LINUX JOURNAL SECURITY GnuPG Hacks | Guarddog | Mono Primer | AJAX Galore | Firewall Scripting | Eclipse Plugins MARCH 2006 ISSUE 143

GnuPG Hacks | Guarddog | Mono Primer | AJAX Galore | Firewall Scripting | Eclipse Plugins

LINUX JOURNAL™

Since 1994: The Original Magazine of the Linux Community
MARCH 2006 | www.linuxjournal.com

LISTEN TO THE SOUNDS OF LINUX VIA SONOS

BARK UP THE RIGHT TREE FOR FIREWALL MANAGEMENT

GET YOUR LINUX ON A STICK

TAPPING INTO AMAZON WEB SERVICE

AJAX E-MAIL SOLUTIONS

Put mod_security to work on your Apache server

Secure that ssh server, soldier!

ARE YOU SECURE?

LOCK DOWN EVERYTHING FROM FILES TO YOUR SECURITY SYSTEM ITSELF

LIDS takes file security to the kernel

Perl script your way to firewall security

AN SSC PUBLICATION
USA $5.00
CAN $6.50
03
0 71486 03102 4

LOST
in a sea of server problems?
Get Rescued Today with the AlterPath™ OnBoard!
Download a FREE White Paper on Service Processor Management at
www.cyclades.com/spm

AlterPath OnBoard
HP
iLO
Dell
DRAC
IPMI
Sun
ALOM
IBM
RSA

The competition doesn't stand a chance.

If you base deployment decisions on performance and price, Coyote Point's for you. We've cornered that market.

To prove it we asked The Tolly Group to evaluate our E350si application traffic manager against the competition. The results speak for themselves.

Throughput? Almost 40% more than others in our space. Cost of transactions per second? Up to four times less. Connection rate? In some cases, one-sixth the cost. One-sixth! And we're told Coyote Point is the #1 choice for today's open source networks.

But don't just take our word for it. Get the facts. Call 1.877.367.2696 or write info@coyotepoint.com for your free copy of the full Tolly Report.

COYOTE POINT SYSTEMS INC.

www.coyotepoint.com

CONTENTS

MARCH 2006
Issue 143

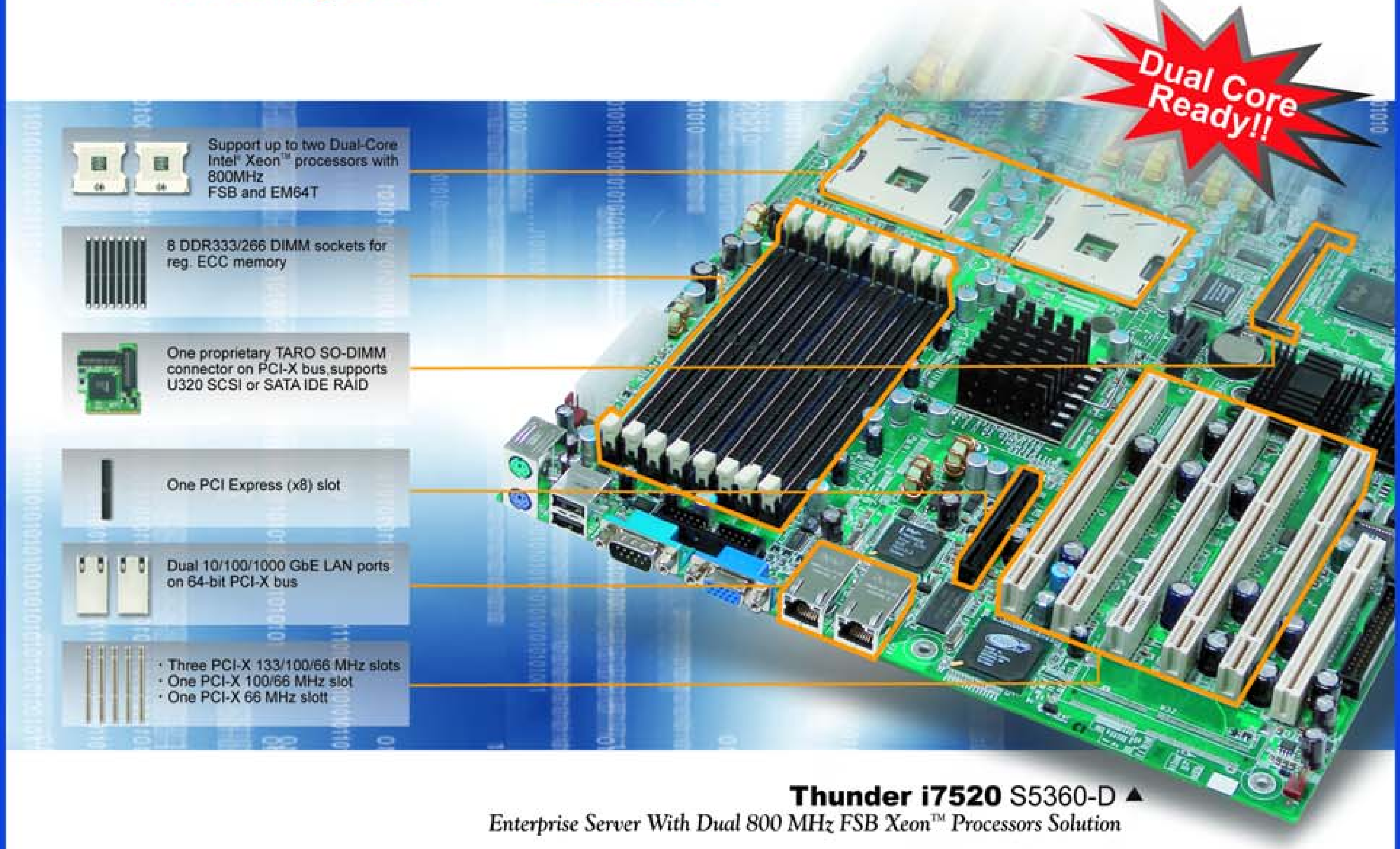
FEATURES

ON THE COVER

TYAN

Fast, Flexible, and Feature-Rich!

PCI Express and EM64T Servers Have Arrived



Support up to two Dual-Core Intel® Xeon™ processors with 800MHz FSB and EM64T

8 DDR333/266 DIMM sockets for reg. ECC memory

One proprietary TARO SO-DIMM connector on PCI-X bus,supports U320 SCSI or SATA IDE RAID

One PCI Express (x8) slot

Dual 10/100/1000 GbE LAN ports on 64-bit PCI-X bus

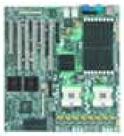
- Three PCI-X 133/100/66 MHz slots
- One PCI-X 100/66 MHz slot
- One PCI-X 66 MHz slott

Thunder i7520 S5360-D ▲

Enterprise Server With Dual 800 MHz FSB Xeon™ Processors Solution

intel inside XEON

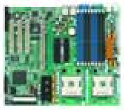
Thunder i7520



S5360-D

- Supports two Dual-Core Intel® Xeon™ processors with 800 MHz FSB and EM64T
- 8 DIMMs for DDR266/333 memory
- Three PCI-X 133/100/66 MHz slots, one PCI-X 100/66 MHz slot, one PCI-X 66 MHz slot and one 33 MHz PCI slot
- One PCI Express™ x8 slot
- One proprietary SO-DIMM connector on PCI-X bus, supports U320 SCSI or SATA
- Dual GbE LAN

Tiger i7320



S5350-D

- Supports two Dual-Core Intel® Xeon™ processors with 800 MHz FSB and EM64T
- 8 DIMMs for DDR266/333 memory
- Two PCI-X 64/66 MHz slots; three 32/33 PCI 2.3 slots
- One proprietary SO-DIMM connector on PCI-X bus, supports U320 SCSI or SATA
- Dual PCI Express GbE LAN

TYAN COMPUTER CORP.

Tyan Computer USA
3288 Laurelview Court
Fremont, CA 94538 USA
Tel: +1-510-651-8868 Fax: +1-510-651-7688
Pre-Sales Tel: +1-510-651-8868 x5120
Email: marketing@tyan.com

For more information about this and other Tyan products, please contact Tyan Pre-Sales at (510) 651-8868 x5120, or contact your local Tyan system integrator/reseller.

www.tyan.com

CONTENTS MARCH 2006 Issue 143

COLUMNS

REVIEWS

IN EVERY ISSUE

INDEPTH

Next Month

WIKIS, BLOGS AND PODCASTING

Are Wikis the wave of the future or headed for the Internet graveyard? We opine, we explain, you decide. In the meantime, how about using Wikis and blogs to ease system administration? It's possible, and we explain how.

Xoops is a powerful object-oriented PHP-based blog/Web content management system. If you want to learn how to set it up, we've got the scoop. If Xoops isn't your scene, we also explain how to install and customize Mediawiki.

And there's more. We have the details of how Jon Watson and Kelly Penguin Girl have done weekly GNU/Linux user podcasts. Learn how to extend Web services, perform remote temperature monitoring with Linux, and create a blog aggregator.

Read about Doc's experience with the Linux-based Sonos Digital Music System. p.36

routerOS: routerBOARD.com

User Management

- support more than 3000 PPPoE or HotSpot clients
  - full RADIUS support for user parameters
    - tx/rx speed, address, filter rules
    - supports RADIUS real time modification of parameters while users are online
- Peer to Peer protocol control (P2P)
  - per client P2P tx/rx rules with burst support
  - P2P pool
  - complete blocking of P2P

Wireless AP and Backbone

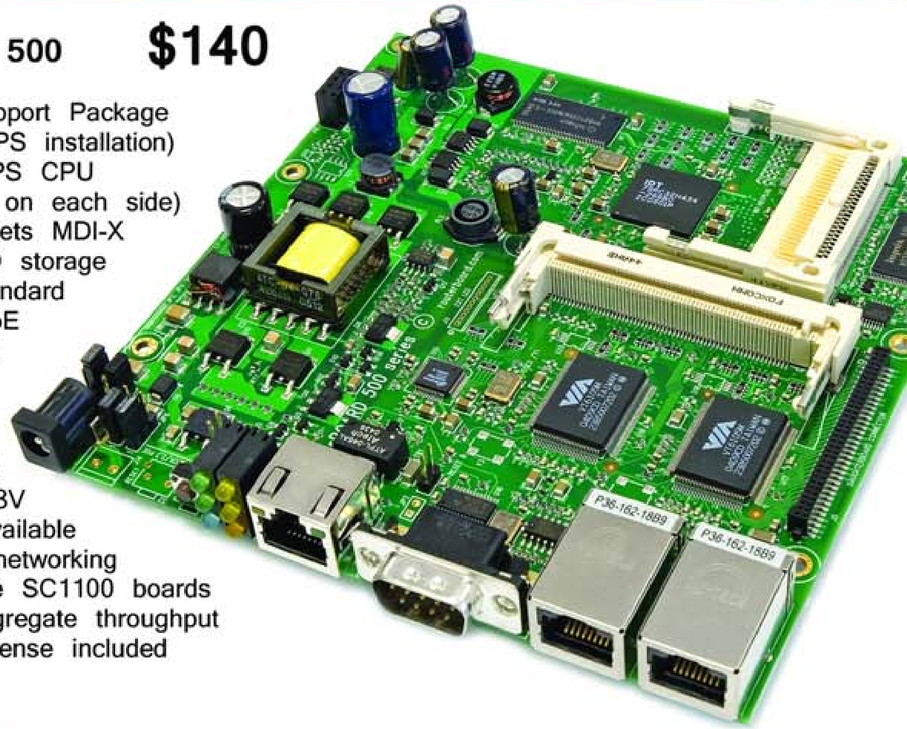
- Wireless monitoring
  - Frequency scanning with detailed report
  - Raw wireless packet sniffer
    - streaming option to Ethereal analyzer
    - option to save to a file format supported by Ethereal
  - Snooper packet inspection
    - analyzes all raw frames received for wireless parameters
    - monitors a single channel or all channels
- Nstreme wireless polling protocol
  - no decrease in speed over long distances (as seen with the 802.11 ACK packet bottleneck)
  - polling improves speed and eliminates contention for access to the wireless bandwidth
  - access point control over Nstreme clients tx data to optimize use of the wireless medium
  - RADIUS support for the access control list including bandwidth settings for wireless clients
- Full 802.11a/b/g support

The above is a brief description of a few features, for more information and a fully featured 24 hour demo go to:

www.mikrotik.com

RouterBOARD 500 $140

- Linux Board Support Package (full Debian MIPS installation)
- 266-400MHz MIPS CPU
- 2 miniPCI (one on each side)
- 3 10/100 Ethernets MDI-X
- 64/128MB NAND storage
- PoE 802.3af standard and passive PoE (also 12V PoE)
- Compact Flash
- Low power
- 32MB DDR (64MB optional)
- 6-24V and 25-48V power mode available
- 2-3x faster for networking than the Geode SC1100 boards
- 200-300Mb/s aggregate throughput
- L3 RouterOS license included



$95

- MDI-X
- 4 separate 10/100 ports

RouterBOARD 44

For the Router Builder !

- rackmount servers and routers
- up to 24 Ethernet ports in a PC
- no more straight/cross cable problems
- server quality VIA VT6105 chips

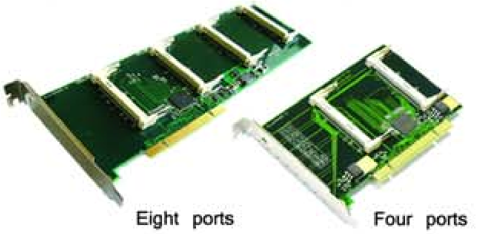
$195

RouterBOARD 230

No feature left behind !

Integrated router with various interfaces. Use as an AP on a tower with up to 500ft PoE. Includes IDE/CF, miniPCI, USB, PCMCIA, UART, PCI, GPIO, LCD controller, Linux SDK, and more.

$120 $65



Eight ports Four ports

RouterBOARD 11/14/18

Multi radio tower !

MiniPCI to PCI adapters for multi radio system. Tested with sixteen radios in one Router/AP.

$240

- PoE
- 10-56V input
- 9x 10/100
- 6x mPCI

RouterBOARD 500 & RouterBOARD 564

The Wireless Switchboard !

For a complete multi-radio tower system, the RouterBOARD 500 can carry a daughterboard (RouterBOARD 564) which adds six ethernets and four miniPCI.

contact sales@routerboard.com or go to www.routerboard.com

LINUX JOURNAL

Editor in Chief
Nick Petreley, ljeditor@ssc.com

Executive Editor	Jill Franklin jill@ssc.com
Senior Editor	Doc Searls doc@ssc.com
Web Editor	Heather Mead heather@ssc.com
Art Director	Garrick Antikajian garrick@ssc.com
Editor Emeritus	Don Marti dmarti@ssc.com
Technical Editor	Michael Baxter mab@cruzio.com
Senior Columnist	Reuven Lerner reuven@lerner.co.il
Chef Français	Marcel Gagné mggagne@salmar.com
Security Editor	Mick Bauer mick@visi.com
Products Editor	James Turner newproducts@ssc.com

Contributing Editors
David A. Bandel • Greg Kroah-Hartman • Ibrahim Haddad • Robert Love • Zack Brown • Dave Phillips • Marco Fioretti • Ludovic Marcotte • Paul Barry • Paul McKenney

Proofreader	Geri Gale

VP of Sales and Marketing	Carlie Fairchild carlie@ssc.com
Director of Marketing	Rebecca Cassity rebecca@ssc.com
International Market Analyst	James Gray jgray@ssc.com
Sales Coordinator	Lana Newlander ads@ssc.com

Regional Advertising Sales
NORTHERN USA: Joseph Krack, +1 206-782-7733 x118, joseph@ssc.com
EASTERN USA: Martin Seto, +1 206-782-7733 x117, mseto@ssc.com
SOUTHERN USA: Laura Whiteman, +1 206-782-7733 x119, laura@ssc.com
INTERNATIONAL: Annie Tiemann, +1 206-782-7733 x111, annie@ssc.com

Advertising Inquiries ads@ssc.com

***Linux Journal* is published by SSC Media Corporation and is a registered trade name of SSC Publications, Inc.**
PO Box 55549, Seattle, WA 98155-0549 USA • linux@ssc.com

Publisher	Phil Hughes phil@ssc.com
Accountant	Candy Beauchamp acct@ssc.com

Editorial Advisory Board
Daniel Frye, Director, IBM Linux Technology Center
Jon “maddog” Hall, President, Linux International
Lawrence Lessig, Professor of Law, Stanford University
Ransom Love, Director of Strategic Relationships, Family and Church History Department,
Church of Jesus Christ of Latter-day Saints
Sam Ockman, CEO, Penguin Computing
Bruce Perens
Bdale Garbee, Linux CTO, HP
Danese Cooper, Open Source Diva, Intel Corporation

Subscriptions
E-MAIL: subs@ssc.com
URL: www.linuxjournal.com
PHONE: +1 206-297-7514
FAX: +1 206-297-7515
TOLL-FREE: 1-888-66-LINUX
MAIL: PO Box 55549, Seattle, WA 98155-0549 USA
Please allow 4–6 weeks for processing address changes and orders
PRINTED IN USA

USPS *LINUX JOURNAL* (ISSN 1075-3583) is published monthly by SSC Media Corporation, 2825 NW Market Street #208, Seattle, WA 98107. Periodicals postage paid at Seattle, Washington and at additional mailing offices. Cover price is $5 US. Subscription rate is $25/year in the United States, $32 in Canada and Mexico, $62 elsewhere. POSTMASTER: Please send address changes to *Linux Journal*, PO Box 55549, Seattle, WA 98155-0549. Subscriptions start with the next issue. Back issues, if available, may be ordered from the Linux Journal Store: store.linuxjournal.com.

LINUX is a registered trademark of Linus Torvalds.

MBX is the Industry Leader for Server Appliances

From design to delivery we are dedicated to building a partnership with you.

MBX RP-1013 Platform

- Intel® Celeron 336 Processor at 2.8 GHz
- 1U Rackmount Chassis 16.5” Deep
- 512MB PC4200 DDR2 Memory
- Maxtor 80GB Serial ATA Hard Drive
- Eight Gigabit NIC’s, 4 ports with by-pass
- Optional 16x2 LCD with Keypad
- On-board Compact Flash Socket
- Brandable With Your Color and Logo
- Custom OS and Software Install
- No Minimum Quantity Required
- 3 Year Warranty

$1,499 other configurations available
please call for pricing

MBX RP-1110 Platform

- Intel® Celeron 336 Processor at 2.8 GHz
- 1U Rackmount Chassis
- 512MB PC3200 DDR Memory
- Maxtor 80GB Serial ATA Hard Drive
- Dual On-board Gigabit NIC’s
- Custom OS and Software Install
- No Minimum Quantity Required
- 3 Year Warranty

$899 other configurations available
please call for pricing

MBX is the leader in custom appliances. Many premier application developers have chosen MBX as their manufacturing partner because of our experience, flexibility and accessibility. Visit our website or better yet, give us a call. Our phones are personally answered by experts ready to serve you.

MBX systems

www.mbx.com

1-800-681-0016

Intel, Intel Inside, Pentium and Xeon are trademarks and registered trademark of Intel Corporation or its subsidiaries in the United States and other countries. Lease calculated for 36 months, to approved business customers. Prices and specifications subject to change without notice. Setup fee may apply to certain branding options. Motherboard Express Company. 1101 Brown Street Wauconda, IL. 60084.

letters

SSC
HOME PBX GIVES EXTENSIONS AND VOICE MAIL TO THE WHOLE FAMILY
LINUX JOURNAL
Coming to DVD
Your home videos with Kino and DVDStyler
State of the art video production
At home with Linux
HOME PROJECTS
LINUX PHONE HOME
The Skype voice-over-IP phone service works great with a headset. But can you extend Skype to use the telephones in your house?
GET YOUR WINDOWS GAME ON WITH LINUX
PLUS
Broadcast Your Music From Network-Attached Storage To Your Stereo
A (Relatively) Cheap Terabyte Home Backup System

Tribute to Geoffrey Robertson

I wanted to contact you some time ago with a mention of a person I think you should honour as someone contributing to the Linux Community in Sydney, Australia. Forgive me if this has been mentioned already by others, and I know that I am sending this using another operating system, but I felt that it was significant to mention the efforts of one Geoffrey Robertson who runs the Introduction to Linux courses through the Technical College of Advanced Education (TAFE) further education courses at Granville, Sydney. A longtime member of the Sydney Linux User Group (SLUG, **www.slug.org.au**), he has taken on some courses in basic usage and advanced usage of Linux, devoting time to assisting people with getting started and some advanced techniques in using the Linux operating system. Actually, I would be surprised if his name hadn't already been mentioned as a person who has done much for advancing Linux in Australia. I know he has given much of his personal time both to attending the slug group, and teaching related courses, such as the LPI courses. I personally feel you should mention Geoffrey Robertson as amongst those who contribute especially to the advancement of Linux and open source.

Michael Kortvelyesy

Praise and Suggestions

Well, you've really done it this time. You put out a fantastic January 2006 issue. Articles on video production and DVD authoring—loved them. The new Work the Shell series by Dave Taylor—love it. The focus on hardware projects—love it and want more of it.

You could really top off the gEDA article with a follow-up tutorial on using the gEDA suite to lay out, simulate and produce an actual circuit complete with a home-etched PCB. Maybe a scrolling LCD display or motor driver. The following month could cover the Linux driver to interface to the project.

I'd also like to see how to snoop the PCI bus to figure out how that darn Windows-only driver talks to the PCI card. I'll admit, I have a vested interest with that one. Also, you've run lots of firewall configuration stories, but nobody has ever talked about firewall rules. I'd like to see a listing and discussion of rules for protecting oneself from the various known attacks—more than just blocking incoming connection and spoofing.

Other than that, keep up the great work. I've just renewed for my ninth year.

Doug Wright

Love *LJ* Subscription Service

In April of 2003, my mother asked me what I wanted for my birthday. I told her I would like a subscription to *Linux Journal*, so she got me one for two years. In April 2005, she asked me again, and I asked her to renew my subscription. She called the subscription line for *Linux Magazine* and asked them to renew my subscription (which didn't exist). They went along with her anyway, and now I have a two-year subscription to *LM*. The other magazine doesn't even hold a candle to *Linux Journal*. I finally decided to get another subscription after seeing the issue on MythTV in my local Fry's store. I thought I would hurry and sign up so I could get the issue. I used the subs@linuxjournal.com method, so I could guarantee the December 2005 issue. I spoke with Jon-Mark about this, and after some negotiating, he gave me a discount on my renewal *and* the December 2005 issue! I have never gotten that level of customer service from a company—EVER. His dedication to please the customer was admirable. I know he probably doesn't work directly for SSC, but you should rest easy in having SDS as your subscription partner.

I just hope my mom doesn't call *Linux Magazine* in April 2007!

Jason

On Memory

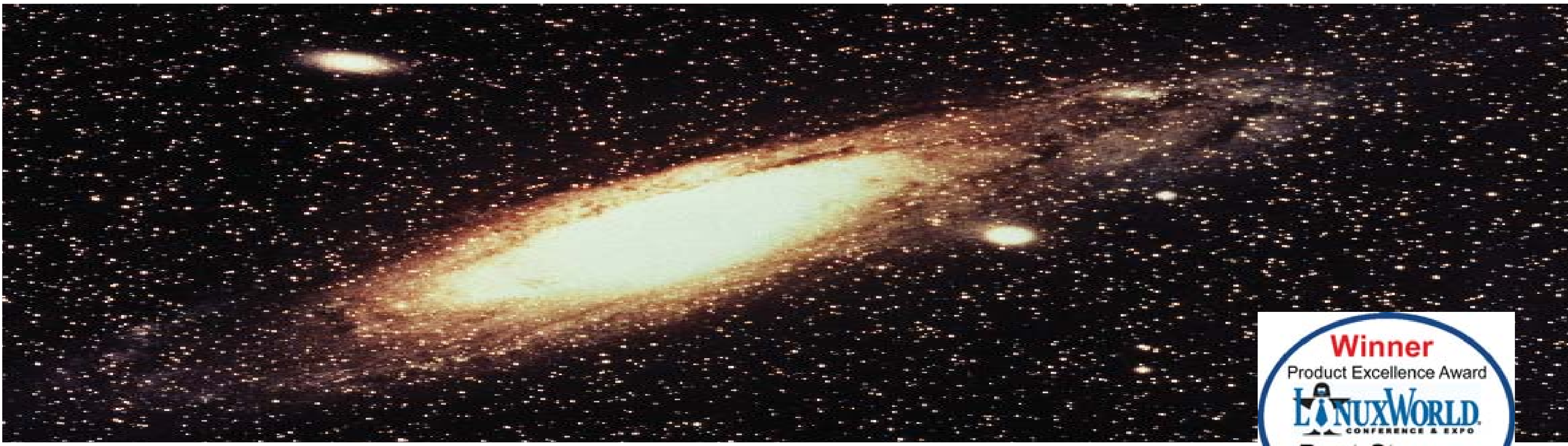
Great article ["Monitoring Virtual Memory with vmstat" by Brian K. Tanaka, *LJ*, December 2005]! I had a thought that pestered me when reading it, and I thought I'd drop you folks a note about it.

I was under the impression (from the good ol' days) that paging was the manipulation of the instruction space and swapping was the manipulation of the data space.

Now, it might be that I'm showing my age, but as I remember it (I'm saying this without a full dose of coffee yet), if memory space begins to get used beyond a particular value as judged by the kernel, the first thing it'll try to do is page out unused instruction space (that is, a loaded program that is not running) but keep the data space in core (see, I'm old) until it can't hold out any longer. Then, the next thing it'll try to do, if paging doesn't give it enough space, is to swap out data to the swap device to gain more working room. (Now on Linux specifically, which uses free memory for disk buffering/caching, the order and priorities of who gets tossed out first may very well change.)

If I really stretch my brain, I seem to remember that paging out in some cases was a lightweight process of basically marking a page as no longer part of a program's instruction space, and putting it back on the "available" queue. (I'm simplifying here.) But when the

MORE SPACE. LESS MONEY.



Winner
Product Excellence Award
LINUXWORLD
CONFERENCE & EXPO
Best Storage Solution

UNLIMITED AFFORDABLE NETWORK STORAGE

Everybody needs more space. And they need to spend less money. What if you can both have more space and spend less money?

What if you could put 7½ terabytes in only 3 rack units? What if that 7½ terabytes cost less than $10,000? Including the SATA disk drives. Imagine if you could glue it all together with a RAID appliance into one system. What if you could add as much storage as you wanted, one shelf at a time, and never have to `fork lift' anything?

Coraid's new SATA EtherDrive Storage allows you to do just that. Using industry standard SATA disk drives, EtherDrive Storage connects disks directly to your Ethernet network. Each disk appears as a local drive to any Linux, FreeBSD or Solaris system using our open ATA-over-Ethernet (AoE) protocol. Since the disks just appear as local drives you already know how to use them.

The EtherDrive® SATA Storage Shelf is a 3U rack mount network appliance that contains 15 SATA drive slots. Its triple redundant power supply protects you from your most likely failure. Its dual Gb Ethernet interfaces allow your data to go fast; 200MB per second. And at a very affordable price. List price for the EtherDrive Storage Shelf, without disks, is only $3,995.

Our companion product, the RAIDBlade RAID controller, allows a virtually unlimited number of Storage Shelves to be combined into a set of logical AoE storage devices.

Now you can have unlimited storage at a very affordable price. For complete information, visit our website at www.coraid.com, or call, toll-free, 1-877-548-7200. And we'll show how we've made network storage so affordable, you can have all the space you want.

www.coraid.com
info@coraid.com
1.706.548.7200

CORAID

system needs that page of instructions, it triggers a page fault to try to page in that piece of code from the disk, which is the really costly part of the process.

The granularity of how much to reclaim by paging or by swapping is a kernel parameter that seems to operate under the belief that if we're starting to swap, go for the gusto and swap lots of stuff now, as one big task to save having to do it again for a while.

There's also the question of who pays for this overhead work. Page outs are counted against the process trying to get more memory and page ins are counted against the code that needs the pages. This also applies to swapping. Again, this is based on what's left of some grey matter suffering from caffeine deficiency.

Now, unless my memory fails me...what was I saying...oh yeah, if I'm wrong, then the inevitable question is, where do paged-out pages go? To the swap space? If that's the case, then what's the difference between swap and page space?

Thanks for your time and keep on hacking!

Michael C. Tiernan

Video Editing

Thanks a lot for your article on Linux video editing ["Linux Video Production: the State of the Art" by Dan Sawyer, *LJ*, January 2006]—a very interesting read. I'm a bit surprised that you didn't address the legal complications surrounding mpeg-encoding at all—is this, in practice, no problem, especially considering that you presumably use these patented algorithms in a commercial setting? Not being a video geek, I don't know how good Theora is at present—I've heard high praise from some, but OTOH it's still very new, and not supported in any video (hardware) equipment I know of.

(My background: I am a Debian developer, and Debian's commitment to free software means that software using patented algorithms can, in most cases, not be included in the Debian distribution—that's why I probably pay a bit more attention to such legal matters than other Linux users.)

Adrian von Bidder

Correction

In the January 2006 issue, Dave Taylor's Work the Shell column "Exploring Pipes, Test and Flow Control" states, "Many modern shells have a version of the test command built in to the shell itself, considerably speeding up shell script execution. Using the [symbol ensures you'll use the built-in version if available, but explicitly calling test means that you'll likely not have that performance enhancement when running your scripts."

This seems intuitive, but it's incorrect. At least for the past decade, all modern shells (bash, ksh, zsh) treat [and test as equivalents. In other words, if [is a built-in, you'll find that test is as well.

Aron Griffis

A Newbie Request

Great work with the new column Work the Shell and the vmstat article in the December 2005 issue. I would like to see more articles for newbies like these. There are many topics to cover, such as system startup, UNIX programming, useful command-line tools and so on.

Nerox

Ubuntu Is Winning

Not long ago, Ubuntu was just another distro hoping to make an impact. Like hundreds of others before it, Ubuntu had hoped to catch the eye of random Linux users. Maybe one day it would even become a Top 50 distro with a few hundred followers.

But now? According to **distrowatch.com**, Ubuntu is the top distro on the planet! I must say I'm not surprised. This is how Linux was meant to be. As far as I'm concerned, Ubuntu *is* Linux.

Paul Panks

Music in Every Room

The article "Wireless Home Music Broadcasting" by John MacMichael [*LJ*, January 2006] caught my attention as it resembles a different take on a project of my own: music in every room. Both my project and John's utilize a large collection of ripped MP3 and OGG files on a NAS. However, in my case, the plan is to hang flat computer speakers from the wall in each room, and plug them in to my roving PDA (a Zaurus SL-5500). The PDA will access the NAS via an 802.11b compact Flash card. At least, that's the theory; in practice, Opie Media Player 2 terminates with signal code SIGSEGV when I try to play any audio file, either mounted locally or NFS. Perhaps I'll find another MP3 player that will work; I'm not giving up.

Frank Brown

LINUX JOURNAL

At Your Service

PRINT MAGAZINE

SUBSCRIPTIONS: Renewing your subscription, changing your address, paying your invoice, viewing your account details or other subscription inquiries can instantly be done on-line, **www.linuxjournal.com/subs**. Alternatively, within the U.S. and Canada, you may call us toll-free 1-888-66-LINUX (54689), or internationally +1-206-297-7514. E-mail us at subs@linuxjournal.com or reach us via postal mail, Linux Journal, PO Box 55549, Seattle, WA 98155-0549 USA. Please remember to include your complete name and address when contacting us.

LETTERS TO THE EDITOR: We welcome your letters and encourage you to submit them to ljeditor@ssc.com or mail them to SSC Editorial, PO Box 55549, Seattle, WA 98155-0549 USA. Letters may be edited for space and clarity.

WRITING FOR US: We always are looking for contributed articles, tutorials and real-world stories for the magazine. An author's guide, a list of topics and due dates can be found on-line, **www.linuxjournal.com/author**.

ADVERTISING: *Linux Journal* is a great resource for readers and advertisers alike. Request a media kit, view our current editorial calendar and advertising due dates, or learn more about other advertising and marketing opportunities by visiting us on-line, **www.linuxjournal.com/advertising**. Contact us directly for further information, ads@linuxjournal.com or +1 206-782-7733 ext. 2.

ON-LINE

WEB SITE: Read exclusive on-line-only content on *Linux Journal*'s Web site, **www.linuxjournal.com**. Also, select articles from the print magazine are available on-line. Subscribers to the print magazine receive full access to issue archives; please contact Customer Service for further information, subs@linuxjournal.com.

FREE e-NEWSLETTERS: Each week, *Linux Journal* editors will tell you what's hot in the world of Linux. Receive late-breaking news, technical tips and tricks, and links to in-depth stories featured on **www.linuxjournal.com**. Subscribe for free today, **www.linuxjournal.com/enewsletters**.

servers ▶ DIRECT™ GO STRAIGHT TO THE SOURCE!

Big business power, small business price tag

Robust ServersDirect Systems powered by the 64-bit Intel® Xeon™ Processor meet your needs today and grow with you into the future

2U Dual Core + SAS Servers

SDR-2115A 2U SAS Advanced Application Server

Provides ideal solution for running multiple applications or functions simultaneously while designed for high performance enterprise requirements.

- 2U rack designed with 6 x 1" Hot-swap SAS / SATA-II Drive Bays
- Dual Xeon™ Dual Core 800MHz processors supported
- Supermicro® board with Intel® E7520 Chipset
- Support up to 16GB DDRII 400 SDRAM memory
- Maximum drive capacity support up to 882GB (SAS) or 3TB SATA-2
- ATI Rage XL SVGA PCI video controller with 8 MB of video memory
- Adaptec AIC9410 8-Port Serial Attached SCSI (SAS) Controller
- RAID 0, and 1 support
- Dual Intel® 82541PI Single-Port Gigabit Ethernet Controllers

1U Appliance Server

SDR-1110T

WORLD'S ONLY Sub-Thousand!
Dual Core Server in 1U Solution

- Intel® Pentium® DUAL CORE 2.8 2X1M 800MHZ Processor
- 1U Chassis with 300W power supply
- Supermicro® server board with Intel® E7230 (Mukilteo) Chipset
- Kingston 512MB 667MHz DDR2 ECC RAM (2x256MB)
- 1pc x Seagate 80GB SATA 7200RPM hard drive
- 2 x 1" Hot-swap SATA drive bays
- Integrated ATI Rage XL SVGA PCI video controller
- 2x Intel® 82573V (Tekoa) PCI-e Gigabit LAN Ports
- Built-in SATA ICH7R Controller 4x SATA (3 Gbps) Drive with RAID 0, 1, 5, 10 Support

$999

3U Xeon™ Storage Server

SDR-3309T

Highly manageable storage server supporting up to 8TB of SATA hot-swap Storage

- Intel® Xeon™ Processor 2.8Ghz with 800FSB 1MB Cache (Dual Processor Option)
- Intel® Extended Memory 64 Technology
- 3U Chassis with 650W Redundant Power Supply
- Intel® server board with Intel® E7520 (Lindenhurst) Chipset
- Kingston 1024MB DDR333 ECC Reg. (2x512MB)
- 1pc x Western Digital 250GB SATA RAID Drive
- 16 x 1" Hot-swap SATA drive bays
- Integrated ATI Rage XL SVGA PCI video controller
- Dual Intel® Gigabit Ethernet Controllers
- 2 SATA Channels with RAID 0 and 1

$2,699

4U Enterprise Server

SDR-3309T

Easily scalable storage solution with Hot-swap functionality for growing business

- Intel® Xeon™ Processor 3.0Ghz with 800FSB 2MB Cache (Dual Processor Option)
- Intel® Extended Memory 64 Technology
- 4U Chassis with 16 hot-swap bays & 650W redundant power supply
- Intel® server board with Intel® E7520 (Lindenhurst) Chipset
- Kingston 1024MB DDR333 ECC Reg. (2x512MB)
- 1pc x Western Digital 250GB SATA RAID Drive
- 16 x 1" Hot-swap SATA drive bays
- Integrated ATI Rage XL SVGA PCI video controller
- Dual Intel® Gigabit Ethernet Controllers
- 2 SATA Channels with RAID 0 and 1

$3,499

5U Advanced Storage Server

SDR-5302T

The absolute best storage capacity available in a 5U format, at a incomparable cost/TB ratio

- Intel® Xeon™ Processor 3.0Ghz with 800FSB 2MB Cache (Dual Processor Option)
- Intel® Extended Memory 64 Technology
- 5U Chassis with 24 hot-swap bays & 950W redundant power supply
- Supermicro® server board with Intel® E7520 (Lindenhurst) Chipset
- Kingston 1024MB DDR2 400 ECC Reg. (2x512MB)
- 12pcs x Western Digital 250GB SATA RAID Drive
- 1pc x 3Ware 9550SX-12 port RAID Controller Card
- Integrated ATI Rage XL SVGA PCI video controller
- Dual Intel® 82541PI Single-Port Gigabit Ethernet Controllers

$5,999

SERVERS DIRECT CAN HELP YOU CONFIGURE YOUR NEXT HIGH PERFORMANCE SERVER SYSTEM - CONTACT US TODAY!

Our flexible on-line products configurator allows you to source a custom solution, or call and our product experts are standing by to help you assemble systems that require a little extra. Servers Direct - your direct source for scalable, cost effective server solutions.

1.877.727.7887 | WWW.SERVERSDIRECT.COM

intel® Xeon® inside™

Intel, Intel Inside, the Intel Inside logo, and Intel Xeon are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

diff -u

WHAT'S NEW IN KERNEL DEVELOPMENT

A new cryptographic filesystem, **eCryptFS**, has been sent to the kernel developers for consideration. **Phillip Hellewell** has been working with **Michael Halcrow**, who presented a detailed design of eCryptFS at the 2005 Ottowa Linux Symposium. eCryptFS may be "stacked" on top of other filesystems, using the **FiST**-stackable filesystem framework written by **Erez Zadok**. The current version supports per-mount decryption only, essentially to support testing and debugging of the basic features. Advanced policy and per-file public key support is planned after some amount of testing can be done on the existing infrastructure. One of the most interesting features of eCryptFS is that it stores its cryptographic metadata within the files themselves, allowing cool features like securely transferring files across untrusted domains.

Mark Gross submitted a special character driver for the **Intel NetStructure MPCBL0010** single-board computer that will ship in the fall. The MPCBL0010 is essentially intended for use in telecom devices, which often need to synchronize their operations with other hardware. Mark's driver enables this synchronization via the onboard FPGA (Field-Programmable Gate Array) intended for that purpose. And, a sysfs interface provides easy control over this synchronization to the system developer. Mark also included an ioctl interface, primarily so the driver could be tested under 2.4 kernels, but the ioctl probably will be dropped in any final version of the patch accepted into the 2.6 tree.

The saga of **software suspend** continues to be broad and sweeping. **Rafael J. Wysocki** recently posted some patches to split the entire **swsusp** infrastructure into two independent kernel subsystems. One subsystem is responsible for snapshotting the running system, and the other is responsible for reading and writing the snapshotted data to and from swap. One of the benefits of this division is that it allows a significant portion of swsusp's functioning eventually to be migrated to user space. Aside from that, the new system allows more memory efficiency, and it does away with certain size limitations and reliance on global variables. **Pavel Machek** also has gone over these patches and approved them. As we watch big changes like code forks, reunifications, subsystem divisions and so on, it's important to remember that in the beginning, software suspend was deemed impossible because certain hardware state just couldn't be saved. It's no surprise that this feature's problems remain large.

The **git** revision control system continues to develop at a hot pace. If you haven't tried it, you should. The **Ubuntu** distribution's kernel development is now done with git, and **ethtool** development recently migrated to git as well. As a side point, it was pointed out recently to **Randal L. Schwartz** (now using git for Web site development) that git is binary-safe and easily handles image files, compressed tarballs and anything else one might throw at it. Other folks, like **Jeff Garzik**, have been experimenting with creating a peer-to-peer storage back end for git, allowing users to query a larger git network, rather than a single standalone system. File renaming in git continues to be a hard sell from **Linus Torvalds**, as he insists that rename tracking can be done automatically and does not require the user informing the system of a rename. Although no longer the primary git maintainer, Linus continues to influence development strongly, and he remains the biggest evangelist of git features, often pointing out powerful and non-obvious idioms to mailing-list readers.

Adrian Bunk has taken over from **Rusty Russell** as the **Trivial Patch Monkey** maintainer. As created by Rusty, the Trivial Patch Monkey collects and submits patches that are so trivial they could not possibly be wrong. Originally, many such trivial patches would get lost in the shuffle. Contributors wouldn't know precisely where to submit them, and the developers who might receive them (including Linus Torvalds) often just let them drop on the floor, choosing instead to focus on more significant work. Rusty decided to pick up these patches and submit them regularly until they finally would be accepted. With each kernel release, he would initiate the semi-automated process of sending these patches along, with the form and timing most likely to appeal to Linus. Now Rusty has apparently moved on, and Adrian will perform a similar task. The Trivial Patch Monkey is not unlike the new w.x.y.z stable tree (dubbed the sucker tree by Linus). Both are largely thankless tasks that lack the thrill of participating in new feature development. And, both make a large difference to the community, though we don't spend much time thinking about them.

—Zack Brown

On the Web

Are you still writing programs with the same tools and in the same manner as you did five, seven or even ten years ago? Thinking it might be time to modernize your programming arsenal? Follow along as Collin Park takes a step away from 20+ years of C coding and ventures into Python waters. In his new series on LJ.com, Collin tests out Python by putting it to work solving various puzzles, including the "Coconuts" problem (**www.linuxjournal.com/article/8728**) and Sudoku (**www.linuxjournal.com/article/8729**).

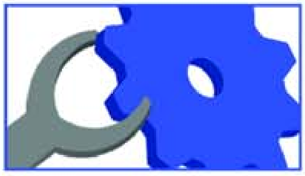
Exclusively for LJ.com readers, read an excerpt from Chapter 10, "Adding Your Code to the Kernel", of *The Linux Kernel Primer: A Top-Down Approach for x86 and PowerPC Architectures* (**www.linuxjournal.com/8730**). In our excerpt, authors Claudia Salzberg Rodriguez, Gordon Fischer and Steven Smolski "follow a device driver from how the device is represented in the filesystem...through the specific kernel code that controls it."

Finally, graduate student Ryan Mauer shares the results of his recent project on Xen. Ryan is a student of our regular LJ.com contributor Professor Richard Sevenich at Eastern Washington University. Ryan intended his project to be "an example of how Xen Virtualization can be utilized to prototype a Linux cluster with only a single physical computer, thereby minimizing the up-front hardware costs, as well as providing a way to perform a feasibility study early in the cluster implementation process." Read the article and learn the results of his work.

EmperorLinux

...where Linux & laptops converge

You choose your laptop from a wide selection of top tier laptops manufactured by Dell, IBM, Lenovo, Sharp, and Sony. **You choose your distribution** from among the most popular Linux distributions. We'll install your distribution; add our custom kernel; then configure your laptop for full hardware support, including: X at the native resolution, wireless, power management, 3-D graphics, optical drives...



The Toucan: 5 lb Linux

- ThinkPad T series by Lenovo
- 14.1" SXGA+/15.0" UXGA
- X@1400x1050/1600x1200
- ATI FireGL graphics
- 1.6-2.26 GHz Pentium-M 7xx
- 40-100 GB hard drive
- 512-2048 MB RAM
- CDRW/DVD or DVD-RW
- ACPI suspend/hibernate
- Ask about our Sharp laptops

The Rhino: 7 lb Linux

- Dell Latitude D810/M70
- 15.4" WUXGA screen
- X@1920x1200
- NVidia Quadro or ATI Radeon
- 1.73-2.26 GHz Pentium-M 7xx
- 40-100 GB HD (7200 rpm)
- 512-2048 MB RAM
- CDRW/DVD or DVD±RW
- 802.11a/b/g wireless, GigE
- Ask about our Sony laptops

```
To:  support@emperorlinux.com
From:  customer@homebase.net
Subject:  Configuration of 8

Just bought a new wirele
to learn how to config                ess
my PC and my laptop so               wireles
anywhere in my house.

And I still want it to work   my office, too.
```

Let EmperorLinux do the rest. Since 1999, EmperorLinux has provided pre-installed Linux laptops to universities, corporations, and Linux enthusiasts. We specialize in the configuration of Linux on the finest laptop and notebooks. We offer a range of the latest Linux distributions a[illegible] boot options. All systems come with one year of Linux technical support [illegible] manufacturers' warranty.

Introducing the Raven X41 Tablet

Linux Tablet Features

- Pen/stylus input to screen in X
- Handwrite commands to screen focus
- Handwrite notes and convert to text
- Pressure sensitive stylus in GIMP
- Rotate screen orientation

Linux Laptop Features

- ThinkPad X series by Lenovo
- 12.1" XGA w/ X@1024x768
- 1.5 GHz Pentium-M 758
- 60 GB hard drive
- 512-1536 MB RAM
- 802.11a/b/g wireless, GigE
- ACPI hibernate

www.EmperorLinux.com 1-888-651-6686

Model prices, specifications, and availability may vary. All trademarks are the property of their respective owners.

LJ Index, March 2006

1. Percentage of persons aged 12 to 24 who prefer MP3 players to radio: 85
2. Percentage of persons aged 12 to 24 who listen to satellite radio: 2
3. Thousands of persons in the US who downloaded a podcast during 2004: 820
4. Millions of persons in the US who downloaded a podcast during 2005: 4.8
5. Percentage of podcast listeners in the US who download on a weekly basis: 20
6. Conservative estimate of podcast listeners in the US by 2010, in millions: 45
7. Aggressive estimate of podcast listeners in the US by 2010, in millions: 75
8. Number of Google results for "podcasting" on September 25, 2004: 24
9. Millions of Google results for "podcasting" on December 6, 2005: 78
10. Thousands of Ubuntu/GNOME Linux desktops deployed in schools by Macedonia: 5
11. Number of schools to which the new Macedonian Linux desktops are going: 468
12. Number of computer labs also getting Linux desktops: 182
13. Percentage of surveyed Micro Center customers who are receptive to purchasing a Linux desktop: 75
14. Position of Red Hat in a list of popular Linux distributions: 1
15. Position of Debian among the fastest-growing Linux distributions: 1
16. Red Hat share of Linux Web servers: 34
17. Debian share of Linux Web servers: 25
18. Fedora share of Linux Web servers: 16
19. SUSE share of Linux Web servers: 11
20. Millions of active Debian sites: 1.2

Sources: 1–7: Bridge Ratings | 8, 9: Doc Searls | 11, 12: *The GNOME Journal* | 13: Linspire & Micro Centers | 14–20: Netcraft

—Doc Searls

They Said It

Fear, because what is free is never fully appreciated.

—STEVE GILLMOR, blogs.zdnet.com/Gillmor/?p=189

Remember, Linux is a species, and we aren't fighting anyone here. We are merely evolving around everyone else, until they aren't left standing because the whole ecosystem changed without them realizing it.

—GREG KROAH-HARTMAN, LINUX-ELITISTS

The Straight Talk People℠
SINCE 1991

ABERDEEN

SCALABLE LINUX NAS. YOU'RE NOT DREAMING!

All the features that made you choose Linux driving the most scalable, high performing, competitively priced NAS appliance in the marketplace today.

- Best fit for Unix/SunMicro/Linux environments or mix of Windows & Non-Windows environments
- Browser based GUI management
- Substantially faster NFS and CIFS perfomance compared to Windows Storage Server
- Extremely virus resistant—Read-only Disc-On-Memory (DOM) operating system provides integrity, avoids corruption and allows for easy upgrade
- Embedded iSCSI target with unlimited initiators
- Multiple schedulable volume snapshots
- PCBackup Utility included allows multiple file versions and instant backup of any modified file
- NAS-2-NAS Replicator included
- Novell Netware bindery mode support
- Available with 500GB 8.5ms 7200rpm hot-swap SATA II 3Gb/s hard drives with 16MB cache featuring Rotational Vibration Safeguard and staggered (delayed) spin-up
- SATA II 3Gb/s enables the highest level of performance at low cost of ownership
- 300MBytes/sec per drive data transfer rates—twice as fast as regular SATA and three times as fast as Ultra ATA/100
- Single controller for up to 24 drives—single 12TB partion
- Intel RAID 6 Engine to support extreme performance RAID 6—can protect mission-critical data from two concurrent disk drive failures
- Status indication via HDD activity/fault LEDs and audible alarm
- Management port/firmware supports browser-based RAID manager, SMTP email notification, SNMP agent
- Native Command Queuing (NCQ) for extreme performance
- "Smooth Stream" technology for enhanced video streaming
- Easily scalable with Aberdeen XDAS units

intel inside XEON

ABERDEEN ABERNAS 170 SERIES

1U Network Attached Storage with Hardware RAID 6

- Up to 2TB of Network Attached Storage in a 1U format
- Intel® Pentium® 4 processor 531 supporting Hyper-Threading Technology, 3.0E GHz with 800MHz FSB and 1MB Cache
- 1GB Dual Channel DDR400 SDRAM (Low Latency)
- Single controller for all drives with RAID level 0, 1 (10), 3, 5 and 6
- 4 x Hot-Swap Hard Drives with single partition capability
- Slim DVD Drive
- 300W Power Supply
- Linux based proprietary NAS software (see above for features and benefits)
- Disc-On-Memory (DOM) operating system provides integrity and avoids corruption
- **5-Year Limited Warranty**

AberNAS 170 **$3,495**

- 1TB of Network Attached Storage
- 4 x 250GB Hot-Swap SATA Hard Drives with 8MB cache

AberNAS 176 **$4,295**

- 1.6TB of Network Attached Storage
- 4 x 400GB Hot-Swap SATA Hard Drives with 8MB cache

AberNAS 178 **$4,995**

- 2TB of Network Attached Storage
- 4 x 500GB Hot-Swap SATA II 3Gb/s Hard Drives with 16MB cache

ABERDEEN ABERNAS 270 SERIES

Network Attached Storage with Hardware RAID 6

- Up to 4TB of Network Attached Storage in a 1U format
- Intel® Pentium® 4 processor 531 supporting Hyper-Threading Technology, 3.0E GHz with 800MHz FSB and 1MB Cache
- 1GB Dual Channel DDR400 SDRAM (Low Latency)
- Single controller for all drives with RAID level 0, 1 (10), 3, 5 and 6
- 8 x Hot-Swap Hard Drives with single partition capability
- Slim DVD Drive
- 460W Redundant Power Supply
- Linux based proprietary NAS software (see above for features and benefits)
- Disc-On-Memory (DOM) operating system provides integrity and avoids corruption
- **5-Year Limited Warranty**

AberNAS 271 **$4,995**

- 2TB of Network Attached Storage
- 8 x 250GB Hot-Swap SATA Hard Drives with 8MB cache

AberNAS 272 **$7,495**

- 3.2TB of Network Attached Storage
- 8 x 400GB Hot-Swap SATA Hard Drives with 8MB cache

AberNAS 273 **$8,995**

- 4TB of Network Attached Storage
- 8 x 500GB Hot-Swap SATA II 3Gb/s Hard Drives with 16MB cache

"terrific for storage-intensive tasks" *PC Magazine*

ABERDEEN XDAS 500 SERIES

SCSI-to-SATA RAID Direct Attached Scalable Storage

- **Up to 12TB of Direct Attached Storage**
- Daisy Chain Units for Scalability
- OS and Host Independent
- Supports Dual Host for Server Failover Clustering
- 2 SCSI Host Channels
- Up to 16 x 500GB 7200 RPM Hot-Swap SATA II 3Gb/s Hard Drives with 16MB cache
- Intel® 80321 I/O Processor
- Modular/Cableless internal design
- RAID Controller Smart LCD Display
- RAID level 0, 1, 3, 5, 6, 10, JBOD
- HotSpare, HotSwap & Auto-Rebuild
- Multiple RAID arrays/LUNs
- Fast RAID Initialization and Fast Rebuild process
- Dual Flash ROM for Redundant Firmware Images
- Optional Fibre Channel Interface
- **5-Year Limited Warranty**

XDAS 501 4TB 2U 8-bay	$8,875
XDAS 502 6TB 2U 12-bay	$11,475
XDAS 503 8TB 3U 16-bay	$14,575
XDAS 504 12TB 4U 24-bay	$22,975

Intel, Intel logo, Intel Inside, Intel Inside logo, Celeron, Intel Xeon, Itanium, Pentium and Pentium III Xeon are trademarks or registered trademarks of Intel Corporation. lj007

888-297-7409
www.aberdeeninc.com/linux

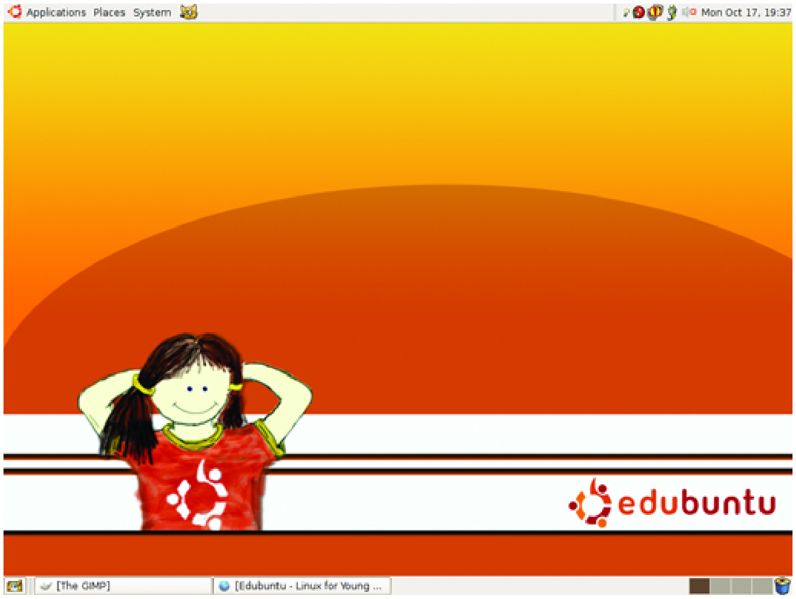
Edubuntucation

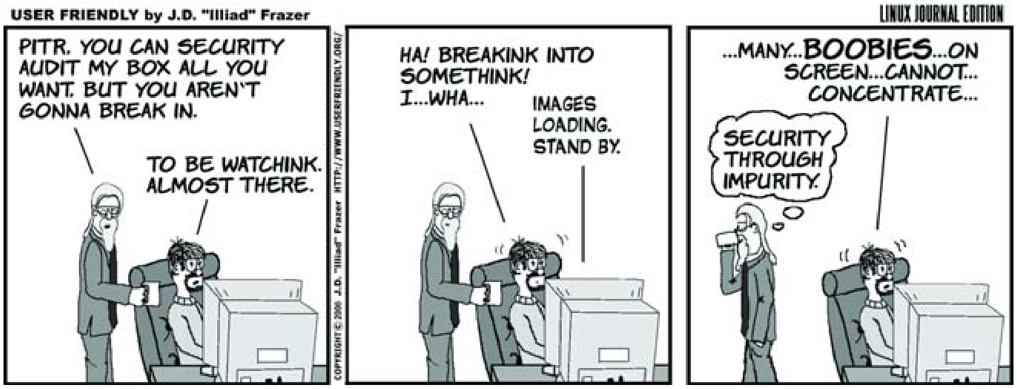
I knew Ubuntu (**www.ubuntu.org**) had reached a milestone when my friend John, a Windows expert of long standing, told me he now tests hardware combinations with Ubuntu. “When I loaded XP on this new box I put together yesterday, it was a nightmare. It couldn’t find peripherals, wouldn’t load all kinds of stuff. Then I booted it with Ubuntu and it found everything, just like that. So I knew the machine and the peripherals were fine.”

But what’s good for experts like John still might not be simple and easy enough for schools. That’s why we now have Edubuntu (**www.edubuntu.org**), a new Ubuntu distro that’s customized for classroom use. Says the edubuntu.org Wiki, “As an educator, you’ll be able to set up a computer lab or establish an on-line learning environment, in an hour or less—then administer that environment without having to become a fully-fledged Linux geek.”

Edubuntu is built on the 2.6 Linux kernel and GNOME 2.12. It contains more than 16,000 pieces of software and fits on a bootable CD. It is also pointedly noncommercial. The Edubuntu Manifesto begins, “Edubuntu will always be free of charge, and there is no extra fee for the ‘enterprise edition’. We make our very best work available to everyone on the same Free terms.” The Manifesto also commits to a regular and predictable six-month release schedule interval. The first official release of Edubuntu 5.10 came out on October 13, 2005. The next release should then be due in April of this year.

—Doc Searls




USER FRIENDLY by J.D. "Illiad" Frazer
LINUX JOURNAL EDITION
PITR, YOU CAN SECURITY AUDIT MY BOX ALL YOU WANT, BUT YOU AREN'T GONNA BREAK IN.
TO BE WATCHINK. ALMOST THERE.
COPYRIGHT © 2000 J.D. "Illiad" Frazer HTTP://WWW.USERFRIENDLY.ORG/
HA! BREAKINK INTO SOMETHINK! I...WHA...
IMAGES LOADING. STAND BY.
...MANY...BOOBIES...ON SCREEN...CANNOT... CONCENTRATE...
SECURITY THROUGH IMPURITY.

The Edge at Micro Centers

Micro Center is a chain of 19 computer gear stores in 13 states. You find them where techies are concentrated: Santa Clara, Tustin, Madison, Chicago, Denver, Houston, Cambridge and Fairfax. You find them on-line too at **microcenter.com**.

If you go into their stores, you now find desktop Linux doing something more than bringing down the price of some bottom-end Windows-less PC. Desktop Linux is actually featured. Or, in retail lingo, merchandised.

When the decision to promote desktop Linux was made, Kevin Jones, VP of Merchandising for Micro Center, sent out a letter that said:

> We know we can’t just randomly plunk new desktop Linux computers around our vast stores and expect them to sell well. To become viable, a product line has to be prominently displayed, easy to test drive, and be backed by both a knowledgeable salesperson and post-sale service and support. Micro Center’s retail model is based on the “store within a store” concept—products are housed in their own separate sections within the store, where trained Micro Center staff can respond to questions about the specific products in their sections.

This progress isn’t limited to the chain’s off-line stores. A search for “linux” at **microcenter.com** brings up 13 pages of results. And, if you want to know one reason why the on-line store performs so well, go do “What’s this site running?” at Netcraft.

Eleven servers come up, all running Linux.

—Doc Searls

Thinkmate server and workstation products offer more configurations and more customizable options than any other system builder.

intel inside XEON

Thinkmate 1U Server, 2x Serial-ATA or SCSI drives with Intel® Xeon™ Processors

Dozens of customizable systems online, unlimited possibilities by phone.

- Rackmount Servers
- High-Performance Servers
- Storage Servers
- Pedestal Servers
- Silent Workstations
- Blade Servers
- Clustering
- Notebooks

Operating System Options:

Thinkmate systems are available with either No OS, or pre-loaded with Linux or Microsoft Windows operating systems. Thinkmate also offers dual-boot and virtualization options.

100% True Hardware Customization:

Thinkmate is an innovative provider of an extensive variety of computer solutions. We completely customize all of our machines to match your individual needs. Our online quoting and ordering system has more customizable options than any other system builder on the web. If you can't find exactly what you need on our site, then give us a call and we would be more than happy to help you find it!

Service:

Thinkmate takes customer service to a new level. All of our systems have a minimum of a 3-year advanced replacement warranty and offer up to a 3-year next business day onsite warranty through IBM Global Services. We understand mission critical situations and provide superior services to keep all of our customers satisfied.

GSA Scheduling:

GSA Schedule
Contract GS-35F-0313M

We offer rapid GSA scheduling for custom configurations. If you have a specific hardware requirement, we can have your configuration posted on the GSA schedule within 2-4 weeks.

THINKMATE (800) 371-1212
WWW.THINKMATE.COM

REUVEN M. LERNER

Amazon Web Services

All it takes is a URL to start tapping in to the rich pool of resources made available by Web services.

Back when I was in college, there weren't many options for buying technical books. I could buy them new at the high-priced campus bookstore, I could buy them from a high-priced competitor around the corner, or I could buy used copies from other students, who advertised their wares at the end of every semester. Regardless, my ability to buy books was dictated by my location, coupled with my ability to learn what was available.

So, it probably won't surprise you to learn that I was an early customer of on-line bookstores, patronizing both Bookpool and Amazon before the summer of 1995. The combination of excellent prices and wide selection, along with convenience, was a dream come true. Much as I might hate to admit it, I probably spent just as much on books from on-line stores as I would have at their brick-and-mortar counterparts. However, although my book-buying budget was unchanged, the number of books I could buy, as well as the variety that was available, was unparalleled in the physical world.

Things got even better when Amazon opened its doors to third-party booksellers. Now I could not only compare new book prices from the comfort of my living room, but I could browse and buy used books as well. The number of interesting books available for less than $1 US (plus shipping) has turned me into something of a book-buying monster; the shelves of my graduate-school office are filled with books that I hope will be useful in my research, but that I bought largely because the opportunity existed. When I hear about an interesting book, my first instinct now is to check at Amazon—or even better, at isbn.nu, which compares prices across multiple sites.

Over the years, Amazon has assembled a huge database of information about books. I'm sure that this database of books, buyers and sellers continues to be an important source for Amazon's decision-makers. But a few years ago, Amazon decided to do something surprising—they opened part of their internal database to third-party developers, in a program known as Amazon Web Services (AWS). Using AWS, developers can perform nearly every task they would normally be able to do on the Amazon site, using a client-side program rather than a Web browser. AWS also includes a number of features aimed at booksellers, for pricing and inventory management.

In the latter half of 2005, Amazon unveiled a number of new initiatives that fit under its "Web services" umbrella, only some of which are related directly to selling and buying books. At about the same time, eBay announced that it would no longer be charging developers to use its Web services, making it possible to query two of the largest databases of sales data. And, of course, Google has long offered Web services of its own; although data is currently limited to the main index, it is probably safe to assume that it is a great resource.

This month, we begin to explore the world of commercial Web services, looking especially at ways in which we can integrate data from external Web services into our own applications. Along the way, we'll see some of the different ways in which we can invoke Web services, some of the different offerings that are available to us and how we might be able to build on existing Web services to create new and interesting applications.

What Are Web Services?

During the Web's first decade or so, it was mostly designed for user interaction. That is, most HTTP clients were Web browsers, and most of the content downloaded by those browsers was HTML-formatted text intended for people to read.

At a certain point, developers began to consider the possibility that they could use HTTP for more than just transmitting human-readable documents. They began using HTTP to transmit data between programs. The combination of HTTP as a transmission protocol and XML as a data format led to XML-RPC. Because XML and HTTP are platform-neutral, one did not have to write both the client and server programs in the same language, or even use the same operating system. XML-RPC thus provides a means for cross-platform RPC (remote procedure calls), with far less overhead than other similar approaches to the same problems (such as, CORBA middleware) might require.

XML-RPC was and is a good, clean and lightweight protocol, but it lacked some of the sophistication, error handling and data types that many developers wanted. Thus, SOAP (originally short for the Simple Object Access Protocol) introduced a number of extensions to make it more formal, including a separation between the message envelope and body.

XML-RPC and SOAP both assume that the server will be listening for method calls at a particular URL. Thus, a server might have an XML-RPC or SOAP server listening at /server, or /queries, or some such URL. The client is then responsible for indicating which method it needs in the request. In XML-RPC, we use the methodName tag. Parameters and metadata are all passed in the XML envelope, which is sent as part of an HTTP POST submission.

A different technique, known as REST, identifies the method calls in the URL itself. It passes parameters like a standard GET request. REST has a number of nice features, especially its simplicity of implementation and use. And, debugging REST is easy, because you can enter the URLs into a Web browser instead of a specialized program. However, a large number of people are still using SOAP and XML-RPC, especially when working with complex data structures.

Web services form the core of what is increasingly known as service-oriented architecture, or SOA, in the high-tech world. A Web service brings together all of the advantages of the Web—platform independence, language independence and the ability to upgrade and change the service without having to distribute a new version.

SOA makes it possible to create new services, or even to unveil new versions of existing services, either by replacing an existing implementation or by unveiling a new implementation in parallel with the old one. Those who use Web services can benefit from improved speed and efficiency, or from completely new APIs, without having to worry about incompatibilities or installation problems. In addition, as long as developers follow the service's published specification, they can use whatever language and platform they want, creating anything from an interactive desktop application to an automated batch job that crunches through gigabytes of data.

Amazon's Web Services

Amazon was one of the first companies to begin working with Web services. AWS is now a suite of different APIs, some of which have to do with Amazon's catalogs, and others (for example, the Mechanical Turk and Amazon's Simple Queue Service) are more generalized services. The most popular service is known as the E-Commerce Service (ECS). ECS makes it possible to retrieve product data from several of Amazon's stores, get detailed information about particular items and vendors, and also perform basic operations having to do with e-commerce, including the creation and manipulation of shopping carts.

ECS has two basic modes of operation, known as search and lookup. Searches return a list of products matching a set of criteria—for example, all of the books written by Larry Wall, or books with the word Python in the title or movies directed by Woody Allen. Lookups are meant for when you know the specific ID code associated with a product, known as an ASIN (Amazon Standard ID Number). The ASIN for books is the same as its International Standard Book Number (ISBN); other types of products have ASINs defined by Amazon.

So, let's say I'm interested in finding out whether Amazon stocks the Pragmatic Programmers' book about Ruby on Rails, and how much it costs. Because I'm looking for a particular item, I should use the ItemLookup operation. But this means that I need to know the ISBN, which I find is 097669400X. (ECS expects the ISBN without any hyphens or other punctuation.) Finally, I have to get a value for AccessKeyId, an ID number that tells Amazon which developer is accessing the system. (Getting an AccessKeyId is free and easy; see the the on-line Resources for details.)

The base URL for ECS REST requests is http://webservices.amazon.com/onca/xml?Service=AWSECommerceService.

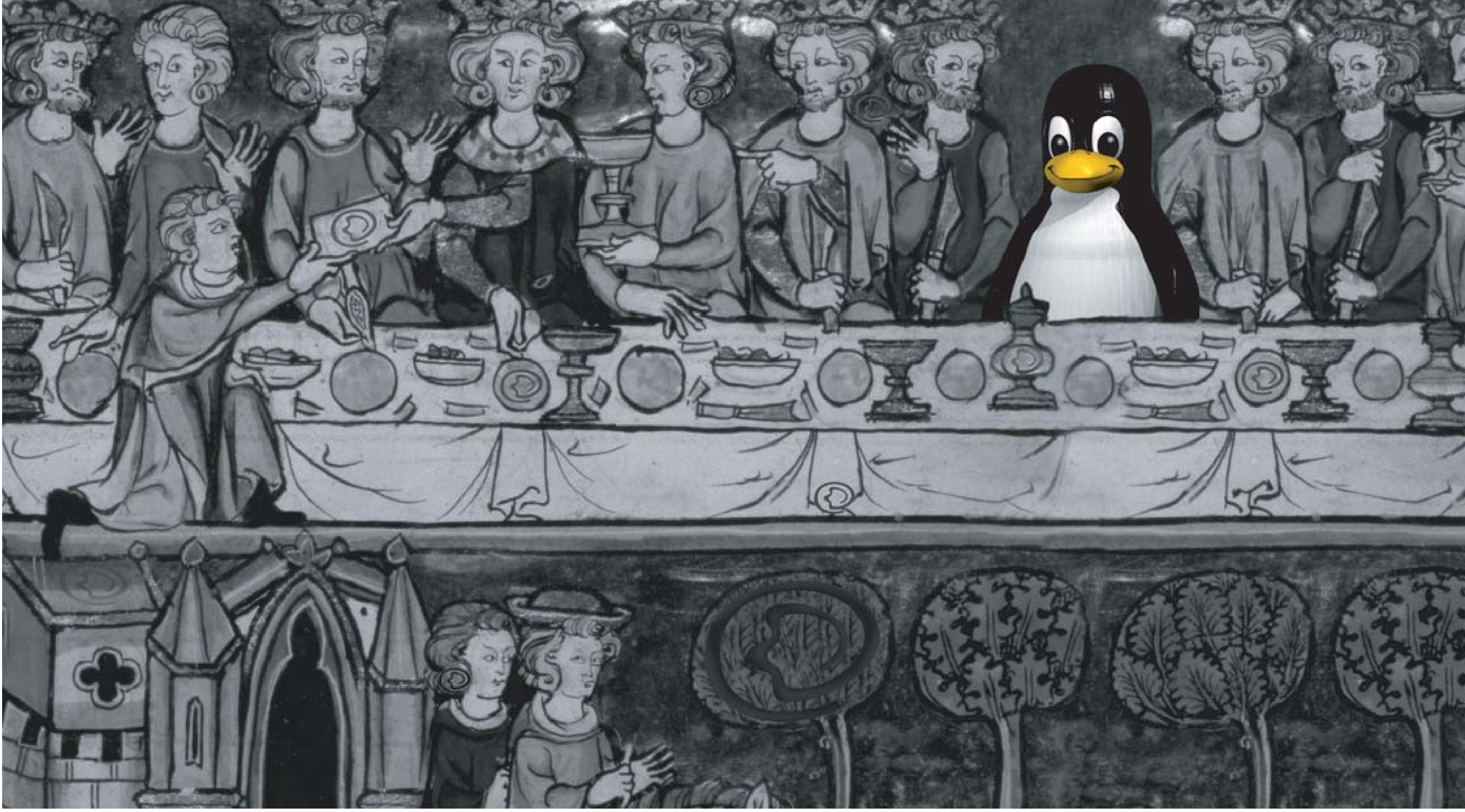
To indicate the operation, AccessKeyId and ItemId, we add name-value pairs onto the URL, using the name=value format and separating the pairs with ampersands (&). Our combined URL thus looks like this: http://webservices.amazon.com/onca/xml?Service=AWSECommerceService&Operation=ItemLookup&AWSAccessKeyId=XXX&ItemId=0735619530.

If you put the above into a Web browser (replacing the XXX with an actual AccessKeyId value), you should see the XML document (with a content-type of text/xml) returned from Amazon's server. That document begins with an ItemLookupResponse tag and is then divided into two sections, OperationRequest (which describes the request that you made, including your browser's UserAgent header and all of the arguments you passed to the service) and Items (which contains the responses from Amazon).

For example, here is the response that I received from my request to Amazon:

```
<ItemLookupResponse>
    <OperationRequest>
    <HTTPHeaders>
        <Header Name="UserAgent" Value="Mozilla/5.0 (Macintosh; U; PPC
Mac OS X Mach-O; en-US; rv:1.8) Gecko/20051111 Firefox/1.5"/>
    </HTTPHeaders>
    <RequestId>1NBTWT1FHDEHJK2G16CT</RequestId>
    <Arguments>
        <Argument Name="Operation" Value="ItemLookup"/>
        <Argument Name="Service" Value="AWSECommerceService"/>
        <Argument Name="AWSAccessKeyId" Value="XXX"/>
        <Argument Name="ItemId" Value="097669400X"/>
    </Arguments>
    <RequestProcessingTime>0.00745105743408203</RequestProcessingTime>
    </OperationRequest>

    <Items>
    <Request>
    <IsValid>True</IsValid>
    <ItemLookupRequest>
    <ItemId>097669400X</ItemId>
    </ItemLookupRequest>
    </Request>
    <Item>
        <ASIN>097669400X</ASIN>
        <DetailPageURL>
http://www.amazon.com/exec/obidos/redirect?tag=
➥ws%26link_code=xm2%26camp=2025%26creative=
➥165953%26path=http://www.amazon.com/gp/
➥redirect.html%253fASIN=097669400X%2526tag=
➥ws%2526lcode=xm2%2526cID=2025%2526ccmID=
➥165953%2526location=/o/ASIN/
➥097669400X%25253FSubscriptionId=XXX
        </DetailPageURL>
        <ItemAttributes>
        <Author>Dave Thomas</Author>
        <Author>David Hansson</Author>
        <Author>Leon Breedt</Author>
        <Author>Mike Clark</Author>
        <Author>Thomas Fuchs</Author>
        <Author>Andrea Schwarz</Author>
        <ProductGroup>Book</ProductGroup>
        <Title>
        Agile Web Development with Rails (The Facets of Ruby Series)
        </Title>
        </ItemAttributes>
    </Item>
    </Items>
</ItemLookupResponse>
```



There are several particularly useful fields in the previous XML. You can see how much time it took for Amazon to process our request (0.008 seconds, in this case), which might be useful if we need to debug and/or benchmark our application. The DetailPageURL contains the URL to which we can refer users who want to see information about this product on the Amazon site. And, we get information such as the title and author(s), which might be useful when displaying book information.

And indeed, it should be easy to see how we can parse this XML, displaying parts or all of it in a Web, GUI or console application. Or, we can add some part of this data to a larger database application that we are creating, making sure not to violate Amazon's restrictions on the use of retrieved data.

Response Groups

As useful as the above information is, it still doesn't answer all of my original question, which is whether Amazon stocks the Pragmatic Programmers' book about Ruby on Rails, and how much it costs. I know that the Rails book is available from Amazon, but I don't know how much it costs. This is because ECS returns a small amount of data by default, corresponding to what we saw above. We can tailor the information that Amazon returns to us by specifying one or more response groups. Each response group corresponds to one or more types of data that ECS will return in its response.

To get basic pricing information about a book, we thus can ask to see the OfferSummary response group: http://webservices.amazon.com/onca/xml?Service=AWSECommerceService&Operation=ItemLookup&AWSAccessKeyId=XXX&ItemId=0735619530&ResponseGroup=OfferSummary".

Instead of the previous listing, which described the book itself, we now get a list of the lowest new and used prices for a particular book. Here is the XML response from the above query:

```
<ItemLookupResponse>
<OperationRequest>
<HTTPHeaders>
<Header Name="UserAgent" Value="Mozilla/5.0 (Macintosh; U; PPC Mac
OS X Mach-O; en-US; rv:1.8) Gecko/20051111 Firefox/1.5"/>
</HTTPHeaders>
<RequestId>0SNXJ8T5V2JA18M8AJQC</RequestId>
<Arguments>
<Argument Name="ResponseGroup" Value="OfferSummary"/>
<Argument Name="Operation" Value="ItemLookup"/>
<Argument Name="Service" Value="AWSECommerceService"/>
<Argument Name="AWSAccessKeyId" Value="XXX"/>
<Argument Name="ItemId" Value="097669400X"/>
</Arguments>
<RequestProcessingTime>0.0331768989562988</RequestProcessingTime>
</OperationRequest>
<Items>
        <Request>
        <IsValid>True</IsValid>
        <ItemLookupRequest>
        <ItemId>097669400X</ItemId>
        <ResponseGroup>OfferSummary</ResponseGroup>
        </ItemLookupRequest>
        </Request>
        <Item>
        <ASIN>097669400X</ASIN>
        <OfferSummary>
        <LowestNewPrice>
        <Amount>2295</Amount>
        <CurrencyCode>USD</CurrencyCode>
        <FormattedPrice>$22.95</FormattedPrice>
        </LowestNewPrice>
        <LowestUsedPrice>
        <Amount>2341</Amount>
        <CurrencyCode>USD</CurrencyCode>
        <FormattedPrice>$23.41</FormattedPrice>
        </LowestUsedPrice>
        <LowestCollectiblePrice>
        <Amount>3495</Amount>
        <CurrencyCode>USD</CurrencyCode>
        <FormattedPrice>$34.95</FormattedPrice>
        </LowestCollectiblePrice>
        <TotalNew>41</TotalNew>
        <TotalUsed>12</TotalUsed>
        <TotalCollectible>2</TotalCollectible>
        <TotalRefurbished>0</TotalRefurbished>
        </OfferSummary>
        </Item>
</Items>
</ItemLookupResponse>
```

As you can see, the initial portion of the response is the same. But the second half of the response, inside of the <Items> tag, is different, with LowestNewPrice, LowestUsedPrice and LowestCollectiblePrice tags showing us how much we can buy this book for.

We also can ask for other response groups, mixing and matching their names as necessary. For example, we can request the Medium response group, giving us not only information about the request and the book, but also the images (in a number of sizes) associated with the book, the book's size and weight, and editorial reviews. If we want to go beyond that, getting reviews of the book that have been left by Amazon customers and lists of similar products, we can request the Large response group.

Summary

Amazon's Web services provide us with a tool to look through a huge database of product information, for both personal and commercial use. In addition, ECS gives us a taste of what it is like to create REST-style queries, and how we might parse the results. Finally, just as Web developers often learn from the HTML and JavaScript on existing sites, we can learn how to create good Web services for our own use by studying the way in which Amazon has done theirs. In particular, I like Amazon's concept of response groups, which allows us to mix and match the types of responses we might get—something that I may well emulate in my own Web services.

Next month, we'll build on what we saw here, creating a Web service of our own that aggregates data from Amazon and my local public library to give me a personalized book lookup system.

Resources for this article: www.linuxjournal.com/article/8748.■

Reuven M. Lerner, a longtime Web/database consultant, is a PhD student in Learning Sciences at Northwestern University. He lives outside of Chicago with his wife and three children, including newborn son Amotz David.

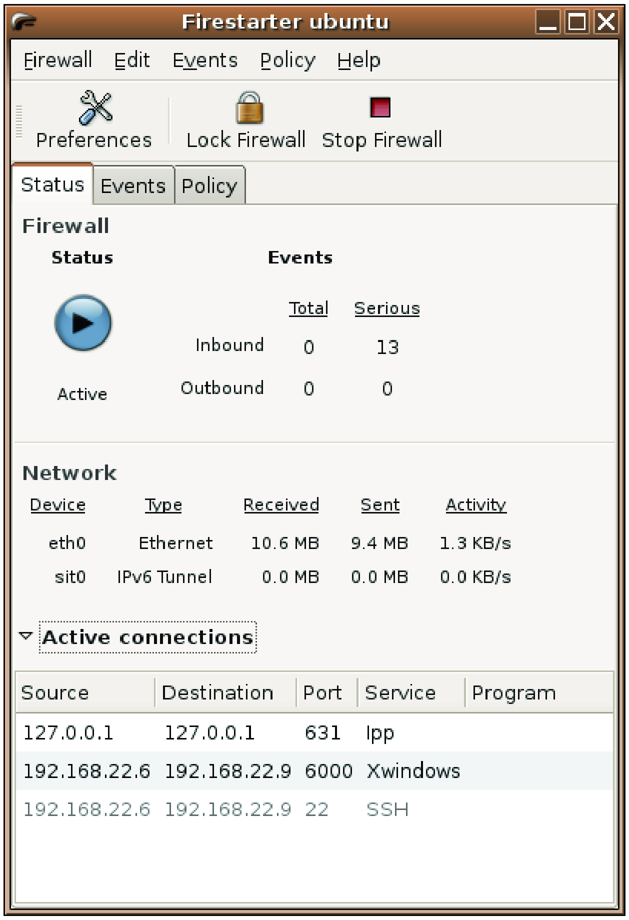
MARCEL GAGNÉ

The Best Security...Barks!

Thank goodness that Guarddog's bite is better than its bark.

No, François, I don't notice anything wrong with our Internet connection. Ah, I see, you installed a new firewall and now you can't get out. Hmm...let me have a look at that configuration. I think I see the problem, *mon ami*. Your configuration is completely unforgiving, but you have excellent security. Nothing gets in, but nothing gets out either. Perfectly secure.

Yes, François, I am just kidding. Extreme comparisons are everywhere when it comes to security, *mon ami*. I've heard it said that the best way to secure a server is to unplug it and leave it in a closet. If we are going to get silly about this, why stop there, I say? Encase the server in concrete and bury it in a lead-lined vault 50 feet below the surface. All joking aside, *mon ami*, there has to be a balance between acceptable security and a completely unusable system. That's the focus of tonight's menu, and as soon as our guests arrive, we'll serve up some very nice firewall applications.



Firewall

Status: Active

Events	Total	Serious
Inbound	0	13
Outbound	0	0

Network

Device	Type	Received	Sent	Activity
eth0	Ethernet	10.6 MB	9.4 MB	1.3 KB/s
sit0	IPv6 Tunnel	0.0 MB	0.0 MB	0.0 KB/s

Active connections

Source	Destination	Port	Service	Program
127.0.0.1	127.0.0.1	631	Ipp	
192.168.22.6	192.168.22.9	6000	Xwindows	
192.168.22.6	192.168.22.9	22	SSH	

Figure 1. Firestarter's interface is clean and easy to work with.

But they are already here, François. Welcome, everyone, to *Chez Marcel*, where fine Linux fare and exquisite wines find the perfect match. My faithful waiter will help you to your tables and then he will fetch the wine. The 2002 Belle Glos Pinot Noir from Sonoma sounds perfect—I think you will find it in the North wing where Henri is currently restocking, François.

Linux vendors often provide some kind of firewall with their distribution, but not all do. Normally, you access these through whatever system administration tool your vendor provides. Sometimes the firewall tools are essentially the command-line iptables software. There's nothing wrong with building a firewall using only the command line, but for many, a little directed, simplified, graphical help is quite welcome. The firewall generators I cover today have another advantage besides being easy to use and configure. Both allow you to modify the firewall in real time. Each starts with a very strict configuration for incoming traffic (unless specifically allowed, all traffic is denied). They are also distribution-agnostic. Should you decide to move from one distribution to another, you can use the same tools.

Ah, François, it is good to have you back. Please, pour for our guests.

The first item on tonight's menu, Tomas Junnon's excellent Firestarter, is an easy-to-use, graphical firewall application that provides you with real-time response and configuration of your security rules. When you run Firestarter (command name, `firestarter`), you are prompted for the root password. The first time you run it, the program starts a Firewall Wizard to help you get started. Because the first screen is basically a welcome screen, read the message, then click Forward.

Next, you'll come to the Internet connection sharing screen. Single-user desktops won't have to worry about this and simply can move forward to the next screen. However, if your PC is going to act as a NAT gateway for other PCs in your home or office, click the Enable Internet connection sharing check box. Once again, you have the option of specifying which Ethernet card (or dial-out connection) you will be using

Polywell PC Appliance Solutions

OEM Service for Small to Medium Size Projects

AMD Dual-Core technology Enables one platform to meet the needs of multi-tasking and multi-threaded environments; providing platform longevity

Allows users to run 32- and 64-bit applications as they desire – without sacrificing performance

1U 4-way, 64GB DDR, 2TB RAID

- 2 x AMD® Opteron™ Dual-Core Processors 280+ with Hyper Transport Technology
- Upto 64GB 400MHz ECC DDR (16 Sockets)
- Upto 2TB 4 x 500G Swap Drive per 1U Rack
- 1 x PCI-X 133MHz, 1 x PCI-E Solt
- Dual Gigabit Ethernet, ATI Graphics, 4 SATA-RAID
- Slim CD-ROM Drive, Optional DVD-RW or CDRW
- Optional Slim Floppy Drive
- 1U 24" Depth Rack Chassis with upto 600W PS
- 4 x Swappable Drive Bays (SATA or SCSI)
- Supports Linux, FreeBSD or Windows
- Custom Configuration Available
- Please call for other Options

1114AIS-2050M, 280+,32GB, 2TB **$12950**
1114AIS-2050M, 265+,16GB, 1TB **$6,299**
1112ES-2200A, 244+, 2GB, 500G **$1,999**

4024AIS 4U 12TB NAS/SAN **$14,999**
4024AIS 4U 6TB NAS Storage **$7,999**

Linux Appliance PCs

- Custom Made Odd Size Chassis
- AC or DC Power Supply
- Low Power Voltage AMD Sempron™ Processor
- or High Performance AMD Athlon™ 64 Processor
- Diskless or Flash OS Boot Drive
- Swapable Hard Drive, CD-ROM, FDD
- Integrated Graphics, Ethernet, USB
- Optional LCD LED Control Module
- IS2 Audio, MPEG2/4 Hardware Video
- Upto 4 Ethernet Ports or 4 Serial Ports
- We have over 18 years OEM Experience in Set top Box, Digital Media Player, POS Kiros, Thin Client, Networking Appliance,

SX2500SPLJ11B
OEM Appliance starts at **$299**

64GB DDR 4-way Workstation

- 2 x AMD® Opteron™ Dual-Core Processors 280+
- Upto 64GB 400MHz ECC DDR (16 Sockets)
- 2 x 133MHz PCI-X, 1 x PCI-E x16 Slots
- Dual Gigabit Ethernet, 4 x SATA-RAID Controller
- Quiet and Cool 12-Bay Tower + 600W 80Plus P/S
- 250G HD, DVD-RW, Floppy, Optional Card Reader
- 8-Layer Motherboard with Special Quiet Cooling
- On-board ATI Graphics, Sound Blaster 7.1 Sound
- Supports 64/32-bit Linux, FreeBSD or Windows
- Special for Large Memory Intensive Applications
- Built-to-Order or Configure-to-Order

PolyStation 2050M
4-Way Two Dual-Core Processors
Up to 64GB memory, 16 Sockets

64G RAM, 2x280+, QuadroFX4500 **$22,999**
32G RAM, 2x265+, QuadroFX3400 **$9,999**
16G RAM, 2x244+, QuadroFX1300 **$4,699**

1U Power Saving ISP Server

- AMD Sempron™ or Opteron™ Processor
- 512M DDR 400MHz Memory
- 80GB Hard Drive
- 10/100Mbit Ethernet
- We provide Drive Image Service
- 1U 14" Short Rack, allow 2 x 1U per Rack
- Low Power Usage to save your Data Center Cost
- Perfect Entry Level ISP Server or Appliance System
- IDE Flash Drive is available
- Supports Linux, FreeBSD or Windows
- Custom Configuration is Available
- Please call us to discuss your specification

Order# VX2500SP1U-17LJ11A
starts at **$399**

Pick the chassis to fit your application

2U 8-way, 5U 16-way Servers

- 8 or 4 AMD® Opteron™ Dual-Core Processors 865+ with Hyper Transport Technology
- Upto 128GB DDR Memory for 16-way (32 sockets)
- Upto 64GB DDR Memory for 8-way (16 sockets)
- 4x Gigabit LAN, 8x SATA RAID-5 for 16-way
- 2x Gigabit LAN, 4x SATA, U320 SCSI for 8-way
- 4 x 133/100/66MHz PCI-X Slots for 16-way
- 2 x 133, 2 x 66MHz PCI-X, 1x PCI Slots for 8-way
- On-board ATI Graphics, USB 2.0
- 5U 26" Rack 1300W 3+1 Redundant P/S 16-way
- 2U 27" Rack 700W PFC P/S for 8-way
- Supports Linux, FreeBSD or Windows
- Custom Configuration Available
- Please call for other Options

5U 16-way 865+, 32GB, 2TB, 8800U5 **$25,999**
2U 8-way 865+, 8GB, 750GB, 8422C **$9,500**

Mainstream Linux Systems

- AMD® Athlon™64 or X2 Dual-Core Processors with Hyper Transport Technology
- 512MB to 4GB Dual Channel DDR Memory
- 80GB to 500GB Hard Drive (SATA-RAID-0/1/5)
- 2 PCI, 2 PCIe, Gigabit LAN, 7.1 Audio, 1394a
- nForce 430 Chipset, GeForce 6100 Graphics
- Desktop, Tower, MiniBox or Rackmount Chassis
- Internet Server or Linux Appliance Configuraiton

939NX4LX starts at **$399**

Polywell OEM Services, Your Virtual Manufacture
Prototype Development with Linux/FreeBSD Supports
Small Scale to Mass Production Manufacturing
Fulfillment, Shipping and RMA Repairing

AMD 64 Opteron

AMD 64 Athlon X2

AMD64 Investment Protection
Migrate to 64-bit platforms seamlessly.
Add 64-bit application as necessary.

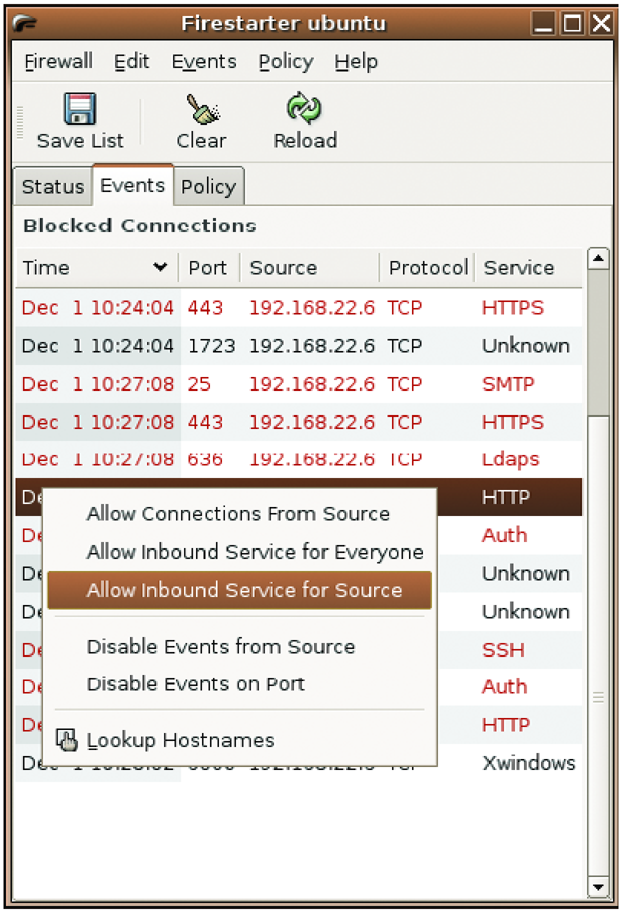
888.765.9686
www.Polywell.com/us/LJ

POLY
POLYWELL

AMD64 architecture reduces I/O bottlenecks, increases bandwidth, and reduces memory latency. Critical information gets to those who need it quickly and efficiently.

Polywell Computers, Inc 1461 San Mateo Ave. South San Francisco, CA 94080 650.583.7222 Fax: 650.583.1974

Opteron, Sempron and ATHLON are trademarks of Advanced Micro Devices, Inc.. Quadro, nForce and Nvidia are trademarks of NVIDIA Corporation. All other brands, names are trademarks of their respective companies.


Firestarter ubuntu
Firewall Edit Events Policy Help
Save List
Clear
Reload
Status
Events
Policy
Allow Connections From Source
Allow Inbound Service for Everyone
Allow Inbound Service for Source
Disable Events from Source
Disable Events on Port
Lookup Hostnames

Blocked Connections

Time	Port	Source	Protocol	Service
Dec 1 10:24:04	443	192.168.22.6	TCP	HTTPS
Dec 1 10:24:04	1723	192.168.22.6	TCP	Unknown
Dec 1 10:27:08	25	192.168.22.6	TCP	SMTP
Dec 1 10:27:08	443	192.168.22.6	TCP	HTTPS
Dec 1 10:27:08	636	192.168.22.6	TCP	Ldaps
De				HTTP
De				Auth
De				Unknown
De				Unknown
De				SSH
De				Auth
De				HTTP
De				Xwindows

Figure 2. Rules to allow traffic can be created on the fly from Firestarter's Events tab.

as your default route to the Internet. Right below that, there's an option for providing addresses via a DHCP server. If you don't have the DHCP server package installed on your system, this option is grayed out.

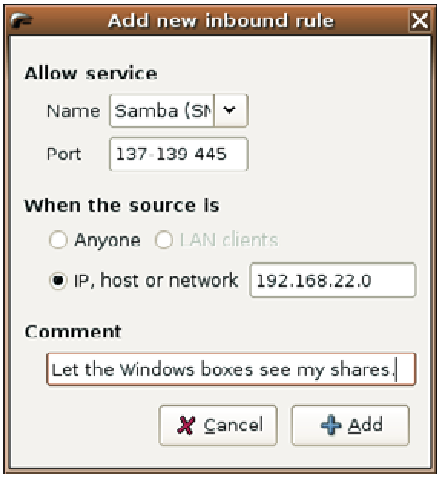
When you have made these selections, click Forward, and you are pretty much done with the Wizard. Look at the screen closely before you click Save and Quit. There's a check box labeled Start firewall now clicked on by default. With the defaults created by the Wizard, Firestarter's rules are fairly restrictive to inbound traffic (as you would expect) and that's not generally a problem. But, as the on-screen tip will inform you, this can be a problem if you are setting this up remotely. Unless you are at the workstation in question, uncheck the Start Now option. We're all done. Click Save, and Firestarter activates your new firewall and launches the status window (Figure 1).

The interface is simple with a three-tabbed view. The tabs are labeled Status, Events and Policy. The status view is the one you are most likely to be interested in on a regular basis. The display shows the firewall's run state (Active or Disabled), the inbound and outbound connections, as well as the traffic through your various interfaces. At the bottom of the window is an Active connections section that is closed by default. Click the arrow beside the label to view those connections.

I should point out that Firestarter starts by blocking every inbound service imaginable. Consequently, if you try running it on your server instead of your desktop, you'll find that no one will be able to access anything, including what you might think of as *safe* services, such as your Web server. All outbound traffic, however, is permitted, so normal desktop functions such as reading e-mail, surfing the Web or chatting on IM clients is unaffected. The Active connections window (mentioned above) shows you all of these attempts to connect as they happen, but they fade out and vanish after a few seconds. To discover what connection events occurred so that you can decide what to allow in, click on the Events tab. There, you will find a log of all traffic to your machine (Figure 2).

Right-click on one of these entries and a pop-up menu provides you with a number of options on dealing with these connections. For instance, if this is a port 80 (HTTP service) event, you may want to check Allow inbound Service for Everyone. You may feel differently, however, about a port 22 secure shell connection where you check only Allow inbound Service for Source. To allow a particular IP address (a PC on your internal network for instance), select Allow Connections From Source. You also can choose to stop logging connections either from a particular host or for a particular port number or service.

Now, I don't personally think that sysadmins wait to see who comes knocking before they allow certain services into their systems. If you are running a Web server, you probably want port 80 enabled. The same logic applies if you have a Samba server and you need to allow the people in your office to access the shares on that server. To get around this business of dealing with events as they occur, click on the Policy tab. This window is broken up into two horizontal sections or panes. The top one deals with wholesale connections from a specific host or group of hosts, and the bottom pane deals with individual services and the ports on which these services run. If you've added rules using the Events tab, you will see them here. To add other rules without going through the Events dialog, right-click in either the top or bottom pane and select Add rule from the pop-up menu. A friendly little dialog appears to make the process easy (Figure 3).



Allow service

Name: Samba (SN

Port: 137 139 445

When the source is

○ Anyone ○ LAN clients

● IP, host or network: 192.168.22.0

Comment

Let the Windows boxes see my shares.

Figure 3. Adding an inbound rule with Firestarter.

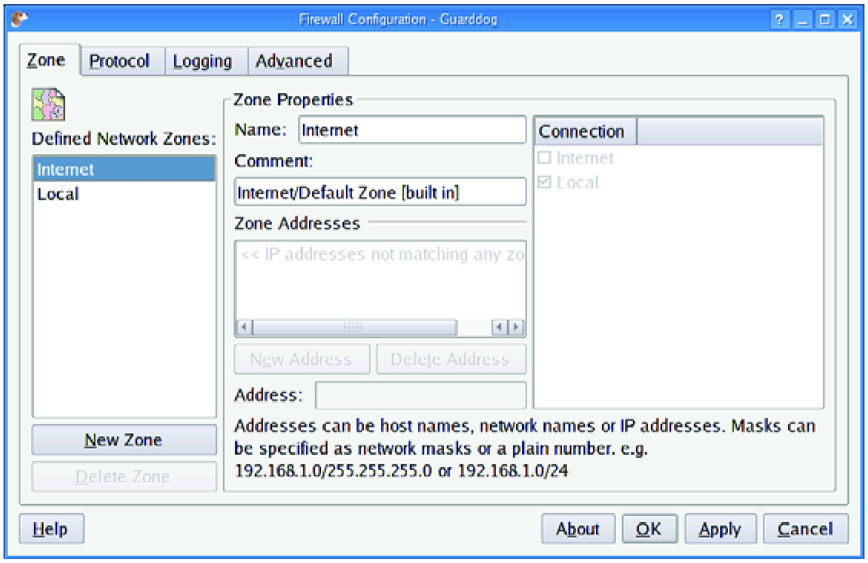
Let's add a rule to allow PCs on my local network to access the Samba service. At the top of the dialog is a drop-down list of possible services (for example, DHCP, BitTorrent, IMAP and so on). I select Samba (SMB) from the list. You will notice that for known services, the port (or ports) will be filled in automatically. Next, use the radio button under the When the source is label to allow everyone or a specific host or network. In this case, I'm adding my own class C network. Finally, I can choose to add some kind of comment in the field at the bottom. Click the Add button and that's it. The new rule appears in the Policy window. Click the Apply Policy button at the top of Firestarter's main window to apply your new policy.

Incidentally, the policies you build here don't require that you be running Firestarter. The program stores the firewall information in the /etc/rc.firewall file. Because this is a boot-level script, the firewall already will be running whenever you reboot your system.

This seems like an excellent time to take a break and relax while François refills everyone's glass. While he does so, let me tell you about another philosophy regarding security. Many years ago, I was informed that the best possible security alarm system you could buy for your house was a dog. Forget the fancy electronic gizmos and remote monitoring, I was told. Get yourself a large German Shepherd. It is perhaps with this thought in mind that the second item on tonight's menu was inspired. Simon Edwards' Guarddog is a graphical firewall configuration tool that looks to bring canine security to your Linux system. Although Guarddog is great for desktops, it is an ideal tool for even complex server configurations.

Before I take you on a little tour of Guarddog, I should point out that it is possible to run it as a nonroot user, but any changes you make will not be saved. That's because root permission is required to modify firewall rules. Obviously, it's better to run this application as root, unless, of course, you just want to learn how it works first. This isn't a bad idea for reasons I'll mention shortly. There is one other warning I want to pass on to you. Guarddog stores its firewall rules in /etc/rc.firewall, and as such, it is possible (though not likely) that you may already have a file there. What is strange here (and maybe a little amusing) is that Guarddog installs a file by this name and can trip over it on startup. Not a big problem, but if you see a message to that effect, just understand that it is probably okay. Let's enter the root password and start the program with full access to the firewall.

Figure 4. The Guarddog firewall program's main window.



Firewall Configuration - Guarddog

Zone Properties

Name: Internet

Comment: Internet/Default Zone [built in]

Zone Addresses: << IP addresses not matching any zo

Connection: ☐ Internet ☑ Local

Addresses can be host names, network names or IP addresses. Masks can be specified as network masks or a plain number. e.g. 192.168.1.0/255.255.255.0 or 192.168.1.0/24

Guarddog's main interface consists of four tabbed windows labeled Zone, Protocol, Logging and Advanced (Figure 4). The Zone tab comes with two predefined zones. Local refers to traffic bound for the local address. Internet, on the other hand, is traffic leaving your system and bound for the Internet. This is very important. Guarddog makes it relatively easy to create complex firewalls using demilitarized zone (DMZ) configurations, multiple cards and so on. For now, let's concentrate on a basic desktop firewall configuration. That's one machine connected to the Internet.

As soon as you start Guarddog (command name `guarddog`) and click Apply, your firewall is activated with all inbound and outbound traffic blocked. As this is a highly restrictive configuration, you are quite safe. Maybe a little too safe—nothing gets in or out; one good reason why you might want to experiment with it by running nonroot in the beginning. This isn't quite as strange as it might seem at first. More complex firewalls with systems in a DMZ are routinely blocked from the internal network with only a few external services turned on. Should you get yourself in a overly secure corner, click the Advanced tab, check the Disable firewall box in the upper left-hand corner, then click the Apply button at the lower right. The Advanced tab also has a button to return your Guarddog configuration to its all-restrictive factory defaults.

One way or another, we need to permit some traffic. Click on the Protocol tab, and you'll see a list of categories representing different types of traffic. They are Chat, Data Serve, File Transfer, Game, Interactive Session, Mail, Media, Miscellaneous, Network and User Defined.

Each has a plus sign beside the category with individual protocols listed in a submenu. Click on each protocol, and you'll see a short description in the bottom-left pane along with an appraisal of the security risk the protocol represents. To the right of each protocol name is a check box. By clicking on the box, each protocol can be blocked, permitted or rejected (Figure 5). As I have mentioned, the port is blocked by default. Click once and the protocol is permitted. Click again and the packet is rejected.

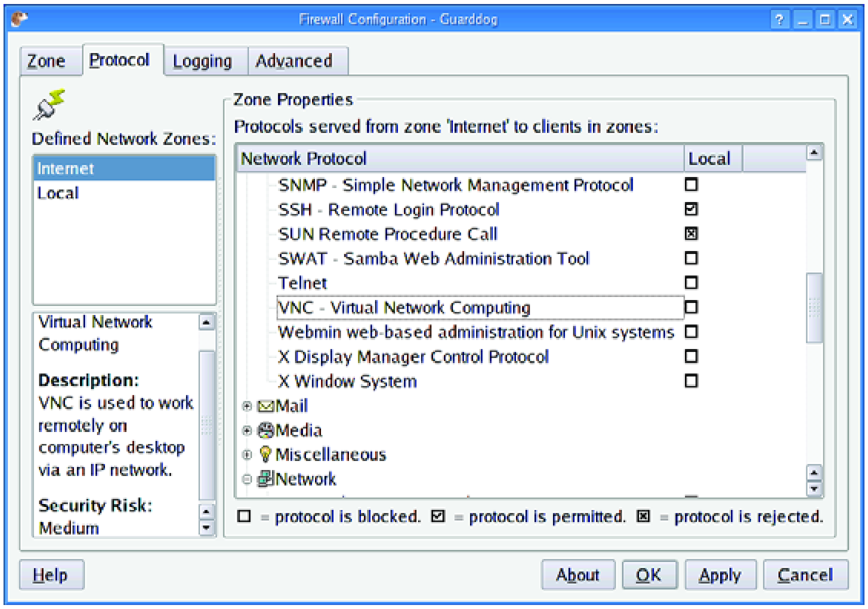
Given the restrictive nature of this firewall, I started out by going down the list of protocols in the Internet zone and permitting everything I needed (for example, instant messaging, e-mail, Web browsing and so forth). This is what you want for a desktop workstation where pretty much all outbound traffic is permitted. Once you have made your changes, click the Apply button at the bottom of the main window to activate your new firewall configuration. A small pop-up window will warn you that any change to a live firewall could have an impact on existing connections. Click Continue to reactivate the firewall.

If you are running some kind of server (such as Samba file sharing), you can almost hear the cute little dog snarling, *non*? Perhaps you also run the secure shell (SSH), so that you can access this computer from another in your home or office. Click on the Local zone and select those protocols you serve. Remember, this is inbound traffic now, so you probably don't want to be quite as generous.

On that note, I fear that closing time is almost upon us. No need to rush out though. My faithful waiter, François, will happily refill your glasses one final time before we say, "*Au revoir*". Please raise your glasses, *mes amis*, and let us all drink to one another's health. *A votre santé! Bon appétit!*

Resources for this article: www.linuxjournal.com/article/8745.■

Marcel Gagné is an award-winning writer living in Mississauga, Ontario. He is the author of the all new *Moving to Linux: Kiss The Blue Screen of Death Goodbye!* 2nd edition (ISBN 0-321-35640-3), his fourth book from Addison-Wesley. He also makes regular television appearances as Call for Help's Linux guy. Marcel is also a pilot, a past Top-40 disc jockey, writes science fiction and fantasy, and folds a mean Origami T-Rex. He can be reached via e-mail at mggagne@salmar.com. You can discover lots of other things (including great Wine links) from his Web site at www.marcelgagne.com.



Defined Network Zones:
Internet
Local

Zone Properties
Protocols served from zone 'Internet' to clients in zones:

Network Protocol	Local
SNMP - Simple Network Management Protocol	☐
SSH - Remote Login Protocol	☑
SUN Remote Procedure Call	☒
SWAT - Samba Web Administration Tool	☐
Telnet	☐
VNC - Virtual Network Computing	☐
Webmin web-based administration for Unix systems	☐
X Display Manager Control Protocol	☐
X Window System	☐
⊕ Mail	
⊕ Media	
⊕ Miscellaneous	
⊖ Network	

Virtual Network Computing

Description:
VNC is used to work remotely on computer's desktop via an IP network.

Security Risk:
Medium

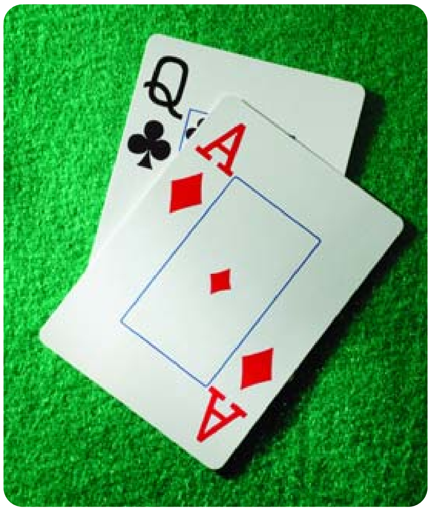
☐ = protocol is blocked. ☑ = protocol is permitted. ☒ = protocol is rejected.

Figure 5. Guarddog protocols are permitted, blocked or rejected with a click of the mouse.

DAVE TAYLOR

Writing a Shell Game

Bash a little time away with *Blackjack*.



We've spent the last three columns talking about the basic nuts and bolts of shell script programming, so I think it's time to start digging into a real shell script, and build something interesting and useful. Well, interesting, at least!

What I would like to do—and up front I admit that this might be a crazy hard problem for a shell script—is to try to write a rudimentary *Blackjack* game. It's simple enough that it should be manageable, but it's hard enough that we'll really have to flex our scripting muscle to get everything working. Needless to say, it won't have a fancy graphical interface!

Onward to Vegas

We'll go into the specific rules of *Blackjack* as needed, but for now all you need to know about *Blackjack* is that each player gets two cards from a deck of standard playing cards, and that players can then request additional cards, trying to get their point total as close to 21 as possible, without going over that value. All face cards are worth 10 points each, and an Ace is worth 1 or 11, depending on how the player wants it to count.

The first challenge is to create a virtual deck of cards, but this is easier than you might think, because it can be represented simply by an array of 52 elements, with the first 13 representing one suit, the second 13 a second suit and so forth. So, card #37 might be a Jack of Hearts, for example.

It turns out that shell scripts can use arrays, so let's start by creating a 52-element array and populating it with the values 1–52:

```
card=1
while [ $card -lt 53 ]
do
  deck[$card]=$card
  card=$(( $card + 1 ))
done
```

If you're used to Perl, you might be thinking that a for loop would be a more logical choice for this sort of task, but for loops in shell scripts lack the ability to step through a range of values. Arrays in the Bourne Shell are easy to work with: simply specify a reference index and the array will be grown to that size dynamically.

Now we have a representation of a deck of cards, but it's perfectly sorted, so the next step is to write some code that will shuffle the deck. This proves to be a bit more tricky, as you might expect!

The basic idea is that we'll randomly pick a number between 1 and 52, and then see if its card is available or not. So the initial deck we created that's sorted is used as the source for the shuffled deck, which will actually end up in a new array. Here's the basic piece of code for the random card selection:

```
while [ $errcount -lt $threshold ]
 do
    randomcard=$(( ( $RANDOM % 52 ) + 1 ))
    errcount=$(( $errcount + 1 ))

    if [ ${deck[$randomcard]} -ne 0 ] ; then
      picked=${deck[$randomcard]}
      deck[$picked]=0         # picked, remove it
      return $picked
    fi
 done
```

There's a lot to see here, but let's talk about the basic logic first: although we're going to pick a card randomly between 1 and 52, and then see if it has already been picked, we also need to make sure we don't end up trapped in an infinite loop because of a mediocre random number function. That's managed by keeping track of the number of guesses you have to make with the

Flexibility to power the enterprise.

From mail servers to databases, ZT X9000 series servers powered by the 64-bit Intel® Xeon® Processor can run the full range of 32-bit applications and offer extended flexibility for your 64-bit needs. So you can create powerful, all-purpose IT infrastructure that enhances business agility – and the bottom line.

ZT Revolution 4U Server X9544

Dual Intel® Xeon® Processors 3 GHz
(2MB L2 Cache, 3 GHz, 800MHz FSB)

- Intel® E7520 Chipset Server Board
- 2GB ECC Registered DDR 333MHz SDRAM (Up to 16GB)
- 1 x Seagate® 36GB 15,000rpm SAS Hard Drive (O/S)
- 3 x Seagate® 73GB 15,000rpm SAS Hard Drive (Raid 5)
- 6 x 1" Hot-swap SAS Drive Bays
- 64bit High Performance SAS RAID Controller
- 16x DVD-RW & Floppy Drive
- 2 x Intel® Gigabit NIC Controller
- 2U Rackmount Chassis w/ 500W Redundant Power Supply
- Super Doctor III Server Management Software
- 3-Year Limited Warranty

FREE SHIPPING ! **$4,499**

ZT Optimum Tower Server X9554

Intel® Xeon® Processor 3 GHz
(2MB L2 Cache, 3 GHz, 800MHz FSB)

- Intel® E7320 Chipset Server Board
- 1GB ECC Registered DDR2 400MHz SDRAM (Up to 8GB)
- 4 x Seagate® 250GB SATA 8MB Cache Hard Drive
- 4 x 1" Hot-swap SATA Drive Bays
- 4 Channel SATA RAID Controller (RAID 0,1,5 &10 Supported)
- 16x DVD-RW & Floppy Drive
- 2 x Intel® Gigabit NIC Controller
- Mid-Tower Chassis w/ 650W Redundant Cooling Power Supply
- Microsoft® Windows® SBE Server 2003 STD w/ 5 CAL
- Super Doctor III Server Management Software
- 3-Year Limited Warranty

$2,299

ZT Extreme Quality Workstation DC X6006

Intel® Pentium® D Processor 840
(2 x 1MB L2 Cache, 3.20GHz, 800MHz)
genuine Microsoft® Windows® XP Professional Edition w/ SP2

- Intel® D945GM Chipset Mainboard
- 1GB DDR2 667MHz Dual Channel
- 2 x Seagate® 250GB SATA2 8MB Cache Hard Drive (RAID 1)
- Up to 8 Drive Bays for Hard Drive Ungradable
- On-board RAID 0,1,5 & 10 Supported
- 16 x Dual Layer DVD±RW Drive
- Intel® 10/100/1000 LAN & IEEE 1394
- Mid Tower Chassis w/ 380 Watt Silent Power Supply
- Internet Pro Keyboard & Optical Mouse
  (Bundle 14 Free Programs Over $800 Value)
- 3-Year Limited Warranty

FREE SHIPPING ! **$1,399**

- 3 year warranty with lifetime tech support
- Reseller and volume pricing available.
- Personal attention (Dedicated Technical Sales Team)
- Call now to customize using the latest technology

Find out how ZT can help maximize your Business Solution

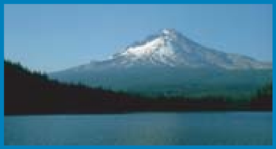
Go to **ztgroup.com/go/linuxjournal**

Call **866- ZTGROUP** (866-984-7687)

promote code : Lj0306

ZT GROUP

Purchaser is responsible for all freight costs on all returns of merchandise. Full credit will not be given for incomplete or damaged returns. Absolutely no refunds for merchandise returned after 30 days. All prices and configurations are subject to change without notice and obligation. Opened software is non-refundable. All returns have to be accompanied with an RMA number and must be in re-sellable condition including all original packaging. System's picture may include some equipments and/or accessories, which are not standard features. Not responsible for errors in typography and/or photography. All rights reserved. All brands and product names, trademarks or registered trademarks are property of their respective companies. Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, Pentium, and Pentium III Xeon are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.



variable errcount. The threshold can be adjusted to allow more or fewer guesses for each card. I have it set to 10 as a default value.

You can see that working with arrays makes variable references quite a bit more tricky. Setting the value isn't too bad, as shown earlier, but referencing the array requires the addition of curly braces, so the reference to `${deck[$randomcard]}` is to the randomcard slot in the array deck.

Otherwise, don't let all the notation distract you as this is a fairly straightforward loop. Try *threshold* times to pick a card randomly out of the array *deck* that hasn't already been chosen (for example, had its value set to zero rather than the initialized value).

The other interesting piece of this code block is the RANDOM variable. Every time you reference $RANDOM, you get a different number between zero and MAXINT (a very large integer value), automatically, without having to initialize anything or do any special work. Try it yourself by typing `echo $RANDOM` at the Bourne Again Shell command prompt.

This isn't the full code segment, because we also need to have a fall-through, a block of code that is used when the random guesses don't produce a desired card and we instead need to step through the array deck linearly to find one that's available. Typically, it'd be used only at the very end of the shuffle when there are only a few cards left. This code looks like:

```
randomcard=1

while [ ${deck[$randomcard]} -eq 0 ]
do
   randomcard=$(( $randomcard + 1 ))
done

picked=$randomcard
deck[$picked]=0              # picked, remove it
return $picked
```

This should be even easier to read now that you're becoming familiar with arrays.

I'm going to stop here for this month, and we'll pick up the card shuffling task again next month, including an explanation of how to make it a shell function and utilize it in the main game script itself. Stay tuned!■

Dave Taylor is a 25-year veteran of UNIX, creator of The Elm Mail System and most recently author of both the best-selling *Wicked Cool Shell Scripts* and *Teach Yourself Unix in 24 Hours*, among his 16 technical books. His main Web site is at www.intuitive.com.

Introductory Bundle: Two ZonePlayers and Controller

DOC SEARLS

The Sound of Linux

Getting wowed by the Linux-based Sonos Digital Music System.

On November 25, 2005, I wrote "Building an Open Source House" (see the on-line Resources) on the *Linux Journal* Web site. Mostly, I was looking for some last-minute (or -week) advice about equipment and wiring before we put up sheetrock at the new house we're building. We should be in the house by the time you read this. It will be our seventh home in seven years, and hopefully our last for a long time.

It's a dream home on a Santa Barbara hillside overlooking the town and the ocean. It's also a Faraday cage, with 11 tons of steel girders inside its walls and under its decks, thick fieldstone and stucco on its exterior and a roof of solid copper. It's not a reception-friendly place for an old radio freak like myself—but hey, some compromises are easy to make.

One compromise I wasn't willing to make was with unnecessarily proprietary audio, video and Internet-based services. I didn't want anything that put us inside some company's silo.

The same went for lighting. My wife rejected a variety of centrally controlled lighting "solutions", because they all required dependencies on specialized professionals with exclusive relationships with manufacturers of specialized gear that could be operated only by specialists using old Windows laptops with serial ports that plugged in to central control units in the garage. Not to mention light switches with labels corresponding to moods and stuff. Plus, prices four times to *X* times higher than plain-old light switches that anybody can understand.

There are lots of ways you can go down the same expensive dead-end route with, say, home theater equipment or whole-house audio. I have a friend with a whole-house audio setup that nobody knows how to operate, including himself and the outfit that sold and installed it. Last summer, I asked for advice from Mark Cuban, the billionaire owner of the Dallas Mavericks and founder of HDnet, which supplies programming to high-definition TV customers. He told me it was a big mistake to build a proprietary whole-house audio system. He did that the first time around and regretted it. "Go open", he said. "It's the only way."

That is why I wrote that piece on the *Linux Journal* Web site.

In it, I explained that, for the last few houses, my open audio distribution system has been a simple FM radio hack. At the main sound source (usually the receiver at the middle of our home theater setup in the family room), I put a Ramsey FM-100 transmitter, which radiates on an otherwise unused FM channel. The power is only .25 watts, and the signal barely gets out past the yard, but it's plenty strong inside the house where receivers in other rooms pick up and play the signal off their FM tuners. Most of our receivers are ones we grabbed cheap at garage sales. They have analog dials, with simple knobs for volume and tuning, and they sound great through speakers that are just as good. In our nine-year-old son's room is a great old mid-1980s Technics receiver that puts about 50 watts per channel through a pair of original Advent loudspeakers. The receiver cost $5 US at one garage sale, and the speakers cost $10 US at another. Next to the receiver is a Technics turntable with a Shure phono cartridge that sounds better playing my old Deutche Grammaphone vinyl recordings of Beethoven's nine symphonies (the 1963 series, with Herbert von Karajan, purchased almost that long ago) than the CD player spinning the same recordings remastered in digital form.

Sonos Controller

Still, FM is not the best medium for hi-fi audio. What would be better, if anything, that isn't some kind of silo?

In my *LJ* Web site piece, I mentioned the Sonos system, which I had written up in a small feature in November 2005's *Linux Journal*. Sonos sells high-quality amplifiers called ZonePlayers that each drive pairs of speakers and connect to each other wirelessly. These connect to audio collections on PCs or network-attached storage (NAS) devices to line-in sources (such as satellite radio, cable or satellite TV, iPods or whatever) and radio streams from the Net itself. I also had seen Sonos at CES last year and liked what the system did. I also said it appeared to be a silo.

One reader of the Web piece was Alan Graham, a writer whose works include a book, *The Best of the Blogs*, for which I had contributed the forward a couple years back. Alan wrote to tell me that I had not only misjudged Sonos, but that I should avail myself of the company's proximity to my house. Somehow, I had missed the fact that Sonos was right here in Santa Barbara. In fact, it was only a few blocks away. Most important, they had built out the whole Sonos system on Linux, and might make a good story.

So, I went over to check the place out, talk with some of their Linux hackers and see what was up with the company.

I've been to a lot of startups. Usually they're in funky industrial quarters on the cheap side of the railroad tracks. Not Sonos. Instead, they're in one of the most attractive Spanish buildings in a Spanish town that's been doing Spanish since the 1700s. The digs are a mix of offices and cubicles, with a staff energy that's as upbeat and positive as any I've seen. Although they wouldn't give me financial specifics, they did say they've grown every month.

More important, everybody seemed engaged. "What Internet station do you like?" one guy asked. I told him WUNC in Chapel Hill. "Cool", he said. "We'll add that to the selection." When figuring the IP address of WUNC's stream proved a bit problematic, other geeks joined in and they surmounted the problem. I overheard "What can we do for you?" and "How can we help?" several times while touring the facility.

At the end of the tour, I sat down with Steve Holmgren, a principal engineer at the company and a UNIX/Linux hacker of long standing.

Turns out Sonos grew out of networking: "We asked, 'How do we bring basic technologies from the Internet, and from the Open Source world, into the home?'", he said. "We started very early on looking at everything, including Microsoft's embedded technologies. Obviously there were costs there. Meanwhile, we had a lot of background in UNIX and Linux, and knew it was a lot more approachable."

Also flexible—Steve continued:

> One of the things that got us there was evaluations of microprocessors. With Linux, we could develop software independently of hardware. We could do development, and bring up all our services, long before the hardware was ready. In fact, we could architect the whole thing in the complete absence of hardware. We put together a simulator for our controller on X Windows, with a prototype handheld scroll wheel and everything else. We put in a Flash interpreter that runs on top of that, so we could do a nice graphical display. All of that was running way in advance of any hardware. Linux allowed us to do that.

This was also a relief. Steve continued, "I've been involved in so many projects where all you heard was 'We're waiting for the hardware.' There were all these serialized dependencies. Not the case here. We had a great deal of parallelism in development. We could get way downstream much earlier than we would have otherwise."

As for the development itself, he said:

> It's all C and C++ running on our own embedded Linux implementation. We did it all from the ground up. We started with Red Hat because that's what we knew best, but then we pulled in whatever we needed for our own purposes. We started developing on the 2.4 kernel, so we've stuck with that. We're an embedded implementation, constrained on memory and don't have big iron needs, so we're happy there. We write a lot of our own stuff. We have a loadable audio driver module that we wrote and pulled in, for example. In fact, we did development on a PC-based Linux box and cross-mounted that with a development system via NFS, booted the system dynamically across the Net, brought over the driver module and debugged it. We did that over and over again. Nice integration, booting up embedded boards, things like that.

The microprocessor they ended up using was the Hitachi SH. "We liked the floating point and the PCI interface that's built in to it", he said. A fun coincidence—back around the turn of the 1990s, I worked with Hitachi Semiconductor on rolling out the SH in the US. (One rumor had it that the processor was named after Sonic the Hedgehog. Sega was a big Hitachi customer back in those days.)

"We're steeped in Linux here", Steve said. "It's part of the infrastructure. We have it so tuned at this point that I couldn't imagine ever doing anything else. It's wide open. If we ever want to change hardware, we can do that easily. We're flexible that way. If another processor vendor comes along with better features and pricing, we have the ability to move."

Linux and open source are also involved in the company's own central service offerings out to customers:

> We have a network server that implements SOAP, is open source and publicly available on SourceForge. It's called Anacapa. We named it after Anacapa Street here in Santa Barbara, but later I found out that it's also a Chumash word that means "constantly changing", which makes complete sense. We use it in our support infrastructure. We can come into the customer's system and gather statistics, do diagnostics and provide services. There are an enormous number of statistics that we can put to use—error logs and so on. All HTML- and XML-based.

I said, "So what you've got is a wireless home LAN that serves as an audio system and that can publish, by HTTP and XML, stats out to Sonos itself, to do diagnostics and stuff like that?"

"Yes", he said. "And we use SOAP as a control architecture to run commands between the different nodes. It's a peer-to-peer level mesh network. So its stable and very reliable."

"Is there one central unit that needs to be wired?" I asked.

"There is one that needs to be connected by Ethernet to the router. That's more for performance than anything else. Beyond that, they can all be wireless. You can have any combination of wired and wireless. You have fantastic audio quality, and you don't lose anything with N nodes. It's endlessly extensible."

But still, I wasn't sold. For that, I needed to set up a couple of ZonePlayers in my own house and put them through the paces.

So I took advantage of their Introductory Bundle: two ZonePlayers and a Controller for $1,199 US. There's a 30-day money-back guarantee, "no questions asked", they say. Two business days after my visit, the bundle showed up on my doorstep.

I hooked one up to the speakers in the family room, and the other to the speakers in the living room (which in this house are in opposite corners of a long L). Now, I needed to get both of them on the Net. For that, the back of each ZonePlayer has a four-port 10/100 switch. Each port has a light to indicate activity, which is handy. In our house (which we remodeled a couple years ago), every room has several RJ45 wall jacks connected by CAT-5e cabling to a patch panel in the wall of a bedroom closet upstairs. Each ZonePlayer came with an Ethernet cable, so I used one of these to connect the family-room player to a wall socket, then went upstairs, opened the wiring panel and patched the connection through to a hub connected to our Cox Business Internet cable modem. Then I followed directions that came with the gear and quickly realized we weren't getting out on the Net. A call to their 800-number got me immediately to David, a support guy working in Sonos' offices down the street (rather than somewhere in India or wherever companies put their outsourced tech support these days).

After a brief geek-to-geek conversation, I remembered Cox requires that I let them know the MAC address of everything new on the local network. This is easy with ZonePlayers, because the serial number on the back of each unit is also its MAC address. But I didn't want to make more calls, so I went upstairs and patched the ZonePlayer through the hub from our Cox High Speed Internet household service, which isn't so picky and has faster downstream speeds anyway (3Mb vs. 1.5Mb for the business, which is also more expensive, but

ONE COMPROMISE I WASN'T WILLING TO MAKE WAS WITH UNNECESSARILY PROPRIETARY AUDIO, VIDEO AND INTERNET-BASED SERVICES.

THE MOST REMARKABLE THING ABOUT THE SONOS SYSTEM IS THE WIRELESS NETWORKING, WHICH IS ROBUST BEYOND ANY OF MY EXPECTATIONS.

that's another story). We were on.

I registered the service, and things began to roll. I got the other ZonePlayer on the wireless mesh, using only the controller, which looks like a wide-bodied white iPod. It features a scroll wheel, buttons for Zones, Music, back (|<<), forward (>>|), pause (||) and going up a level (one of those bent arrows that looks like a sideways U). There are also three soft buttons along the bottom of a large and vivid color display. The volume control is a +/– rocker switch, and you use the scroll wheel to choose which zones it's controlling. You can control the volume for any or all of the ZonePlayers, which you select with the scroll wheel. Each ZonePlayer also has its own mute and volume controls.

For music, you press the music button and navigate with the scroll wheel. The bull's-eye button makes your choices. Getting the hang of it is easy.

Each ZonePlayer comes with a CD that installs control software for Windows or OS X. In addition to providing a console for monitoring and controlling the system, it administrates the music library served over the system from the desktop.

When I observed the absence of a Linux version of the same software, I was transferred to Sean Sullivan in the company's Cambridge, Massachusetts office. Sean said he uses nothing but Linux at home (all Gentoo) and doesn't miss the desktopware. "I get along fine with just the handheld controller", he said. "All my music is on a NAS box." In fact, he recommends keeping music on a network-attached storage device in any case. "Your basic NAS is a Linux box running Samba", he said. With the handheld controller (another Linux device), you simply enter the Samba address of the NAS, and there's your music. Sean is partial to Buffalo Tech products, by the way. He says "that's mostly what you see when you walk around the company." He also said there was nothing other than market demand keeping the company from making Desktop Controller software for Linux. "It's just UPnP", he said. UPnP stands for universal plug and play.

To test it out, I installed the Sonos Desktop Controller on an old OS X laptop that has a large pile of MP3s on it. In very little time, that same music was now on the handheld controller, ready to play. Given how lame that old box is, the performance was remarkable. The controller roughly replicated the functionality of an iPod. In fact, you might think of the Sonos system as a very flexible whole-house iPod, without Apple's proprietary silo.

Even though I have a large MP3 collection (mostly ripped from many shelves of CDs, plus an assortment of old vinyl albums), I'd usually rather listen to Internet radio. Veteran *Linux Journal* readers know I've been harping about Internet radio since the late 1990s. For all those years, I've wanted an Internet radio that's easy to tune and that can play through a good household sound system.

Well, now I have it. And I'm in love.

Sonos provides customers with a large assortment of stations, sorted by genre. More can be added through the desktop software, once you find the URL of the stream you want. I did, and promptly added a half-dozen favorites. You can also contact Sonos and ask them to add stations to the defaulted list. "We love it when people do that", said a customer-support guy.

Each ZonePlayer also has a line-in input, through two RCA jacks, so you can play a CD player, an FM tuner, an MP3 player and anything else you want through it. I jacked in a new Sirius Satellite Radio tuner, and it worked perfectly.

ZonePlayers also have a pair of line-out jacks, along with a subwoofer jack as well. I eagerly hooked these up to my Ramsey FM transmitter to drive my legacy audio distribution system—and was met with my first and only disappointment with the Sonos system. It turns out that the line output is volume-controlled. So, if that ZonePlayer is turned down or muted, so is the line output.

This means I can't drive the FM transmitter with it—or anything else I can imagine. After a series of phone calls and e-mail exchanges, I learned that fixed line output should be a selectable feature by the time you read this.

Meanwhile, I'm requesting it anyway, on the company forum. I'm also requesting a Linux version of the desktop software, plus the ability to add stations through the Controller. Given the openness and responsiveness of the Sonos staff, I'm optimistic about all those requests—plus lots of others I see when I cruise the forums' threads.

The most remarkable thing about the Sonos system is the wireless networking, which is robust beyond any of my expectations. A few months back, we experimented here at the house with Apple's AirTunes system, which sends audio from iTunes on a laptop through an Apple Airport Extreme Wi-Fi base station to an Apple Airport Express Wi-Fi base station, and out that through a stereo headphone jack to our family-room audio system. It failed. The signal dropped out constantly, and it was vulnerable to people walking around the room. None of the devices involved were more than 20 feet from each other. With the Sonos system, the two ZonePlayers are at opposite corners of the house. One is located alongside a Linksys Wi-Fi base station that can't even be picked up on a laptop at the other ZonePlayer location. Yet the music through the second ZonePlayer sounds beautiful, with no drop-outs at all. Internet radio, which sometimes has problems staying connected in iTunes, is rock solid. Last night, we were listening to jazz and classical stations from France, The Netherlands, Norway and North Carolina. Nothing dropped out. Nothing was degraded. And each station came up almost instantly when we tuned from one to the other.

What's more, the Sonos system gets along with all four of our household Wi-Fi stations, plus any number of laptops that come and go, plus our 2.4GHz Panasonic home PBX, which has a total of six stations, all working perilously close to the Wi-Fi band. Sonos tech-support guys told me Panasonic 2.4GHz stuff sometimes causes problems, but we have had none in our case.

I had thought at first that the Sonos was something of a silo, because it used the Wi-Fi band in a nonstandard, nonvisible way. But one of the technicians told me the purpose for that was neither lock-in nor secrecy: "We just don't want to interfere with anything else you've got going on."

And they don't.

The Sonos gear isn't cheap. ZonePlayers run $499 US and controllers run $399 US. Two things help rationalize the purchases. One is that many features of both are software-upgradeable, so they're future-proofed to a degree that's become uncommon in home electronics, much of which is made to be tossed out in two or three years. The other is that they are very solid and well made. Each ZonePlayer is smaller than a shoebox and has the heft of a storage battery. When I toured Sonos' facilities, I was impressed by the quality and construction of the ZonePlayers I saw disassembled on desks and workbenches.

Audio performance is also terrific. The 50-watt per-channel output spec may seem underpowered, but these ZonePlayers seemed no weaker than the 60-watt Pioneer and the 100-watt Technics receivers they replaced at the two locations. And the sound seemed better to me in both cases.

The system will play MP3, AAC/MPEG-4 and WAV audio files. It won't play DRM'd files like the AAC variety sold by Apple on its Music Store or similarly crippled offerings from the Windows Media silo. (It would be nice to see OGG added to the list. I'll request that too.)

Of course, there are other choices in the same market category. Among the responses that came to my original request for help were several pointing to Slim Devices' SqueezeBox, a Linux-based player and controller that works with music sources on your PC (including Linux PCs). My old friend Andrew Leyden of PenguinRadio also pointed to his company's Solutions WebRadio. There are others as well. If you're in the market, I suggest kicking all tires.

Meanwhile, I'll be keeping my Sonos bundle.

Resources for this article: www.linuxjournal.com/article/8753.■

Doc Searls is Senior Editor of *Linux Journal*.

[HARDWARE]

Let Your Finger Do the Booting

FingerGear offers Linux on a stick. JAMES TURNER

To begin, we need to indulge in a little truth-in-advertising exercise. FingerGear's Computer-On-a-Stick is not, in fact, a computer of any kind. There's nary a processor to be found on the little beastie. What it is, in fact, is a nicely packaged bootable Linux image squeezed onto a USB memory stick along with some NVRAM to let you store content. When you plug it in to a late-model PC that supports booting from USB storage devices and tell the BIOS to boot from it, it fires up a 2.6-based Debian Linux distribution, preconfigured with Firefox, OpenOffice.org, Evolution and Gaim. The processor, system memory, graphics card, networking and display of the host system are used.

The first time you boot off the stick, it sets up a password so that if stolen, people can't get their hands on your data. Beyond that, it's a single-user device, so no multiple desktop environments are going to be happening. The innovating thing (and what sets the FingerGear product apart from a bootable CD) is that your home filesystem and all other system configurations move around with you, stored on up to 1GB of nonvolatile RAM. The 256MB sticks start at $99 US, with the 1GB versions at $179 US. The intended use is for road warriors who may find themselves at a client with time to kill and a PC in front of them. By plugging in the stick, they are instantly set up to read their mail, continue editing documents they have been working on and chat with their friends via IM, without the hassle of configuring the local mail client on the client's PC and so forth.

I tested the unit on a Toshiba laptop and the *Linux Journal* test PC (an AMD 3200+). In the case of the laptop, there is no option to boot from USB devices, so I used the enclosed mini-CD to do the initial boot, after which the FingerGear stick took over. Unfortunately, in spite of the recent 2.6 kernel, it totally failed to recognize my Wi-Fi chipset. Of course, if you've already got a laptop, why are you using the FingerGear product?

Testing on the *Linux Journal* test system was more fruitful. Although the BIOS supports booting from a USB device, I got the ever-helpful "Boot failed" message when I tried. Again, booting from the mini-CD solved the problem. Once up, DHCP automatically configured the networking and I was off. Firefox worked fine, and I was even able to do things like install the Macromedia Flash plugin. The Office suite performed as expected. Boot time was nearly instantaneous.

The Computer-On-a-Stick is a clever idea, but one has to question the practicality of the intended use. I kept finding myself envisioning attending a typical tradeshow and proposing to the staff running the public press PCs that I be permitted to reboot one of their PCs. The same thought applies to most corporate network admins. You could, of course, apply the "It is better to ask forgiveness than permission" maxim, but it wouldn't be advisable most places I've worked. The "plug it in and it works" networking would probably also have difficulties in any setting with extensive firewalling and proxy configuration required. So I'm not sure how many settings would actually work out practically with the FingerGear concept.

There's also the issue of security. Properly packed with a hacker toolkit, one of these sticks could be the ultimate penetration tool. Boot it up, and own the attached network. Thankfully for the sleep of administrators around the world, the current release of the product doesn't provide any way to access the local disk. However, FingerGear has indicated that a future product will allow just that functionality, which, under friendly conditions, would let an administrator boot up a toasted disk drive and fix things. Under less-sincere circumstances, it would be just the toy to go data-raiding in any physically accessible computer you happened across.

In summary, the Computer-On-a-Stick is a nice idea that may be the right solution for you. Whether it is or not will depend largely on what type of computers you plan to use it with. If you frequently find yourself in locations with generic computers that you will have permission to reboot, it will definitely let you surf, read mail, edit documents and IM without leaving a trace on your hosts' computers. But if the thought of rebooting other people's systems makes you nervous, you might just want to settle for a plain memory stick and other solutions, such as Web mail.■

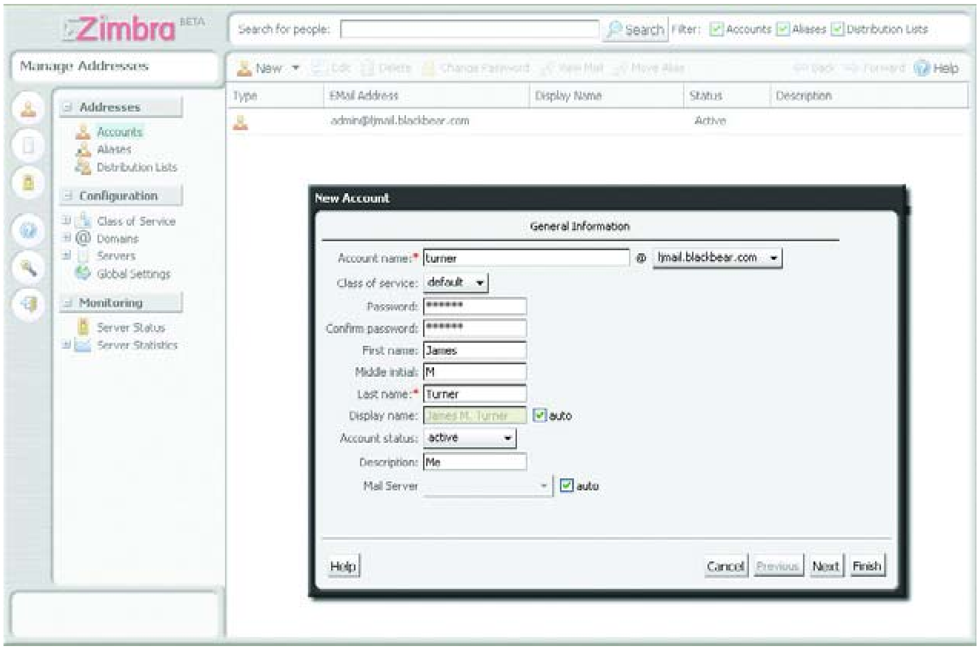
VENDOR: FingerGear
URL: www.fingergear.com
PRICE: $99 US for the 256MB stick; $179 US for the 1GB stick

James Turner is Product Review Editor for *Linux Journal*. He has written two books on Open Source Java development and is a Senior Software Engineer with Axis Technology, LLC.

[SOFTWARE]

Battle of the Ajax Mail Packages

Scalix and Zimbra offer promising e-mail solutions that exploit Ajax to offer rich Web clients. JAMES TURNER



Type	EMail Address	Display Name	Status	Description
	admin@lmail.blackbear.com		Active	

New Account

General Information

Account name:* turner @ lmail.blackbear.com
Class of service: default
Password: ******
Confirm password: ******
First name: James
Middle initial: M
Last name:* Turner
Display name: James M. Turner ☑ auto
Account status: active
Description: Me
Mail Server ☑ auto

Figure 1. Both products come with a Web-based administration interface.

Traditionally, there have been two paths to choose from when considering mail servers. The Redmond path was some variety of Microsoft Exchange Server with Outlook as the client, and possibly POP3/IMAP and Web mail as a backup when out of the office.

The other path, the path of the penguin, was Sendmail or Postfix, or possibly a more obscure mail transport agent (MTA) with POP3 and IMAP as the connection to the mail client of your choice. If you wanted Web mail, you'd use a package such as SquirrelMail running under Apache. There were, of course, other choices, such as Lotus Notes, but by and large, most e-mail installations used one of these two solutions.

Recently, the e-mail landscape has changed dramatically. For one thing, rich client tools such as Gmail and Yahoo Mail have shown the promise of Ajax (Asynchronous JavaScript And XML), taking Web mail from a standby of last resort for travelers to a fully usable replacement for an e-mail application such as Outlook or Evolution. More significantly, several companies either have reached or are very close to the Holy Grail of open-source e-mail, complete Exchange compatibility.

I'm sure there are many die-hard Linux folks out there who are silently saying, "who cares?" But the reality is that in most corporate-IT environments, Outlook and Exchange are a well-entrenched aspect of the company mentality. And, it's hard to blame companies for clinging to them. The terrible twosome are full of useful features, such as meeting and calendar integration, that make them highly useful. On the other hand, it would be difficult to find a Windows sysadmin willing to describe administering an Exchange server as a pleasurable experience.

At last, these beleaguered MCSEs have a choice that doesn't involve dumping Outlook and training their employees to use an entirely new mail system. Projects such as OpenExchange, Zimbra and Scalix promise the ability to phase out Windows-based Exchange servers without the end users noticing.

Two of these projects, Scalix and Zimbra, are particularly promising because they include highly functional Ajax clients as part of their offerings. In this article, we look at the two, head to head.

Zimbra is an open-source project with a proprietary network edition, which includes features such as product support, clustering and, in the future, Outlook connectivity via MAPI. If you can make do without these features, you're free to run the open-source edition and get support in the forums. The network edition isn't cheap though, running you $28 US/user with a 500-user minimum (or $1,500 US for a 50-user small-business license). Significantly, Zimbra is still in beta, although it's well along in the development cycle.

Scalix, in comparison, is fully closed source. It offers two different versions, a community edition and an enterprise edition. As with Zimbra, the enterprise edition will cost you money, and it comes with support. The difference is that the Scalix community edition provides all the functionality of the enterprise edition. However, the advanced features, such as MAPI compatibility (which lets you use Outlook directly with the mail server for calendar and contact management), are available only for 25 users. After that, you'll be paying $60/user.

Installation Quirks

We tested both products under Fedora Core 4. For Zimbra, that and Red Hat Enterprise Linux 4 are your only official Linux choices (at least for a supported, binary install). Scalix offers those distributions as well, but adds several flavors of SUSE to the supported list. Both products install without much hair pulling; you answer a few simple questions (at least, simple if you're familiar with setting up mail servers), and the installation scripts do the rest.

At this point, I need to mention one of the irritating quirks of Zimbra. It installs its SMTP, POP3, IMAP and HTTP/HTTPS servers in high-numbered ports, and then uses iptables to map to them. So, for example, port 80 gets mapped to port 7070, where Zimbra runs its Web-mail client. This can come as a nasty surprise if you install Zimbra on a host with an existing Web server.

By comparison, Scalix keeps all its network ports off existing Web services, although it does take over mail-related ports such as SMTP and IMAP, but that's what you'd expect a mail server to do.

Scalix has its own dangers for the unwary. You had better be familiar with LDAP and how it specifies distinguished names. Scalix is all about LDAP. To be fair, Scalix is trying to operate as a drop-in replacement for Exchange, and Exchange makes heavy use of LDAP in its Active Directory architecture. So this isn't an unexpected development. However, for a sysadmin familiar with Sendmail doing a first-time install of Scalix, a close reading of the documentation is in order.

Configuring the Products

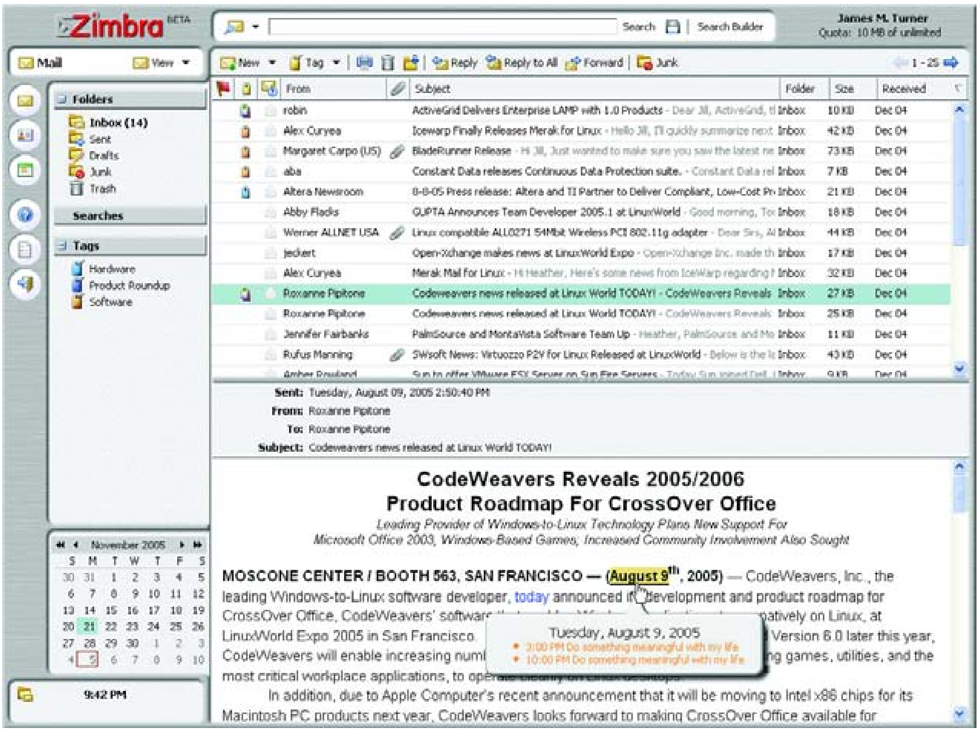
Both Scalix and Zimbra offer command-line and Web-based configuration tools. And in both cases, you can do much more from the command line than you can from the Web. The philosophy seems to be that the Web should be used for ordinary day-to-day operations, such as adding a new user, and the command line is for more complex or less frequently used ones.

One headache both products share is that they have a ton of these command-line programs. Zimbra has 74 programs you can use to control its operation, and Scalix has 341 (yep 341) programs in its bin directory, and they are so closely named that you may go mad trying to remember the differences. For example, try figuring out whether you should be using omdelapppdl or omdelapppdln. As I said, a close reading of the manual is in order before you try anything fancy.

Zimbra comes configured with SpamAssassin and ClamAV already installed. Scalix supports any Milter-based spam and antivirus tools. It wasn't that difficult (with a little help from the very responsive support board when I made a stupid mistake) to install them.

You've Got Mail

There's no question that the Zimbra Webmail interface is both more featureful and colorful. For example, put your mouse over a date and you see the calendar for that date. Mouse over an e-mail address, and you see the contact information for that person. Mouse over a Web address, and you see a thumbnail of the site. Unfortunately, it's still a bit glitchy, especially under Firefox. This is not a good thing for a product that wears an open-source pedigree so proudly. Hopefully, these issues will be resolved before the final release.



From	Subject	Folder	Size	Received
robin	ActiveGrid Delivers Enterprise LAMP with 1.0 Products - Dear Jill, ActiveGrid, tl	Inbox	10 KB	Dec 04
Alex Curyea	Icewarp Finally Releases Merak for Linux - Hello Jill, I'll quickly summarize next	Inbox	42 KB	Dec 04
Margaret Carpo (US)	BladeRunner Release - Hi Jill, Just wanted to make sure you saw the latest re	Inbox	73 KB	Dec 04
aba	Constant Data releases Continuous Data Protection suite. - Constant Data rel	Inbox	7 KB	Dec 04
Altera Newsroom	8-8-05 Press release: Altera and TI Partner to Deliver Compliant, Low-Cost Pr	Inbox	21 KB	Dec 04
Abby Flacks	GUPTA Announces Team Developer 2005.1 at LinuxWorld - Good morning, To	Inbox	18 KB	Dec 04
Werner ALLNET USA	Linux compatible ALL0271 54Mbit Wireless PCI 802.11g adapter - Dear Sirs, Al	Inbox	44 KB	Dec 04
jeckert	Open-Xchange makes news at LinuxWorld Expo - Open-Xchange Inc. made th	Inbox	17 KB	Dec 04
Alex Curyea	Merak Mail for Linux - Hi Heather, Here's some news from IceWarp regarding t	Inbox	32 KB	Dec 04
Roxanne Pipitone	Codeweavers news released at Linux World TODAY! - CodeWeavers Reveals	Inbox	27 KB	Dec 04
Roxanne Pipitone	Codeweavers news released at Linux World TODAY! - CodeWeavers Reveals	Inbox	25 KB	Dec 04
Jennifer Fairbanks	PalmSource and MontaVista Software Team Up - Heather, PalmSource and Mo	Inbox	11 KB	Dec 04
Rufus Manning	SWsoft News: Virtuozzo P2V for Linux Released at LinuxWorld - Below is the la	Inbox	43 KB	Dec 04
Amber Rowland	Sun to offer VMware ESX Server on Sun Fire Servers - Today Sun joined Dell, I	Inbox	9 KB	Dec 04

Sent: Tuesday, August 09, 2005 2:50:40 PM
From: Roxanne Pipitone
To: Roxanne Pipitone
Subject: Codeweavers news released at Linux World TODAY!

CodeWeavers Reveals 2005/2006
Product Roadmap For CrossOver Office

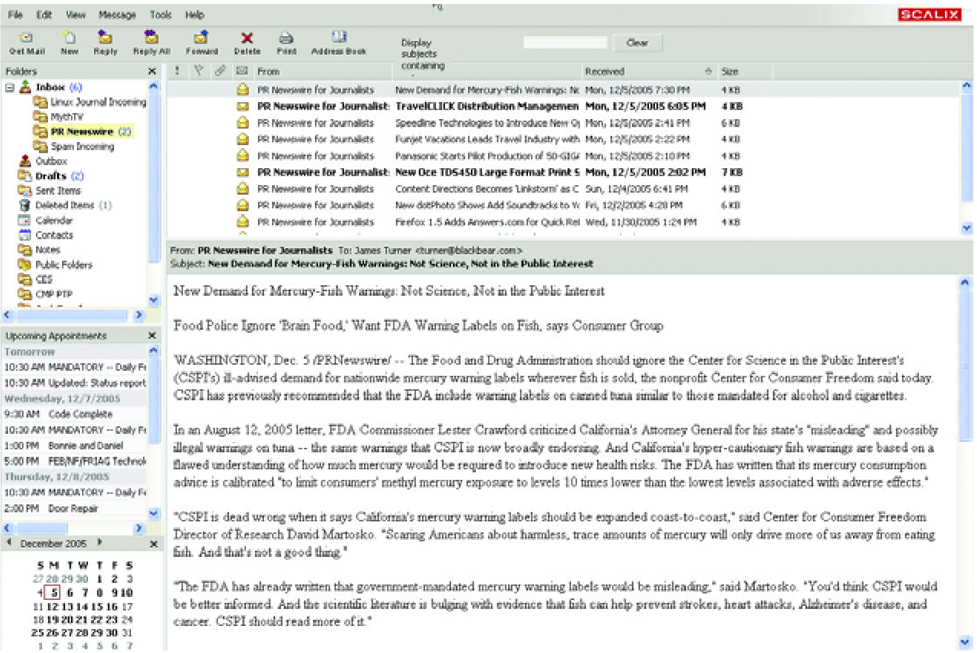
Leading Provider of Windows-to-Linux Technology Plans New Support For Microsoft Office 2003, Windows-Based Games, Increased Community Involvement Also Sought

MOSCONE CENTER / BOOTH 563, SAN FRANCISCO — (August 9th, 2005) — CodeWeavers, Inc., the leading Windows-to-Linux software developer, today announced it development and product roadmap for CrossOver Office, CodeWeavers' softwar … atively on Linux, at LinuxWorld Expo 2005 in San Francisco … Version 6.0 later this year, CodeWeavers will enable increasing num … ng games, utilities, and the most critical workplace applications, to ope…

Tuesday, August 9, 2005
- 3:00 PM Do something meaningful with my life
- 10:00 PM Do something meaningful with my life

In addition, due to Apple Computer's recent announcement that it will be moving to Intel x86 chips for its Macintosh PC products next year, CodeWeavers looks forward to making CrossOver Office available for

Figure 2. Zimbra offers mind-boggling feature-rich Web mail.



From		Received	Size
PR Newswire for Journalists	New Demand for Mercury-Fish Warnings: Nc	Mon, 12/5/2005 7:30 PM	4 KB
PR Newswire for Journalist:	**TravelCLICK Distribution Managemen**	**Mon, 12/5/2005 6:05 PM**	**4 KB**
PR Newswire for Journalists	Speedline Technologies to Introduce New Q	Mon, 12/5/2005 2:41 PM	6 KB
PR Newswire for Journalists	Funjet Vacations Leads Travel Industry with	Mon, 12/5/2005 2:22 PM	4 KB
PR Newswire for Journalists	Panasonic Starts Pilot Production of 50-GIG/	Mon, 12/5/2005 2:10 PM	4 KB
PR Newswire for Journalist:	**New Oce TDS450 Large Format Print S**	**Mon, 12/5/2005 2:02 PM**	**7 KB**
PR Newswire for Journalists	Content Directions Becomes 'Linkstorm' as C	Sun, 12/4/2005 6:41 PM	4 KB
PR Newswire for Journalists	New dotPhoto Shows Add Soundtracks to Y	Fri, 12/2/2005 4:20 PM	6 KB
PR Newswire for Journalists	Firefox 1.5 Adds Answers.com for Quick Ref	Wed, 11/30/2005 1:24 PM	4 KB

From: **PR Newswire for Journalists** To: James Turner <turner@blackbear.com>
Subject: **New Demand for Mercury-Fish Warnings: Not Science, Not in the Public Interest**

New Demand for Mercury-Fish Warnings: Not Science, Not in the Public Interest

Food Police Ignore 'Brain Food,' Want FDA Warning Labels on Fish, says Consumer Group

WASHINGTON, Dec. 5 /PRNewswire/ -- The Food and Drug Administration should ignore the Center for Science in the Public Interest's (CSPI's) ill-advised demand for nationwide mercury warning labels wherever fish is sold, the nonprofit Center for Consumer Freedom said today. CSPI has previously recommended that the FDA include warning labels on canned tuna similar to those mandated for alcohol and cigarettes.

In an August 12, 2005 letter, FDA Commissioner Lester Crawford criticized California's Attorney General for his state's "misleading" and possibly illegal warnings on tuna -- the same warnings that CSPI is now broadly endorsing. And California's hyper-cautionary fish warnings are based on a flawed understanding of how much mercury would be required to introduce new health risks. The FDA has written that its mercury consumption advice is calibrated "to limit consumers' methyl mercury exposure to levels 10 times lower than the lowest levels associated with adverse effects."

"CSPI is dead wrong when it says California's mercury warning labels should be expanded coast-to-coast," said Center for Consumer Freedom Director of Research David Martosko. "Scaring Americans about harmless, trace amounts of mercury will only drive more of us away from eating fish. And that's not a good thing."

"The FDA has already written that government-mandated mercury warning labels would be misleading," said Martosko. "You'd think CSPI would be better informed. And the scientific literature is bulging with evidence that fish can help prevent strokes, heart attacks, Alzheimer's disease, and cancer. CSPI should read more of it."

Figure 3. Scalix: any resemblance to Microsoft Outlook is purely coincidental.

What Zimbra is currently lacking, however, is any kind of direct Outlook support. Even though the Web site claims Zimbra will interface directly with Outlook, this is in fact a TBA feature. So at least for the time being, Zimbra is available only via its Web interface or by IMAP/POP3.

By comparison, Scalix is almost pedestrian in appearance on the Web. If you don't look carefully, you could swear that you're using Outlook. That is probably by design, as Scalix wants to replace Exchange seamlessly. You can do pretty much everything via the Web interface that you can do directly from Outlook, except for anything having to do with mail filtering.

It's when you add the Scalix plugin to Outlook that Scalix really shines, however. I use Exchange on a daily basis at my workplace, and I am now using Scalix for my personal e-mail outside of work. Honestly, there's no practical difference between the two if you use Outlook. The mail-filtering options are a little different, but you really have to look hard to see where the two diverge. Among the more useful features that it shares in common with Exchange is the ability to define filtering rules that run directly on the server. And, because ActiveSync talks to Outlook, you can sync your PDA to your calendar, mail and contacts.

Which to Choose?

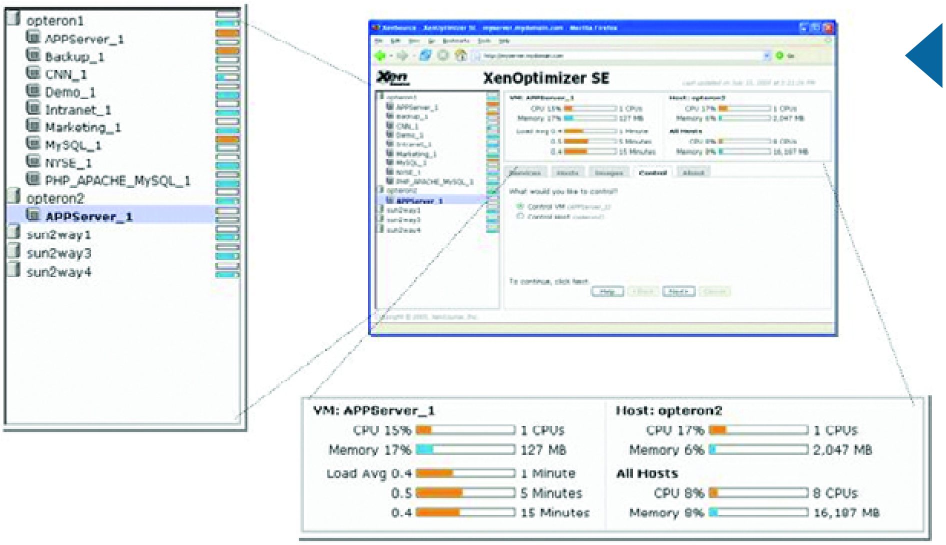
If you're trying to pick one over the other, I'd have to recommend that you start by trying each of them out, because they both have free community editions. Zimbra is probably more of a one-click setup than Scalix, and it definitely involves less in-depth knowledge of things like LDAP. It also has a sweet Web interface that should only get better as it is further developed. On the other hand, it is still in beta as of this writing, and lacks Outlook connectivity.

Scalix shows all the signs of an Enterprise-facing solution. It's less intended for casual users setting up a personal server than for a departmental or corporate environment with many users and complex requirements. That being said, it wasn't that much of a strain to get it set up for my personal domains. But for me, the killer feature is the Outlook connectivity (and especially the free 25 licenses). Until clients such as Evolution become better integrated with PDAs and other groupware technologies, many of us are going to be stuck with Outlook as a mail client, and only Scalix is offering a free solution that everything can talk to.■

See page 76 for more on Ajax in an interview with Ben Galbraith.

James Turner is Product Review Editor for *Linux Journal*. He has written two books on Open Source Java development and is a Senior Software Engineer with Axis Technology, LLC.

www.faircom.com/go/?securelinux
Citibank demands
unrivaled security
for banking applications
at over 4,000 branches.
FairCom database
technology makes
it possible.
FairCom®
Other company and product names are registered trademarks or trademarks of their respective owners. © 2005 FairCom Corporation



VM: APPServer_1
CPU 15% 1 CPUs
Memory 17% 127 MB
Load Avg 0.4 1 Minute
0.5 5 Minutes
0.4 15 Minutes

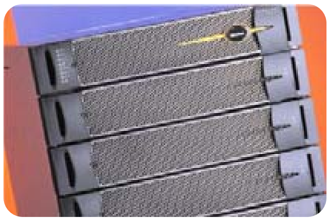
Host: opteron2
CPU 17% 1 CPUs
Memory 6% 2,047 MB
All Hosts
CPU 8% 8 CPUs
Memory 8% 16,187 MB

XenSource's Xen Optimizer

If we're talking new products, we must have a virtualization item in there somewhere. XenSource is announcing the release of XenOptimizer in beta form, with the product to follow in early 2006. It is also releasing the 3.0 version of the underlying Xen technology. According to XenSource, XenOptimizer offers production-grade capabilities, superior performance and lowers the total cost of ownership for a data center. Administrators can provision virtual servers using a simple drag-and-drop GUI dashboard. This has been your moment of Xen.
www.xensource.com

Stratus Technologies' ftServer T60

Stratus Technologies has announced that its über-reliable ftServer T60 will be the first piece of Stratus hardware to support Linux, specifically Red Hat Enterprise Linux. This will add, for the first time, a Linux distribution to the Stratus product offerings, which already include Windows and the proprietary Stratus VOS operating system.
www.stratus.com

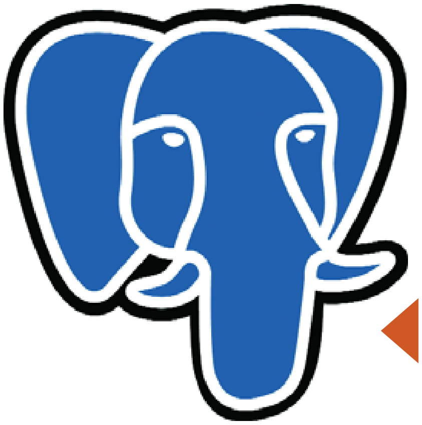


WinSystems' CompactFlash Card

The heart of any embedded Linux application is usually a CompactFlash (CF) card. Unfortunately, not all of them live in 72° living rooms. WinSystems has released a series of CF cards designed to work from a bone-chilling –40°C to a blazing 85°C. These cards, available in sizes ranging from 128MB up to 2GB, are engineered for reliable performance and long lifetimes, without sacrificing speed.
www.winsystems.com

Digium's Asterisk 1.2

Your open-source PBX just got an IQ upgrade. Digium has released the first major revision of the open-source Asterisk PBX Project since September 2004. Asterisk 1.2 includes more than 3,000 new or improved features, such as improved voice mail, SIP protocol support and the use of sound files for music on hold.
www.digium.com



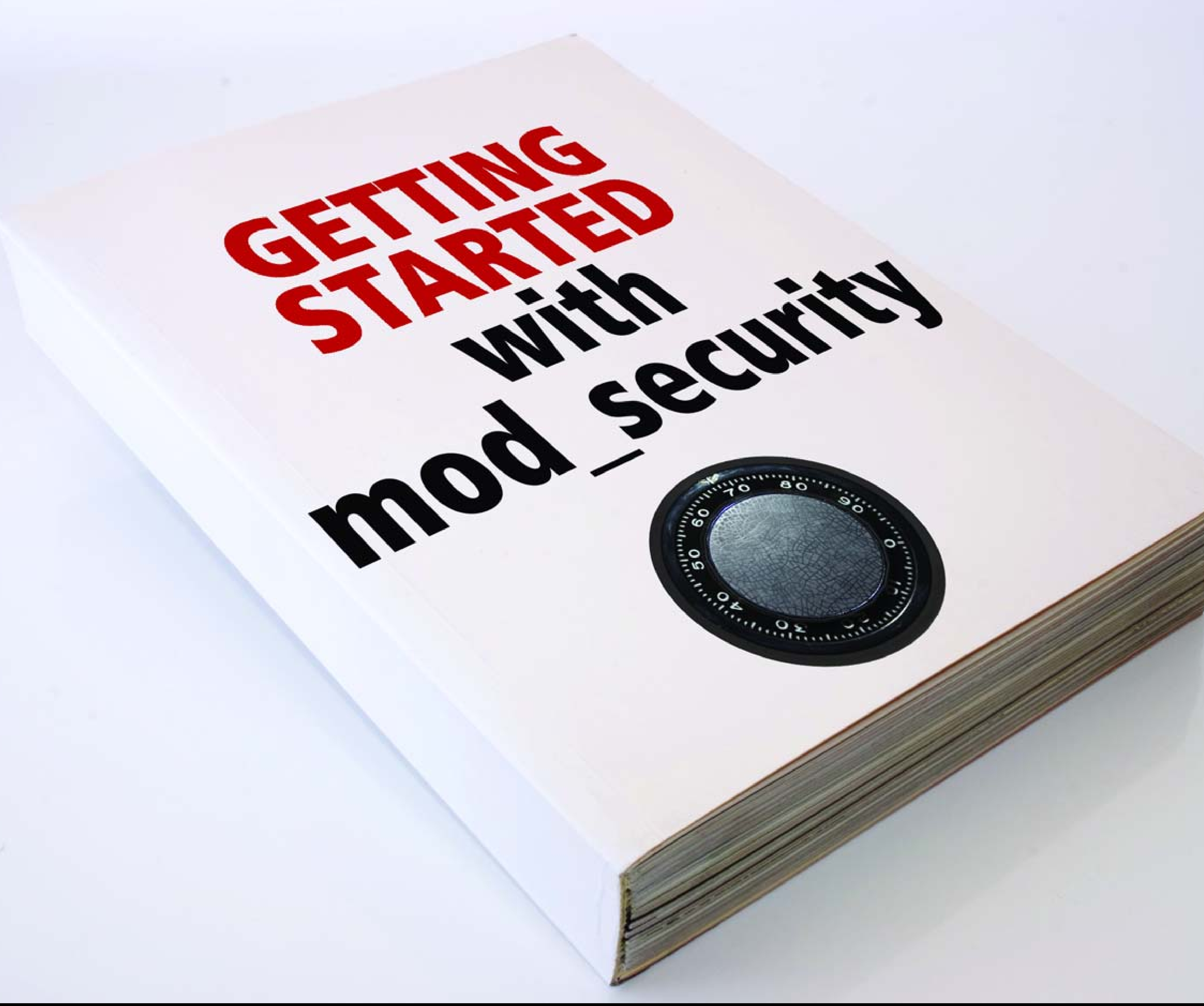
PostgreSQL Global Development Group's PostreSQL 8.1

Get out your SQL queries and spiff up your inserts. The PostgreSQL Global Development Group has released PostgreSQL 8.1. In addition to the usual performance improvements and bug fixes, the 8.1 release adds roles, which allow database rights to be assigned to entire groups rather than to individuals, and the ever-popular two-phase commit (which, as we all know, "allows ACID-compliant transactions across widely separated servers").
www.postgresql.org

VersaLogic Corp.'s EPM-VID-3

Just because you're trying to package your embedded Linux application onto one of those tiny PC/104 cards doesn't mean you can't have cranking video performance. With only 8MB of RAM, you won't be using VersaLogic Corp.'s EPM-VID-3 to play *Silent Hill*, but the ATI Rage Mobility M1-based add-on card is just the thing for applications that require up to three heads running at up to 1600x1200 at 24 bits. With built-in hardware MPEG decoding, it'll let you stream your video without taxing those underpowered embedded processors.
www.VersaLogic.com

Please send information about releases of Linux-related products to James Turner at newproducts@ssc.com or New Products c/o *Linux Journal*, PO Box 55549, Seattle, WA 98155-0549. Submissions are edited for length and content.



GETTING STARTED with mod_security

The first steps toward securing your Web site with the versatile mod_security Apache module.

Mick Bauer

WHAT IS MORE IMPORTANT than Web security? No matter how advanced your firewall, how compartmentalized your network and how strong your encryption, it all comes crashing down if your Web applications are vulnerable. On the one hand, there's no substitute for stringent user-input validation and other secure programming practices. But on the other hand, the stakes are too high to operate without *some* sort of safety net.

Ivan Ristic has given us just such a safety net: his excellent Apache module mod_security acts as an application-layer proxy between users and your Web applications. The mod_security module can stop SQL injection, cross-site scripting and other input-based Web attacks dead in their tracks, with only minimal effort on your part, and with no impact at all on either your Web developers or your users.

In this article, I tell you what you need to know to install and begin configuring mod_security on your own Apache-based Web server.

Why You Need mod_security

Space doesn't permit a comprehensive explanation of the entire range of threats that mod_security was designed to help mitigate. If you're new to Web security, your first stop should be the Open Web Application Security Project (OWASP) Web site (see the on-line Resources), home of the OWASP Top Ten Most Critical Web Application Security Vulnerabilities. A reasonable second stop is Chapter 10, "Securing Web Servers", of my book *Linux Server Security*, 2nd edition, or Ivan Ristic's book *Apache Security*.

For our purposes here, suffice it to say that of the different types of vulnerabilities in Web servers, by far the most typical is poor or incomplete user-input validation. In fact, many of the items on the OWASP Top Ten list are really just subsets of this family of problems; command injection and cross-site scripting, for example, are types of user-input abuse. User input, of course, includes not only the URLs requested in HTTP GET requests, but also the data sent in POST commands.

The mod_security module gives your Apache Web server increased ability to inspect and process input from Web clients before it's acted on by the scripts or processes waiting for the input. The mod_security module even lets you inspect Web server output before it's transmitted back to clients. I love this feature: it allows you to watch out for server responses that might indicate that other filters have failed and an attack has succeeded!

The mod_security module also lets you automatically log events and session data that Apache wouldn't ordinarily log. This is useful not only for forensics purposes, but also for fine-tuning your mod_security rules. If you create stringent mod_security filters that you're worried may be triggered by legitimate traffic, you can set those filters only to log rather than actually dropping or redirecting the requests that trigger them.

But wait, there's more: mod_security works against encrypted Web traffic too! Because mod_security has access to transaction data before SSL encryption and after SSL decryption, mod_security can filter HTTPS traffic just as effectively as it filters HTTP.

Why wouldn't you need mod_security? Arguably, if you have a "brochureware" Web site that involves no databases or cgi scripts, serving up instead only static Web pages, mod_security might not be worth the trouble of setting up. I would suggest, however, that even on such a server, mod_security still might do some good for you, for example, in inhibiting certain types of information-gathering attacks. Read on, and decide for yourself.

Getting and Installing mod_security

The mod_security module runs on both Apache 1.3 and Apache 2.0. Although for most Linux distributions, you'll need to install mod_security from source, Debian has its own binary packages for mod_security.

If you run Debian, install the package mod-security-common, plus either libapache2-mod-security or libapache-mod-security, depending on whether you run Apache version 2 or 1, respectively. Although Debian's mod_security packages are for mod_security version 1.8.7, rather than the more-advanced version 1.9, this article is sufficiently basic to apply equally to versions 1.8.7 and 1.9.

If you run SUSE or Red Hat Enterprise Linux, you need to download the latest source code from **www.modsecurity.org** and compile it using the apsx or apsx2 command (part of SUSE's apache-devel and apache2-devel packages, respectively, and RHEL's httpd-devel package). All you need to do, once you've got apsx or apsx2 installed and have obtained the source code file mod_security.c, is issue one of these two commands from within the directory containing mod_security.c:

```
/usr/sbin/apxs -cia mod_security.c
```

or

```
/usr/sbin/apxs2 -cia mod_security.c
```

See the ModSecurity User Guide, or the mod_security source code's INSTALL file, for more information on installing mod_security from source.

Configuring mod_security

The mod_security module, like all other Apache modules, is controlled from httpd.conf in Apache 1.3, or apache2.conf in Apache 2.x. On the one hand, mod_security's configuration parameters are straightforward to use and well documented. But on the other hand, as of this writing, there is no default configuration; the assumption is that you know enough about your environment and about Web security to create your own configuration from scratch.

And indeed, only you (and your Web developers) know what sorts of input are legitimate for the Web applications on your particular server. However, a minimum default configuration would be nice to start out with, wouldn't it? Luckily, one *is* provided, in the ModSecurity User Guide.

The rest of this article consists of a dissection of this minimum configuration, which should give you a taste of mod_security's power. For a more complete reference on mod_security configuration parameters and more-advanced examples, see the on-line Resources for this article.

Rather than presenting the entire configuration in one imposing list, let's break it up into manageable chunks. Listing 1 contains some basic settings.

The first line in Listing 1 simply checks to see whether mod_security even has been enabled; if it isn't, the subsequent parameters are ignored. The parameter SecFilterEngine controls whether mod_security's filtering engine is enabled. The default value is Off, so you need to set this explicitly either to On, which causes mod_security to inspect all data, or DynamicOnly, which turns filtering on but tells mod_security to ignore requests for static content (specifically, it ignores requests with null handlers). Note that the DynamicOnly setting may not behave precisely how you expect; although it can save CPU cycles, some testing is in order if you use DynamicOnly.

SecFilterDefaultAction is very important. It defines the default action to take on filter matches. In Listing 1, this is set both to log the matching request and deny it with a status code 403 message. Obviously, you can specify multiple actions, separated by commas.

SecFilterScanPOST, if set to On, tells mod_security to inspect not only GET requests, but POST payloads as well.

Setting SecFilterCheckURLEncoding to On causes hexadecimal-encoded values within URLs to be checked for valid values (0-9, A-F).

SecFilterCheckUnicodeEncoding can be set to On if your Web server understands Unicode and uses UTF-8 encoding.

Finally, SecFilterForceByteRange specifies the range of allowable ASCII values in GET requests and in form data within POST requests.

On to our next set of parameters—Listing 2 shows some settings related to logging.

SecUploadDir specifies a place for mod_security to store files uploaded via POST requests for processing, but it won't actually use this unless SecUploadKeepFiles is set to On. You probably don't want to enable this feature unless you've got a script, specified by a SecUploadApproveScript directive, that's ready to scan such files, for example, a script that invokes ClamAV

Listing 1.

Beginning of mod_security Parameters in apache2.conf/httpd.conf

```
<IfModule mod_security.c>
        SecFilterEngine On
        SecFilterDefaultAction "deny,log,status:403"
        SecFilterScanPOST On
        SecFilterCheckURLEncoding On
        SecFilterCheckUnicodeEncoding Off
        SecFilterForceByteRange 1 255
```

and can return the results to mod_security. See the ModSecurity User Guide for more information on the SecUploadApproveScript parameter.

Setting SecAuditEngine to On, RelevantOnly or DynamicOrRelevant enables mod_security's powerful logging facility, which captures much more information than Apache's default logs. On causes all requests to be logged by mod_security, RelevantOnly logs only those requests that trigger mod_security filters and DynamicOrRelevant logs both relevant requests and requests with non-null handlers. SecAuditLog specifies the file to which mod_security should write its logs.

SecFilterDebugLog, obviously enough, specifies the file to which mod_security should log internal debugging information. Setting SecFilterDebugLevel to 0 turns off debug-logging; if you're actually having problems with mod_security, or are fine-tuning its configuration, you can set this to 1 for significant events (which will also be written to the audit log), 2 for info messages or 3 for still-more-detailed info messages.

Now, at last, we arrive at the real power of mod_security: customized filters. Listing 3 shows three such filters.

Note the blank lines between filter groups. I inserted these to illustrate that appending the string chain to the end of a filter links it to the next one, such that the last filter in the chain will be evaluated only if the request first matches all prior filters in the chain. In this sense, chain is a little like an if-then statement.

The first pair of filters in Listing 3 checks to see whether the request is *not* a GET or a HEAD request; if not, it then checks to see if the request contains anything *other* than form data (`content-type "application/x-www-form-urlencoded"`) or an uploaded file (`encoding-type "multipart/form-data"`), which are the only two types of encoding mod_security can parse. If both filters match, that is, the request isn't form data or a file, the request is denied (see SecFilterDefaultAction in Listing 1).

Note that our actual filter values (`"!^(GET|HEAD)$"` and `"!(^application/x-www-form-urlencoded$|^multipart/form-data;)"`) are regular expressions. It's impossible for you to create your own custom filters unless you're comfortable with regular expressions; if you aren't, you may want to see Jeffrey Friedl's book *Mastering Regular Expressions*, 2nd edition (O'Reilly Media, 2002).

Listing 2.

Logging-Related Parameters

```
SecUploadDir /tmp
SecUploadKeepFiles Off
SecAuditEngine RelevantOnly
SecAuditLog logs/audit_log
SecFilterDebugLog logs/modsec_debug_log
SecFilterDebugLevel 0
```

The second pair of filters in Listing 3 first checks to see if the request is a POST request. If so, it then checks to see whether the HTTP parameter Content-Length is set to null; if so, the request is rejected. POST requests are supposed to have proper lengths; if the length is null, this almost certainly suggests an attack of some kind.

Our last example filter, which unlike the first two is a single-line filter, protects us from non-null values for the HTTP parameter Transfer-Encoding. In other words, we *want* Transfer-Encoding to be set to null in HTTP requests, because the most common thing to set this to is chunked, which is practically never necessary but has been associated with attacks in the past.

Finally, we end with an </IfModule tag to indicate that we're done specifying mod_security parameters. In practice, the statements in Listings 1–3 would be in a single contiguous block; I split them into three groups only for readability.

Listing 3.

Some Custom Filters

```
SecFilterSelective REQUEST_METHOD
    ➥"!^(GET|HEAD)$" chain
    SecFilterSelective HTTP_Content-Type
    ➥"!(^application/x-www-form-urlencoded$|^multipart/form-data;)"

    SecFilterSelective REQUEST_METHOD "^POST$" chain
    SecFilterSelective HTTP_Content-Length "^$"

    SecFilterSelective HTTP_Transfer-Encoding "!^$"
</IfModule>
```

If you prefer to maintain your mod_security settings in a special file, such as mod_security.conf, you can use an include statement within httpd.conf or apache2.conf, for example:

```
Include /etc/apache2/mod_security.conf
```

Enabling mod_security

Once you've configured mod_security in httpd.conf or apache2.conf, you're ready to enable it. In the case of Apache 1.x, your httpd.conf needs to contain the line:

```
LoadModule security_module libexec/mod_security.so
```

and possibly also:

```
AddModule mod_security.c
```

If you run Apache 2.x, your apache2.conf file needs the line:

```
LoadModule security_module modules/mod_security.so
```

This is true unless you run Debian and installed its mod_security deb packages, in which case you need to run only the following command (as root) from a command prompt:

```
a2enmod mod-security
```

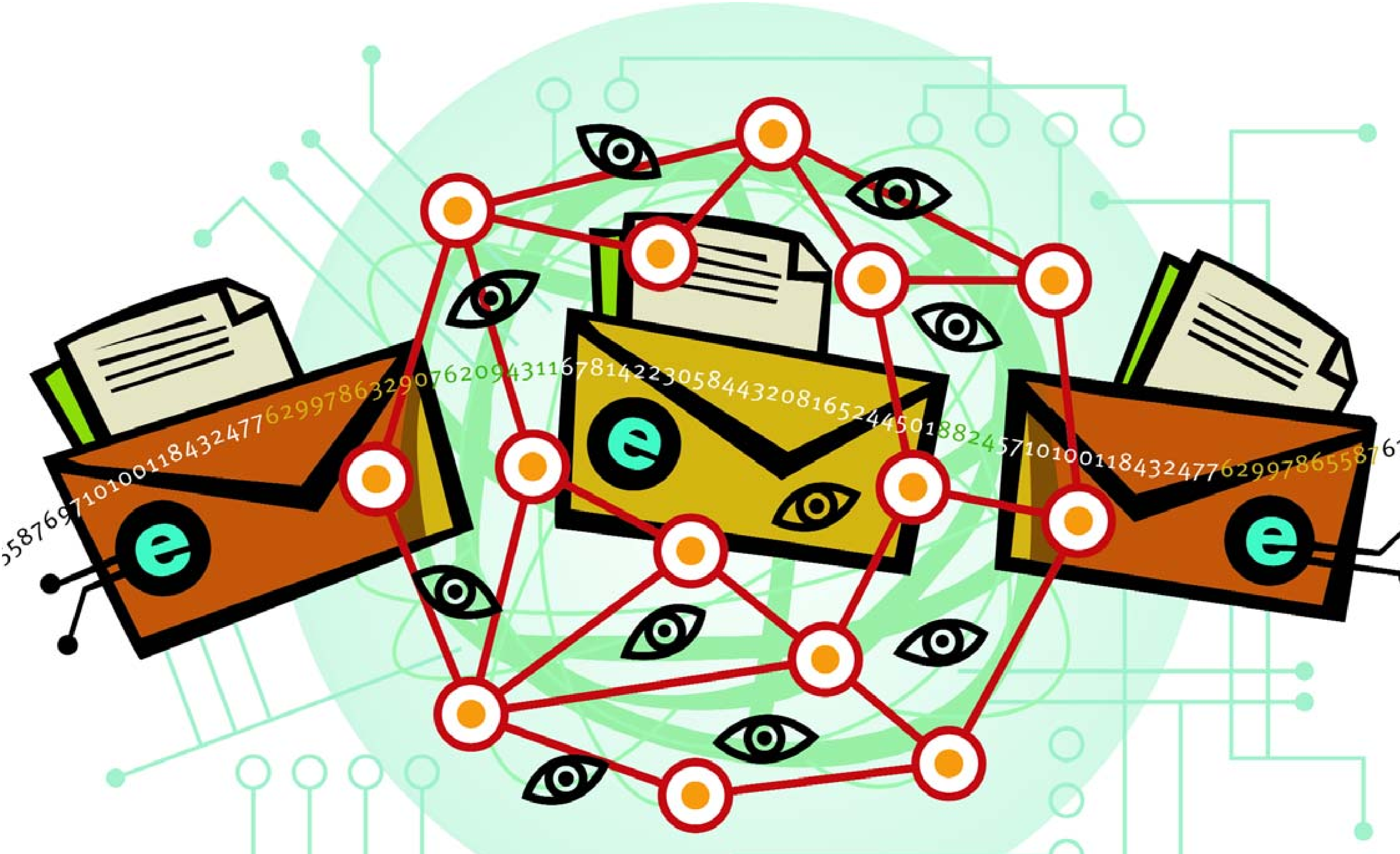
Once mod_security is enabled, you need to restart Apache in order to load the module. After you do this, be sure to test your Web applications to make sure you didn't Denial-of-Service attack yourself via your mod_security configuration!

Conclusion

With that, you should be ready to explore some more-advanced filters that watch specifically for requests that your site shouldn't expect to see. I strongly encourage you to take this next step; although I think this article should have given you a good starting point, you can find examples of much more powerful filters in the "ModSecurity For Apache User Guide" and other documents on the modsecurity.org Web site. Good luck, and stay safe!

Resources for this article: www.linuxjournal.com/article/8744.■

Mick Bauer (darth.elmo@wiremonkeys.org) is Network Security Architect for one of the US's largest banks. He is the author of the O'Reilly book *Linux Server Security*, 2nd edition (formerly called *Building Secure Servers With Linux*), an occasional presenter at information security conferences and composer of the "Network Engineering Polka".



GnuPG Hacks

GnuPG does a lot more than just encrypt and decrypt e-mail and attachments.

Tony Stieber

Have you wondered about using cryptography, but found it too confusing? Are complicated software packages, passphrases, keys, key rings, certificates and fingerprints too daunting?

You don't need all that. With no prior experience and nothing to remember, GnuPG can do basic and immediately useful cryptography. GnuPG even may be installed on your Linux system already.

GnuPG and OpenPGP

The GnuPG is the GNU Project's implementation of the OpenPGP standard. Also known as the Gnu Privacy Guard, it is a sophisticated public key cryptosystem with more than 70 command-line options, plus an internal command-line and menu environment. It has been ported to several operating systems and has precompiled binaries available from the GnuPG Web site (see the on-line Resources). Like all GNU software, it can be used freely under the GNU General Public License.

The OpenPGP standard, RFC 2440, is based on the Pretty Good Privacy system developed by Phil Zimmermann in 1991. OpenPGP is also the basis for commercial products on even more operating systems. An OpenPGP system is the most common file encryption system you will encounter.

Getting Started

First, let's begin with some GnuPG features that don't need a passphrase. After that, we'll choose a passphrase and use it to encrypt something. Note that GnuPG is the name of the software, but the name of the command is gpg.

Make sure GnuPG is installed and in your path:

```
gpg --version
```

You should get something like this:

```
gpg (GnuPG) 1.4.1
Copyright (C) 2005 Free Software Foundation, Inc.
This program comes with ABSOLUTELY NO WARRANTY.
This is free software, and you are welcome to
redistribute it under certain conditions.
See the file COPYING for details.

Home: ~/.gnupg
Supported algorithms:
Pubkey: RSA, RSA-E, RSA-S, ELG-E, DSA
Cipher: 3DES, CAST5, BLOWFISH, AES, AES192, AES256, TWOFISH
Hash: MD5, SHA1, RIPEMD160, SHA256, SHA384, SHA512
Compression: Uncompressed, ZIP, ZLIB, BZIP2
```

334

The version number, date and other details may vary. The examples shown in this article should work for most current and future versions of GnuPG.

Now, type:

```
gpg /dev/null
```

You might get something like this:

```
gpg: /home/you/.gnupg: directory created
gpg: new configuration file `/home/you/.gnupg/gpg.conf'
 ➥created
gpg: WARNING: options in `/home/you/.gnupg/gpg.conf'
 ➥are not yet active during this run
gpg: keyring `/home/you/.gnupg/secring.gpg' created
gpg: keyring `/home/you/.gnupg/pubring.gpg' created
gpg: processing message failed: eof
```

This is perfectly normal the first time you run GnuPG. If it doesn't happen, it simply means you've run GnuPG before, or your .gnupg directory already exists.

Binary File Shields

Most e-mail programs support file attachments, but command-line e-mail programs, such as /bin/mail, don't. Sometimes it's more convenient to keep all the data in the message body. But binary files must be ASCII-encoded to prevent them from being corrupted in transit.

You may have tried to use uuencode and found it confusing or that it didn't work. Not all systems have a command-line MIME encoder. However, GnuPG has an ASCII-encoding option very similar to MIME, but without all the complexity, overhead and features.

To wrap a file in PGP ASCII armor, type:

```
$ gpg --enarmor < filename.bin > filename.txt
```

To unwrap a file already in PGP ASCII armor, type:

```
$ gpg --dearmor < filename.txt > filename.bin
```

Table 1. Password and passphrase strengths compared with estimated time to crack.

Type	Length	Bits	Total Bits	Time to Crack
Single word of any language	8 characters	24	24	Seconds
Random mono-case letters	8 characters	4.7	37	Minutes
Random mono-case letters	16 characters	4.7	75	Decades
base64 [A-Za-z0-9+/=]	10 characters	6	60	Months
base64 [A-Za-z0-9+/=]	20 characters	6	120	Uncrackable?
Completely random printable	6 characters	6.5	40	Minutes
Completely random printable	8 characters	6.5	52	Hours
Completely random printable	12 characters	6.5	78	Decades
Completely random printable	15 characters	6.5	97	Centuries
Completely random printable	20 characters	6.5	130	Uncrackable?
Diceware passphrase	2 words	12.9	26	Seconds
Diceware passphrase	4 words	12.9	51	Hours
Diceware passphrase	6 words	12.9	78	Decades
Diceware passphrase	8 words	12.9	120	Uncrackable?

Warning: despite the name, the OpenPGP ASCII armor has *absolutely no security*. If you do want security and data compression, see the Quick and Clean Encryption section below and use a good passphrase.

Better Checksums

Do you suspect a file you just received is corrupted? Traditionally, the `sum` or `cksum` command is run over the file before and after it was sent and the outputs are compared. But there are three different incompatible versions of these commands, and even the same version can produce completely different output on different machines due to processor endian issues. Even worse, sometimes they won't even detect corrupted files. By chance alone, even when they are compatible, they sometimes will produce the same output for different files. The 32-bit output of the sum and cksum commands is simply too small for reliability, much less security. The popular SSH v1 CRC-32 compensation attack is the same vulnerability.

You could use `md5sum` instead, but there are different versions of this command. Each version has slight differences in formatting of filenames, whitespace and hexadecimal case. These differences in format prevent `diff` from running cleanly. In addition, there are known security vulnerabilities in the MD5 hash algorithm used by md5sum. And, sometimes md5sum isn't even installed.

GnuPG avoids these problems, because it produces the same output regardless of operating system or processor architecture. GnuPG also supports newer and more secure algorithms:

```
$ gpg --print-md sha1 filename
filename: E83A 42B9 BC84 31A6 6450  99BE 50B6 341A 35D3 DCEB
```

It also will take multiple files:

```
$ gpg --print-md sha1 *.txt
test.txt: E0D6 3F44 4253 CED5 9205  4047 4AA6 4E0F FD0F 130D
test2.txt: 32AC 34F9 B7AF 1972 C015  E5EE 456E 89BD CC3C 7246
```

If you still need MD5, that's available too:

```
$ gpg --print-md md5 filename
filename: 26 E9 85 5F 8A D6 A5 90  6F EA 12 12 83 C7 29 C4
```

The more recent GnuPG versions also support much more secure hash algorithms, such as SHA-512:

```
$ gpg --print-md sha512 filename
filename: FC37410D 9336DD60 22AEB6A2 A42E82F1 2EA3470D 4982E958 B35C14A0
          CF381CD2 3C4CBA35 BE5F11CB 05505ED2 DBF1C7A0 397EFF75 007FAEBB
          30B43B30 6514990D
```

By the way, you can validate these --print-md examples by creating a file called filename containing the single line: `The Linux Journal`.

Your hash values should have exactly the same hexadecimal value as those in this article if the contents of the file is the same.

Quick and Clean Encryption

Want to encrypt a file, but don't know where to start? Here's a quick and clean introduction to file encryption using GnuPG:

```
$ gpg -c test.txt
Enter passphrase:
Repeat passphrase:
```

When encrypting, GnuPG asks for a passphrase twice, just like when you set a new password. The new encrypted file has the same name, but with the extension .gpg added. The original file is left intact.

The -c stands for conventional encryption, also known as symmetric encryption. Normally, GnuPG defaults to public key encryption, but we haven't generated or loaded any public keys, so for now we have to stay with conventional.

This type of encryption is most useful only if you want to decrypt your files, but you don't trust where your files are stored. For example, easily lost or stolen storage can be protected with this type of encryption. This type of encryption is especially useful for off-site backups.

To extract the encrypted file, simply type:

```
$ gpg filename.gpg
```

GnuPG automatically detects that the file is encrypted with a passphrase and asks for that passphrase. Then it writes the decrypted data to a file with the same name but without the .gpg extension. As with encrypting, the encrypted file is left intact. If you want the output file to be written to a different filename, use standard redirection, exactly as with the --dearmor example. Note that both input and output redirection must be used, or GnuPG becomes confused:

```
$ gpg < filename.gpg > filename.txt
```

If you want someone else to decrypt the file, you have to tell this person the passphrase without leaking the passphrase to anyone else. A simple and straightforward way to do this is in person. That might seem not very useful, as the original file also could be given in person. But that passphrase can now be reused safely multiple times on different files in the future. Just like passwords, however, passphrases should be changed regularly. Never reuse a passphrase with other people, unless you want them to decrypt all of the files you ever encrypted with that passphrase.

Note: this warning is normal when using passphrase encryption in GnuPG. This can be avoided with public key encryption:

```
gpg: WARNING: message was not integrity protected
```

Passphrases

The passphrase is a secret that keeps the other secrets, which makes it the most important part of GnuPG security. Unfortunately, in practice, passphrases are also the weak part. This is because creating good passphrases is difficult, and remembering them is even more difficult.

I highly recommend Diceware, but if it doesn't appeal to you, take a look at the Wikipedia article (see Resources) or the passphrase Web pages recommended by your favorite Web search engine.

Regardless of what method you choose, a simple guide to passphrase security is that longer is usually better (Table 1).

The time estimates in Table 1 are wide, because money and time can be traded evenly. Computing power keeps getting cheaper, so time to crack keeps getting shorter. Cracking costs start at free and go up.

If you cannot remember a GnuPG passphrase, the data encrypted with that passphrase is probably gone forever. There are no known back doors in GnuPG nor any way to recover a lost passphrase short of guessing. How long it takes depends on how good the passphrase was. A good 20-character passphrase could take billions of years to guess, even using all current and future computers.

Generate a Passphrase

Here's a quick hack for generating a very secure passphrase using GnuPG itself. The passphrase will not be easy to remember or type, but it will be very secure. The hack generates 16 random binary bytes using GnuPG then converts them to base64, again using GnuPG. The final sed com-

Table 2. A short list of GnuPG options mentioned in the article.

Short Option	Long Option	Description
	--version	Version and algorithm information
	--help	Help
-a	--armor	Turn on ASCII encoding when encrypting
	--enarmor	Input binary, output ASCII
	--dearmor	Input ASCII, output binary
	--print-md HASH	Print a message digest using the specified HASH
-c	--symmetric	Conventional symmetric encryption with a passphrase
-o	--output	Specify a particular output file, use - for stdout

mand strips out the headers leaving a single line that can be used as a passphrase:

```
gpg --gen-random 1 16 | gpg --enarmor | sed -n 5p
```

Encrypted Tarballs

Instead of using gzip to compress tarballs, use GnuPG. The tarballs will end up being about the same size, but they also will be encrypted. By the way, don't bother trying to gzip or otherwise compress any encrypted files. Encrypted data is usually incompressible. This is because data compression and encryption are closely related mathematically. Because of this, most cryptosystems, GnuPG included, automatically compress before encryption. There is also a slight gain in security by compressing.

You will be prompted for a passphrase twice, just like when encrypting before:

```
tar -cf - these files here | gpg -c > these-files-here.tgp
```

To extract the files, enter the password entered above:

```
gpg < these-files-here.tgp  | tar -xvf -
```

Automating GnuPG

If you want to use GnuPG in a script and don't want to be prompted for the passphrase, put the passphrase in a file called passphrase.txt, and use this to encrypt:

```
[$ cat passphrase.txt | gpg --passphrase-fd 0 -c < filename.txt > filename.gpg
```

Note: decrypting is nearly identical, simply drop the -c and switch the files around:

```
$ cat passphrase.txt | gpg --passphrase-fd 0 < filename.gpg > filename.txt
```

If you're going to e-mail the encrypted file, perhaps for off-site backup, add the -a option to turn on ASCII armor. The net effect is the same thing as --enarmor used earlier, but it includes encryption. This also produces smaller files than uuencoding or MIME, because by default, GnuPG compresses data before encryption.

To finish off the hack, we also mail the encrypted file at the same time. Note the use of -o - to force GnuPG's output to stdout:

```
$ cat passphrase.txt | gpg --passphrase-fd 0 -ac -o - filename.txt | mail user@example.com
```

By the way, putting the passphrase in a file can be extremely dangerous. Anyone who obtains a copy of that passphrase file can then decrypt any file it has ever encrypted. Someone even could create new files with the same passphrase, resulting in secure and undetectable forgery. Make sure your passphrase file, indeed the entire computer, has the security you expect.

Automating tasks inherently requires cutting humans out of the loop, so this security weakness is difficult to avoid. However, GnuPG can help even here by using public key encryption.

GnuPG Troublehacking

Do you have an OpenPGP-encrypted file, but no key ring and no idea what to do with it? Perhaps someone sent you an encrypted file and assumed you would know what to do. Maybe he or she doesn't know what to do either.

If the file has either a .pgp or .gpg extension, you can try decrypting it with GnuPG. Also, check the file with a text editor to see if it contains something like this:

```
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.2.5 (GNU/Linux)

jA0EAwMCwg21r1fAW+5gyS0KR/bkeI8qPwwQo/NOaFL2LMXEYZEV9E7PBLjjGm7Y
DGG4QnWD5HSNOvdaqXg=
=j5Jy
-----END PGP MESSAGE-----
```

If it does, it's an ASCII-armored PGP-encrypted file.

This particular file is a real encrypted file containing the same value as used in the --print-md examples above and is encrypted with a passphrase of the same value.

Simply running GnuPG on an unknown file produces some useful information. If it prompts you for a passphrase, you'll need to get (or guess) the passphrase used to encrypt the file:

```
gpg unknown_file
```

If it's not an OpenPGP file, you'll get something like this:

```
gpg: no valid OpenPGP data found.
gpg: processing message failed: eof
```

If you get something else, however, maybe the file is encrypted with a public key that you don't have. The file also could be corrupted. A common mistake is to send binary files through e-mail or FTP transfer in ASCII mode.

GnuPG has a special diagnostic option to help troubleshoot these problems. The OpenPGP message format is internally formatted as packets; the --list-packets option dumps out information about those packets:

```
gpg --list-packets unknown_file.gpg
```

In addition to the standard information, this option also prints the full key ID of the public key that the file is encrypted with, if any, and what algorithms were used. It could be that the file was encrypted with a PGP 2.x public, sometimes called a legacy key. PGP 2.x predates the OpenPGP standard, so the standard GnuPG cannot decrypt it. Most PGP implementations made in the past several years are usually OpenPGP-compatible, so merely asking the sender to generate a compatible OpenPGP-encrypted file should do the trick.

There also are several different cryptographic algorithms supported by OpenPGP. Most have only some of these algorithms implementationally. Use `gpg --version` to see what might be missing.

Details on the packet format, such as the internal algorithm numbers, can be found in the OpenPGP standard RFC 2440.

GnuPG mostly uses long command-line options, but some options also have short single-letter options from the original PGP. For example, -v is --verbose, not --version.

Learning More

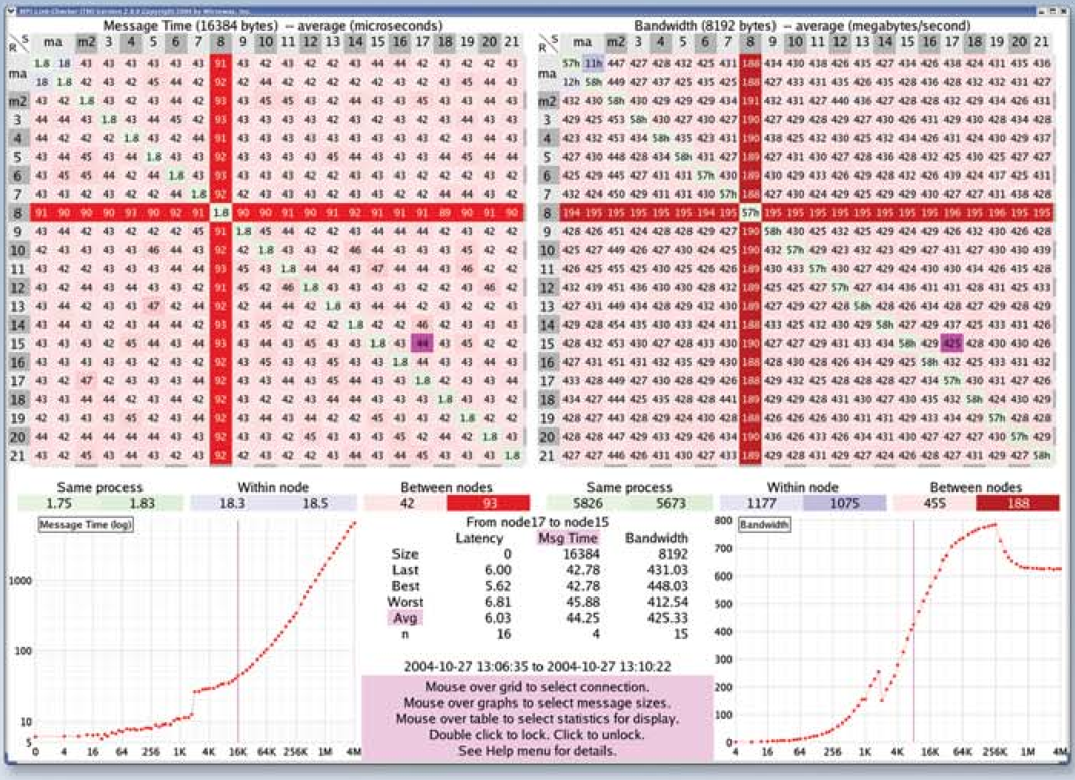
There are several good introductions to using the more common features of GnuPG, such as the GnuPG MiniHOWTO by Brenno de Winter at the GnuPG Web site (see Resources). They explain in detail how to use the more common public key cryptography features of GnuPG.

The GnuPG mailing lists are also very useful and fully archived on the GnuPG Web site. Werner Koch, the GnuPG lead developer, frequently posts to the mailing lists and is of invaluable help.

Resources for this article: www.linuxjournal.com/article/8743.■

Tony Stieber is an information security professional specializing in UNIX systems, cryptology and physical security. He has been learning Linux since 1999, UNIX since 1987 and computers since before 1980. He does not yet know what the next decade will offer.

X Marks the Slow Node!



Message Time (16384 bytes) – average (microseconds)

R \ S	ma		m2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
ma	1.8	18	43	43	43	43	43	43	91	43	42	43	42	42	43	44	44	42	43	42	42	43
	18	1.8	42	43	42	45	44	42	92	42	44	42	42	42	42	42	43	42	43	45	44	43
m2	43	42	1.8	43	42	43	44	42	93	43	45	45	43	42	44	43	43	45	43	43	44	43
3	44	44	43	1.8	43	44	45	42	93	43	43	43	43	42	43	42	43	42	43	44	43	43
4	44	42	42	42	1.8	43	42	44	91	43	43	43	43	43	43	43	43	43	42	43	44	43
5	43	44	45	43	44	1.8	43	43	92	43	43	43	43	45	44	43	43	43	44	45	44	44
6	43	45	45	44	42	44	1.8	43	93	43	43	43	42	42	43	43	43	42	42	42	43	42
7	43	43	42	43	42	42	44	1.8	92	42	43	43	43	42	43	43	42	42	44	44	43	42
8	91	90	90	90	91	90	92	91	1.8	90	90	91	90	91	92	91	91	91	89	90	91	90
9	43	44	42	43	42	42	42	45	91	1.8	45	44	42	42	43	44	44	44	42	43	42	42
10	42	43	43	43	43	46	44	43	92	42	1.8	43	43	42	46	44	43	43	43	45	42	42
11	43	42	42	43	43	43	44	44	93	45	43	1.8	44	44	43	47	44	44	43	46	42	42
12	43	42	44	43	44	43	43	42	91	45	42	46	1.8	43	43	43	43	42	42	43	46	42
13	43	44	42	43	43	47	42	44	92	42	44	44	42	1.8	43	44	44	42	43	42	42	43
14	43	44	43	42	43	44	44	42	93	43	45	42	42	42	1.8	42	42	46	42	43	43	43
15	43	43	43	42	45	44	43	44	93	43	44	43	45	43	43	1.8	43	44	43	45	42	42
16	43	43	43	43	43	42	43	42	92	43	45	43	43	45	43	43	1.8	44	43	43	44	43
17	43	42	47	42	43	43	43	44	92	43	43	44	43	45	44	43	43	1.8	42	43	43	44
18	43	43	44	44	42	43	44	42	92	43	42	42	43	44	44	43	43	43	1.8	43	43	42
19	42	43	43	43	45	42	43	44	92	43	44	43	44	42	42	45	43	43	42	1.8	42	42
20	44	42	44	44	44	44	43	43	92	43	43	42	45	43	43	43	45	42	44	42	1.8	43
21	43	42	45	43	44	43	42	43	92	42	43	42	42	43	44	43	44	45	43	43	43	1.8

Same process		Within node		Between nodes	
1.75	1.83	18.3	18.5	42	93

Bandwidth (8192 bytes) – average (megabytes/second)

R \ S	ma		m2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
ma	57h	11h	447	427	428	432	425	431	188	434	430	438	426	435	427	434	426	438	424	431	435	436
	12h	58h	449	427	437	425	435	425	188	427	433	431	435	426	435	428	436	428	432	432	431	427
m2	432	430	58h	430	429	429	429	434	191	432	431	427	440	436	427	428	428	432	429	434	426	431
3	429	425	453	58h	430	427	430	427	190	427	429	428	429	427	430	426	431	429	430	428	434	428
4	423	432	453	434	58h	435	423	431	190	438	425	432	430	425	432	434	426	431	424	430	429	437
5	427	430	448	428	434	58h	431	427	189	427	431	430	427	428	436	428	432	425	430	425	427	427
6	425	429	445	427	431	431	57h	430	189	430	429	433	426	429	428	432	426	439	424	437	425	431
7	432	424	450	429	431	431	430	57h	188	427	430	424	429	425	429	429	430	427	427	431	438	428
8	194	195	195	195	195	195	194	195	57h	195	195	195	195	195	195	195	195	196	195	196	195	195
9	428	426	451	424	428	428	429	427	190	58h	430	425	432	425	429	424	429	426	432	430	426	428
10	425	427	449	426	427	430	424	425	190	432	57h	429	423	432	423	429	427	431	427	430	430	439
11	426	425	455	425	430	425	426	426	189	430	433	57h	430	427	429	424	430	430	434	426	435	428
12	432	439	451	436	430	430	428	432	189	425	425	427	57h	427	434	436	431	431	428	431	425	433
13	427	431	449	434	428	429	432	430	189	427	429	427	428	58h	428	426	434	428	427	429	428	429
14	429	428	454	435	430	433	424	431	188	433	425	432	430	429	58h	427	429	437	425	433	431	426
15	428	432	453	430	427	428	433	430	190	427	427	429	431	433	434	58h	429	425	428	430	430	426
16	427	431	451	431	432	435	429	430	188	428	430	428	426	434	429	425	58h	432	425	433	431	432
17	433	428	449	427	430	428	429	426	188	429	432	425	428	428	428	427	434	57h	430	431	427	426
18	434	427	444	425	435	428	428	441	189	429	429	428	431	430	427	430	435	432	58h	424	430	429
19	428	427	443	428	429	424	430	428	188	426	426	426	430	431	431	429	433	434	429	57h	428	428
20	428	428	447	429	433	429	426	434	190	436	426	433	426	434	431	430	427	427	427	430	57h	429
21	427	427	446	426	431	430	427	433	189	429	428	431	429	427	424	426	428	427	431	429	427	58h

Same process		Within node		Between nodes	
5826	5673	1177	1075	455	188

From node17 to node15

	Latency	Msg Time	Bandwidth
Size	0	16384	8192
Last	6.00	42.78	431.03
Best	5.62	42.78	448.03
Worst	6.81	45.88	412.54
Avg	6.03	44.25	425.33
n	16	4	15

2004-10-27 13:06:35 to 2004-10-27 13:10:22

Mouse over grid to select connection.
Mouse over graphs to select message sizes.
Mouse over table to select statistics for display.
Double click to lock. Click to unlock.
See Help menu for details.

MPI Link-Checker™ to the Rescue!

A single slow node or intermittent link can cut the speed of MPI applications by half. Whether you use GigE, Myrinet, Quadrics, InfiniBand or InfiniPath HTX, there is only one choice for monitoring and debugging your cluster of SMP nodes: Microway's MPI Link-Checker™.

This unique diagnostic tool uses an end-to-end stress test to find problems with cables, processors, BIOS's, PCI buses, NIC's, switches, and even MPI itself! It provides instant details on how latency and bandwidth vary with packet size. It also provides ancillary data on inter-process and intra-CPU latency, and includes FastCheck!, which runs in CLI mode and checks up to 100 nodes per second. **A complimentary one year license for MPI Link-Checker™ is installed on every Opteron based Microway cluster purchased in 2006.**

Wondering what's wrong with your cluster's performance, or need help designing your next one? Microway designs award-winning single and dual core AMD Opteron based clusters. Dual core enables users to increase computing capacity without increasing power requirements, thereby providing the best performance per watt. Configurations include 1U, 2U, and our 4U QuadPuter™ RuggedRack™–available with four or eight dual core Opterons, offering the perfect balance between performance and density.

Microway has been an innovator in HPC since 1982. We have thousands of happy customers in HPC, Energy, Enterprise and Life Science markets. Isn't it time you became one?

Call us first at 508-746-7341 for quotes and benchmarking services. Find technical information, testimonials, and newsletter at www.microway.com.

Excellence in
CLUSTER
Technology
64-bit
Turnkey Solution
WINNER
ClusterWorld

▲
Microway® Quad Opteron™ Cluster with
36 Opteron 880s, redundant power,
45 hard drives and Myrinet™ in our
CoolRak™ cabinet.

Microway®
23 Years of Expertise Built In

AMD
64
Opteron™

DEMONS SEEKING DÆMONS—A PRACTICAL APPROACH TO HARDENING YOUR OPENSSH CONFIGURATION

A few simple configuration tweaks could save you sleepless nights over whether or not someone might crack your SSH server.

Phil Moses

Chances are, if you are the owner or administrator of a Linux machine, you access it remotely from time to time, if not constantly. Be it a workstation at home, a co-located server or a hobby machine, if you are accessing Linux remotely, there is a good chance that you are using the OpenSSH server on the remote machine with some type of SSH client locally. (If you are not, you probably should be.) Although it is true that the OpenSSH server and clients do a tremendous job at encrypting the traffic that passes between systems, it also is true that any dæmon listening for connections is a door handle waiting to be turned by the black hats, the evildoers or the crackers. The less-desirable folks in these situations are, as the title states, demons seeking dæmons, a person or group of people that usually are up to no good seeking listening dæmons that, depending on the configuration of the machine, may or may not be secure. Hackers can be defined as people who have relatively benign motives for breaking into a system. Crackers often are thought of as hackers with malicious intent. Neither the former nor latter is welcome on my machines. In this article, I expand on the basic OpenSSH configuration and cover ways to improve the security of the SSH dæmon to offer more protection to your machines. If you have a machine that suffers a compromise, your machine may be helping to spread your unpleasantness to others as well. The Internet is one of the largest insecure data routes on the face of our planet.

OpenSSH provides the means for secure communication over insecure channels. The file sshd_config is the ruling party in the game of secure shell configuration. The sshd_config file consists of multiple options that can be changed to help improve the security of the listening dæmon. Although it may seem that because it is a remote access tool it should be secure right out of the box, this is hardly the case. For the most part, a default installation of the OpenSSH server will provide you with a relatively secure default configuration but one that can be improved substantially by the machine's administrator.

When planning for remote access initially, it is suggested that you consider three major things for the access of your machines:

1. Who will be allowed access to the machines?

2. How will this access be provided?

3. From where will this access be allowed?

We are going to assume that we will be using the OpenSSH server to provide remote access. This leaves us with the questions of who will be allowed remote access and from where they will be allowed. For some, this may be simple; perhaps the machine supports only a single user and remote access is carried out from a single domain. For others, this can be quite a challenge when multiple users that travel frequently are the machine's users.

WHO IS ON THE INVITE LIST FOR THIS DEVILISH PARTY?

The first and foremost person on a Linux machine is the root user. This is universally known, and it also should be universally known that if you need to have remote root access to a machine, there are many better ways to access as root than simply using SSH and logging in as root. If you think about the fundamentals of a brute-force attack attempt, it is obvious that the most relevant account that will be attacked is the root account. One need not guess whether the account is present; it is there. The sshd_config file lets us specify that root is not allowed to log in remotely at all through the PermitRootLogin directive.

I fully believe that the saying "an ounce of prevention equals a pound of cure" is highly accurate when dealing with remote-use accounts. Two options allowed in the sshd_config file, UsersAllow and UsersDeny, are more than an ounce of prevention, and although it may be one extra step when adding an account, modifying the UsersAllow for each account added provides that pound of cure that you may (thankfully) never need to seek. To expand on the UsersAllow directive, you cannot specify only particular users, but you also can specify particular users at specific hosts. So, if in advance you know exactly who will need to log in and from where, the minimal time overhead associated with adding these directives to the sshd_config file provides the peace of mind for you to know you are allowing remote access for only specific accounts from specific machines. Valid users can be retrieved from the /etc/passwd file in standalone machines or from the corresponding files in NIS or LDAP environments. Listing 1 is an example of parsing the previous month's security files to verify which accounts have logged in successfully using SSH.

Listing 1.

Parsing the Logs for Successful Logins

```
cat secure* | grep Accepted | awk -F´ ´ ´<\\>
{print $1" "$2" "$9}´ | uniq -u
Aug 30 juser
Aug 22 kuser
Aug 23 user
Aug 15 foo

...
Aug 24 13:23:19 foohost sshd[16348]: Accepted
password for phil from 127.0.0.1 port 47338 ssh2
Aug 24 13:23:25 foohost sshd[16398]: User root
not allowed because not listed in AllowUsers
```

MONITORING THOSE DEMONS AND KEEPING THEM IN THEIR PLACE

Keeping a watchful eye on the demons seeking dæmons is relatively easy and the (expected) default setup should be confirmed in the configuration file. With the SyslogFacility set to AUTH, your sshd will log (via syslog) to (paths and filenames may vary depending on distribution) /var/log/messages and /var/log/secure. It is highly recommended that a program such as Psionic's logwatch be used to monitor your system logs. Logwatch will take care of parsing the logs, and you will be able to decipher the sshd authorized logins as well as failures. There is a distinct difference between an invalid user and an authentication failure. An authentication failure is a failure that occurs on an account that is present on the machine, and an invalid user is exactly that. This can become relatively important when you are choosing account names as well as contemplating who will be on the AllowUser and DenyUser lists. For example, you may not have an actual person named amanda using your machine, but you are using the amanda open-source backup program. This said account, if not added to the DenyUser specification, will trigger an authentication failure rather than an invalid user flag. Although not necessarily required, I add the system accounts that are active to the DenyUsers list just to be on the safe side. The most recent log entries from sshd scans show that the system accounts have in fact been added to the probe list (Listings 2 and 3).

Listing 2.

Log Entries from Failures Due to the Account Not Being Authorized in sshd_config AllowUsers

```
User mail not allowed because not listed in
AllowUsers
User adm not allowed because not listed in
AllowUsers
```

Listing 3.

Log Entries from Invalid Accounts

```
Aug 28 06:04:15 foo sshd[11602]: Failed password
for illegal user a... from 10.0.0.1 port 35078 ssh2
Aug 28 06:04:17 foo sshd[11604]: Illegal user aaa
from 10.0.0.1
Aug 28 06:04:19 foo sshd[11604]: Failed password
for illegal user aaa from 10.0.0.1 port 35417 ssh2
Aug 28 06:04:21 foo sshd[11606]: Illegal user qqq
from 10.0.0.1
```

Because user names have been mentioned, it is now appropriate to discuss the possibility of the demons (the evildoers) having one of the two credentials required for a login. In the event of a Web server hosting per-

sonal accounts or from e-mail headers, it is relatively easy to determine a user name on a particular machine. With this, the demon has half of the user name/password combination, and if the scanner goes beyond simply scanning common accounts and passwords, it is easy to take the sshd scan one step further and begin brute-force attempts at those accounts that already have been determined to exist on a machine.

There is no need to re-invent the protocol, only the need to improve the current configuration. OpenSSH provides a strong end-to-end encryption method for networked machines. Updates continuously are released to the code to address any insecurities that may come about. One of the most relevant releases is the change from SSH v1 to SSH v2. Both version 1 and 2 sshd servers have their own keys. In other words, with SSH1 and SSH2, neither private nor public keys intermix. These keys are independent of each other. Just as the keys are independent of each other, so are the protocols, and it is possible through the Protocol directive in the configuration to allow either protocol 1, protocol 2 or both. SSH1 is depreciated but is still in use in many organizations and applications. It is advisable to check your sshd_config file, and if you are not dependent on SSH1, disable this and run only protocol 2 on your server. This eliminates any chances of falling victim to an insecurity associated with version 1.

Earlier, while you were perusing your password file to build your user list, you probably noticed that there is an sshd user with a home directory of /var/empty and a name listed as Privilege-separated SSH. If this user does not exist, the following is of particular importance, and you will want to look further into running sshd in privilege-separated mode. Privilege separation in sshd is a multipart process that entails the sshd process of creating a privileged monitor process, which creates an sshd process with the privileges of the user. This user-owned process in turn spawns the shell process. The privilege separation process is run via chroot and is restricted to the /var/empty directory. For those of you familiar with running processes in a chroot environment, this privilege separation is the same. It allows protection to the listening dæmon if a buffer overflow or similar compromise is discovered. The /var/empty directory should be root-owned, empty and it should not be world- or group-writable. If an sshd user does not exist, privilege separation will not work, and systems that lack mmap or anonymous memory mapping compression must be disabled.

Consider a situation where a machine has a minimal amount of users that are accessing it through SSH. Quite possibly, you own a machine that is accessed only by a couple of accounts, and then su or sudo is used for administrative purposes. Consider also the scripts that often are run to seek the machines that are running an SSH server. Although it is possible that the scripts may do a full-system port scan to expedite the scanning and identify possible victims, a specific port (22 in the sshd case) is often the only port scanned, and if found open, it is expanded upon. The logical alternative to this, especially in machines with minimal users logging in, is to run sshd on an alternate port. Specifically, in the sshd_config file, one of the very first options is the port. By changing the port from 22 to an alternate port, you can write off a good amount of the scripts that are scanning for open port 22. This is such a trivial configuration change, but it is one that will result in a drastic lessening of brute-force attempts (Listing 4).

Listing 4.

Changing the Port

```
The strategy used for options in the default
# sshd_config shipped with
# OpenSSH is to specify options with their
# default value where
# possible, but leave them commented.
# Uncommented options change a default value

Port 13
Protocol 2
```

Given even the slowest typist on the planet, what would be the expected time to allow them to enter a password? Assuming an eight-character password, would it be eight seconds? Give them two seconds a character, and they have a hearty 16 seconds. Allow them 20 seconds of network latency, and we are at just more than 30 seconds, which seems like a more than generous amount of grace time. This is often surpassed with the default sshd configuration, though with the LoginGraceTime sometimes set as high as 120 seconds. This is the maximum amount of time that the server allows for a successful login. Ask yourself, if one were to knock on your house door and you were behind it, what would the maximum amount of time for deciding whether to let this person or people in? Coupled with this, we have another unique login directive named MaxStartups. This MaxStartups directive can be a very powerful deterrent when fighting the SSH scanners. MaxStartups specifies the maximum number of concurrent unauthenticated connections to the SSH dæmon. Note that this means unauthenticated connections. Therefore, if a script were running, trying to brute-force its way into the machine, and the script was able to fork processes, it could launch multiple (maybe even hundreds) of login attempts almost simultaneously. A good rule of thumb is to use one-third the number of your total remote users with a maximum setting of 10.

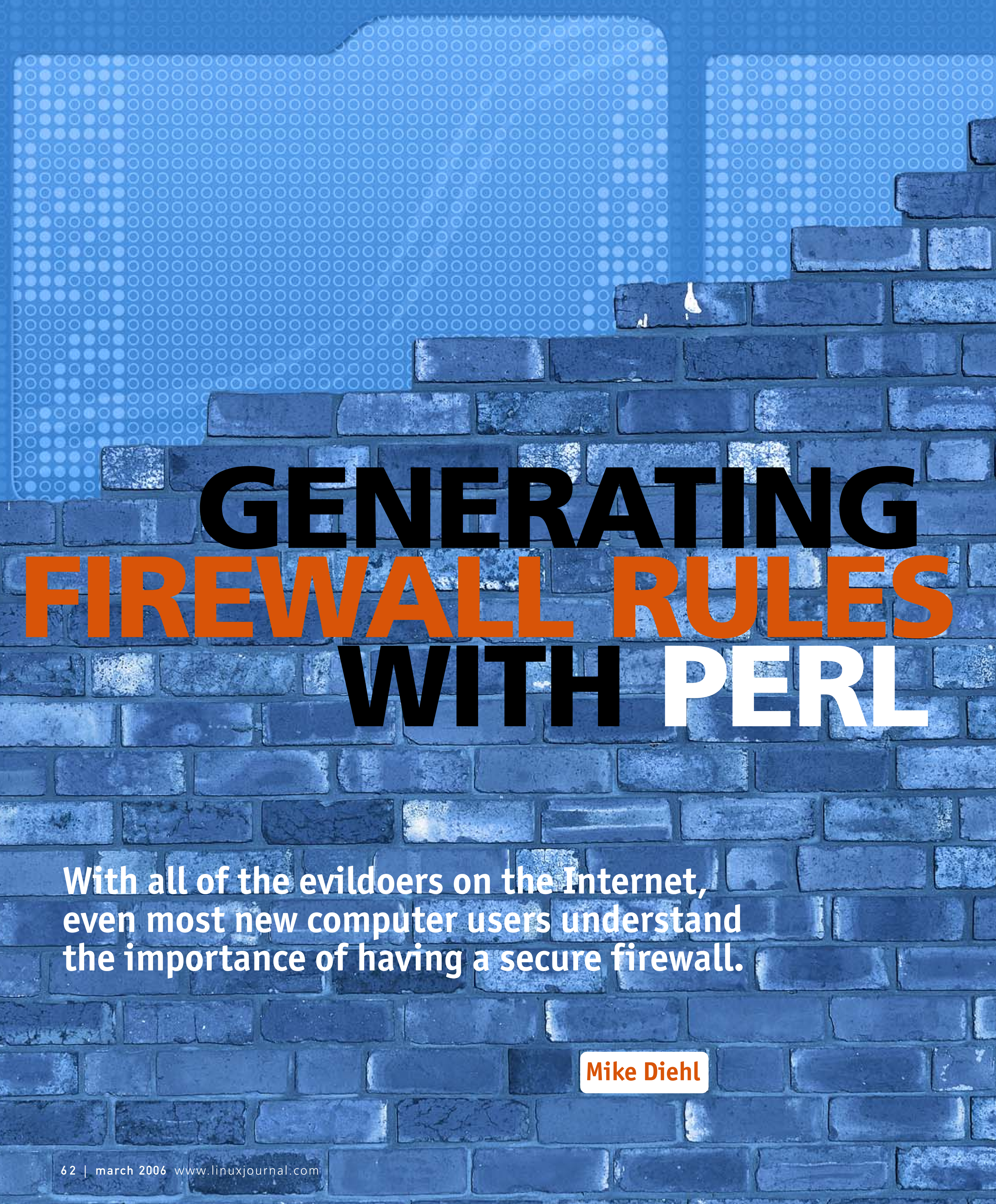
INITIATING THE CHANGES

There is little to be considered to implement the changes mentioned. The default configuration is merely a guide, and it is the administrator's responsibility to expand on the guide and harden the sshd configuration. Prior to making the changes, it is highly recommended that you temporarily start sshd on an alternate port to provide yourself with a back door should you misconfigure the primary sshd and lose the connection. When issuing a restart on sshd, it is possible to make a mistake in the configuration file, which will result in the dæmon failing to restart (if it is first stopped). Doing `ssh -p <alternate port>` will allow a second dæmon to run and provide you with a secondary secure connection should the first one fail due to a configuration error. We are after all, working remotely, and if we lose the SSH dæmon without an alternate, physical access to the console will be required to make further modifications. Even though it may seem obvious, it is worth mentioning that you must issue a SIGHUP or restart the SSH dæmon for any changes to take place. To expand further on the idea of a second port being opened, it is possible to add a startup script for a second sshd to run with an alternate sshd_config file that specifies no options other than a single-user account from a single source. This essentially allows you to guarantee yourself access from a (presumed) secure machine if the initial dæmon is ever shut down.

SUMMARIZING THE CHASE

For Linux systems administrators, it really comes down to you or a group of people against the world. You are on one end, providing access to your machine, and on the other end is a world of network-connected people, many of whom would like to have access to your machine. Usually the tools that are used to exploit the SSH dæmon are built with the default configurations in mind. It is the low-hanging fruit that is often the target, and it is your job to know your local environment and needs to remove that low-hanging fruit before it gets picked by others. A compromised machine causes not only havoc within your environment, it also presents a risk for the other multimillion or billion computers connected worldwide. OpenSSH provides an outstanding tool for remote access. Comparing the tool to a crescent wrench is a fair analysis. Both the wrench and OpenSSH are delivered with a wide range of capabilities. Just as you will need to adjust a crescent wrench to make the most of it, adjusting the default configuration of OpenSSH will maximize your remote-access capabilities while also providing a more secure environment.■

Phil Moses spends his days managing Linux systems for the Physical Oceanography Research Division at Scripps Institution of Oceanography and spends his time off contemplating access to those remote areas of the world that are less traveled. Phil can be reached at philmoses@cox.net.



GENERATING FIREWALL RULES WITH PERL

With all of the evildoers on the Internet, even most new computer users understand the importance of having a secure firewall.

Mike Diehl

Like most Linux users, I started out using a simple Bash script to configure the firewall policy on my Linux machines. Eventually, I got tired of writing the same code over and over again, so I decided to use a few program loops to try to factor out some of the redundancy. I also decided that I'd like to separate the actual policy from the rest of the program; this meant that the program would be reading external configuration files. As my Perl skills are vastly better than my Bash skills, I decided to write my firewall rules in Perl.

The program I'm outlining in this article could just as easily have been written in Bash or another scripting language (or even C++, for that matter). The language isn't important. The important thing to realize is that once you write a program like this and debug it, all you have to do to modify security rules is change a configuration file and rerun the script. The configuration files should have an intuitive format so that they are easy for humans to read, understand and modify.

Listing 1 shows the Perl script. I practice top-down programming, so the first several lines of code should give you a good idea of what the program does. Hopefully, you should be able to follow what the program does even if you aren't a Perl programmer.

As you can see, the program isn't very long and certainly isn't very complicated. However, the program is flexible enough to allow me to whitelist or blacklist either individual machines or entire networks completely. As we'll see later on, the build_chains() and add_rules() functions implement a rule-pruning algorithm that keeps the Linux kernel from having to evaluate irrelevant rules.

The set_ip_forwarding() function does what its name implies; it tells the Linux kernel either to forward IP packets, or not to forward packets. The function accepts a single parameter, either 0 or 1, which determines whether the kernel will forward. The script initially turns all forwarding off while it loads the firewall policy. Then, right before the script exits, the script turns forwarding back on. The reason for these extra steps is that we want the router to be in a safe state while we load the actual rules. It's better to block all traffic than it is to allow even one attack through.

The load interfaces() function reads in the names of the network interfaces and assigns mnemonic labels to them. These labels are then used in the rest of the configuration to refer to the actual interfaces. Being able to refer to an interface as lan or even vpn_to_work cuts down on misconfigurations. This also makes it easy to make changes in order to tailor the firewall for use by my friends. In many cases, I simply adjust the interfaces.conf file to reflect my friend's network and suddenly, my friend has a reasonable firewall configuration.

The script works via four configuration files: interfaces.conf, good_hosts.conf, bad_hosts.conf and ports.conf.

Listing 2 shows the contents of my interfaces.conf file. As you can see, I've got six network interfaces in my router. My Internet connection is on eth5. I've got a 10/100TX Ethernet for the house wiring. I've got a Gigabit Ethernet connecting my MythTV PVR to the router for file storage. I've got interfaces for the Wi-Fi and VoIP. Finally, I have a VPN connection to some of my friend's computers. It's much easier to remember that lan is my 10/100 copper network as opposed to trying to remember whether eth3 is my VoIP or Wi-Fi interface. The last thing you want to do is apply the right firewall rule to the wrong interface.

The init() function does the initial setup for the iptables environment. First, we flush, or remove, all of the rules and user chains. Then, we clear all of the rule counters. Later on, these counters will allow us to determine how many packets were caught by each rule in our firewall. Then, the script sets up the IP masquerading. I also put in a rule that allows traffic that is related to an already established connection to pass through the firewall without further evaluation. This keeps the entire rule set from having to be evaluated for each incoming packet. The rules apply only to each new connection request.

The set_default_policy() function configures how we treat network traffic in the absence of any other firewall rules. In this case, I'm interested only in policing incoming traffic; the policy accepts outbound traffic and traffic that the kernel has to route to its final destination. Trivial modifications to this script would allow you to configure policies for each direction. By default, my script denies traffic and requires the administrator to list explicitly all of the allowable traffic. This is the safest way to build a firewall, as opposed to a firewall that allows traffic by default and relies on the administrator to deny dangerous traffic specifically. You can never know in advance all of the dangerous traffic, so denying everything but well-understood traffic is a good idea.

The add_good_hosts() function creates firewall rules that allow all traffic from hosts or networks listed in the good_hosts.conf file. Note that I don't tie these rules to any particular interface. Traffic from whitelisted hosts or networks can come in on any interface. I usually put an entry in this file for my workstation at my home office as well as the network at work. This way, even if I make a silly mistake that would have kept me from logging in to my router remotely, I can still get in from work or my office workstation to undo the change. Of course, this also assumes that my workstation and the network at work haven't been compromised. Usually, the contents of this file are quite short indeed.

Conversely, the add_bad_hosts() function creates firewall rules that block all traffic from hosts or networks listed in the bad_hosts.conf file. This function works almost exactly like the add_good_hosts() function with one important difference. When traffic from a blacklisted host comes to the router, the router will not only log this fact, it will also include the comment from the bad_hosts.conf file in the log. This way, I can look at my log file and see why a particular host was blocked. A useful improvement to this function would be to have it place the bad host rules in a separate chain and have that chain called early on in the rule set. This would give you the ability to add and delete hosts conveniently from this chain from an external program, perhaps in response to entries in your server log files.

The build_chains() function builds a series of firewall rule chains. I build a separate chain for each combination of interface and protocol. For example, if I had a Linux router with eth0, eth1, eth2 and eth3, I would create chains for eth0-tcp, eth0-udp, eth1-tcp, eth1-udp and so on. Then, I build the rules necessary to send the decision-making process down the appropriate chain. What we end up with is a decision tree that determines what to do with each packet entering the router. Unlike a linear list of firewall rules, the decision tree prevents the kernel from having to evaluate obviously irrelevant rules. For example, a TCP packet coming in on the WAN interface will never be tested against the rules meant for UDP packets on the Wi-Fi interface.

I haven't done any objective testing to see if this tree-pruning actually makes a significant performance improvement. On the other hand, once the program is written and debugged, it costs me nothing to change the configuration files and have this decision tree generated automatically. So even if it improves performance by only a small amount, it adds so little to the program's complexity that I think it makes sense to do it.

The add_rules() function is where most of the work is done. This function reads the contents of ports.conf, which is shown in Listing 5. Before we discuss the add_rules() function in detail, we should discuss the format and content of the ports.conf file.

The ports.conf file contains one line for each firewall rule. Each line contains three columns and an optional comment preceded by the # character. The first column is the user-defined label for the interface that the rule will be applied to. The second column is the protocol, that is, tcp, udp or the special case, all. Using all for the protocol creates a rule that allows all traffic on the interface in question. Finally, we have the port number. For example, the first line of the file creates a rule that allows SSH traffic to come in on the wan interface.

You'll notice that I have a rule that allows all traffic on the lo, or loopback, interface. This is important, because without this rule, many programs break in ways that are hard to diagnose. You also may be asking why I go to the effort of creating so many firewall rules for my LAN interface, only to have an all at the end. I do this for several reasons. The primary reason is that until my kids grow up and get on the Internet, I trust the traffic on my local network. However, by having rules for each service I run, I'm able to

Listing 1.

firewall.pl

```
#!/usr/bin/perl

$default_policy = "DROP";

$iptables = "/sbin/iptables";
$work_dir = "/root/fw";

set_ip_forwarding(0);

load_interfaces();

$protocols{tcp}++; $protocols{udp}++; $protocols{icmp}++;

init();

set_default_policy();

add_good_hosts();
add_bad_hosts();

build_chains();
add_rules();

set_default_action();

set_ip_forwarding(1);

exit;

###################################################

sub    load_interfaces {
    my($int, $name);
    local(*FILE);

    open FILE, "$work_dir/interfaces.conf";
    while (<FILE>) {
        chomp($_);
        if ($_ eq "") { next; }

        ($name, $int) = split(/\s*=\s*/, $_);
        $interface{$name} = $int;
    }
}

sub    init {
    iptables("-F");  # flush rules
    iptables("-t nat -F");
    iptables("-X");  # delete chains
    iptables("-Z");  # zero counters

    iptables("-t nat -A POSTROUTING -j MASQUERADE");
    iptables("-A INPUT -m conntrack --ctstate ESTABLISHED
        -j ACCEPT");
}

sub    set_default_policy {
    iptables("-P INPUT $default_policy");

    iptables("-P OUTPUT ACCEPT");
    iptables("-P FORWARD ACCEPT");
```

```
    return;
}

sub    build_chains {
    my($interface, $protocol, $chain);

    foreach $interface (keys %interface) {
        foreach $protocol (keys %protocols) {
            $chain = "$interface-$protocol";

            iptables("-N $chain");
            iptables("-A INPUT -i $interface{$interface}
                -p $protocol -j $chain");
        }
    }
}

sub    add_rules {
    local(*FILE);

    open FILE, "$work_dir/ports.conf";
    while (<FILE>) {
        chomp($_);
        $_ =~ s/#.?//;
        if ($_ eq "") { next; }

        ($int, $proto, $port) = split(/\t/, $_);

        $i = $interface{$int};
        $chain = "$int-$proto";

        if ($proto eq "all") {
            foreach $proto (keys %protocols) {
                $chain = "$int-$proto";
                iptables("-A $chain -i $i -p $proto -j ACCEPT");
            }
            next;
        }

        if ($proto eq "udp") {
            iptables("-A $chain -i $i -p udp --dport $port
                -j ACCEPT");
            iptables("-A $chain -i $i -p udp --sport $port
                -j ACCEPT");
        }

        if ($proto eq "tcp") {
            iptables("-A $chain -i $i -p tcp --dport $port --syn
                -j ACCEPT");
            iptables("-A $chain -i $i -p tcp --dport $port
                -j ACCEPT");
        }
    }
}

sub    set_default_action {
    my($interface, $protocol, $chain);

    foreach $interface (keys %interface) {
        foreach $protocol (keys %protocols) {
            $chain = "$interface-$protocol";
            iptables("-A $chain -j LOG
                --log-prefix DEFAULT_$default_policy-$chain-");
            iptables("-A $chain -j $default_policy");
        }
    }
}

sub    iptables {
    my($line) = @_;
    print "$iptables $line > /dev/null\n" if ($debug);
    $result = system("$iptables $line > /dev/null");
    if ($result != 0) {
        print "X: ($result) iptables $line\n";
    }
}

sub    set_ip_forwarding {
    my($value) = @_;
    local(*FILE);

    print "Setting IP forwarding to $value.\n";
    open FILE, ">/proc/sys/net/ipv4/ip_forward";
    print FILE $value;
    close FILE;
}

sub    add_good_hosts {
    my($host, $comment);
    local(*FILE);

    open FILE, "$work_dir/good_hosts.conf";
    while (<FILE>) {
        ($host, $comment) = split(/\t/, $_);

        iptables("-A INPUT -s $host -j ACCEPT");
        iptables("-A OUTPUT -d $host -j ACCEPT");
    }

}

sub    add_bad_hosts {
    my($host, $comment);
    local(*FILE);

    open FILE, "$work_dir/bad_hosts.conf";
    while (<FILE>) {
        chomp($_);
        ($host, $comment) = split(/\t/, $_);

        iptables("-A INPUT -s $host -j LOG
              --log-prefix $comment");
        iptables("-A OUTPUT -d $host -j LOG
              --log-prefix $comment");

        iptables("-A INPUT -s $host -j DROP");
        iptables("-A OUTPUT -d $host -j DROP");
    }
}
```

Listing 2.

interfaces.conf

```
lo = lo
gig = eth0
lan = eth1
wifi = eth2
voip = eth3
wan = eth5
tun = tun0
```

Listing 3.

good_hosts.conf

```
127.0.0.1     Loopback
224.0.0.0/8     Multicast
10.4.0.0/16     VPN
10.0.1.1/32     Home office
```

Listing 4.

bad_hosts.conf

```
216.250.128.12   My_comment
www.microsoft.com       Microsoft
```

Listing 5.

ports.conf

```
wan     tcp     22     # ssh
wan     tcp     25     # smtp
wan     tcp     80     # http
wan     udp     53     # dns
wan     udp     1194     # openvpn
wan     udp     5060     # sip
wan     udp     4569     # iax2
wan     udp     10000:20000     # rtp
lo     all
lan     tcp     22     # ssh
lan     tcp     25     # smtp
lan     udp     53     # dns
lan     tcp     53     # dns
lan     udp     67     # dhcp
lan     udp     68     # dhcp
lan     tcp     80     # http
lan     tcp     111     # portmapper
lan     udp     111     # portmapper
lan     tcp     143     # imap
lan     tcp     443     # https
lan     tcp     2049     # nfs
lan     udp     2049     # nfs
lan     tcp     3306     # mysql
lan     udp     4569     # iax2
lan     udp     5060     # sip
lan     tcp     5432     # postgresql
lan     tcp     10000     # webmin
lan     all
gig     all
tun     all
wifi     udp     1194     # openvpn
voip     udp     5060     # sip
voip     udp     4569     # iax2
voip     udp     53     # dns
voip     tcp     22     # ssh
voip     udp     10000:20000     # rtp
voip     tcp     80     # http
```

extract statistics about how much traffic each service generates. Also, security is an iterative process. Over time, I'll add rules that will further tighten my firewall; eventually, I'll remove the final all from the policy.

Now, back to the add_rules() function. Even though this is the longest function in the entire program, it's still not too hard to understand. The sections of code that deal with tcp and udp rules simply create two rules for each rule in the ports.conf file. One rule is tied to the destination port number; the other rule is tied to the source port number. At first, this may seem odd, because we are policing only inbound traffic. What we're doing is making sure that both inbound and outbound connections are allowed to pass. For example, a packet coming in on the WAN interface with the destination port set to 80 corresponds to an inbound connection to my Web server. On the other hand, an incoming packet on my WAN interface with the source port set to 80 is coming from an outside Web server in response to a request that came from inside my network.

The code that handles the all rules is a special case. In this case, we create a rule on the given interface for each of the protocols. In hindsight, this might be overly complex, but it has an interesting side effect. If the router encounters a packet containing an unknown protocol, such as IPSec, the firewall will fall back to its default policy even though we've asked it to pass all traffic on this interface. So, in a sense, "all protocols" actually means "all known protocols". I think this is a good thing.

For what it's worth, the script will put firewall rules into the kernel in roughly the same order that they appear in the ports.conf file. I say roughly, because the rules will be put into the appropriate chain depending on which interface and protocol they match against. But within each chain, the rules will be executed in order.

The set_default_action() function creates rules that determine what happens to packets that don't match any previous rules. This sounds very similar to the purpose of the set_default_policy() function, but there is a subtle difference. The set_default_policy() function configures the default firewall policy, and the set_default_action() function creates firewall rules that catch unmatched traffic before the kernel falls back to the default policy, essentially capping each chain. Once these rules match a packet, they create a log entry for the packet, and then they implement whatever policy we want, in this case, DROP. Once again, the log entries allow me to determine what traffic is being dropped and why.

I'm not trying to tell you that this program is perfect, nor will it do everything you want it to do. You might even find bugs in it. In fact, by the time you read this article, I'll probably have made several improvements to the script. As it is right now, the script isn't able to configure any firewall policy for the ICMP protocol. It would be nice to be able to allow outbound ping requests and deny incoming requests, for example. It would also be useful to be able to configure firewall policy for outgoing and routed traffic. And because I'm using VoIP, I'm thinking of changing my script to allow me to configure Quality of Service (QoS). If you come up with useful modifications to this script, I'd like to hear about them.

But there you have it, such as it is. In less than 200 lines of Perl code, I'm able to implement a quite flexible and efficient firewall policy containing potentially hundreds of individual rules. At the same time, making changes to my firewall policy is simple enough that even most beginning Linux users can make correct changes.■

Mike Diehl works for SAIC at Sandia National Laboratories in Albuquerque, New Mexico, where he writes network management software. Mike lives with his wife and two small boys and can be reached via e-mail at mdiehl@diehlnet.com.

LINUXWORLD® CONFERENCE & EXPO

Conferences: April 3 – 6, 2006
Expo: April 4 – 6, 2006

Introducing: OpenSolutions WORLD™

Boston Convention & Exposition Center

BOSTON'06

2 Conferences
10 Tracks
100+ Sessions
Over 200 Exhibitors

LinuxWorld Conference tracks

- *Mobile & Embedded Linux*
- *Network Management*
- *Kernel and Driver Development*
- *Linux on the Desktop*

OpenSolutions World Conference tracks

- *Business Case*
- *Security*
- *Open Source Applications*
- *Enterprise Application Development*
- *Dynamic IT: Cluster/Grid Virtualization*
- *Emerging Trends*

Open source means business.

Find out what it can mean for your business at LinuxWorld Conference & Expo—in ten tracks and more than 100 in-depth sessions, tutorials, and workshops led by the open source movement's top minds.

Go beyond Linux.

Expand your vision at OpenSolutions World, a new conference at LinuxWorld covering the full spectrum of open source solutions and strategies for the enterprise.

Get the full picture.

Explore a comprehensive exhibition of open source products, technologies, and services from more than 200 key Linux and open source vendors—all under one roof.

Put it to work.

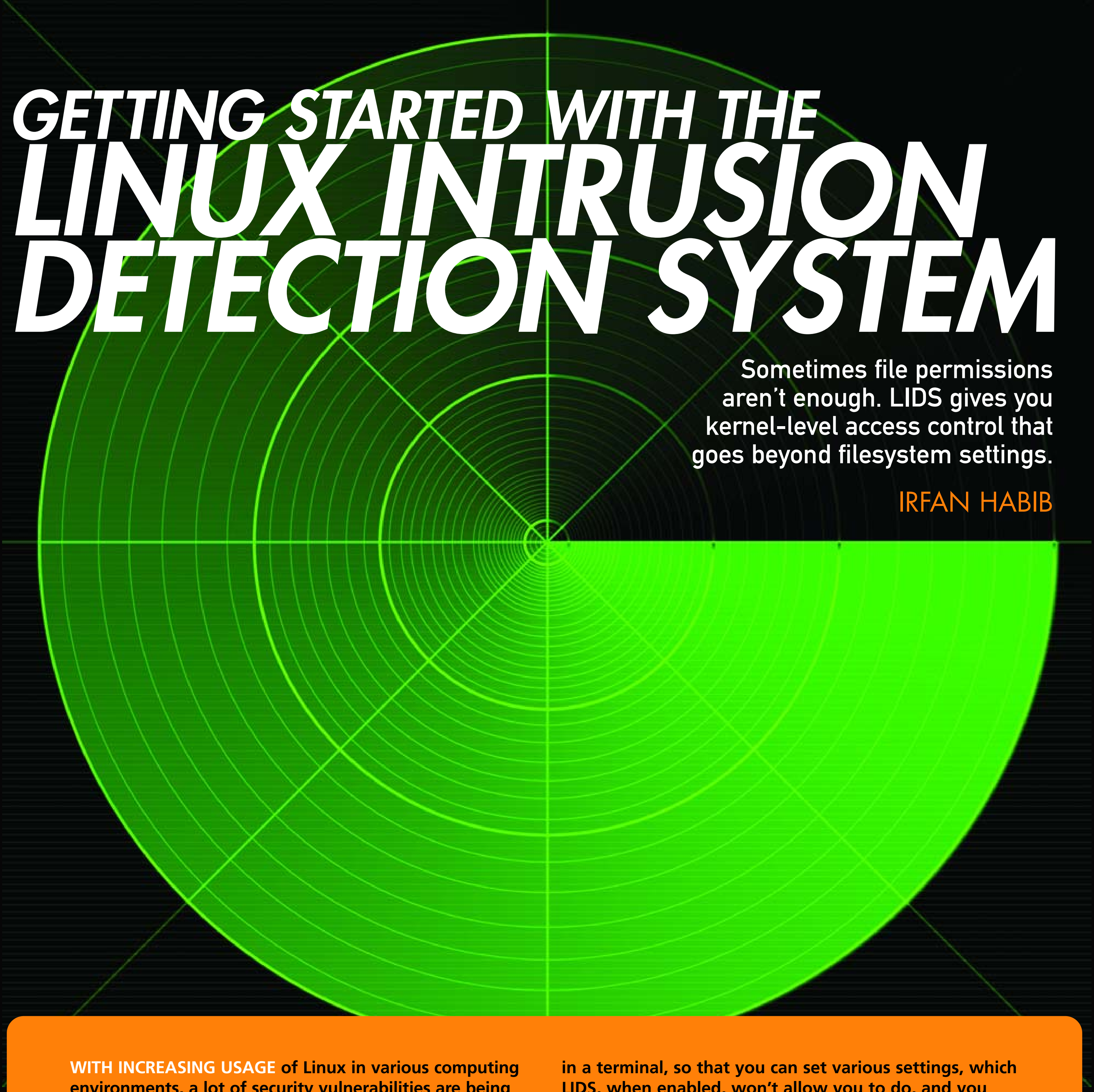
Come to LinuxWorld Conference & Expo April 3 – 6, 2006, and harness the power of the entire open source community for your business. The future of enterprise technology is wide open.

Register by 3/3 and save
Enter priority code D0102 and save up to $500
www.linuxworldexpo.com/boston

IDG INTERNATIONAL DATA GROUP   IDG WORLD EXPO

D0102

GETTING STARTED WITH THE LINUX INTRUSION DETECTION SYSTEM



Sometimes file permissions aren't enough. LIDS gives you kernel-level access control that goes beyond filesystem settings.

IRFAN HABIB

WITH INCREASING USAGE of Linux in various computing environments, a lot of security vulnerabilities are being discovered in GNU/Linux-based systems. Due to the open nature of application development in the Open Source world, a lot of vulnerabilities are being addressed very quickly. But, it may happen that a patch is not addressed in a timely manner, and in the meantime, all the systems running the application are exposed. Malicious users can possibly gain root privileges and wreak havoc with these systems. This is where the Linux Intrusion Detection System (LIDS) comes to the rescue.

LIDS is a patch to the Linux kernel; it implements access control and a reference monitor. LIDS is configured with its two admin tools, lidsconf and lidsadm.

lidsadm is the utility that allows you to disable LIDS in a terminal, so that you can set various settings, which LIDS, when enabled, won't allow you to do, and you can view the current status of your LIDS installation with this tool.

lidsconf is the tool that allows you to add and remove access control to certain files, which can be binaries or any other files. LIDS refers to these files as objects, and the capabilities we allow or disallow are referred to as subjects. LIDS overrides things like filesystem permissions. You can literally use LIDS to make it impossible to access virtually any object, whether it's a file, raw device, memory or I/O, even if you're trying to access the object as the root user.

In short, LIDS is a complete security model implementation for the Linux kernel.

Installation

The developers of LIDS have included installation instructions in the INSTALL file. However, I describe the main tasks in this article.

The stable releases of LIDS are created against a vanilla source of the Linux kernel. It is recommended that the LIDS patch be applied only to the original kernel source, not to the distribution-specific source, as it may lead to various compilation errors, as most distributions customize the kernel for their own use. LIDS is known to have problems when used on non-i386 architectures.

For example, lids-2.2.1-2.6.13.tar.gz should be applied to the 2.6.13 kernel.

After patching the kernel with:

```
patch -p1 /dir_to_the_patch_file/patch-lids-2.2.1-2.6.13
```

You can run `make [x/menu]config` and select the LIDS options from the security section and compile the kernel with:

```
make

make modules_install
```

(if you configured any parts of the kernel as modules).

Copy the bzImage from /kernelpath/arch/i386/boot to your /boot directory, and re-initialize your bootloader. Restart into your LIDS-enhanced kernel.

You can see the status of your LIDS installation by typing:

```
lidsadm -V
```

If you get an error, LIDS was not installed into the kernel; check your kernel configurations and recompile.

Setting Access Controls

Before we set access controls for various server applications, here is the general syntax of lidsconf:

```
lidsconf -A [-s subject] -o object [-d] [-t from-to] [-i level] -j ACTION
```

The subject is a program upon which a capability is added. The object can be a binary, directory, socket name or a capability.

The -d switch tells LIDS that the domain is an exec domain. The -t lets you set a specific time dependency for the capability and -i defines the inheritance level.

The -j switch is an action that can be one of the following:

- DENY: denies access to the object.
- READONLY: sets the object to read-only.
- APPEND: mostly used for logs, this allows a certain program to append only that file, not remove it.
- WRITE: allows other binaries to write on the file.
- GRANT: used in conjunction with a capability, used to grant the subject a capability.
- IGNORE and DISABLE: two options that allow you to disable the setting of any permission on a certain object and disable some extension features, respectively.

The capabilities LIDS supports are the following, as can be seen by typing:

```
lidsadm -h|grep CAP
```

- CAP_CHOWN: chown/chgrp.
- CAP_DAC_OVERRIDE: DAC access.
- CAP_DAC_READ_SEARCH: DAC read.
- CAP_FOWNER: owner ID, not equal user.
- ID CAP_FSETID: effective user ID, not equal owner.
- ID CAP_KILL: real/effective ID, not equal process.
- ID CAP_SETGID: set*gid(2).
- CAP_SETUID: set*uid(2).
- CAP_SETPCAP: transfer capability.
- CAP_LINUX_IMMUTABLE: immutable and append file attributes.
- CAP_NET_BIND_SERVICE: binding to ports below 1024.
- CAP_NET_BROADCAST: broadcasting/listening to multicast.
- CAP_NET_ADMIN: interface/firewall/routing changes.
- CAP_NET_RAW: raw sockets.
- CAP_IPC_LOCK: locking of shared memory segments.
- CAP_IPC_OWNER: IPC-ownership checks.
- CAP_SYS_MODULE: insertion and removal of kernel modules.
- CAP_SYS_RAWIO: ioperm(2)/iopl(2) access.
- CAP_SYS_CHROOT: chroot(2).
- CAP_SYS_PTRACE: ptrace(2).
- CAP_SYS_PACCT: configuration of process accounting.
- CAP_SYS_ADMIN: tons of admin stuff.
- CAP_SYS_BOOT: reboot(2).
- CAP_SYS_NICE: nice(2).
- CAP_SYS_RESOURCE: sets resource limits.
- CAP_SYS_TIME: sets system time.
- CAP_SYS_TTY_CONFIG: tty configuration.
- CAP_MKNOD: mknod operation.
- CAP_LEASE: taking leases on files.
- CAP_HIDDEN: hidden process.
- CAP_KILL_PROTECTED: kill protected programs.
- CAP_PROTECTED: protect the process from signals.

Setting Up a LIDS-Enabled Server

This article assumes that you have installed LIDS and its associated administration tools.

We will set up a system with tight security settings, and the services that will be allowed to run are MySQL, Apache and Bind.

The sample commands below assume that the Apache installation resides in /usr/local/apache, with a log directory of /var/log/httpd, and also assumes your Apache configuration directory is /etc/httpd. MySQL is assumed to be installed in /usr/local/mysql. Obviously, you'll want to change the commands to suit your installation if it differs.

It is beyond the scope of this article to cover everything necessary to secure your system completely. However, these examples of how access control is administered in LIDS should get you started.

Setting Up a System

After you restart LIDS, you can begin adding access controls to various system binaries and libraries. The following sets the /sbin, /bin, /usr/bin and /lib to read-only:

```
lidsconf -A -o /sbin -j READONLY

lidsconf -A -o /bin -j READONLY

lidsconf -A -o /usr/bin -j READONLY

lidsconf -A -o /lib -j READONLY
```

Next, we define some additional access controls for /opt, /etc and /usr/local/etc, which should be read-only, and we deny all access to /etc/shadow and the boot manager file:

```
lidsconf -A -o /etc -j READONLY

lidsconf -A -o /usr/local/etc -j READONLY

lidsconf -A -o /etc/shadow -j DENY

lidsconf -A -o /etc/lilo.conf -j DENY
```

Because we have denied all access to /etc/shadow, the system will not be able to authenticate logins, thus we need to allow login and vlock to have read-only access to the file. Additionally, su also should have read-only access to the /etc/shadow file:

```
lidsconf -A -s /bin/login -o /etc/shadow -j READONLY

lidsconf -A -s /usr/bin/vlock -o /etc/shadow -j READONLY

lidsconf -A -s /bin/su -o /etc/shadow -j READONLY
```

We need to set some other access controls for su, in order for it to work with UIDs and GIDs, and access the /etc/shadow file:

```
lidsconf -A -s /bin/su -o CAP_SETUID -j GRANT

lidsconf -A -s /bin/su -o CAP_SETGID -j GRANT

lidsconf -A -s /bin/su -o /etc/shadow -j READONLY
```

Now, we need to allow init, login and associated applications to have write access to log files:

```
lidsconf -A -o /var/log -j APPEND

lidsconf -A -s /bin/login -o /var/log/wtmp -j WRITE

lidsconf -A -s /bin/login -o /var/log/lastlog -j WRITE

lidsconf -A -s /sbin/init -o /var/log/wtmp -j WRITE

lidsconf -A -s /sbin/init -o /var/log/lastlog -j WRITE

lidsconf -A -s /sbin/halt -o /var/log/wtmp -j WRITE

lidsconf -A -s /sbin/halt -o /var/log/lastlog -j WRITE

lidsconf -A -s /etc/rc.d/rc.sysinit \
-o /var/log/wtmp -i 1 -j WRITE

lidsconf -A -s /etc/rc.d/rc.sysinit \
-o /var/log/lastlog -i 1 -j WRITE
```

Now, we set up access control for root's home folder. We allow only the bash history file to be appended:

```
f -A -o /root -j READONLY

lidsconf -A -s /bin/bash -o /root/.bash_history -j APPEND
```

Finally, we allow the init program to kill processes on shutdown:

```
lidsconf -A -s /sbin/init -o CAP_INIT_KILL -j GRANT

lidsconf -A -s /sbin/init -o CAP_KILL -j GRANT
```

Now, we allow fstab and init scripts to mount filesystems, kill processes and unmount filesystems:

```
lidsconf -A -s/etc/fstab -o CAP_SYS_ADMIN \
-j 1 -j GRANT

lidsconf -A -s /etc/rc.d/init.d/halt \
-o CAP_INIT_KILL -i 1 -j GRANT

lidsconf -A -s /etc/rc.d/init.d/halt \
-o CAP_KILL -i 1 -j GRANT

lidsconf -A -s /etc/rc.d/init.d/halt \
-o CAP_NET_ADMIN -i 1 -j GRANT

lidsconf -A -s /etc/rc.d/init.d/halt \
-o CAP_SYS_ADMIN -i 1 -j GRANT
```

Setting Access Controls for the Apache Web Server

Apache needs to have setuid and setgid capabilities. We also need to allow Apache to access log files and deny other applications from accessing the httpd binary:

```
lidsconf -A -s /usr/local/apache/bin/httpd \
-o CAP_SETUID -j GRANT

lidsconf -A -s /usr/local/apache/bin/httpd \
-o CAP_SETGID -j GRANT

lidsconf -A -o /etc/httpd -j DENY

lidsconf -A -s /usr/local/apache/bin/httpd \
-o /etc/httpd -j READONLY

lidsconf -A -o /usr/local/apache -j DENY
lidsconf -A -s /usr/local/apache/bin/httpd \
-o /usr/local/apache -j READONLY

lidsconf -A -o /var/log/httpd -j DENY

lidsconf -A -s /usr/local/apache/bin/httpd \
-o /var/log/httpd -j APPEND

lidsconf -A -s /usr/local/apache/bin/httpd \
-o /usr/local/apache/logs -j WRITE
```

MySQL

For MySQL, we need to deny other applications' access to the mysql binary. We also need to restrict access to the mysql/var directory so that it's append=only, and allow read-only access for the mysqld dæmon to the mysql directory:

```
lidsconf -A -o /usr/local/mysql/var -j APPEND

lidsconf -A -o /usr/local/mysql -j DENY

lidsconf -A -s /usr/local/mysql/libexec/mysqld \
-o /usr/local/mysql -j READONLY

lidsconf -A -s /usr/local/mysql/libexec/mysqld \
-o /usr/local/mysql/var -j WRITE
```

Bind

Bind needs a lot of capabilities to run:

```
lidsconf -A -s /usr/sbin/named  \
-o CAP_NET_BIND_SERVICE 53 -j GRANT


lidsconf -A -s /usr/sbin/named \
-o CAP_SETPCAP -j GRANT

lidsconf -A -s /usr/sbin/named \
-o CAP_SYS_CHROOT -j GRANT

lidsconf -A -s /usr/sbin/named \
-o CAP_SYS_RESOURCE -j GRANT

lidsconf -A -s /usr/sbin/named \
-o CAP_SETUID -j GRANT

lidsconf -A -s /usr/sbin/named \
-o CAP_SETGID -j GRANT
```

Login

Login is the program that allows a user to log in to a GNU/Linux system:

```
lidsconf -A -s /bin/login -o /etc/shadow -j READONLY

lidsconf -A -s /bin/login -o CAP_SETUID -j GRANT

lidsconf -A -s /bin/login -o CAP_SETGID -j GRANT

lidsconf -A -s /bin/login -o CAP_CHOWN -j GRANT

lidsconf -A -s /bin/login -o CAP_FSETID -j GRANT
```

After having specified the previous commands, we need to seal the kernel, so that the system can take full advantage of LIDS. We add this line to rc.local:

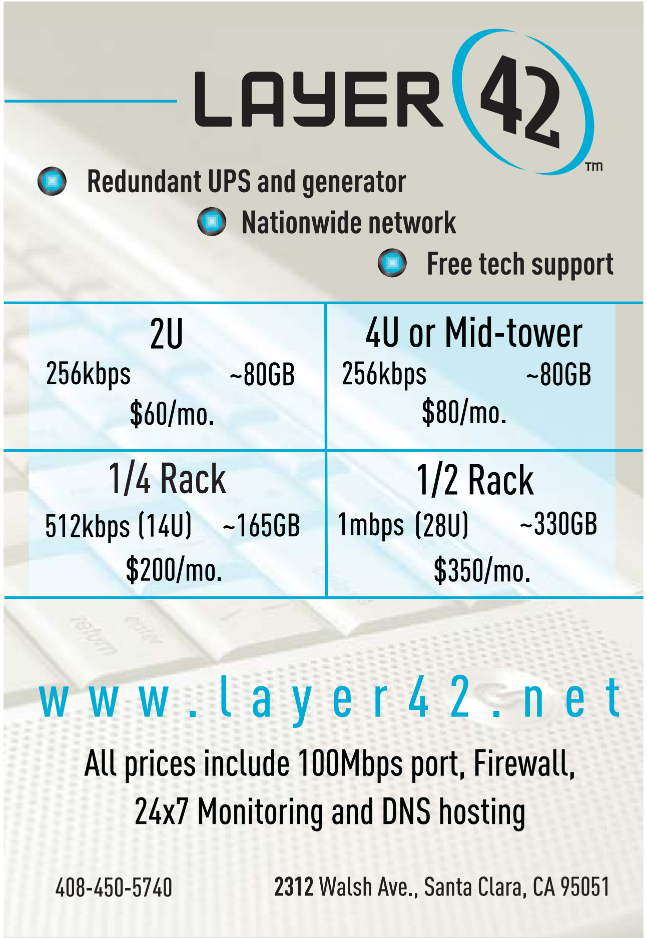
```
lidsadm -I
```

Restart the machine to apply all the new access controls. With the previously mentioned access controls, you will not be able to run the X server as it uses raw I/O, but most servers don't run an X server anyway. If you really need it, add the following access control (this command assumes that your X server binary is located in /usr/X11R6/bin/startx):

```
lidsconf -A -s /usr/X11R6/bin/startx
```

As we can see, LIDS is a powerful addition to the Linux kernel, which can secure your system completely, even from the root user. LIDS is also very easy to use.■

Irfan Habib is a software engineering student at the National University of Science and Technology in Pakistan. He has had great interest in Linux and open-source technology since high school—everything from embedded Linux development to Web services. He has been advocating GNU/Linux in Pakistan for the past two years and has written various articles in local magazines and newspapers on the subject.



Single Sign-On and the Corporate Directory, Part IV

We wrap up the single sign-on series with CUPS printing, SSH and firewall rules. TI LEGGETT

Welcome back for the last article on using your single sign-on and corporate directory infrastructure. What we've covered so far is how to set up the infrastructure and how to plug various types of clients running different operating systems in to that infrastructure. The majority of that work benefits your users in enabling them to sign on only once, after which they can use a variety of resources, such as storage shares, printers, e-mail and more.

This month, we cover methods to use Kerberos and LDAP to make your job easier. As always, the sample programs and other files are available from the on-line Resources.

Unified Printing Made Easy

No matter what size your shop is, printing is always a necessity. Unfortunately, printing also can be one of the most error-prone processes as well, especially in a heterogeneous environment. Luckily, the CUPS (Common UNIX Printing System) Project has been established. The goals of CUPS are to provide a standards-based printing solution and to provide unified printing for UNIX-based systems. Today, it's the default printing system for most Linux distributions as well as Apple OS X.

Setting up a basic print server using CUPS is simple. To get a basic understanding of CUPS and a working install, you should read Colin Topliss' article "Centralized Printing Using CUPS" (see Resources). Make sure to configure the CUPS server on one of your Samba servers if you want to enable Windows clients to print. We cover how to do this shortly.

The first thing to do after setting up your print server is enabling encryption using SSL. You should create a certificate signing request, or CSR, and sign it with your CA. Save the certificate and key in /etc/ssl/cups as cups-cert.pem and cups-key.pem, respectively. Also, make sure that they're owned by the user that cupsd uses, usually lp, and that the permissions are set properly on the private key, 0400. Next, make some changes to /etc/cups/cupsd.conf:

```
ServerCertficate /etc/ssl/cups/cups-cert.pem
ServerKey /etc/ssl/cups/cups-key.pem
```

Save your changes and restart cupsd.

Keeping Track of Your Print Resources

One of the most difficult tasks of print management is keeping track of all the printers to manage. Gone are the days when all the printers existed in a central location. Now printers, more than likely, are scattered around the office, attached to people's workstations, and what-not. Worse, the fact that these printers are different makes and models increases the challenge of organizing them.

The CUPS Web site (see Resources) states that LDAP support is scheduled for inclusion in version 1.3. Version 1.1 is currently stable, and 1.2 has been in testing for some time now. However, this needn't stop us from using LDAP as a way to inventory all the printers in the office and even provide a way to automate printer addition to a CUPS server.

The IETF has been thinking about this and has developed RFC 3712, "Lightweight Directory Access Protocol (LDAP): Schema for Printer Services". I've taken the liberty of converting this RFC into an actual schema for use with OpenLDAP and included it in the on-line Resources. Include this schema in your slapd.conf file and restart slapd. Now we can add information about our printers:

```
dn: ou=printers,o=ci,dc=example,dc=com
objectClass: organizationalUnit
ou=printers

dn: printer-name=pr-laser,ou=printers,o=ci,dc=example,dc=com
objectClass: top
objectClass: printerAbstract
objectClass: printerService
objectClass: printerIPP
printer-name: pr-laser
printer-location: A101
printer-info: laserjet.ppd
printer-more-info: http://www.hp.com
printer-make-and-model: HP LaserJet
printer-uri: socket://pr-laser.example.com
```

Most of these are self-explanatory, but printer-info and printer-uri might need a little explaining. We use the printer-info attribute to specify the PostScript printer definition, PPD, to use for this printer, in this case laserjet.ppd. The printer-uri attribute is used to define the URI to contact the printer. The socket:// device is usually used for HP JetDirect connections to a printer. To find all the devices your print server supports, use the lpinfo command, which is usually kept in /usr/sbin:

```
# /usr/sbin/lpinfo -v
network socket
direct hal
```

```
network http
network ipp
network lpd
direct scsi
serial serial:/dev/ttyS0?baud=115200
direct usb:/dev/usb/lp0
network smb
```

Your output may vary depending on what options were enabled when CUPS was compiled.

You now have a printer listed in LDAP, but what can you do with it as CUPS doesn't support LDAP? At the very least, you have a central place for keeping track of all your printers and their capabilities. I've written a small Perl script that queries LDAP for all the printers in the directory, and then creates a script that can be used to add all the printers to a CUPS server. It doesn't do much, but it gives you a start on how you can use LDAP to supplement CUPS and make management a bit more tractable. If you decide to use some of the attributes, such as printer-sides-supported, printer-finishings-supported and printer-media-supported, you could easily extend the script to call lpoptions to set printer-specific settings automatically as well.

Printer Clients

One of the great things about CUPS is that the default settings for it allow it to discover other CUPS servers and the printers served by them. That means for Linux and OS X clients to use your new server, it's as easy as starting cupsd, waiting about 30 seconds, and you're off and running. Luckily, it's not much harder to get Windows clients up and running either, using Samba. Following are the required changes to the smb.conf file:

```
[global]
        ...
        load printers = Yes
        printing = cups
        printcap = cups
        printer admin = root

[printers]
        comment = All Printers
        path = /var/spool/samba
        browseable = no
        public = yes
        guest ok = yes
        writable = no
        printable = yes

[print$]
        comment = Printer Drivers
        path = /etc/samba/drivers
        browseable = yes
        guest ok = no
        read only = yes
        write list = root
```

The parameters in the global section enable CUPS printing support. The printers section makes all the printers listed in the printcap file automatically available to Windows clients. The print$ section turns on automatic driver download, or Point 'n' Print, for Windows clients. What this means is that Windows clients won't be required to install print drivers for each printer they install. When they initially connect to the printer, clients will download and install a set of generic CUPS print drivers, removing the need for the user or the administrator to worry about Windows print drivers. Save your changes and restart Samba.

Before Point 'n' Print is a reality, there are still a few more things to do. First, you should download the most recent stable CUPS drivers, version 1.1.16 as of this writing, from the Easy Software Products FTP server to your CUPS/Samba server. Untar the bundle and run the install script, cups-samba.install. If the installer puts the cups.hlp file in /usr/share/drivers, move it into /usr/share/cups/drivers with the rest of the drivers. Next, make sure the print driver share directory, /etc/samba/drivers, exists. Finally, you need to add the drivers to the Samba share. If you've removed the root Samba user out of LDAP, you'll need to re-add it for these next two steps, as you need to be a uid 0 user. Refer to Part III of this series [February 2006] if you're not sure how to do this:

```
# smbclient //localhost/print\$ -Uroot -c 'mkdir
 ➥W32X86; put /etc/cups/ppd/pr-laser.ppd
 ➥W32X86/pr-laser.ppd; put
```

```
 ➥/usr/share/cups/drivers/cupsdrvr.dll
 ➥W32X86/cupsdrvr.dll; put
 ➥/usr/share/cups/drivers/cupsui.dll
 ➥W32X86/cupsui.dll; put
 ➥/usr/share/cups/drivers/cups.hlp
 ➥W32X86/cups.hlp'
#  rpcclient localhost -Uroot -c 'adddriver
 ➥"Windows NT x86" "pr-laser:cupsdrvr.dll
 ➥:pr-laser.ppd:cupsui.dll:cups.hlp:NULL:RAW:NULL"'
```

These two commands refer specifically to the printer we added to LDAP above, pr-laser. You need to run these two commands for each printer served by your CUPS server that you want Windows clients to access. Adding these commands to the printer creation script might be a good idea if you have many printers.

Now, if you browse to your Samba/CUPS server from a Windows client, you'll see a Printers and Faxes share. If you choose that share, you'll see all the printers served via CUPS. If you right-click on a printer and choose Connect..., it automatically downloads and installs the drivers and connects to the printer, making it available to print from that client. That's it!

Automating LDAP and Kerberos Administration

Up until now, LDAP administration has been done by hand-editing LDIF files and using the command-line OpenLDAP tools. Craig Swanson and Matt Lung give some excellent pointers in their "OpenLDAP Everywhere Revisited" article (see Resources) to some GUI utilities for managing LDAP, but they overlooked one that I think needs mentioning, GQ. Although GQ is not in active development, the 1.0 beta1 version has proved to be stable and extremely useful. If GQ keeps segfaulting, though, you probably need to apply a patch to util.c (see Resources). One of the great things about GQ is its support of SASL authentication. This allows us to make modifications to LDAP using the GUI. In addition, I've found that browsing the schema has shown me object classes and attributes I probably would never have found otherwise.

If you've been a sysadmin for more than five minutes, you know the power of scripting common tasks. LDAP administration can be rather wordy, so being able to script those common tasks is invaluable. Both Perl and Python have very powerful LDAP modules. You've already been introduced to the Perl interface from last month's article's smb-create-password.pl and smb-new-machine.pl, but Python's LDAP modules are just as useful. Perl also has interfaces for Kerberos and SASL. Instead of going into an API description of each of these modules, I'm going to show you how to use them while also showing you new and different ways to use LDAP and Kerberos.

Managing Users and SSH Keys

Included in the Resources is an OpenSSH schema. One of the first uses of this schema you might think of is keeping public keys of hosts in one location, a kind of known_hosts directory. In fact, that is why this schema was created. Future versions of OpenSSH will be able to use name service switch, NSS, to look up host keys instead of always requiring a local file containing them all. This is great because you'll no longer need to push and pull known_hosts files when hosts are added or removed, but unless you've patched your versions of OpenSSH, it's not that useful yet.

At the Computation Institute, we have a large cluster that many outside collaborators use. The cluster has its own network home directories, so it doesn't mount the central NFS ones. We also didn't want password-based logins where passwords are transmitted over the wire. Normally, this would be a fine time to enforce GSSAPI-based authentication, except we don't have control over the collaborator's desktop. So, I asked a colleague of mine to write a script to automate creating the user's home directory and adding a user's SSH key to her .authorized_keys file if she provided one. Because Python is his language of choice, the mkhomedirs.py script was born.

Here's how it works. When users are granted access to the cluster, they are put into the cluster-users netgroup, which is also served from LDAP. The mkhomedirs.py script, run every hour from cron, checks the list of current users in the cluster-users netgroup to see which ones don't have home directories. When it finds a user without a home directory, it creates one and copies over necessary files, such as those from /etc/skel. Once the user provides an SSH key, the key is added to the user's sshPublicKey attribute in LDAP. The mkhomedirs.py script also checks to see which users don't have a ~/.ssh/authorized_keys file. If a user doesn't have that file and has a key in LDAP, it creates the file and adds the key to it, allowing the user to log in. This script doesn't impose the restriction that a user's authorized_keys file must contain only those keys that are in LDAP, but it would be trivial to add that functionality. A common trick in a cracker's toolbox is to add his or her SSH key to another user's authorized_keys file. If you require all keys in a user's authorized_keys file to be in the directory, you can send off warnings when an unknown key has been added to a user's authorized_keys file.

Automatic Firewall Rules Generation

Another way you might use LDAP is to create iptables rules for your hosts automatically. We achieve this by enumerating all the services for a host and all the networks that are allowed to access that service in LDAP:

```
dn: cn=login,ou=hosts,o=ci,dc=example,dc=com
objectClass: top
objectClass: ipHost
cn: login
ipHostNumber: 192.168.1.2

dn: cn=sshd,cn=login,ou=hosts,o=ci,dc=example,dc=com
objectClass: top
objectClass: ipService
cn: sshd
ipServicePort: 22
ipServiceProtocol: tcp
ipServiceProtocol: udp
description: SSH Daemon

dn: cn=all-local,cn=sshd,cn=login,ou=hosts,o=ci,
➥dc=example,dc=com
objectClass: top
objectClass: ipNetwork
cn: all-local
ipNetworkNumber: 192.168.1.0
ipNetmaskNumber: 255.255.255.0
description: Local Network
```

Next, we need something that will traverse all the hosts and give us iptables rules for each one. In the on-line Resources, I've provided a script I've written, create-iptables.sh, which does exactly that. It depends on several Perl modules to which I've provided links in the Resources. What it does, briefly, is copy a prefix file for each host that has some rules that apply for all hosts and sets up the chains we use in the script. Next, it makes sure that all the IPs the host uses are allowed to connect back to the host. It then traverses the services, opening holes for those networks listed for each service. Finally, it appends the default rule set, which is to drop all packets. All the scripts are written to the directory iptables-scripts, and all previous scripts are saved to iptables-backups. You should create these directories before running the script. These scripts can then be pushed out to the proper hosts and run to keep host rules up to date.

You could easily modify this script to generate other pieces, such as /etc/hosts.allow and network device ACLs for added security. Another use for this type of directory structure is to generate custom scans for nmap or nessus to eliminate false positives.

More LDAP Uses

The last example I've included is generating a dhcpd.conf file for your DHCP server. This script requires that the hosts in LDAP be members of both the ipHost and ieee802Device object classes and have their macAddress and ipHostNumber attributes assigned. It's not a very sophisticated script, in that it won't make sure that a host's IP is valid. It also won't handle a host that has multiple IPs or multiple subnets served by the same DHCP server.

There is a patch for ISC's DHCP server to add support for getting information directly out of LDAP, but I prefer to wait for patches to be vetted and included in the main distribution before use on production servers. For those who are curious, I've included a link in the Resources.

Many more applications are including LDAP support directly, or there are patches available. There is an LDAP sdb back end for BIND 9 for storing zone info in LDAP, and sudo has the ability to get sudoers information from LDAP. However, remember, if there's something you want to do with LDAP for your organization that requires new attributes or object classes, you can contact IANA to be assigned your own OID for use.

Extending Kerberos Use

Up until now, we've been dealing with extending the use of LDAP, but there are more ways we can make use of Kerberos as well. One important piece in your organization for which you might want single sign-on enabled is authenticating for Web resources. Many modern browsers, such as IE 6.0, Mozilla, Firefox and Safari, already (or can be made to) support GSSAPI negotiation. To make use of this, you can install and enable the Apache mod_auth_kerb module. It can negotiate ticket-based authentication for single sign-on or present the user with a traditional user name/password box and authenticate the user to the KDC.

One other extension of Kerberos has come in the form of NFSv4. Version 4 of NFS has included stronger security as part of the protocol. It has ACL support and can use a user's Kerberos credentials for access and rights. The CITI group at the University of Michigan is spearheading the Linux implementation of NFSv4 and has links to all the patches you'll need for the user-space tools. Recent 2.6 kernels come with support for NFSv4 and rpcsec_gss, but some distributions don't enable the support by default. The necessary packages can be emerged on Gentoo systems, and the support is fully there in Red Hat Enterprise Linux 4.

Wrapping Up

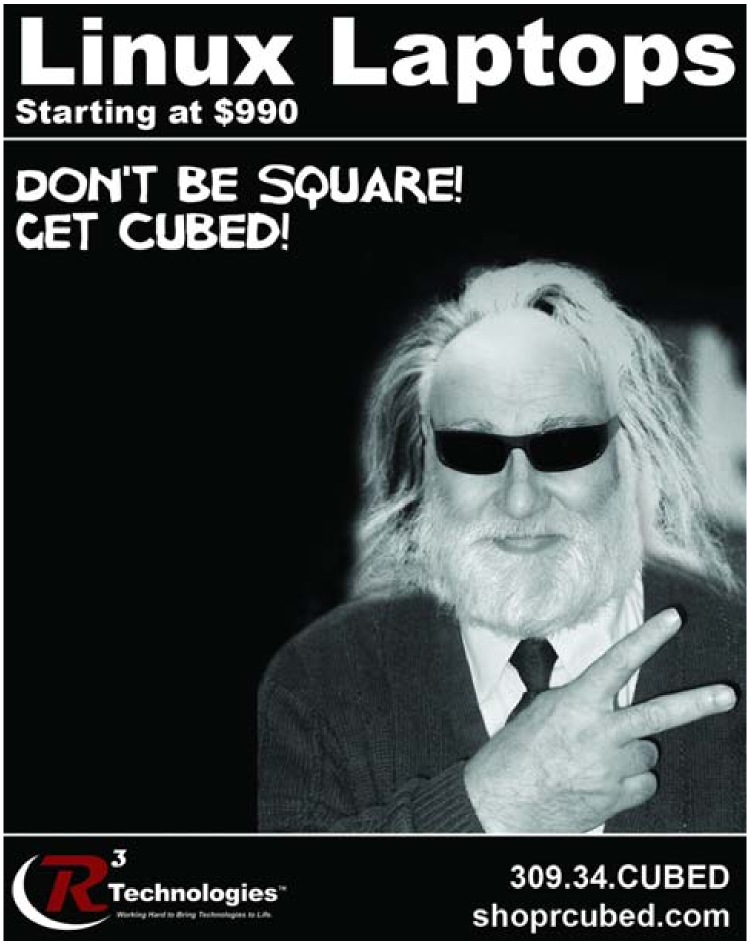
We've come a long way in this series of articles. You should have a scalable directory and single sign-on environment. We've gone over how to integrate heterogeneous clients into the infrastructure. Lastly, we've covered how you, the sysadmin, can more easily manage and leverage your LDAP and Kerberos environments.

Acknowledgements

This work was supported by the Mathematical, Information, and Computational Sciences Division subprogram of the Office of Advanced Scientific Computing Research, Office of Science, U.S. Department of Energy, under Contract W-31-109-ENG-38.4:08. Thanks to Justin Binns for the mkhomedirs.py script.

Resources for this article: www.linuxjournal.com/article/8749.■

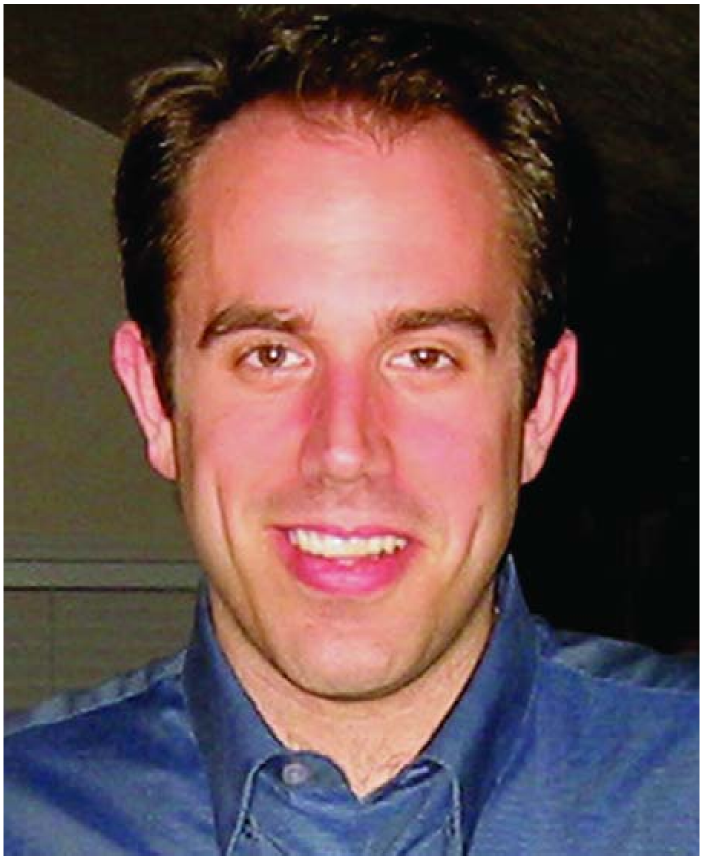
Ti Leggett (leggett@mcs.anl.gov) is a systems administrator for the Futures Laboratory of the Mathematics and Computer Science Division at Argonne National Laboratory. He also has a joint appointment with the Computation Institute at the University of Chicago.



[INTERVIEW]

Tough on Grease but Easy on Web Servers

Linux Journal talks with Ben Galbraith about Asynchronous JavaScript And XML, more commonly known as Ajax. KEVIN BEDELL



Ben Galbraith, co-founder of Ajaxian.com, is a specialist in enterprise architecture using Java/Swing and Asynchronous JavaScript and XML.

LJ: For our readers who are unfamiliar with Ajax, can you describe what it is and what need it's filling?

BG: Ever use Google Maps? If not, visit **maps.google.com** and play around with it for a few minutes. It should blow your mind. That's Ajax—wicked cool Web applications that work on any browser without any browser plugins, just ordinary HTML and JavaScript.

Technically, Ajax refers to a specific technique: allowing a Web page to spawn a background thread to send a request to a server, receive a response and update the Web page dynamically without ever refreshing the page. In other words, with Ajax, you don't have to click on Form Submit and wait for the browser to come back with a new page to interact with a Web application. Instead, the Web app can be sending and receiving data constantly while you interact with a Web page.

A great example of how this changes the game is **www.tadalist.com**. That Web site offers a simple service: creating your own personal to-do list. But, if you use it, you'll quickly see that instead of the traditional clunky Web interface for marking to-do items as completed and adding new items and so on, you get this rich interface that lets you do things like add, complete and modify items, all without reloading the page.

For years, Web applications have had this awful reputation for sucky interfaces. We've all wished we could do better, and Ajax makes that possible.

LJ: A lot of people are using the phrase Web 2.0 now. What is Web 2.0, and what role is Ajax playing in building it?

BG: It turns out that the changes wrought on conventional Web applications by Ajax are so great that many folks are claiming it represents a rebirth of the Web—Web 2.0, as it were. Some people hate the meme, and others love it; I'm indifferent. But what is clear is that as of 2005, we're seeing a new wave of exciting Web applications, and Ajaxian techniques are at the heart of them.

For years, the de facto Web e-mail experience sucked. Sure, there was the odd browser-specific offering, such as Oddpost, but most of us were stuck with this crap interface that paled in comparison to a desktop app. Now, Google, Yahoo and others are offering these rich, cross-browser mail apps that rival and in some ways trump desktop offerings.

The Web computer store has followed the same UI that Dell pioneered in the late 1990s all this time—scroll down to the bottom of the screen and click on the refresh price button to figure out costs and so on—up until Ajax. Recently, Apple introduced a 2.0 revision of their Web store, and they finally got it right, introducing a live page that refreshes the price of the computer live as you change new options.

Amazon used to have this annoying little rating page—they had it for years—where you'd go and fill out this tedious Web form to rank your products. This year, using Ajax, they introduced a live rating system that lets you rank your stuff without leaving to go to a separate page or filling out a form—and reportedly the number of items being rated has increased by an order of magnitude.

On Ajaxian.com, the Web site I co-founded with Dion Almaer to track Ajax, we see new ventures based on new Ajax-powered Web applications springing up all the time. There's investment capital behind a lot of these concerns. It feels a little like the 1990s again.

So that's Web 2.0—a new energy in the Web, leading to exciting changes to some of our favorite sites, and a bunch of new sites we'll see over the next few months and years. This new energy is directly caused by Ajax—by the realization that this tired old Web medium has a bunch of new tricks in it after all.

Some might say, "Wait a minute—this Ajax stuff isn't new! It's been around for ages." And indeed, that's true. Ajax is pretty much exactly what Microsoft called DHTML in 1997 (actually, it's a subset). Why has it caused all kinds of excitement in 2005? Well, it turns out that with the release of Mozilla 1.0, the key Ajax technologies become cross-browser. There wasn't a big press release or announcement—I think the Moz folks just did it to increase their compatibility with IE-specific sites—but as people discovered that DHTML was possible and easy in a cross-browser way, the Web lit up.

LJ: One of the biggest roadblocks to the deployment of Linux on the desktop is the requirement to run in-house developed applications, because in many companies these applications are written using Microsoft technologies that require Windows to be on the desktop. In those companies, this keeps Linux off the desktop. Is it realistic to think that Ajax could provide a way to build business applications that are truly OS-independent?

BG: Absolutely. The excitement of Ajax is what happens when you free developers from the Microsoft cage. All of the techniques that are lumped under the Ajax bandwagon were generally available on Internet Explorer first—some of them as long as eight years ago. These technologies—the ability to send a request from a Web page without refreshing, the ability to interact *easily* with the Web page DOM and so forth—were ignored by most developers until they become available in Mozilla/Firefox and Safari. Even though during this period IE enjoyed a ridiculously dominant share, the community just wasn't interested in cutting minority players out of the loop.

So I think that Ajax is all about platform independence, and the Web 2.0 meme took off only once the Ajaxian technologies were truly cross-platform.

Is Ajax powerful enough to build full-on business apps that are competitive with desktop offerings? That's hard to say. Certainly, the folks at **zimbra.com** think it is. Like many before them, they've created a Web-based PIM using Ajaxian techniques, but unlike many of their predecessors, they're openly gunning for Microsoft market share. Having seen the eye candy coming in Office 12, I wish them luck.

"THIS NEW ENERGY IS DIRECTLY CAUSED BY AJAX— BY THE REALIZATION THAT THIS TIRED OLD WEB MEDIUM HAS A BUNCH OF NEW TRICKS IN IT AFTER ALL."

In fact, that leads me to an interesting point. Ajax means dramatically better Web applications than we've ever had before. But at the same time, we're seeing desktop technologies poised to take a quantum leap. Apple pioneered the revolution, introducing their beautiful OpenGL-based Quartz-rendering engine years ago. But now Microsoft, with their version (Direct3D-based Avalon), is taking gorgeous graphics mainstream, and they're going beyond Apple by making it easier to develop such applications than it is with Apple's tools.

And of course, the Linux community is keeping right up, offering the same type of effects on top of the Cairo-rendering library.

It will be very interesting to see what happens. Ajax takes the Web to the types of UIs that we've been doing in desktop applications for the past ten years, but just as this is happening, desktop applications are literally blasting off to the next

cari.net cares
about your Dedicated Server budget!
Our unbeatable pricing helped save over 3000 piggy-banks last year alone!
Better Servers. Better Service.
$59/mo
Celeron D 3.0GHz, 1GB RAM
160GB SATA, 1200 GB/month
$139/mo
Xeon HT 3Ghz
2GB RAM
160GB SATA
1200 GB/mo
Upgradable to Quad!
cari.net
Cari.net/LJ or 888.221.5902

level, and who knows when cross-browser techniques will catch up. Some might say it's all about meaningless eye candy, but man, sex sells.

Still, there's hope for Ajax. Firefox 1.5 and Safari .next introduce SVG support, meaning that Web applications will be able to render high-quality, *interactive* vector graphics live in the browser, and drive these graphics using Ajax techniques (SVG can be modified on the fly using the same DOM API that we use to modify HTML). That may make up some of the difference, but it's entirely unclear how well IE will support SVG (there may be a way to do it by bridging SVG to Microsoft-specific stuff, but it's unlikely IE will provide seamless native support).

Further complicating the mix is Java. Java hasn't had a good reputation for desktop applications in the past, but there are some major innovations in the desktop space coming in Java 6 (the next version, due out sometime in 2006), and they've got some exciting things on the drawing board for Java 7. With Quartz, Cairo, and D3D/Avalon, each of the major OS platforms has a really high-quality graphics rendering engine, able to power cool applications. If the Java folks can successfully bridge all of those engines into a meaningful common denominator—that would be amazing for the industry. I'm not holding my breath, but it's a real opportunity.

"THE EXCITEMENT OF AJAX IS WHAT HAPPENS WHEN YOU FREE DEVELOPERS FROM THE MICROSOFT CAGE."

I got off on a tangent there, but yes—Ajax will power some exciting new cross-browser business applications, but at the same time, we're going to see desktop applications get jaw-dropping amazing. Time will tell which versions the market prefers.

LJ: I'm seeing the emergence of IDEs supporting Ajax development. Which of these do you see gaining traction? Or is everybody still just using vi and emacs?

BG: I see most folks using their traditional editors. There are some interesting Web-based editor tools out there, but nothing that I've seen anyone actually use.

LJ: As Ajax is really a client/browser-side technology, are you seeing server-side developers pick it up?

BG: Yes, without a doubt. I'm seeing folks that know nothing about JavaScript learning about how to do Ajax because it offers such a compelling upgrade to the UI that they really don't have a choice. The good news is that all of this Web 2.0/Ajax excitement has led to the creation of incredibly easy-to-use frameworks that make Ajax easy.

Prototype, Scriptaculous, dojo, DWR for Java folks, JSON for pretty much any language and many other tools can make it so easy to do all kinds of great Ajax effects.

And, the server-side frameworks have already started to build Ajax right in, and will continue to do so. In the coming years, server-side developers will probably do some pretty amazing Ajax without writing much of any JavaScript at all.

LJ: Are there new security risks associated with Ajax development?

BG: Nothing fundamental, though there are a few exploits here and there that arise as we push the browsers in a new direction. However, I should mention Greasemonkey.

I hate Microsoft Money, and any other personal finance packages I've used. On the surface, they seem to have all of the right features, but the interface never quite works the way I want it to, and I'm constantly stuck doing these stupid manual tasks and jumping through hoops. What I really want is the ability to tweak the way the program's interface works.

With Greasemonkey, you can do that—to Web applications. Greasemonkey is a Firefox plugin that lets you inject JavaScript code into a Web page. So, if you don't like something about Amazon.com's UI, change it! You have full access to the page's DOM, so you can do whatever you like. Furthermore, Greasemonkey is a community for people to share their custom features. For example, there's a great plugin for making Amazon show you the price of its items on other Web sites.

While we've all known for ages that anything you send in HTML can be hacked and that our server endpoints need to be prepared to receive all kinds of malformed requests, as Ajax pushes more logic to the client, some of us may forget that lesson, and tools like Greasemonkey make it trivial for people to take advantage of poorly written applications.

Talk about exciting—finally, the ability for a community to take a commercial, off-the-shelf app and modify it easily to do all kinds of new things. You might argue that open source has empowered that for years, but the Greasemonkey concept takes that to a whole new level—a whole new audience that doesn't know how to use CVS, gcc, C++ and so on.

Ajax doesn't introduce new security risks, but it may facilitate the creation of insecure Web sites.

LJ: For many of our readers to get permission to use Ajax, they'll need reference sites to show their management. What are some good reference sites for Ajax development?

BG: Google Maps remains the flagship app. Of course, you should visit **ajaxian.com**, where we constantly showcase new Ajax applications. Check out **zimbra.com** to see the latest attempt at emulating a desktop app in a browser; Gmail is an example of a more Webish attempt at Ajax-style rich interaction. See some of the demos at **script.aculo.us** to see what's possible (easy drag and drop, transition effects and so on). Backbase.com (**www.backbase.com**) also offers some great demos of how Ajax can change specific vertical application types.

LJ: What are some good resources for our readers who are interested in learning?

BG: Some folks have said favorable things about our own site, Ajaxian.com, being a good resource. Dion Almaer—my Ajaxian partner and the site's editor—does a really good job of putting new information on the site daily. You'll definitely keep up with what's happening!

For the Ajax newbie, there are some great books coming out from all of the publishing houses, such as *Ajax in Action* from Manning, *Ajax Foundations* from Apress and more. Dion and I have got one coming out too: *Pragmatic Ajax*, published by the Pragmatic Press. My favorite bit in that book is a chapter where we walk you through building your own version of Google Maps from scratch.

LJ: Thanks for the opportunity to talk with you!■

Rapid GNOME Development with Mono

How to get started with GNOME monkeyshines using the open-source .NET system Mono.

ROBERT LOVE

Mono is an open-source implementation of the .NET development platform, a powerful and now open development platform. Mono contains a number of components: a Common Language Infrastructure (CLI) virtual machine, a C# compiler and a set of class libraries. Mono implements the C# language and runtime environment according to ECMA standards 334 and 335, respectively.

Mono—which is the word for monkey in Spanish—provides various class libraries, including an open-source implementation of the .NET Framework SDK. In this article, however, we discuss one of Mono's brightest assets: its GNOME support, in the form of Gtk#.

Gtk# is a .NET language binding for the Gtk+ toolkit and various other GNOME libraries. More than a simple wrapper, Gtk# provides a powerful platform for developing GUI software in the GNOME environment. Gtk#'s language bindings utilize good object-oriented principles and C#-style design to make GNOME development easy and natural, yet flexible and powerful.

In this article, we investigate the construction of a simple C# application, starting with a trivial "Hello, World" application and building it into a basic Wikipedia search tool. Our only dependencies will be Mono and Gtk#. Packages are available for most distributions—see the on-line Resources.

Hello, World!

Let's start by constructing the most basic Mono application possible, which prints "Hello, World!" to the console:

```
using System;

class first {
    public static void Main (string[] args)
    {
        Console.WriteLine ("Hello, World!");
    }
}
```

Fire up your favorite editor, enter this code and save it as first.cs. We can then compile the program into an executable image with the following:

```
$ mcs first.cs
```

Finally, we can run it via the following command:

```
$ mono first.exe
```

```
Hello, World!
```

This application implements the first class. Every application needs an entry point, an initial function inside of the class for the Mono runtime to jump to and begin the program's execution. As with C and C++, this is the Main function. The prototype of this function is:

```
public static void Main (string[] args)
```

In our program's Main, we invoke a single function, WriteLine, which is found inside the Console class. This function, similar to printf(), writes a line of text to the console. It can be used to output the values of variables too:

```
int x = 5;
String s = "wolf";

Console.WriteLine ("x={0} s={1}", x, s);
```

This gives us:

```
x=5 s=wolf
```

Hello, World! in Color

We do not, however, have to confine our "Hello, World!" to the console; with Gtk#, we can build a trivial GUI dialog to hoist our message onto the world:

```
using System;
using Gtk;

class Two {
    static void WindowDelete (object o, DeleteEventArgs args)
    {
        Application.Quit ();
    }

    static void InitGui ()
    {
        Window w = new Window ("My Window");

        HBox h = new HBox ();
        h.BorderWidth = 6;
        h.Spacing = 6;
        w.Add (h);

        VBox v = new VBox ();
        v.Spacing = 6;
        h.PackStart (v, false, false, 0);

        Label l = new Label ("Hello, World!");
        l.Xalign = 0;
        v.PackStart (l, true, true, 0);

        w.DeleteEvent += WindowDelete;
        w.ShowAll ();
    }

    public static void Main (string[] args)
    {
        Application.Init ();
        InitGui ();
        Application.Run ();
    }
}
```

As before, enter the code via your favorite editor. This time, save it as two.cs. To compile this program, we need to tell the Mono compiler that we want to use the Gtk# assembly:

```
$ mcs two.cs -pkg:gtk-sharp
```

Running it, however, is the same:

```
$ mono two.exe
```

The application creates a small window, titled My Window, and writes "Hello, World!" into the window (Figure 1). The window is a GtkWindow, the label a GtkLabel. Gtk lays out windows via boxes. Boxes are invisible widgets—existing solely for the purpose of layout—into which other widgets are packed. The arrangement of widgets within a box determines the physical layout of the widgets within the window. Although it is possible in Gtk to arrange widgets using tables, most programmers prefer boxes for their flexibility and power—plus, once you get the hang of them, they are not difficult to use.

Gtk provides two types of boxes: vertical and horizontal. A vertical box, called a vbox, defines the vertical arrangement of widgets—vboxes arrange widgets into columns. A horizontal box, known as an hbox, defines the horizontal arrangement of widgets, by arranging them into rows. Widgets are packed into boxes, boxes are packed into other boxes, and the boxes are added to windows.

A new hbox is created via:

```
HBox h = new HBox ();
```

And a new vbox is created via:

```
VBox v = new VBox ();
```

The new objects representing the boxes have various properties that one can set to manipulate the look and feel of the box. In our previous example, we set two properties on the hbox:

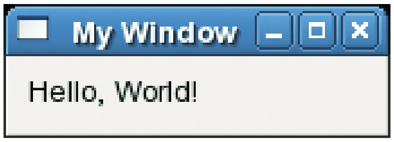


Figure 1. My Window

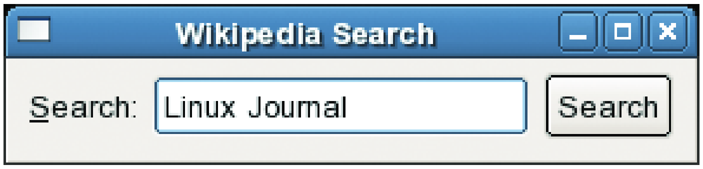

Search: Linux Journal

Figure 2. The Fancy GUI

```
h.BorderWidth = 6;
h.Spacing = 6;
```

Here, we set the border of and the spacing around the hbox to six pixels each. This provides a net spacing of 12 pixels around the hbox. Coincidentally, for purposes of aesthetics and consistency, the GNOME HIG (Human Interface Guideline) dictates a minimum spacing of 12 pixels between widgets—thus the six and six pixels in this example are perfect.

To add a box to a window, the Add() member function is called on the window in question and provided to the box:

```
w.Add (h);
```

To pack a widget into a box, the PackStart() member function is called on the box in question:

```
public void PackStart (Widget child,
             bool expand,
             bool fill,
             uint padding)
```

In our example, we did:

```
v.PackStart (l, true, true, 0);
```

This call packs our label into our vbox. If the expand parameter is true, the widget child expands to fill all available space within the box. If the fill parameter is true, the widget consumes all of its space for rendering; otherwise, if false, the widget uses superfluous space for padding. The padding parameter allows for the addition of extra spacing around the widget, within the box, beyond any padding already provided.

Starting our application is simple. We perform three simple steps:

```
Application.Init ();
InitGui ();
Application.Run ();
```

Application.Init() initializes Gtk# and the application's GUI. It should be one of the first functions that a Gtk# application invokes. After executing this function, applications set up their GUI, create and arrange their widgets, and draw the initial windows and other UI elements. In our program, we do this in the InitGui() function. Once everything is complete and ready to roll, the program calls Application.Run() and the race is off. Our main window pops up because we exposed it, back in InitGui(), via:

```
w.ShowAll ();
```

This exposes the window and all widgets packed therein. Thus, once the application invoked Application.Run(), our UI elements appear.

While executing, the program's responses are handled by the behavior of widgets. Some widgets behave in predetermined ways, not requiring the programmer to write any code manually. Most of the time, however, the programmer wants to handle events personally. This is done by writing an event handler, using the incredibly useful C# events feature, that Gtk# invokes in response to widget interaction.

In our last example, we have one such event handler. We want our application to exit when the user clicks the close box on the main window, so we need to handle the associated event, which is called DeleteEvent. This is done by writing the event handler:

```
static void WindowDelete (object o, DeleteEventArgs args)
{
    Application.Quit ();
}
```

And adding it as an event handler:

```
w.DeleteEvent += WindowDelete;
```

The function Application.Quit() causes Gtk# to destroy the UI, shut down and terminate the application. Consequently, when the user clicks the close box on the main window, our application gracefully exits.

Building a Better Example

Let's turn now to building a more complete—dare I say useful—application: a tool for searching Wikipedia. To be sure, we will not build anything fancy, but we can implement something fun. Let's look at building a simple window, with a text-entry widget. We will allow the user to type a search query into the window and click a button (Figure 2). The application then launches the user's Web browser and looks up the search term on Wikipedia. We build the whole thing, including the GUI and code to launch the Web browser, in only a handful of lines.

We can construct this new application by building on our last example, adding new widgets and the requisite features. Surprisingly, thanks to Gtk#, the additional code is not very much! Here we go:

```
using System;
using Gtk;

class Example {
    public static Entry search_entry;

    public static void ButtonClicked (object o, EventArgs args)
```

Advertiser Index

For advertising information, please contact our sales department at 206-782-7733 ext. 2 or ads@ssc.com. www.linuxjournal.com/advertising

Advertiser	Page #	Advertiser	Page #
Aberdeen, LLC www.aberdeeninc.com	17	Levanta www.levanta.com	29
Advanced Clustering Technologies www.advancedclustering.com	3	Linux Journal www.linuxjournal.com	91, 95
AML www.amltd.com	51	LinuxWorld Conference & Expo www.linuxworldcanada.com	39, 67
APPRO HPC Solutions appro.com	C2	MBX www.mbx.com	9
ASA Computers www.asacomputers.com	55, 65	Microway, Inc. www.microway.com	C4, 57
Cari.net www.complexdrive.com	77	Mikro Tik www.routerboard.com	7
Coraid, Inc. www.coraid.com	11	Open Source Storage www.opensourcestorage.com	21
Coyote Point www.coyotepoint.com	2	Penguin Computing www.penguincomputing.com	23
Cross Tec Corporation www.NetOpUSA.com	40	Polywell Computers, Inc. www.polywell.com	27
Cyclades Corporation www.cyclades.com	1	The Portland Group www.pgroup.com	34, 35
Desktop Linux Summit www.desktoplinuxsummit.com	50	Rackspace Managed Hosting www.rackspace.com	C3
Emac, Inc. www.emacinc.com	73	R Cubed Technologies www.rcubedtech.com	75
EmperorLinux www.emperorlinux.com	15	SBE, Inc. www.sbei.com	25
FairCom Corporation www.faircom.com	45	SD West www.sdexpo.com	61
Fourth Generation Software Solutions www.fourthgeneration.com	59	Servers Direct www.serversdirect.com	13
Genstor Systems Inc. www.genstor.com	53	Technologic Systems www.embeddedx86.com	89
GPL Host, LLC. www.gplhost.com	41	Thinkmate www.thinkmate.com	19
Hurricane Electric www.he.net	31	Tyan Computer USA www.tyan.com	5
Iron Systems www.ironsystems.com	93	Zervex Server Solutions Inc www.zervex.com	8
Layer 42 Networks www.layer42.net	71	ZT Group International www.ztgroup.com	33

```
    {
        String s =
"http://en.wikipedia.org/wiki/Special:Search?search=";
        s += search_entry.Text;
        s += "&go=Go";
        Gnome.Url.Show (s);
    }

    static void WindowDelete (object o, DeleteEventArgs args)
    {
        Application.Quit ();
    }

    static void InitGui ()
    {
        Window w = new Window ("Wikipedia Search");

        HBox h = new HBox ();
        h.BorderWidth = 6;
        h.Spacing = 6;
        w.Add (h);

        VBox v = new VBox ();
        v.Spacing = 6;
        h.PackStart (v, false, false, 0);

        Label l = new Label ("_Search:");
        l.Xalign = 0;
        v.PackStart (l, true, false, 0);

        v = new VBox ();
        v.Spacing = 6;
        h.PackStart (v, true, true, 0);

        search_entry = new Entry ();
        search_entry.ActivatesDefault = true;
        l.MnemonicWidget = search_entry;
        v.PackStart (search_entry, true, true, 0);

        v = new VBox ();
        v.Spacing = 6;
        h.PackStart (v, true, true, 0);

        Button b = new Button ("Search");
        b.CanDefault = true;
        w.Default = b;
        v.PackStart (b, true, true, 0);

        b.Clicked += ButtonClicked;
        w.DeleteEvent += WindowDelete;
        w.ShowAll ();
    }

    public static void Main (string[] args)
    {
        Application.Init ();
        InitGui ();
        Application.Run ();
    }
}
```

We need to add a new assembly, gnome-sharp, to our compiler command line. Assuming you name this program three.cs, you would perform the following:

```
$ mcs three.cs -pkg:gtk-sharp -pkg:gnome-sharp
```

And now run it via:

```
$ mono three.exe
```

This third and final program contains a few new widgets—buttons, labels and text entries—but follows the same basic structure as our second program. If we work backward, from the last box outward to the first, we can get a good feel for the layout of the UI elements without even seeing a screenshot.

The other big difference is a new event, Clicked. We define a function and add it as an event handler:

```
b.Clicked += ButtonClicked;
```

We made the text-entry widget, search_entry, public, and thus our new event handler can grab the contents of the search entry when the user presses the button via search_entry.Text.

In ButtonClicked, we grab this text, construct the Wikipedia URL required for searching for the text, and use the Gnome.Url.Show() function to open the user's preferred Web browser (a global GNOME setting) and send it off to our URL.

Conclusion

Although it is impressive to implement so much in so little, the real boon is that this is a C-like language, not a scripting language. C# retains much of the power and performance of C and adds powerful object-oriented programming constructs.

Let me be frank. I am a C programmer. I spend most of my days hacking the kernel. Higher-level languages are not my cup of tea. Indeed, I am no fan of C++ or Java. Yet, having spent time with C#—working on Beagle, among other C# endeavors—I am thoroughly impressed. C# is an elegant language that readily makes clear an obvious facet: it is quite well designed.

In Mono, we have a free and open C# compiler, runtime and family of libraries, supported by a vibrant Open Source community. Although excellently paired with GNOME development, Mono is a smart tool for many jobs.

Resources for this article: www.linuxjournal.com/article/8750.■

Robert Love is a senior kernel hacker in Novell's Ximian Desktop group and the author of *Linux Kernel Development* (SAMS 2005), now in its second edition. He holds degrees in CS and Mathematics from the University of Florida. Robert lives in Cambridge, Massachusetts.

Stealth E-Mail to the Rescue

How to use stealth e-mail with dynamic DNS and a Treo 650 smart phone.

PETER ZIOBRZYNSKI

Since the early days of e-mail, maintaining my own e-mail server was a sort of indication of being in charge and staying technically fit. The technology involved in a project like this usually includes components that can be reused elsewhere and force one to stay abreast with commonly used communications media.

In the beginning, it was a simple task of connecting a modem, finding a community UUCP server, configuring modem dial-up, uucico and Sendmail. This was sort of the Model T of e-mail. And, it usually included configuration of a Usenet feed with C-News to collect the UUCP addresses of all computers on the relatively small Internet at that time.

With the advent of the real Internet, the scenario is becoming more complex. You have to overcome a number of obstacles created by people trying to break in to your server, snoop the transmission of e-mail packets on the wire and deal with those who want to send you tons of unwanted e-mail. As if this were not enough, workplaces have become so secure that it is sometimes impossible to access your personal e-mail server over the Internet from work during the day.

I used to maintain a Linux server with a static IP on a DSL line running DNS, a firewall (netfilter) with my MTA of choice (Postfix) and the addition of SpamAssassin for spam filtering. I read e-mail on my laptop using IMAP with Netscape Communicator. I use Communicator filters to sort all my incoming mail into various IMAP folders.

This simplistic architecture became history this summer after moving out of the San Francisco Bay Area to Denver, Colorado. The luxury of a static-IP DSL vendor disappeared, and a Nazi-style ISP with a monopoly in the area became a reality. Static IP is not available here (at least for me), and the ISP uses aggressive filtering of the commonly used IP ports. My new workplace is so secure that I had forgotten about carrying my laptop with me or using my work Internet connection to get to my e-mail server. All this is understandable, as ISPs protect themselves from spammers and employers need better security. But, I still want to read my e-mail during the day.

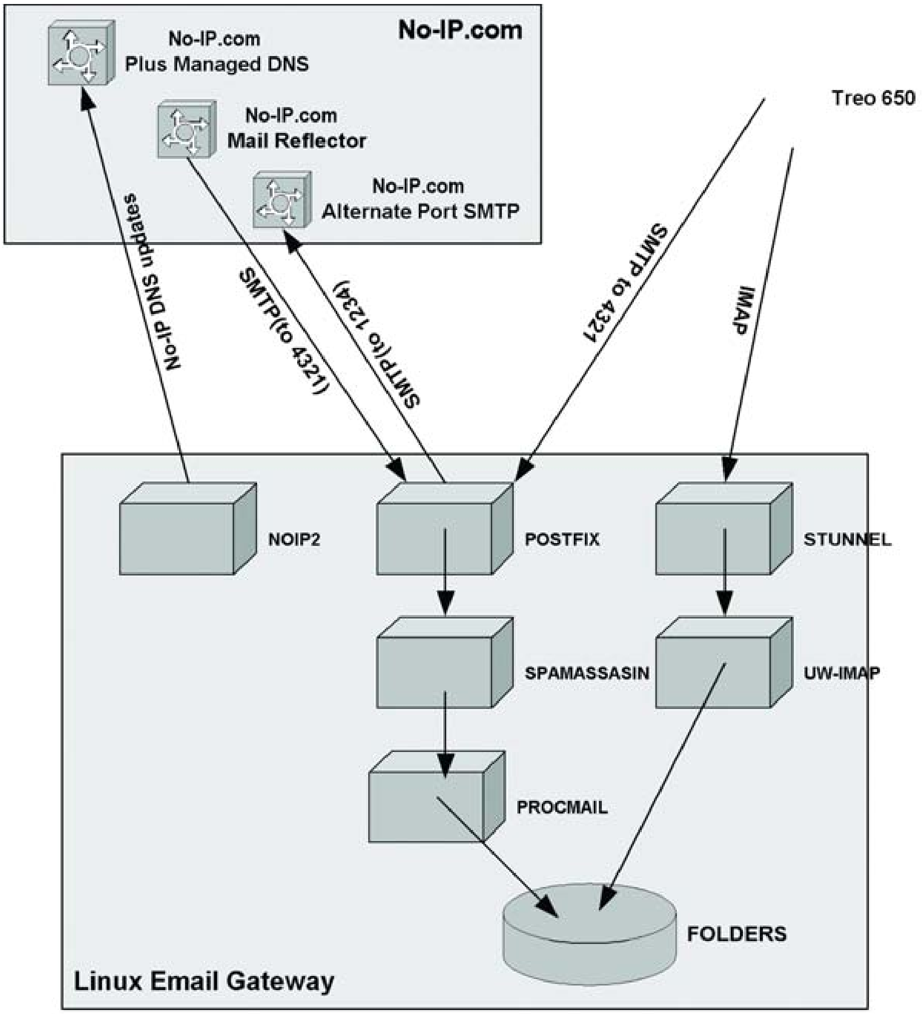


Figure 1. The Layout of the Complete E-Mail Solution

I took it as a personal challenge to overcome these obstacles. The direction I went was to use the smart phone Treo 650 as a personal e-mail reader to bypass the workplace security. I configured my home e-mail server to use new stealth-mode ISPs that allow for dynamic DNS and mail relays to ports of choice.

Here is a summary of the configuration components that I cover in step-by-step configuration details below:

- The e-mail server is running stable Gentoo Linux connected to the Internet via VDSL (very high-speed DSL from Qwest), using a DHCP-assigned dynamic-IP address. My DNS domain registrar is No-IP.com. This registrar uses a custom dynamic DNS setup that detects IP address changes on my side. This is done by running a custom client program on my server—noip2 client connects to the No-IP.com registrar DNS server and updates my DNS records in as often as one-minute intervals. This is called Plus Managed DNS.

- Because my ISP blocks incoming IP port 25, I use the Mail Reflector No-IP.com service that sets an MX record for my domain to its own server and delivers the mail to a custom port on my server.

- My ISP also lists my DHCP addresses with the Internet spam blacklists, so any attempt to deliver e-mail directly from my server is doomed to failure. To overcome this, I use the No-IP.com service called Alternate-Port SMTP, which acts as an outgoing mail relay. I punt all mail to a No-IP.com server using SSL authentication and also a custom port in case my ISP blocks outgoing SMTP.

- My MTA is Postfix, which is quite handy for the stealth configuration with alternate incoming and outgoing ports.

- I use SpamAssassin to filter spam. It is easy to configure and works very well. In brief, its function is limited to processing mail messages and attaching a custom mail header field—an X-Spam-Level rating to each message as spam candidates. The level of spam likelihood is measured by the number of asterisks this field contains. A single * is usually a good indication of spam.

- I could not count on storing e-mail on my smart phone and filtering it there. The phone couldn't handle that much e-mail. So I replaced the client-side Netscape Communicator filter function (to sort incoming mail into IMAP folders) with Procmail. I created a .procmailrc file implementing all spam and mailing-list rules to file messages in the folder hierarchy on the server. This proved to be quite useful and opened the access to my archived e-mail from any location.

- The IMAP server was quite a problem for me. I prefer traditional mailboxes where multiple messages are stored in a single file per folder. Most modern IMAP servers, like Courier or Cyrus, use modern maildir or MH formats, which store each message in its own file. This consumes an insane amount of i-nodes. Unfortunately, the only open-source IMAP server I could find that uses traditional folders is the uw-imap. (CommuniGate Pro uses single files, but it's a commercial server.) The uw-imap server has a number of drawbacks, especially when it comes to SSL-protocol implementation. My tests of uw-imap with the SSL IMAP client that I had in mind for this project (PalmOS VersaMail) showed failed connections or flat failures to connect. To get what I want—the single file mail folders and working SSL—I split the function of IMAP and SSL over two separate servers: stunnel and uw-imap. Stunnel proved to be quite sophisticated in the SSL configuration and level of logging and diagnostic messages.

- The client side of my e-mail configuration originally included stock PalmOS VersaMail shipped with the Treo 650 and part of a Sprint plan. The key factor in this decision was availability of unlimited use of Internet connectivity for a flat $15 US per month fee. The VersaMail IMAP support is quite good, and integration with the Blazer Web browser made the sale for me. Unfortunately, a more-intense use of the VersaMail uncovered problems with its operation. The whole setup depends on a reliable mail server polling for new mail. Unfortunately, VersaMail has a bug that impacts scheduling of the polling, and this makes it rather ineffective. I ended up using the SnapperMail mail client for PalmOS, which is a good example of how nine guys in New Zealand can outrun a big corporation like Palm Software. SnapperMail is one of the best PalmOS applications I have used so far.

There are quite a number of moving parts here, and a diagram is in order (Figure 1).

As you can see from Figure 1, there are three main areas of configuration: Linux server, No-IP.com services and the Treo 650 mail client.

Linux Server Configuration

My selection of the Gentoo Linux distribution for the project was dictated by the very convenient Portage package management. Portage completely frees the user from hunting down required packages. In operation, it resembles Perl CPAN or Debian apt-get. For installation of Gentoo itself, refer to the gentoo.org Web site. The installation of the OS is mostly manual, and it can be a rather lengthy process (some installations even can take days, because you compile everything yourself), but this investment will pay itself back during server management and application configuration.

You also need to get the DNS and SMTP services from No-IP.com, mentioned above. The No-IP.com Web site provides documentation for all services they provide.

The instructions that follow are Gentoo-specific, but it should be fairly easy to adapt this project to a different distribution. You simply need to make sure that the applications you install have the capabilities (like SASL) used for this solution.

Postfix MTA

We begin installation with the core component, Postfix. Standard Gentoo installation comes with a simple MTA ssmtp that needs to be removed before Postfix installation. Also, Postfix needs to be installed (compiled) with SASL support. This is needed for authenticated mail delivery to the No-IP.com relay host (Alternate-Port SMTP service).

The SASL option is turned on with the sasl keyword added to the Gentoo USE configuration variable. In /etc/make.conf, add:

```
/etc/make.conf:

USE="sasl"
```

Install SASL libraries:

```
# emerge dev-libs/cyrus-sasl
```

Now remove and add MTAs:

```
# emerge -C ssmtp
# emerge postfix
```

Add init rc script startup:

```
# rc-update add postfix default
```

Postfix configuration is relatively simple—two configuration files in

/etc/postfix need attention: main.cf and master.cf.

Change the information describing your gateway host by editing the main.cf file for Postfix. Here, the hostname of your gateway is mygateway, and the domain name is foobar.net. The relay host that you will send all your mail to is relayhost.no-ip.com, receiving SMTP on port 1234. Both will be provided by No-IP.com as part of the Alternate-Port SMTP service:

```
myhostname = mygateway
mydomain = foobar.net
myorigin = $mydomain
mydestination = $myhostname, localhost.$mydomain $mydomain
#home_mailbox = .maildir/
relayhost = relayhost.no-ip.com:1234
smtp_sasl_auth_enable = yes
smtp_sasl_password_maps = hash:/etc/postfix/saslpass
smtp_sasl_security_options =
```

Add an extra port (4321) beside 25 to the Postfix master.cf file. This will be used to receive SMTP from the Mail Reflector No-IP.com service and also your Treo 650:

```
4321      inet  n       -       n       -       -       smtpd
```

Create an SASL password file /etc/postfix/saslpass for host relayhost.no-ip.com and user foobar.net@noip-smtp using password ????—all provided by No-IP.com:

```
/etc/postfix/saslpass:

relayhost.no-ip.com     foobar.net@noip-smtp:????
```

Next, generate a dbm map:

```
# cd /etc/postfix
# postmap saslpass
```

As a final touch, you need to enable e-mail relaying from your Treo 650. We use Sprint here, and you will have to find out what Sprint switch IP range will be connecting to your server. The Postfix main.cf parameter mynetworks will have to include the network address of the switch. I use 70.0.0.0/8 beside my home network and a local loop network. It is always best to narrow the range of addresses as much as possible, for security reasons:

```
mynetworks = 192.168.1.0/24 127.0.0.0/8 70.0.0.0/8
```

Spam Filter

You need to install two packages: spamassassin and procmail. The steps (for Gentoo) are as follows.

Install Procmail:

```
# emerge procmail
```

Install SpamAssassin:

```
# emerge spamassassin
```

Update the init rc scripts to start the SpamAssassin server (this is probably done for you if you use a different package manager):

```
# rc-update add spamd default
```

Adjust your Postfix configuration to deliver all mail using Procmail. Add this to /etc/postfix/main.cf:

```
mailbox_command = /usr/bin/procmail
```

Create the main Procmail configuration file /etc/procmailrc, and add this recipe to make e-mail pass through SpamAssassin:

```
DEFAULT=/var/spool/mail/$LOGNAME
:0fw: spamassassin.lock
* < 256000
| /usr/bin/spamc
```

Start the spamd server:

```
# /etc/init.d/spamd start
```

Mail Filing

Establish an IMAP folder hierarchy and Procmail configuration file to file mail in those folders. If you have multiple users, you have to do this for each user. The following configuration uses ~/.m for the folder root directory. The per-user Procmail configuration file is located in ~/.prcmailrc. I use the following .procmailrc file template that implements the essential functionality of separating spam from mail and filing mailing lists. For details, refer to procmailrc(5):

```
PATH=/bin:/usr/bin:/usr/sbin
MAILDIR=$HOME/.m
DEFAULT=$MAILDIR/Mbox
LOGFILE=$HOME/.procmail.log
VERBOSE=yes

# File gentoo-user mailing list into ~/.m/lst/gentoo
:0:
* (^To.*|^Cc.*)gentoo-user@lists.gentoo.org
lst/gentoo

# File jobserve mail into ~/.m/lst/jobserve
:0:
* ^From.*jobserve.com
lst/jobserve

# File SPAM into ~/.m/Spam with some exceptions:
:0:
* ^X-Spam-Level:.*\*
 * !^From.*netflix
 * !^From.*vail
 * !^From.*ebay member
 * !^From.*cnet
Spam

# File SPAM that escaped spamassassin:
```

```
:0
* ^From.*eversave.com
Spam
:0:
* ^From.*sears.com
Spam
```

Now that the mail processing facilities are in place, you can start Postfix and let the mail start flowing in; I can almost guarantee that the first folder with mail will be your ~/.m/Spam:

```
# /etc/init.d/postfix start
```

IMAP Server

The IMAP configuration includes a stunnel SSL front end and the uw-imap back end. The installation for uw-imap is a bit nonstandard, because the default Gentoo configuration does not allow you to build uw-imap with clear-text authentication over an unencrypted channel. The only default uw-imap configuration that works is the one with SSL support. This is not what we need as a server behind stunnel. Gentoo lets you remedy this with a special USE setting to disable SSL and enable clear-text passwords.

The installation command for Gentoo is:

```
# USE="-ssl clearpasswd" emerge uw-imap
```

Next, the stunnel configuration file stunnel.conf needs to include an IMAP section. Edit /etc/stunnel/stunnel.conf:

```
pid = /var/run/stunnel/stunnel.pid
socket = l:TCP_NODELAY=1
socket = r:TCP_NODELAY=1
cert = /etc/ssl/certs/foobar.net.pem
[imaps]
accept  = 993
exec = /usr/sbin/imapd
execargs = imapd
```

You can generate a self-signed SSL certificate for foobar.net.pem with the following commands:

```
# cd /etc/ssl/certs
# openssl req -new -x509 -nodes -out cacert.pem -keyout cakey.pem -days 5000
        Country Name (2 letter code) [AU]:US
        State or Province Name (full name) [Some-State]:CO
        Locality Name (eg, city) []:Highlands Ranch
        Organization Name (eg, company) [Internet Widgits Pty Ltd]:
        Organizational Unit Name (eg, section) []:home
        Common Name (eg, YOUR name) []:foobar.net
        Email Address []:me@foobar.net

# cat cakey.pem cacert.pem > foobar.net.pem
```

With Gentoo, you must now configure the init rc scripts to start stunnel:

```
# rc-update add stunnel default
```

The Treo 650 Setup

As I mentioned, there are two good IMAP clients available for PalmOS. One is the standard application included with the Treo, VersaMail. The other is a commercial application, SnapperMail. My choice was the latter, even in spite of its relatively high cost (approximately $60 US).

Both applications allow for subscribing to a hierarchy of IMAP folders on the server and handling e-mail attachments. SnapperMail is definitely better tested and has a number of features that justify its additional cost.

To install PalmOS applications and generally manage my Treo 650 using Linux, I use pilot-link software. On Gentoo, install it with:

```
# emerge pilot-link
```

I use pilot-link to back up and restore my Treo to a directory on Linux as well as to install applications like SnapperMail.

I use Bluetooth and PPP to connect my Treo to a Linux notebook. You also can use a USB connection. The connection channel for pilot-link tools is conveniently defined with a PILOTPORT environment variable. Use the following for a USB cable:

```
# export PILOTPORT=/dev/tts/USB1
```

or for Bluetooth, use:

```
# export PILOTPORT=net:any
```

I create a directory named treo in my home directory, and run this command to back up my Treo before installing any software:

```
# pilot-xfer -b treo
```

I use the following command to synchronize (incrementally) the Treo with this backup directory:

```
# pilot-xfer -s treo
```

To restore a backup, use the following:

```
# pilot-xfer -r treo
```

Download SME231.zip from **www.snappermail.com** to install the SnapperMail application. Unzip the file and run this command:

```
# pilot-xfer -i SnapperMail-ent.prc
```

The configuration of the Treo 650 with the Sprint network is best done by ordering the Sprint PCS Vision Professional Pack and letting Sprint support walk you through the setup.

SnapperMail also comes with a good 60-page PDF manual, and its setup is really quite intuitive.■

Peter Ziobrzynski is an Independent Consultant based in Toronto, Canada, providing UNIX and Linux consulting services to clients in San Francisco, California, and recently in Denver, Colorado. Peter holds a Master's degree in Engineering from Cracow University of Technology, Poland. He immigrated to Canada in the early 1980s and has been using UNIX since then for work and pleasure. His recent focus is on Linux, and he holds Red Hat RHCE.

Subversion: Not Just for Code Anymore

Here is a subversive way to handle multiple versions of your personal information instead of just versions of code. WILLIAM NAGEL

Have you ever needed some information from a file, only to remember that you modified the file a week ago and removed the very information you're interested in? Or, have you ever spent hours sifting through dozens of inconsistently named copies of the same file trying to find one particular version? If you're like me, the answer is probably a resounding yes to both questions. Of course, if you're a programmer, you've probably already solved that problem in your development activities by using a version control system like CVS or Subversion. What about everything else though? Mom's cherry pie recipe may not change as frequently as rpc_init.c, but if you do decide to create a low-cal version, you're not going to want to lose the original. As it turns out, version control isn't only for source files anymore. Many of the features of Subversion make it ideal for versioning all kinds of files.

With Subversion, you can keep a history of changes made to your files. That way, you easily can go back and see exactly what a given file contained at a particular point in time. You also save space, because it stores deltas from one version to the next. That way, when you make a change to a versioned file, it needs only enough extra space to store the changes rather than a complete second copy of the file. Also, unlike with CVS, delta storage on Subversion also applies to binary files as well as text files.

Subversion makes it easy to access your files from multiple computers too. Instead of worrying whether the copy of the budget report on your laptop reflects the changes you made last night on your desktop system at home, you can simply run an update on your laptop and Subversion automatically updates your file to the latest version in the repository. Also, because all of the versions are stored in a single repository, there is a single location that you need to back up in order to keep all of your data safe.

What to Version

So your interest is piqued. You're sold on the advantages of versioning your files, and you'd like to give it a try. The first question to answer is what files you're going to put under version control. One obvious possibility would be to version your entire hard drive. In practice though, that's not a very practical approach. When you store a portion of a repository's contents locally (in what's called a working copy), Subversion stores a second copy of each file to allow it to compare locally changes you have made with the last version from the repository. Therefore, if you version the entire hard drive, you'll need twice as much hard drive.

There's also little reason to keep full revision history on the largely static parts of your filesystem, such as /usr or /opt. On the other hand, directories that contain a lot of custom files/modifications, such as /etc or /home, are prime candidates for versioning, because the advantage of tracking those changes is more likely to outweigh the disadvantages of extra storage requirements. Furthermore, with Subversion, you can opt to create a working copy from a subtree in the repository hierarchy. That way, you don't need to store any copies of infrequently accessed data locally, which often results in a net reduction in hard drive requirements, even though the files you are storing locally take up twice as much space.

Getting Subversion Up and Going

Now, let's dive in and get Subversion running on your machine. Installing is generally pretty easy. You can, of course, download the Subversion source and compile that, but in most cases, it's going to be much easier to install the precompiled binary package for your Linux distribution of choice. Fortunately, Subversion has matured to the point where such a package is available for almost every major distribution. In fact, I don't know of any off the top of my head that it isn't available for.

Once you have Subversion installed, it's time to create a repository. Let's say you have a documents directory in your home that you'd like to version. First, you need to create a new empty repository using the `svnadmin create` command. For instance, the following creates a new repository in your home directory:

```
$ svnadmin create $HOME/.documents_repository
```

Next, you need to import your existing documents into the newly created repository. To do that, use the `svn import` command with the directory to import and a URL that points to the repository. In this example, the URL refers directly to the repository using a file://-type URL. If your repository will be used only locally, the file:// URL is the easiest way to access a repository (there are other, better ways to access repositories that I'll discuss in a bit though):

```
$ svn import $HOME/documents file://$HOME/.documents_repository
```

When you run the import command, Subversion opens an editor and asks you for a log message. Whatever message you enter will be associated with the newly created repository revision and can be seen by examining the repository history logs. Enter something brief, such as "imported documents directory". As soon as you save the log message and leave the editor, Subversion performs the import and outputs something like the following:

```
Adding         documents/file1.txt
Adding         documents/file2.txt
Adding         documents/file3.jpg

Committed revision 1.
```

You can now safely remove the original $HOME/documents and then re-create it as a working copy of the repository, using the `svn` checkout command:

```
$ rm -rf $HOME/documents
$ svn checkout file://$HOME/.documents_repository $HOME/documents
```

So far, so good. However, if you want to take advantage of Subversion from multiple machines, you're going to need to set up a server. Several options are available to you, but the best choice is generally to use Apache with mod_dav, which serves a Subversion repository using the WebDAV protocol.

From a basic Apache installation, getting WebDAV to work is fairly simple. First, you need to make sure that mod_dav and mod_dav_svn are being loaded:

```
LoadModule       dav_module          modules/mod_dav.so
LoadModule       dav_svn_module     modules/mod_dav_svn.so
```

Next, you need to set up a <Location> directive to point to your repository. For example, if you want your repository to be referenced with the URL http://example.net/bill/documents, and the repository is located in /srv/repositories/bill_documents, you could use the following Location directive:

```
<Location /bill/documents>
   DAV svn
   SVNPath /srv/repositories/bill_documents
   AuthType None
</Location>
```

Or, if you want more security, you could allow for valid users only:

```
<Location /bill/documents>
   DAV svn
   SVNPath /srv/repositories/bill_documents
   AuthType Basic
   AuthName "Bill's Documents"
   AuthUserFile /srv/repositories/bill_documents/passwd
   Require valid-user
</Location>
```

Basics of Using Subversion

Now that you have Subversion set up, let's take a look at some of the basic commands you'll need to know. The basic command-line Subversion client program is called svn, and all of the client commands that you'll use are accessed through that program. To get a complete list of the commands that are available, you can run `svn help`. You can also run `svn help [command]` to get help on a particular command.

The first basic command that you need to know is `svn add`. When you create a new file in a working copy, Subversion doesn't add it to the repository automatically. That way, you can control what gets versioned. For example, it usually would be a waste of space to add an emacs scratch file to your repository. Using `svn add` is easy. You simply need to give it the names of any files or directories to be added, and they will be scheduled for addition to the repository, assuming they reside inside of a valid working copy. Note though, that I said "scheduled". When you issue the `svn add` command, Subversion doesn't actually add the files to the repository yet. Instead, it schedules them to be added at the next commit. That way, you add multiple files with several `svn add` commands and still batch them together so that they are committed as a single revision, along with any already-versioned files that have been locally modified.

So what's a commit? Well, when you modify files inside a working copy, the data isn't sent to the repository automatically. You need to commit your changes to the repository with `svn commit`. The commit command performs the work of actually sending your local changes to the repository to create a new revision. Normally, if you're in the working copy, you can simply issue `svn commit` with no options, and it will recursively commit all changed files under your current directory. However, if you don't want to commit all of the local changes, you can specify only certain files by listing them on the command line.

Once a file has been added to the repository, it can be freely modified locally and Subversion automatically determines what changes have been made in order to send them to the repository when you perform a commit. There is a restriction though. You can't just copy, move or delete files with the standard `cp`, `mv` or `rm` commands. If you do, Subversion won't know about the change and will lose track of the file. Instead, you need to use the Subversion equivalents `svn cp`, `svn mv` and `svn rm`. Syntactically, they work about the same as the local versions that you're used to, but they also schedule their respective actions to be applied to the repository on the next commit.

To find out the current status of a file in your working copy, you can use `svn status`. The status command shows you information such as which files are not under version control, which files have been modified and which files are scheduled for addition. For instance, the following output shows two modified files and one that hasn't been added to the repository:

```
$ svn status
?          .GroceryList.txt.swp
M          Frogs.png
M          GroceryList.txt
```

You also can use the `svn update` command to update your working copy to the latest revision. If you're accessing only the Subversion repository from a single computer, updating isn't necessary. However, if files are being modified from multiple computers, you need to run `svn update` in your working copy to get any changes that have been committed from a different computer.

CONNECTING FROM WINDOWS XP

Whether you use it for games, work, placation of a less-technical spouse or just because you like it, the chances are pretty good that there's at least one Windows machine on your network. The good news is that Subversion was designed as a cross-platform application and is very well supported under Windows. Precompiled binaries of the command-line client are available from the Subversion downloads page. Additionally, there is an excellent GUI client for Windows that integrates with the Windows Explorer, called TortoiseSVN.

Windows XP also supports autoversioning through WebFolders, although you'll want to use the old Explorer-extension version of WebFolders rather than the newer version that was introduced with WinXP, as the new version suffers from incompatibilities. To connect to a repository you simply need to add a new network place and enter the repository URL, with the port number appended. For example, to connect to a repository at example.com/documents, you'd use the URL http://example.com:80/documents.

Autoversioning

Now that I've explained the hard way of using Subversion to keep track of your files, let's take a look at autoversioning. When you use Apache as your Subversion repository server, it uses an extension of the WebDAV protocol for transferring files to and from the repository. An interesting side effect of this is that most operating systems can mount shared WebDAV directories as a network filesystem, much like Samba or NFS. That means you can mount a Subversion repository and directly access the files without needing to store them locally in a working copy. This can have several advantages that make it really nice for dealing with your personal files. For one, a new version is created every time a file is saved. That way, you have a complete save history of your files without worrying about whether you've done a commit recently. You also add files to the repository merely by creating them, and can do copies, moves or deletes with the standard filesystem commands. Furthermore, if you access your repository from multiple computers, you always know that you're accessing the most recent version without remembering to run `svn update`.

Of course, autoversioning does have its downsides. For one, it requires a reasonably fast network connection to the computer that's serving the repository, so it may not be practical for a laptop that's frequently used away from home; although if you have access to a network connection back to the server, it's always possible to copy files to your local hard drive, edit them and then copy them back to the repository. Another downside to autoversioning is that you can access only the most recent repository revision. If you want to access older revisions of files, you have to download them locally, which can be done either by checking out a directory at a specific revision:

```
$ svn checkout -r 1563 http://$MY_SERVER/docs/pics/
```

or by using `svn cat` to download a single file:

```
$ svn cat -r 1563 http://$MY_SERVER/docs/pics/beach.jpg
```

If you're going to use autoversioning to mount your repository under Linux, you need to install davfs. Once it is installed, mounting the repository is easy. All you need to do is run `mount.davfs`, like in the following example, which mounts the repository $MY_SERVER/docs at /mnt/documents:

```
$ mount.davfs http://$MY_SERVER/docs/ /mnt/documents
```

Before you can use autoversioning though, you also have to turn it on in Apache. To do that, you need to add the SVNAutoversioning on option to your <Location> directive for the Subversion repository.

Conclusion

Subversion is a system with a large feature list, many of which I haven't even touched on. You should know enough now to get started with versioning your files though. I've been using it for my files for a while now and find it to be very helpful. I find it especially useful when used with autoversioning, which makes it an almost seamless integration with the filesystem.

Resources for this article: www.linuxjournal.com/article/8751.■

William Nagel is the Chief Software Engineer for a small technology company, and the author of *Subversion Version Control: Using the Subversion Version Control System in Development Projects*. He can be reached at bill@williamnagel.net.

CONNECTING FROM OS X

Okay, I admit it. I'm a Mac guy. As a Mac guy, my PowerBook gets a lot of use on my home network, so being able to access my files from there easily is pretty important to me. Fortunately, Subversion makes my life easy here. Subversion runs on OS X just as easily as it does on Linux, and it is a breeze to install. If you use the Fink package management system for installing open-source software on your Mac, you can install Subversion from there, or you can get standalone binaries.

If you decide to take advantage of autoversioning, you'll also be very pleased with OS X. Mounting an autoversioned repository is as easy as selecting Connect to Server... from the Finder's Go menu and entering the repository's URL. The repository will be mounted in /Volumes, and it will appear on the desktop as a mounted network share.

Developing Eclipse Plugins

A primer on getting started with Eclipse views, editors and plugins.

MIKE MCCULLOUGH

This article presents a set of best practices for use when developing Eclipse plugins for application development environments built on the Eclipse platform. The general principles of plugin development outlined in this article can be applied to many other Eclipse-based development environments, in addition to the downloadable version. Several aspects of the Eclipse plugin development process are covered here, including the View versus Editor debate, the inside or outside choice, some standard widget toolkit (SWT) basics and the usefulness of the Eclipse Plugin Wizard. The advantages of using Eclipse for developing Eclipse plugins also are covered. The article also includes a walk-through of a simple application plugin with an eye toward reuse across multiple Eclipse application plugins.

The View vs. Editor Debate

In Eclipse, the two basic ways of presenting any type of information to the user are with a View or an Editor. Both Views and Editors allow the user to select certain actions to be performed by the plugin by single- or double-clicking on an item, by a right-click pop-up menu or by a top-level pull-down menu item.

The Editor class can do almost everything that the View class can do, plus a whole lot more. Allowing all this extra functionality comes at a price, however, in both system and code complexity. In general, the Editor class requires much more effort to develop than a View, so a certain amount of decision making must occur before embarking on an Editor implementation.

Views are sufficient when simply providing information to a user and allowing certain built-in capabilities is required. Users can input data to Views with relative ease usually by using other widgets in the SWT, such as tables and text boxes. But, what if you want more of a free-form interaction with the user? In addition, what if you want to have user inputs that are persistent across multiple launches of Eclipse?

A good general guideline to use in this debate is the issue of persistence. Although it is possible to retain data from a View in some kind of persistent repository, in most cases this requires some level of work to be done in a file or file-like context. If this is the case, it often is easier simply to implement an Editor instead.

The second most common consideration is the actual data being presented. If the user can select multiple data units and perform actions using them or against them on a one-at-a-time basis, it usually is easier to implement the operation or operations as a distinct View.

In this article, we implement a sample Eclipse plugin. This plugin has a simple goal: to provide generic application-level data to the user. This data is going to be represented as strings, although almost any data type could be substituted. The usual left-click, right-click and double-click actions are going to be enabled, but only double-clicking is modified as a reusable example for all other action implementations.

As there is no immediate need for a persistent resource and as there will be multiple instances of data to select on a one-at-a-time basis, the sample plugin capability is going to be implemented as a View, which we simply call the DataView.

The Inside or Outside Choice

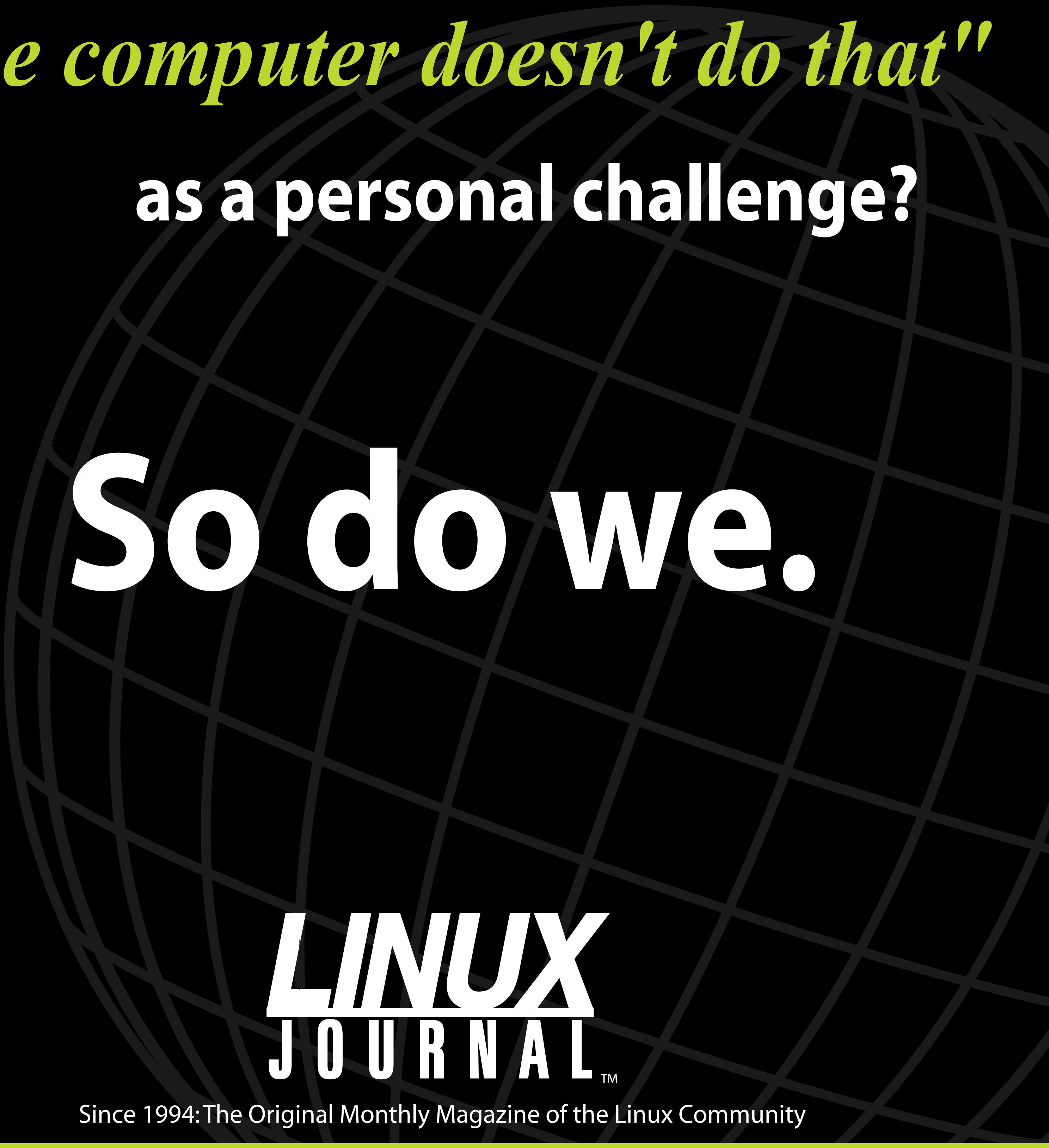
When implementing either Views or Editors, another decision must be made. Should the data be presented to the user within the actual Eclipse environment or outside of it somehow? The SWT provides Form classes that allow you to externalize your application data if you choose.

Editors can be implemented either externally or internally, but external Editors lack easy access to the plugin itself. Surprisingly, existing vendor plugins provide exactly this kind of functionality. In most of these cases, this is chosen because of the loss of plugin access as vendors decide to lock out the user from certain levels of Eclipse functionality. In general, the proper choice for plugin Editors—notwithstanding the user debate over openness in tools—is to implement Editors internally in Eclipse. It simply doesn't make much sense to lose access to the rest of the plugin if you don't have to. Now, what about Views?

Similar to Editors, Views can be implemented either externally as a separate Form class or internally as a View with additional SWT widgets. There are no hard and fast rules here, but there are some basic guidelines to follow when dealing with this decision. In general, two things should be considered. First, can the View data be described as unique and discrete entities, with fields or operations specific to that particular data item? Second, are there always less than about nine of these items? If so, the View can be implemented as a View with a Table or perhaps a View with separate Tabs for each discrete unit.

If the actual number of instances of the data and the types of operations on that data is at all dynamic or unknown—for example, the developer does not know a priori exactly how many items there will be or exactly how many distinct operations to design or to allow for in the future—it probably is best to implement the View as an external Form class.

The sample plugin developed in this article is a simple 100-item implementation



IN GENERAL, THE PROPER CHOICE FOR PLUGIN EDITORS—NOTWITHSTANDING THE USER DEBATE OVER OPENNESS IN TOOLS—IS TO IMPLEMENT EDITORS INTERNALLY IN ECLIPSE.

displaying data with only two distinct fields for each item, a name and a value. Although there are no predefined system requirements for more than nine multiple operations, there also are no explicit multiple operations defined. Therefore, you safely can assume that it will not require a great deal of them either—it is supposed to be simple after all. The DataView plugin therefore should be implemented as an internal View.

Getting Started with the Eclipse Environment

To start the actual plugin development, you need to start with an Eclipse installation. For this example, we downloaded the latest Eclipse version at the time of this writing, v3.0.2, from the Eclipse site. As we use the CDT plugin for C and C++ development extensively in our own organization, we then downloaded the CDT v2.1 Project. It can be accessed under the Eclipse Tools Project from the projects link on the main Eclipse page. You can download both of these as .zip files, which extract into a /eclipse directory. Therefore, make sure you install the Eclipse zip file prior to the CDT zip file. In our case, we were building on Red Hat Linux 9.0 using the GTK- version of both the Eclipse framework and the CDT plugin, but the Motif versions work equally as well. We then brought up Eclipse with `./eclipse` and selected the Plugin Development Environment (PDE) perspective from Window→Open Perspective.

Using the Eclipse Plugin Wizard

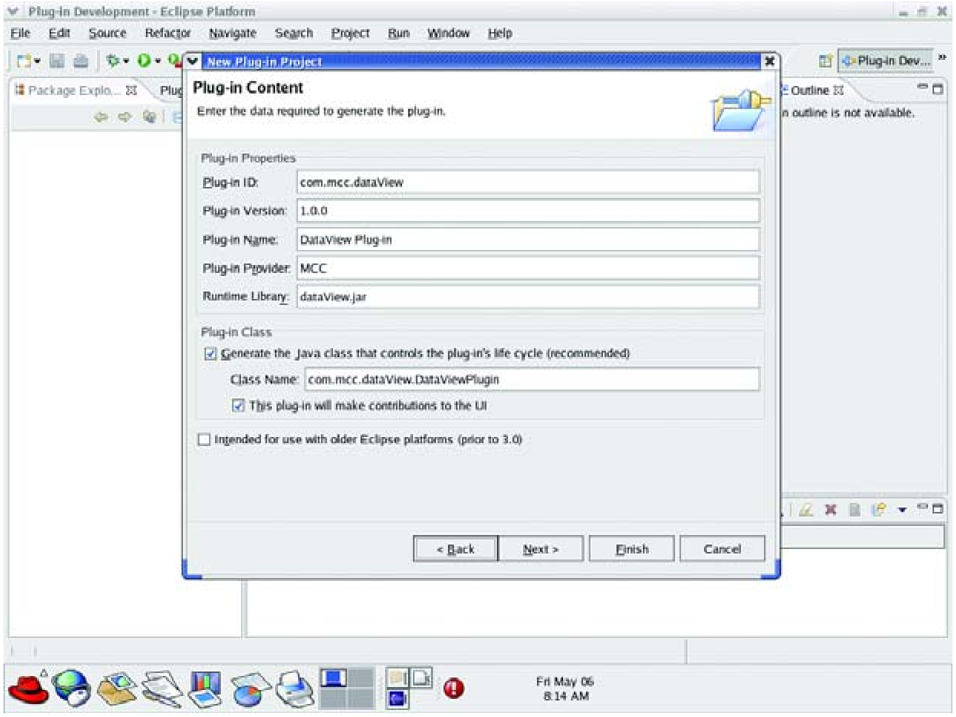
Many texts on Eclipse plugin development walk users through the Hello World type of project. It is this author's belief that although that might be a good start for novice programmers, it is absolutely the worst way for experienced software developers to begin using Eclipse. It takes too long, and worst of all, much of the work has to be redone once you need to create a real plugin. Instead, we usually recommend creating as nearly complete a plugin project as possible, using as many pre-existing templates as the environment allows. Doing so gives you a considerable amount of functionality immediately. You then can develop your own customizations of the existing functionality without worrying about being properly attached or hooked to the normal plugin-type environment.

In the PDE, the Plugin Wizard allows a developer to create a sample plugin project quickly and easily, simply by selecting File→New→Plug-in Project. When prompted for a name of the plugin, we use a common syntax used by other commercial vendors. That is, we name the plugin with the text com.companyName.productName or in this example, com.mcc.dataView, as shown in Figure 1.

It is easy enough to remove functionality from the plugin project once we get started on some actual customizations, so we select Next for two screens until we reach the Templates screen. We then select Create a plugin using one of the template's boxes and choose to use the Custom Plugin Wizard. You then select Next to see the templates to be created.

You could remove specific functionality at this point, but for this exercise, we retain all functionality and simply keep selecting Next until we reach the Main View Settings window. In this window, we rename the Sample View as Data View, as shown in Figure 2. Once you have modified this window appropriately, you can select Finish or cycle through the last of the customization sections, which is View Features. You can move forward and back during this process, so take your time. No changes are made to the environment until

Figure 1. To start a new plugin, select File→New-Plug-in Project to bring up the Plugin Wizard.


Plug-in Development - Eclipse Platform
File Edit Source Refactor Navigate Search Project Run Window Help
Plug-in Dev...
Package Explo...
Outline
n outline is not available.
New Plug-in Project
< Back
Next >
Finish
Cancel
Fri May 06
8:14 AM

Plug-in Content

Enter the data required to generate the plug-in.

Plug-in Properties

Plug-in ID: com.mcc.dataView

Plug-in Version: 1.0.0

Plug-in Name: DataView Plug-in

Plug-in Provider: MCC

Runtime Library: dataView.jar

Plug-in Class

☑ Generate the Java class that controls the plug-in's life cycle (recommended)

Class Name: com.mcc.dataView.DataViewPlugin

☑ This plug-in will make contributions to the UI

☐ Intended for use with older Eclipse platforms (prior to 3.0) the Finish button is selected.

If you mess it up the first time, as this author did, don't hesitate to delete the entire project including the directory contents and start again until you get it right. Once the plugin has been created to your exact template specifications, you are ready to execute the plugin for the first time. For this we use the run-time workbench.

Testing the Plugin Using the Run-time Workbench

One of the most attractive features of the Eclipse framework is its own ability to develop, test, debug and execute plugins in the run-time workbench. Few development environments provide exactly this kind of functionality in such an easy-to-use and intuitive fashion. This removes many of the time-wasting impediments to developers stuck in the long compile-build-debug cycle typical of other development environments.

To execute the DataView plugin, simply select Run→Run As→6 Run-time workbench from the PDE perspective. The Eclipse PDE spawns a completely separate user workspace, called the run-time workspace, and executes the DataView plugin. On the first execution of the plugin, you need to select the Window→Show View→Other top-level menu pull-down, and choose the DataView listed under the specific Views heading that you selected during plugin creation.

In future executions, the run-time workbench functions much as the regular workspace functions and retains the appropriate View layout between multiple launches. This greatly simplifies testing, as re-testing is only a matter of running the run-time workbench again.

One of the few drawbacks to the run-time workbench model is its rough doubling of host RAM usage due to executing the equivalent of two Eclipse sessions on a single machine. In systems with limited RAM, such as laptop environments, this can be a bit slow and frustrating. As JVMs improve, though, this problem does get better.

Experiment with the sample plugin menus and pull-downs to get a feel for what functionality you have created. Even though we don't discuss Editor customizations in this article, you also might want to experiment with creating a simple Eclipse project and then creating a new file with a .mpe extension. Doing so allows you to get familiar with the concept of multipage editors similar to the one used for displaying the plugin.xml file now listed under your new plugin project.

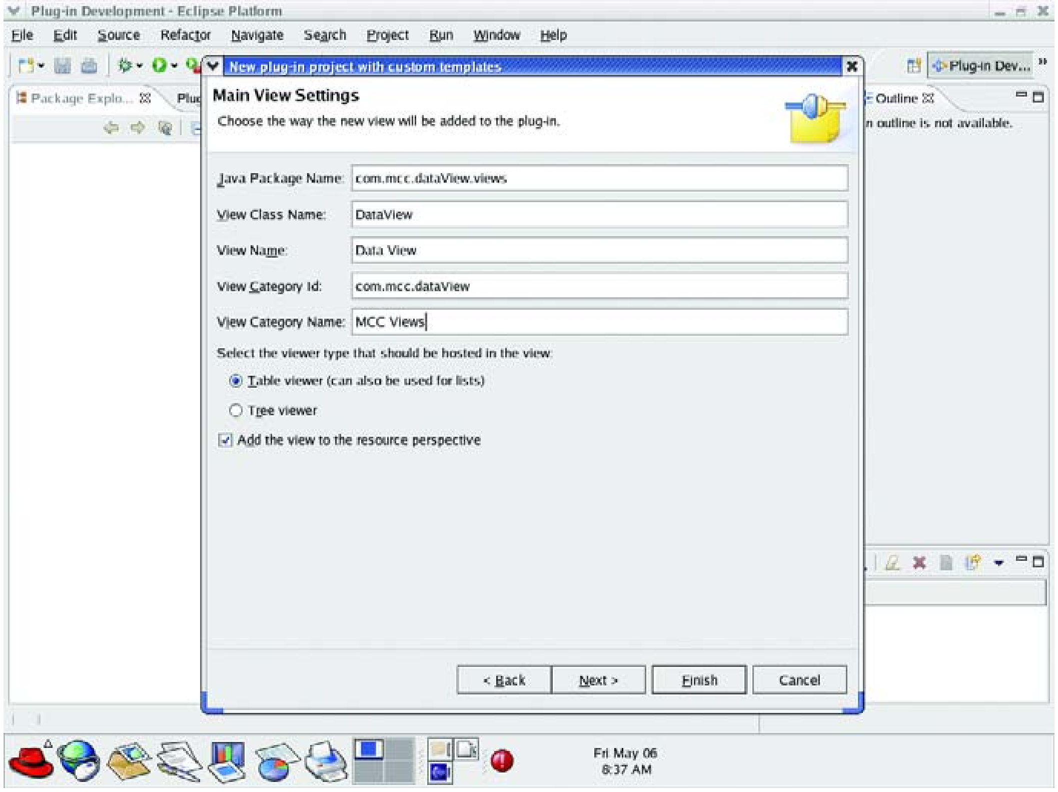
Customizing the Plugin View

The first step in customizing the DataView is to add a new ViewLabelProvider class to the plugin project under the Views folder. This allows you to add data to the table to be displayed in the DataView window when the plugin is executing. The ViewLabelProvider interacts with the ParameterControl class by providing the data stored there, a Name and a Value, to the DataView. A complete listing of this class can be found in the project tar file.

The next step in customizing the DataView is to add the ParameterControl class that is referenced by the ViewLableProvider class to the plugin project under the Views folder. This class

ONE OF THE MOST ATTRACTIVE FEATURES OF THE ECLIPSE FRAMEWORK IS ITS OWN ABILITY TO DEVELOP, TEST, DEBUG AND EXECUTE PLUGINS IN THE RUN-TIME WORKBENCH.

ONE OF THE FEW DRAWBACKS TO THE RUN-TIME WORKBENCH MODEL IS ITS ROUGH DOUBLING OF HOST RAM USAGE DUE TO EXECUTING THE EQUIVALENT OF TWO ECLIPSE SESSIONS ON A SINGLE MACHINE.



Main View Settings

Choose the way the new view will be added to the plug-in.

Java Package Name: com.mcc.dataView.views

View Class Name: DataView

View Name: Data View

View Category Id: com.mcc.dataView

View Category Name: MCC Views

Select the viewer type that should be hosted in the view:

● Table viewer (can also be used for lists)

○ Tree viewer

☑ Add the view to the resource perspective

Figure 2. Give your plugin a name in the Main View Settings window.

maintains the actual parameter names and values to be displayed in the DataView table. Although a relatively simple implementation, it easily can be scaled to a greater number of fields if necessary. A complete listing of this class also can be found in the project tar file.

The third step in customizing the DataView is to add a Table with the appropriate settings to the DataView class (see Listing 1 on the *Linux Journal* FTP site), modify the Plugin class itself to support the UserParameter variable and customize the DoubleClick action to display the table entry data. Note the addition of a new function called UpdateTheTable that provides the latest data to the Table. This function would be the modification point for new application data by way of the filesystem or network or whatever. For this example only, the first four parameters are modified for new data. The full code for our plugin is available from the *Linux Journal* FTP site (see the on-line Resources).

The final modification is to add a ParameterControl variable and its initialization to the plugin itself. This is done by adding the variable declaration to the DataViewPlugin.java file, at the first point after the resourceBundle is declared. The variable declaration should be as follows:

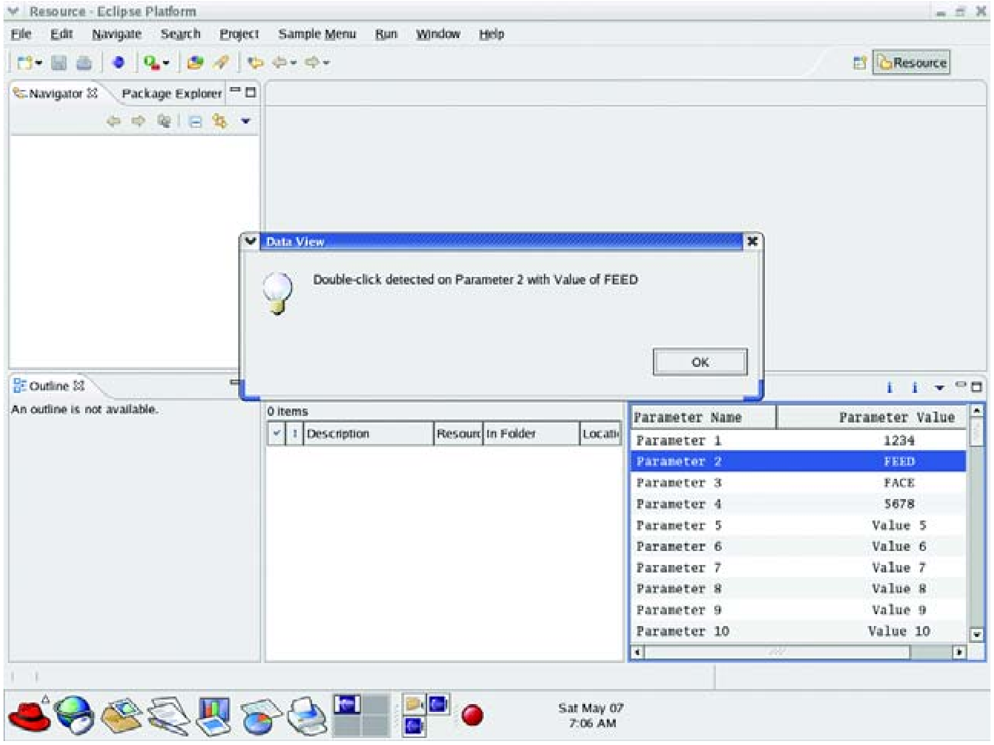
```
//User Parameter functionality
public ParameterControl userParameters[] =
    new ParameterControl[100];
```

Next the initialization section is added at the end of the Plugin constructor as shown:

```
// Additions for User Parameter functionality
int index;
for (index = 0; index < 100; index++)
{
    userParameters[index] =
        new ParameterControl("Parameter "
         + (index + 1), "Value " + (index + 1));

}
```

The final run-time workbench execution of the plugin is shown in Figure 3. In the figure,



Data View

Double-click detected on Parameter 2 with Value of FEED

An outline is not available.

0 items

Parameter Name	Parameter Value
Parameter 1	1234
Parameter 2	FEED
Parameter 3	FACE
Parameter 4	5678
Parameter 5	Value 5
Parameter 6	Value 6
Parameter 7	Value 7
Parameter 8	Value 8
Parameter 9	Value 9
Parameter 10	Value 10

Figure 3. The plugin is finished and responding to user input.

the user has double-clicked on an item, producing a simple user dialog that displays the actual data for the table selection made.

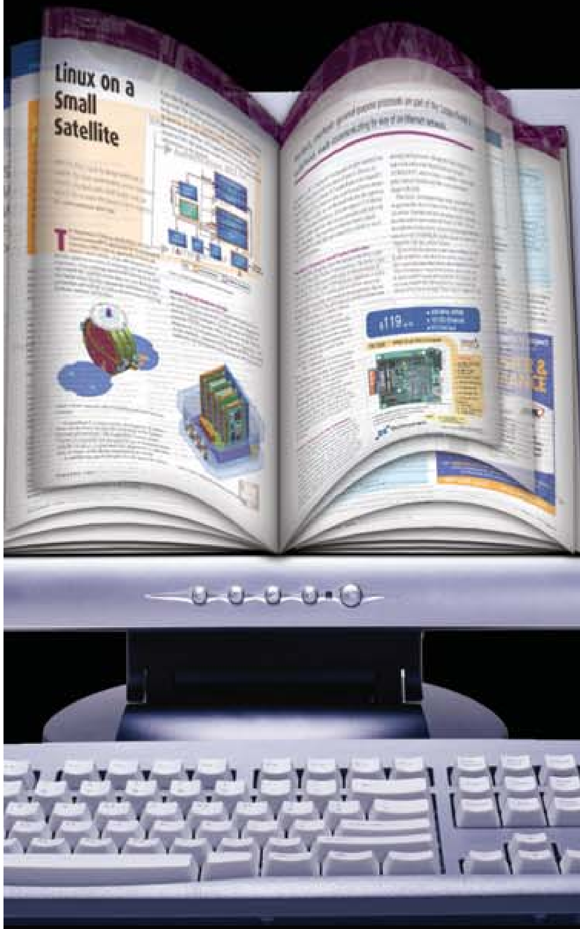
Conclusion

In this article, we discovered some basic rules to follow when making decisions about how an Eclipse plugin should present application data to a user by way of an Eclipse View. We have utilized the Eclipse Plugin Wizard to auto-generate much of the plugin initialization code in a testable and reusable format. We also have reviewed certain usage examples of the SWT, including Tables, Viewers and LabelProviders, and their uses in the context of a User View. Finally, we have seen some of the advantages and disadvantages of using the run-time workbench feature of Eclipse.

Along the way, we created a relatively simple sample plugin that can be used over and over again as a starting point for new Eclipse plugins. The sample plugin easily accommodates future growth in the plugin itself by enabling all typical plugin functionality, such as multipage editors, properties, wizards and reference extensions. This additional plugin functionality now can be implemented in an iterative fashion, allowing not only for future growth of the specific plugin but easier reuse across multiple plugin developments. It also can serve as a starting point for new developers with little or no prior knowledge of Eclipse development. This reusability aspect is one of the most compelling features of the Eclipse framework.

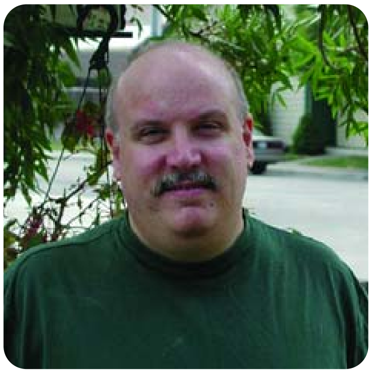
Resources for this article:
www.linuxjournal.com/article/8789.■

Mike McCullough is president and CEO of MCC Systems, Inc. Mike has a BS in Computer Engineering and an MS in Systems Engineering from Boston University. A 20-year electronics veteran, he has held various positions at Wind River Systems, Lockheed Sanders, Stratus Computer and Apollo Computer. MCC Systems is a provider of Eclipse-based software development tools, training and consulting services for the embedded market.



Separation of Church and Choice

When did "choice" become the god of the Open Source community?



NICK PETRELEY, EDITOR IN CHIEF

I recently lodged several criticisms of GNOME in *Linux Journal*'s sister publication *TUX* (**www.tuxmagazine.com**). GNOME fans were outraged, of course. I find it telling that none of them even attempted to explain why the GNOME way of doing things was better than KDE or any other competing desktop.

The closest thing I saw to a defense for a GNOME feature was the argument that "Microsoft plans to do it the same way in the next version of Windows." The claim wasn't strictly true, but that is beside the point. You can read last month's rant if you want to know what I think of the "monkey see Microsoft, monkey do Microsoft" mentality that is infecting the Open Source community.

But, the most confounding response to my criticisms of GNOME was that "You should stop bashing GNOME and praise it because it offers desktop users yet another choice."

Let me be clear that what follows is not a rant about GNOME. (Relax, I'll get to that column all in good time.) This is a rant about defending anything based solely on the fact that it adds another choice for users. This is a very popular defense. I've seen it leveraged against criticisms of many other things in the Linux universe, not only GNOME.

Let me be equally clear that I don't care whether you use GNOME, KDE, Xfce, Blackbox, Fluxbox, Fuzzbox, Jackinthebox, Window Maker, Enlightenment, Fvwm, IceWM, Twm, Ratpoison, Ion or any of the other gazillion desktops or window managers. I like several of the above, depending upon my needs at the time, but I will not lose a wink of sleep over the fact that you prefer something other than what I like. Neither will I be the least bit offended if you disagree with what I believe about what is best in the narrower field of full-featured desktops.

But the fact that we're both entitled to our opinions doesn't mean there isn't an objective standard against which we can measure our opinions. There is. And, even the nastiest of letters I received about my criticisms of GNOME proved that my opinions came closer to that objective standard than the opinions of those who disagreed with me. How can I make such a bold assertion? Easy. First, as I said, nobody really offered any logical defense that anything in GNOME was better than the competition. One has to wonder why not, if GNOME is such a great desktop?

More telling is the fact that almost all (if not all) of those who disagreed with my criticism of the Nautilus "spatial" file manager couldn't respond to specific questions or complaints because they don't use Nautilus in spatial mode. What a way to bolster your case, eh? I don't like it enough to use it, but stop criticizing it because, like GNOME itself, it is a choice.

GNOME is a choice besides what? KDE, Xfce, Blackbox, Fluxbox, Window Maker and so on? The last time I looked, it didn't seem like the progress of Linux was roadblocked by the lack of another desktop or window manager. So what is the source of this notion that something has inherent value based solely on the principle that it provides users with yet another choice?

If I were a restaurant critic, and I happened upon a restaurant that based all its recipes on rat feces, you can count on the fact that I would not defend or praise this restaurant on the sole basis that the dining public could choose it over McDonald's or Ruth's Chris. Crap is crap, and there's no way I'm going to say anything positive about a restaurant that features it on the menu. I don't care what kind of platters the restaurant uses to serve it up.

Granted, that doesn't mean people won't patronize a restaurant of this kind. There's no accounting for taste, an axiom proved by the fact that there are any GNOME users at all. But let's not pretend crap is filet mignon in order to appease the god of choice. If a god of choice did actually exist, I have my doubts that we'd find him dining on rat feces in order to glorify his name. And no "God uses GNOME" letters, please. That's too easy.

The bottom line is this, and it applies to every bit of software, not just GNOME. If you can't defend its design, or you find out its users turn off the very features you claim make it great, then here's my advice. Either go back to the drawing board and make it really great instead of theoretically great, or just deep-six it once and for all. Cremate it and scatter the ashes somewhere they won't stink up the rest of the software base. But don't come to me and defend it based on the fact that it gives users a choice. You'll find no sympathetic ear here.

Yeah, but what do I really think? ■

Nicholas Petreley is Editor in Chief of *Linux Journal* and a former programmer, teacher, analyst and consultant who has been working with and writing about Linux for more than ten years.

FANATICAL™
SUPPORT
IS THE DIFFERENCE

The World's Fastest InfiniBand Switch

From a Company You've Trusted for 23 Years

Microway's **FasTree**™ DDR InfiniBand switches run at 5GHz, twice as fast as the competition's SDR models. FasTree's non-blocking, flow-through architecture makes it possible to create 24 to 72 port modular fabrics which have lower latency than monolithic switches. They aggregate data modulo 24 instead of 12, improving nearest neighbor latency in fine grain problems and doubling the size of the largest three hop fat tree that can be built, from 288 to 576 ports. Larger fabrics can be created linking 576 port domains together.

▲ **72 Port FasTree™ Configuration**

Working with PathScale's InfiniPath HTX Adapters, the number of hops required to move MPI messages between nodes is reduced, improving latency. The modular design makes them useful for SDR, DDR and future QDR InfiniBand fabrics, greatly extending their useful life. Please send email to fastree@microway.com to request our white paper entitled *Low Latency Modular Switches for InfiniBand.*

Microway's **QuadPuter®** includes four AMD single or dual core Opteron™ processors, 1350 Watt redundant power supply, and up to 5 redundant, hot swap hard drives-all in 4U. Dual core enables users to increase computing capacity without increasing power requirements, thereby providing the best performance per watt. Constructed with stainless steel, QuadPuter's RuggedRack™ architecture is designed to keep the processors and memory running cool and efficiently. Hard drives are cooled with external air and are front-mounted along with the power supply for easy access and removal. The RuggedRack™ is also available with an 8-way motherboard and up to 128 GB of memory for power- and memory-hungry SMP applications.

Call us first at 508-746-7341 for quotes and benchmarking services. Find technical information, testimonials, and newsletter at microway.com.

◀ **QuadPuter® Navion™ with hot swap, redundant power and hard drives and dual core Opterons, offering the perfect balance between performance and density**

AMD 64 Opteron™

PathScale™
Accelerating Cluster Performance™

Microway®
Technology you can count on℠

508.746.7341 microway.com

Let's go Xtreme

Introducing Appro *Xtreme*Servers & Workstation with 8 DIMM Sockets per CPU

- 2-way or 4-way, Single or Dual-Core AMD Opteron™ processors
- **Largest memory capacity - 8 DIMM Sockets per CPU, up to 128GB**
- PCI-Express technology to increase I/O bandwidth and reduce system latency
- Outstanding Remote Management – IPMI 2.0 compliant
- Cable-free design, ready to run, simple to install, service and maintain
- Support for Windows® or Linux OS
- Ideal for memory-intensive and I/O-intensive applications

1U / 2U / 3U Servers and Workstation

AMD Opteron™ Processors - AMD64 dual-core technology reduces memory latency and increases data throughput
- Dual-core processors with Direct Connect Architecture deliver the best performance per watt with little or no increase in power consumption or heat dissipation.

APPRO
HPC Cluster Solutions

Appro delivers high-performance computing solutions to help you maximize productivity for a solid ROI. On-site maintenance and installation services are also available.

For more information, please visit www.appro.com
or call Appro Sales at 800.927.5464, 408.941.8100.

AMD 64 Opteron™