

Abort,
Retry,
Ignore...



Computers Are Easy User Group

July 2001

Suggested Retail Price \$1.95

Volume XIV

Issue 7



Calendar
of
Events

!!! IMPORTANT !!!

Meeting dates for
2001
See page 10
for all
confirmed
dates.
Time and Place
remain the same.

Upcoming
CAEUG meeting
Saturday,
July 28
2001
9:45-12 noon

CAEUG
PICNIC
Saturday
August 25
11AM-3PM
Seven Gables
Park
Same place as
last year

Firewalls and Always-On Connections

by Eb Guenther

Introduction

What is a firewall? Why do you need one? How does a firewall work? I will give you some quick answers. For unanswered questions, or more information, attend the Internet SIG on Friday, July 13th at 7 p.m., where we will present a special program about firewalls to complement this issue. Though we emphasize always-on connections, firewalls are not just for broadband. They provide security for any speed connections, even 28.8 kbps or slower dial-up accounts. If you have even a single server running on your PC, or you share resources over a TCP/IP type connection (protocol of the Internet), you need a firewall. Weasel clause: This article is for information only. Any action you take as a result of this article may not fully protect your system, and you do so at your own risk.

What is a Firewall?

A firewall is a software utility or hardware device placed between a private network, such as your home or office LAN, and a public network, such as the Internet, and to block undesirable traffic between them. In addition to blocking undesirable traffic it may act as gatekeeper to your private network, as router to the individual workstations and applications (servers or clients), as a proxy server, and as logger of security information.

See [figure 1](#) for a sample firewall diagram. (on page 4)

Why do you need a firewall?

Are there bad guys out there who want nothing more than to attack YOUR computer? You bet! What could they want with your machine? They want to prove that they can hack your machine. They want your user IDs and your passwords. They want to grab any bonus they might find (like the number to your Swiss bank account ;-). They may want to use your computer as a base for spamming or attacking other computers (in YOUR name!). Any server running on your machine or network is a potential breach of your network's security. Hackers look for vulnerabilities in the way servers handle client requests. Even if you think you have no servers running, a rogue application might have installed its own server without telling you.

Now that Microsoft has blessed us with Visual Basic for Applications' tie-ins to Internet clients like Outlook and Internet Explorer you even must worry about these clients'

(con't on page 4)

TABLE OF CONTENTS

FIREWALLS AND ALWAYS-ON CONNECTIONS BY EB GUENTHER.....	1
HELPLINE.....	3
THE LAMP POST - NUMBER 20 BY JOHN SPIZZIRRI.....	6
MINUTES OF CAEUG MEETING JUNE 23 BY AL SKWARA.....	9

Computer Central

Next show date
SUNDAY, July 29
 College of Dupage
 9:30 A.M. to 3:00 P.M.
 Chicagoland's Oldest and Largest
 Multi-Vendor PC Show & Sale for
 Home and Business

COLLEGE OF DUPAGE
 Main Arena of Physical Education Building
 Corner of Park Blvd & College Road
 Glen Ellyn, IL
 FREE PARKING
 Admission - \$6.00
 (With this coupon admission \$5.00)
www.computercentralshows.com
 E-mail address:
compcent@megsinet.net

COMPUTERCENTRAL
 2001 dates
 July 29, August 26
 September 30
 COD



Announcement on May 9, 2001
 Larry Bothe and Pat Brod
 were married. Congratulations and
 Best Wishes to you both.

In order to have your article or item for sale
 appear in ARI they must be received by the
 10th of the month prior to publication.

MEMBERS HELPLINE

Any member with a specific expertise
 can volunteer to be on the Members
 Helpline. Contact Carl Schow.

Beginners Helpline.....Billy Douglas

Beginner hardware
 problems.....Dick Fergus

QuickBooks, Turbo Tax, IBM Lotus, MS
 Excel, Corel's Quattro Pro....Terry Moye

Win 9x, NT, 2K.....Rick Scalzo
 e-mail.....mitsufan@webcentrix.net

Hardware problems
 & WIN NT4, Linux.....John Spizzirri

For Sale: Royal daVinci PDA with 2 MB
 memory, pc docking cradle (serial), backlit
 display, feature icons for: phonebook, notes,
 time, writing pad, todo list, planner, calculator,
 and memo pad. Takes 2 AAA
 batteries. Features extra stylus, vinyl case and
 pc software PIM. Asking \$75.00
 Contact: Kat hy Groce at kgroce@iwon.com

Start UP Discussion Group

Ask questions and discuss computer
 experiences with the Start UP group.
 Such as:

1. New to Computers? (basic topics)
2. How to use the Web or download
 information
3. How to install hardware/software
4. Discuss how to troubleshoot
 hardware conflicts, learn boot up
 emergency tricks
5. What do you want to know??

Meets before regular meeting from
 9:15 to 9:45

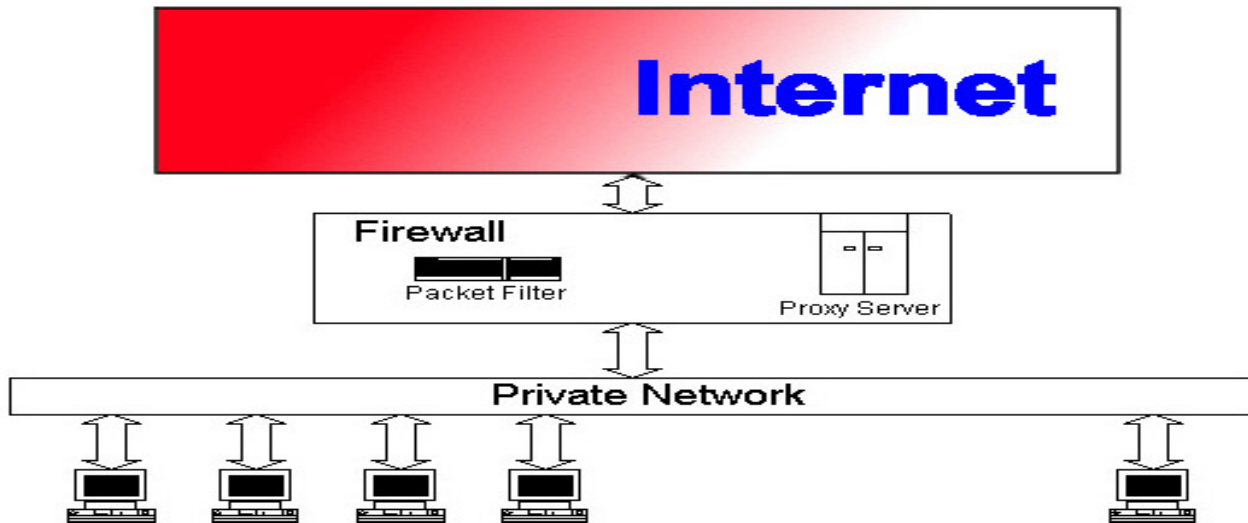


Fig 1. Diagram of a firewall arrangement with optional packet filter and bastion host

vulnerabilities. Unfortunately your firewall would probably not block a VBA attack, but it might log the origin of the attack.

Finally, you might wish to run a server, like FrontPage's personal web server, on your private network for testing web pages before uploading them to the Internet. You surely would not want this server to be accessible to the Internet. A firewall could block access to this server, as well as help you keep an eye on traffic you do allow.

The firewall is your first line of defense against the many threats from the Internet. Properly configured, it would at the very least alert you to strange traffic, at best block it outright.

How does a firewall work?

Firewalls range in complexity from roller skates to space shuttles. I am describing simple ones, equivalent to the automobile. Most firewalls are placed at the edge of the network to be protected. There they intercept all traffic attempting to enter the network or exit from it. They process the traffic according to a set of predefined rules (default rules and user-defined), forwarding some traffic, blocking other traffic and redirecting some.

These rules are the key to how firewalls work. They are based on the way data moves across the Internet. All data is divided into manageable chunks called "packets", the smallest data units transported on the Internet. Even solitary commands are sent as packets. Each such packet is enclosed in an "envelope" marked with the destination address and port (see below), the origin and port, as well as the data type (by Internet protocol: HTTP, FTP, etc.), and the packet type UDP (no

error checking) or TCP (error checking). The ports used in addressing range from 1 to 65535 and serve to associate packets with a specific application (server or client) assigned to the port. If the application is a server it is said to be "listening" on this port. Each of those bits of information serves as a filter item for firewall rules. If one of the monitored attributes triggers a rule the firewall acts according to the rule's associated action. This could be to block the packet with an error message sent to the originator, discard the packet without any message, forward the packet to its destination, redirect it to a different destination, and in all cases optionally log the attempted access. If a packet does not trigger any rule, the default action of the firewall will take over. This might be to allow all traffic through if no rule is matched (bad idea), or to block all traffic by default. Pure firewalls never look at the content of the packet, leaving this to virus scanners. So do not expect your firewall to stop virus attacks contained within the data of the packet. However, content filtering is possible as part of a firewall, and is offered as part of some commercial products.

A simple firewall may just check the port and either block the packet or allow it through. More complicated firewalls may check more than just the port. They may check the protocol to determine if the data and the port are a logical match. They may compare the origin address or destination address against a list of restricted addresses. They may have different rules depending on the direction of the data (inbound or

con't on page 5

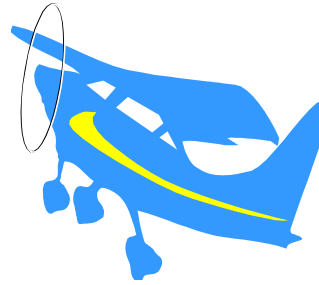
outbound). Various products are routinely combined with firewalls. One product may be called "proxy server", another identical product may be called "gateway". Other names frequently used interchangeably with firewalls may be "router", "filter", "screen", "NAT", or any combination of these terms. There is a lot of overlap in these functions, so different names may mean the same thing. For example, a "screening router" is the same thing as a "packet filter". If you find the descriptions of products confusing, look for descriptions of features rather than just the buzzword for features. Then compare the functions.

The best initial configuration of a firewall is to block everything, and then enable ports or applications as the need arises. Once you enable an outgoing request you usually also enable the incoming replies to your request. This lets you surf the Internet without opening connections to any interior servers.

What firewall do you recommend?

Everyone's needs are different. But if you're on the Internet, you need a firewall! Read the reviews in this issue, and come to the July Internet SIG, where we will discuss different needs. Bring your questions. All HAL-PC members and their guests are welcome. If you need a solution immediately, and you have a single computer to protect, ZoneAlarm is a good choice for the inexperienced. It installs easily, is easy to use, and does a fair job protecting your computer, and it's free – for personal use! It is not a good choice for protecting a whole network. If you have an always-on connection, and more than one computer (a LAN or "local area network"), you will need to protect the entire network. Look into the hardware you already have in place, connecting your ISP (internet service provider) to your network. Perhaps it already has firewall functions. On the other hand, if all your computers were for different individuals in your family, I would guess that ZoneLabs would let you install ZoneAlarm on each machine, and still call it "for personal use". Personally I prefer Tiny Firewall for its greater control over the rule set. But the price you pay for this extra power is for a more complex interface, and more decisions to make.

Eb Guenther is a long time HAL-PC member and Internet consultant to small businesses. Contact Eb at ebg@guenther.com.



Congratulation!
Larry

The National Association of Flight Instructors (NAFI) takes pride in announcing a significant aviation

accomplishment on the part of

Larry S Bothe

an Aviation Safety Counselor for the Indianapolis FSDO and a resident of Seymour, IN. Recently, Larry was designated a Master CFI (Certificated Flight Instructor) by NAFI, his professional aviation organization.

To help put this achievement in its proper perspective, there are approximately 78,000 CFIs in the United States. Fewer than three hundred of them have achieved that distinction thus far. The last six FAA National Flight Instructors of the Year were Master CFIs while Larry is one of only five Indiana CFIs to have earned this prestigious "Master" title.

The Master Instructor designation is a national accreditation that is earned by a candidate through a rigorous process of continuing education. Simply put, the Master Instructor designation is a means by which to identify those outstanding aviation educators, those "Teachers of Flight," who have demonstrated an ongoing commitment to excellence, professional growth, and service to the aviation community.

Through their dedication to excellence, Master Instructors have earned their "black belts" in aviation education. They truly represent the cr me de la cr me of our industry!

NAFI was founded in 1967 and is dedicated to raising and maintaining the professional standing of flight instructors throughout the nation, as well as providing a safe and effective learning environment for student pilots. In addition, NAFI initiates education and support programs throughout the aviation industry.

Sincerely,
G Alexander "Sandy" Hill, MCFI
Director of Education
National Association of Flight Instructors



The Lamp Post

Number 20 by John Spizzirri
June 17, 2001



I recently took a weekend trip to Sault Ste Marie, Michigan (<http://www.saultstemarie.com>). With the gasoline prices now at reasonable levels the ten-hour drive from Chicago is not too bad on the pocket book. It has all the tourist trappings – souvenir shops, miniature golf, and other things for kids. The main attractions are the Soo Locks. Because of the reduced shipping traffic the Sabin and Davis locks were not in operation. Traffic has been reduced due to the increased size of the ‘boats’ or ‘lakers’. Fewer trips can yield the same payload. The new larger super ‘lakers’, about 1,000 feet long and 80 feet wide, can only fit in the Poe lock. The MacArthur lock is used for ocean going vessels or ‘salties’, tour boats, and private craft. The Army Corp of Engineers operate the locks ten months a year 24/7. Unfortunately, you and I have to foot the bill (via income tax) for the 162-person operation because there is no fee of any kind charged to boats going through the locks. Incidentally, Canada operates one lock and charges a toll for its use. If you are interested in seeing the locks but don't want to drive that far you can see them on your computer at

<http://www.crrel.usace.army.mil/ierd/webcams/soo/> . There are four views with the pictures being updated about every two minutes. While I was there I was fortunate to have seen the Edwin H. Gott, a super laker owned by U.S. Steel. A picture of this behemoth is at <http://www.vaxxine.com/jcameron/shiparc/uss/edwinhgott/gott.htm> . From the pictures it is sometimes difficult to understand the immensity of these ships. They are over three football fields long and five to eight stories tall. To look at pictures and statistics about the lakers and salties go to

<http://www.vaxxine.com/jcameron/shiparc/default.htm> or <http://www.boatnerd.com> . Among the various attractions is the Valley Camp, a laker constructed in 1917 which is used as a museum. It has various historical artifacts from the Great Lakes shipping industry as well as a history of the Soo Locks. It has two lifeboats recovered from the Edmund Fitzgerald, a 729-foot laker that sank in a Lake Superior gale on November 10, 1975. The condition of those lifeboats speaks volumes about the ferociousness of lake storms. If you decide to check out the Valley Camp museum, be prepared to walk. The ship is 550 feet long with 3 viewing decks that run almost the full length of the ship. You can get a glimpse of it at

<http://www.soohistoricinc.sault.com/> . One of the tours I did not take this time is the Agawa Canyon Tour Train, which is part of the Algoma Central Railway line. It is a Canadian wilderness tour by rail of the east coast of Lake Superior in Ontario, Canada. The tour lasts one full day and is best traveled in the fall color season. You can get a taste of that tour at

<http://www.agawacanyontourtrain.com/> . No excursion to the Soo is complete without a ride on the Soo Locks tour boats (<http://www.soolocks.com/>). The boats are operated on both the US and Canadian sides of the border. The tours are guided by summer students reading a script of how the locks work as you go through them, as well as various points of interest in the Sault Ste Marie / St. Mary's river area. One of the best parts of any trip to the Upper Peninsula

of Michigan is the food. Pastys, which are hard to find elsewhere, are one of my favorites. A pasty (pronounced pass tee) is much like a meat pie but instead of being cooked in a pie tin the pastry crust is wrapped around the meat, potatoes, carrots, and onion to form what looks like a pillow. You can get pastys shipped to you on the net at <http://www.pasty.com/> . There is also an explanation of how they are made. For dessert there is fudge. Going to the fudge shops and seeing how the fudge is made in copper kettles using wooden paddles with the forming and cooling done on marble slabs is a real treat. You can see some of the fudge cooking (and order some while you're at it) at <http://www.frankenmuthfudge.com/> . The evening entertainment can be handled by Da Yoopers (<http://www.dayoopers.com/>). The people of the Upper Peninsula (UP) of Michigan are called yoopers (Upers, get it). You Guys, Inc. got together and formed a musical comedy group called Da Yoopers. Original comedic songs and outlandish costumes and antics grace every performance. They also sell albums of their 'hit' songs. The bottom line is that a weekend at the Soo costs about \$200-\$350 per person. Not bad for a mini-vacation.

Agere, a communications chipmaker, is dumping the USB 2.0 chip and intends to produce the 1394b chip product. Microsoft's (MS) decision of 2 months ago is starting to have a market effect. The Agere management stated that they wanted the USB 2.0 to disappear. They will continue to support USB 1.

This past month has Redmond all abuzz. Microsoft (MS) heard from the court and seems to be hearing from customers. MS (<http://www.microsoft.com>) may have a problem with the introduction of Windows XP. The U.S. Court of Appeals found the MS was guilty of bundling its software to the exclusion of others. This is called tying or comingling. In WinXP, IE is integrated. MS has made a slight effort this past week to open the door to other software, but what about Windows Media Player, CD burning, remote control, zip file support, online shopping, messenger, and MSN? They are all integrated, too. The DoJ (<http://www.usdoj.gov>) or the various stated involved in the case, could get an injunction to stop the introduction of XP until the case is settled. MS is depending on XP to be a success to continue the company's high growth rate. Last month I reported that MS will spend hundreds of millions of dollars promoting XP. It is imperative to MS (and PC makers) that XP be out before Christmas to spur sales. The US and European markets have been drying up because businesses are not upgrading equipment and software. MS has petitioned the court to reconsider its decision about tying. The main problem they have is that time is running out. The XP release date is October 25th. The courts do not do things very quickly. The next three months are going to be interesting

MS announced partnerships with Cyberlink, InterVideo and Ravisent Technologies, which will mean there will be an 'official' add-on MP3 product. More importantly, it means that MS will NOT directly support MP3 technology. Further, these other three companies do not work for free, thus to have MP3's play on an Xpmachine will cost extra money. Will consumers think that XP is worth the extra expense when their current operating system plays MP3's?

MS has decided to change its licensing policy to its largest 'named' customers. These are customers that buy their licenses directly from MS. In a rumor that surfaced about a week ago MS is supposed to RAISE prices to OEM and computer makers. This seeming contradiction is

in response to the Appeals Court decision that said that MS pricing policies were too 'restrictive' and violated the Sherman Antitrust Act.

MS settled with the state of New Mexico (NM). NM is the first and lonely state to come to an agreement with MS. The agreement states that NM will not pursue MS for break up and that NM will get a cut of any booty that is extracted from MS by the DoJ and the other states.

MS's Great Plains unit, an ERP (enterprise resource planning) software maker, merged with Clarus, an e-procurement company. This is MS's answer to SAP (and other competitors) for small and mid-sized businesses.

MS has placed in its license agreement for wireless Internet tools (for cell phones) language that forbids use of Free Software Foundation's General Public License (GPL) and six other forms of 'viral software' citing Linux and Perl scripting language specifically. Albert Foer, president of the American antitrust Institute in Washington D.C., said, "Microsoft has identified Linux as its potential competitor and is attempting to limit its use." MS is the same company that owns Hotmail and admitted recently that a number of the Hotmail servers run FreeBSD, an open source Unix. (FreeBSD does not use the GPL.)

MS has softened its product activation on WinXP. Now they are telling us that if you change some of your hardware 4 times during an unspecified time period you will be compelled to get a new product activation key from MS. It used to be one time. MS would like us to think that this will be a simple phone call to MS and not an "inquisition under hot lights." Thanks, MS, thanks.

Rich McDilda, who runs the Computer Exchange and Lasercraft, wrote in the Chicago Computer Guide that "MS should not be broken in three parts. It should be broken into fifteen and forced to compete instead of being allowed to bully smaller companies out of the market." I'm not big on forcing anyone to do anything, but I do not like the attack on Linux and the GPL.

The question that must be asked. . Will MS settle or hang tough? How much do they have to lose? Will the DoJ cave in under Ashcroft? Sort of sounds like a soap opera, doesn't it?

I demonstrated KDE at the June CAEUG meeting. I did not show the KIllustrator (KDE Drawing Tool), which is free software included with KDE. It was written by Dr. Kai-Uwe Sattler of the University of Magenburg in Germany. Adobe (<http://www.adobe.com>), the people who bring you this newsletter via PageMaker and Acrobat Reader, threatened Dr. Sattler through their mouthpiece, Reinhard Skuhra Weise, a law firm. Adobe demanded that KIllustrator infringed on Adobe Illustrator. Adobe does not and has no plans to have a Linux version of Illustrator or any other of its programs except Acrobat Reader. Further, Adobe demanded that the name be changed, the product withdrawn from the market, a list of everyone who acquired the product be provided and an accounting of how much money Dr. Sattler made from the product. ITS FREE SOFTWARE!!! HELLLLOOOOOO!! Its good to see that MS is not the only IDIOT software company on earth.

Between you, me and The Lamp Post that's all this month.

Minutes of CAEUG Meeting June 23, 2001

Rick Scalzo called the meeting to order at 9:44 am.

There were 33 in attendance.

The next meeting is scheduled for July 28, 2001.

Raffle items included: Microsoft Casino and Eudora Pro for Windows.

Volunteers for the COD show were discussed. Anyone willing to represent the club at the show can get a free admission. The show lets two members in free and the club will reimburse two other members who work at our table. The reimbursement does not happen until the next monthly meeting.

The minutes were approved as published in the Newsletter.

The Financial Report showed a starting balance of \$4,823.86, income of \$244.79 and expenses of \$86.91 for an ending balance of \$4,981.74.

OLD BUSINESS

Rick has located a refurbished projector for the club, in the price range of \$1,800 to \$1,900.

There was a request for ideas on what software that should be included on the CD. Ideas should be emailed to Rick.

New Business

There was discussion of new products and new technologies.

There was discussion on the club web site. The members were asked about adding a directory of members that would be available with password access. There was support for the directory.

This month's disk of the month is the Linux Operating System and Linux Software.

Mike Goldberg and Roger Kinzie volunteered to serve as co-chairpersons. The club picnic has been scheduled for Seven Gables Park from 11am to 3pm on August 25, 2001. There was some discussion about door prizes for the picnic

The presentation was made by John Spizzirri on the Linux Operating System features.

Respectfully submitted,

Al Skwara

Martha's way #1: Stuff a miniature marshmallow in the bottom of a sugar cone to prevent ice cream drips.

My way: Just suck the ice cream out of the bottom of the cone, for Pete's sake, you are probably lying on the couch with your feet up eating it anyway.

Martha's way #2: Use a meat baster to "squeeze" your pancake batter onto the hot griddle and you'll get perfectly shaped pancakes every time.

My way: Buy the precooked kind you nuke in the microwave for 30 seconds. The hard part is getting them out of the plastic bag.

Martha's way #3: To keep potatoes from budding, place an apple in the bag with the potatoes.

My way: Buy Hungry Jack mashed potato mix and keep it in the pantry for up to a year.

Martha's way #4: To prevent egg shells from cracking, add a pinch of salt to the water before hard boiling.

My way: Who cares if they crack, aren't you going to take the shells off anyway?

Martha's way #5: To get the most juice out of fresh lemons, bring them to room temperature and roll them under your palm against the kitchen counter before squeezing.

My way: Sleep with the lemons in between the mattress and box springs.

FIRST CLASS MAIL

CAEUG
P. O. Box 2727
Glen Ellyn, IL 60138

Meeting place and date information:

The next REGULAR meeting will be held at the Glen Ellyn Library in Glen Ellyn at 9:45 am on
Saturday, July 28, 2001

The library is located 1 block west of Citibank at the corner of Prospect & Duane FREE PARKING
Directions: Park to Duane; go west on Duane to Prospect Street. Please park at the West end of the
lot, away from the building. Thank you.

The meeting(s) are not library sponsored and all inquiries should be directed to Rick Scalzo . Individuals
with disabilities who plan to attend this program and who require certain accommodations in order to
observe and/or participate in the program are requested to contact CAEUG president,
Rick Scalzo at , at least five (5) days prior to the program, so that reasonable accommodation can be
made for them.

Confirmed Meeting dates for 2001: July 28, August 25 CAEUG annual picnic Saturday,
September 22, October 27, November (no meeting),
December 1 (Nov/Dec meeting),

Confirmed Meeting dates for 2002: January 26, February 23, March 23, April 27, May 25

Program for July 28: More Red Hat 7.0 and, if time permits, additional software will be
presented by John Spizzirri. If you would like Red Hat 7.0 installed on your pc, you will need
to bring the cpu, monitor and contact John at spizman@iwon.com so he can be prepared.
The suggested configuration is at least a 1 gig hard drive and 32 Meg of memory.

CD OF THE MONTH: Available at the meeting or by ordering previous
CD's via the CAEUG website.