteer
Todd Weinman
Helen Sun, at large volunteer

Advisory Board

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

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