USENIX '05

April 10–15, 2005
Marriott Anaheim
Anaheim, CA

Join our community of programmers, developers, and systems professionals in sharing solutions and fresh ideas on topics including Linux, clusters, security, open source, system administration, and more.

KEYNOTE ADDRESS by George Dyson, historian and author of *Darwin Among the Machines*

Design Your Own Conference:

Combine Tutorials, Invited Talks, Refereed Papers, and Guru Sessions to customize the conference just for you!

5-Day Training Program
April 10–14
- Now with half-day tutorials
- More than 35 to choose from
- Learn from industry experts
- Over 15 new tutorials

3-Day Technical Program
April 13–15, 4 Tracks
- General Session
  Refereed Papers
- FREENIX/Open Source
  Refereed Papers
- Invited Talks
- Guru Is In Sessions

Choose one subject or mix and match to meet your needs.
Themes include:
- Coding
- Networking
- Open Source
- Security
- Sys Admin

Evening events include:
- Poster and Demo Sessions
- Birds-of-a-Feather Sessions
- Vendor BoFs
- Receptions

Register by March 21 and save up to $300 • www.usenix.org/anaheim05

USENIX '05
Annual Technical Conference

CONTENTS

CONFERENCE AT A GLANCE

Sunday, April 10, 2005

7:30 a.m.–5:00 p.m.	ON-SITE REGISTRATION
9:00 a.m.–5:00 p.m.	TRAINING PROGRAM
6:00 p.m.–7:00 p.m.	WELCOME RECEPTION
6:30 p.m.–7:00 p.m.	CONFERENCE ORIENTATION

Monday, April 11, 2005

7:30 a.m.–5:00 p.m.	ON-SITE REGISTRATION
9:00 a.m.–5:00 p.m.	TRAINING PROGRAM
8:30 p.m.–11:30 p.m.	BIRDS-OF-A-FEATHER SESSIONS

Tuesday, April 12, 2005

7:30 a.m.–5:00 p.m.	ON-SITE REGISTRATION
9:00 a.m.–5:00 p.m.	TRAINING PROGRAM
8:30 p.m.–11:30 p.m.	BIRDS-OF-A-FEATHER SESSIONS

Wednesday, April 13, 2005

7:30 a.m.–5:00 p.m.	ON-SITE REGISTRATION
9:00 a.m.–5:00 p.m.	TRAINING PROGRAM
9:00 a.m.–10:30 a.m.	OPENING REMARKS, AWARDS, AND KEYNOTE
11:00 a.m.–5:30 p.m.	TECHNICAL PROGRAM
6:00 p.m.–7:30 p.m.	POSTER/DEMO RECEPTION
8:30 p.m.–11:30 p.m.	BIRDS-OF-A-FEATHER SESSIONS

Thursday, April 14, 2005

7:30 a.m.–5:00 p.m.	ON-SITE REGISTRATION
9:00 a.m.–5:00 p.m.	TRAINING PROGRAM
9:00 a.m.–5:30 p.m.	TECHNICAL PROGRAM
4:00 p.m.–5:30 p.m.	WORK-IN-PROGRESS REPORTS
7:00 p.m.–8:30 p.m.	CONFERENCE RECEPTION
8:30 p.m.–11:30 p.m.	BIRDS-OF-A-FEATHER SESSIONS

Friday, April 15, 2005

8:00 a.m.–12:00 p.m.	ON-SITE REGISTRATION
9:00 a.m.–3:30 p.m.	TECHNICAL PROGRAM
4:00 p.m.–5:30 p.m.	USENIX GAME SHOW

INVITATION FROM THE PROGRAM CHAIRS

VIVEK PAI

NIELS PROVOS

Dear Colleague,

We're pleased to invite you to attend the 2005 USENIX Annual Technical Conference. This year, we're offering 5 days of training running alongside a 3-day conference program filled with the latest research, security breakthroughs, sessions devoted to Linux and open source software, and practical approaches to the puzzles and problems you wrestle with. You'll also have many opportunities to chat with peers who share your concerns and interests.

USENIX '05 offers 5 days of tutorials led by highly respected instructors covering crucial topics including:

- Practical System and Network Monitoring by John Sellens
- Implementing LDAP Directories by Gerald Carter
- Solaris 10 Security Features Workshop by Peter Baer Galvin
- Inside the Linux Kernel (Updated for Version 2.6) by Theodore Ts'o
- VoIP Principles and Practice by Heison Chak
- Network Security Assessments Workshop—Hands on by David Rhoades

The Technical Program begins with the Keynote Address by George Dyson, historian and author of *Darwin Among the Machines,* and includes many other Invited Talks of note such as:

- Spencer Shepler, *Sun Microsystems*, on NFSv4
- Mark Wirt, *Butterfly.net*, on system support for massively multiplayer online gaming
- Scott Maxwell and Frank Hartman, *NASA JPL*, on Linux and JPL's Mars Exploration Rover Project: Earth-based planning, Simulation, and *Really* Remote Scheduling
- Vernor Vinge, Hugo award-winning sci-fi author of the *Across Real Time* series, *The Witling, True Names,* and *A Fire Upon the Deep,* on possible futures for software

General Session and FREENIX/Open Source Refereed Papers tracks are the premier forum for presenting the latest in groundbreaking research. CiteSeer (http://citeseer.ist.psu.edu/impact.html) ranks the USENIX Annual Technical Conference as one of the top-ten highest-impact publication venues for computer science. Be among the first to check out the latest innovative work on the topics you need most.

Don't miss the opportunity to pose your toughest questions to the experts in the Guru Is In Sessions. Vie for bragging rights and prizes at the USENIX Game Show. Mingle with colleagues and leading experts at the Birds-of-a-Feather sessions and at the various evening social events, including a poster reception, vendor sessions, and a reception to celebrate the 30th Anniversary of the USENIX Association.

USENIX '05 promises to be an exciting showcase for the latest in innovative research and cutting-edge practices in technology. We look forward to seeing you in Anaheim in April.

On behalf of the USENIX '05 Organizers,

Vivek Pai, *Princeton University*
GENERAL SESSION PROGRAM CHAIR

Niels Provos, *Google*
FREENIX/OPEN SOURCE PROGRAM CHAIR

CONFERENCE ORGANIZERS

GENERAL SESSION PROGRAM CHAIR

Vivek Pai, *Princeton University*

GENERAL SESSION PROGRAM COMMITTEE

Atul Adya, *Microsoft Research*
David Andersen, *Massachusetts Institute of Technology*
Andrea Arpaci-Dusseau, *University of Wisconsin*
Ludmila Cherkasova, *Hewlett-Packard Labs*
Tzi-cker Chiueh, *Stony Brook University*
Carla Ellis, *Duke University*
Dawson Engler, *Stanford University*
Steven Gribble, *University of Washington*
Erich Nahum, *IBM Research*
Jason Nieh, *Columbia University*
Timothy Roscoe, *Intel Research*
Mema Roussopoulos, *Harvard University*
Michael Stumm, *University of Toronto*
Joe Sventek, *University of Glasgow*
Mustafa Uysal, *Hewlett-Packard Labs*
Hui Zhang, *Carnegie Mellon University*
Yuanyuan Zhou, *University of Illinois at Urbana-Champaign*

FREENIX/OPEN SOURCE PROGRAM CHAIR

Niels Provos, *Google*

FREENIX/OPEN SOURCE PROGRAM COMMITTEE

Andy Adamson, *University of Michigan*
Matt Asay, *Novell*
Crispin Cowan, *Immunix*
Karen Hackett, *Sun Microsystems*
Jun-ichiro itojun Hagino, *KAME*
Val Henson, *IBM*
Trond Myklebust, *NetApp*
Stephen Tweedie, *Red Hat*
Greg Watson, *Los Alamos National Laboratory*

INVITED TALKS COMMITTEE

Ethan Miller, *University of California, Santa Cruz*
Ellie Young, *USENIX*
Erez Zadok, *Stony Brook University*

GURU IS IN COORDINATOR

Rob Kolstad, *USENIX*

POSTER SESSION CHAIR

Atul Adya, *Microsoft Research*

WORK-IN-PROGRESS SESSION CHAIR

David Andersen, *Massachusetts Institute of Technology*

CREATE YOUR OWN CONFERENCE. We've listened to your feedback and have reorganized the conference to be more flexible for the attendees. Whether your interests lie strictly in security or Linux or include a variety of topics, you can build the conference you need. Mix and match tutorials, refereed papers, invited talks, and guru sessions to focus on just one topic—or sample the best of everything.

Take advantage of our expanded program of more training, research papers, and sessions devoted to the latest information and approaches—theory and practice. Dive in for one day or several, or come for the whole conference; an exciting spectrum of technical content fills every day.

WHY ATTEND: A NOTE FOR MANAGERS

Hiring the best and the brightest is the ultimate goal for any employer. However, keeping current employees up to par is just as important. Technology continues to evolve and truly to stay ahead of the game, your employees must continue to enhance their skills.

The training program at USENIX '05 offers a cost-effective, one-stop shop for training current IT and development employees. Over 35 tutorials taught by the most respected leaders in the field provide an unparalleled opportunity to learn from the best. Tutorials cover everything from open source technologies and security to system administration and defeating spam.

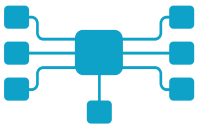
Combining full days of training with days of technical sessions on groundbreaking research makes the USENIX '05 experience even more valuable. Finally, the evening poster/demo sessions and the Birds-of-a-Feather sessions provide your staff with a chance to network with peers and industry leaders to gain that all-important "inside" IT knowledge that will keep your company current and running smoothly.

Keeping up with technology can be costly and time-consuming in this unforgiving economy: take full advantage of this opportunity to have your staff learn from the top researchers, practitioners, and authors all in one place, at one time.

CONFERENCE THEMES

Use the icons throughout the brochure to find the sessions that meet your interests, or check out pp. 27–29 for a full lisiting of program offerings for each theme. Choose a theme or mix and match to build the conference you need.

Coding


Networking


Open Source


Security


Sysadmin

Below is just one example of how USENIX '05 can be customized for your particular needs.

A security tool developer who uses Linux might choose to attend four days of training combined with two days of technical sessions:

Sunday: Training—S1: Hands-on Linux Security Class: Learn How to Defend Linux/UNIX Systems by Learning to Think Like a Hacker *(Day 1 of 2)*

Monday: Training—M1: Hands-on Linux Security Class: Learn How to Defend Linux/UNIX Systems by Learning to Think Like a Hacker *(Day 2 of 2)*

Tuesday: Training—T3: Solaris 10 Security Features Workshop

Wednesday: Technical Sessions
- Invited Talk: Computer Simulations of Thermal Convection and Magnetic Field Generation in Stars and Planets
- Invited Talk: DDoS Defense in Practice and Theory
- FREENIX Refereed Papers

Thursday: Training—R2: Network Security Monitoring with Open Source Tools

Friday: Technical Sessions
- Invited Talk: Linux and JPL's Mars Exploration Rover Project: Earth-based Planning, Simulation, and *Really* Remote Scheduling
- Invited Talk: Possible Futures for Software
- FREENIX Refereed Papers

To meet your needs, the Training Program at USENIX '05 provides in-depth, immediately useful training in the latest techniques, effective tools, and best strategies. The training track offers 5 days of tutorials with 39 half- and full-day sessions to choose from. USENIX tutorials survey the topic, then dive right into the specifics of what to do and how to do it. Instructors are well-known experts in their fields, selected for their ability to teach complex subjects. Attend tutorials at USENIX '05 and take valuable skills back to your company or organization. New topics are woven in with old favorites to create the most comprehensive learning track to date. Register now to guarantee your first choice—seating is limited.

SUNDAY, APRIL 10, 2005 FULL DAY (9:00 A.M.–5:00 P.M.)

S1	Rik Farrow	Hands-on Linux Security Class: Learn How to Defend Linux/UNIX Systems by Learning to Think Like a Hacker *(Day 1 of 2)*
S2	Radia Perlman	Bridges, Routers, Switches, and Internetworking Protocols
S3	Ned McClain	***New!*** Hot Topics in System Administration

SUNDAY, APRIL 10, 2005 HALF-DAY (9:00 A.M.–12:30 P.M.)

S4	Mark-Jason Dominus	Regular Expression Mastery
S5	Jacob Farmer	***New!*** Eliminating Backup System Bottlenecks Using Disk-to-Disk and Other Methods
S6	Gerald Carter	***New!*** Kerberos 5—Revenge of the Three-Headed Dog
S7	Mike Ciavarella	***New!*** Advanced Shell Programming
S8	Peter Baer Galvin	***New!*** Next-Generation Security Tools

SUNDAY, APRIL 10, 2005 HALF-DAY (1:30 P.M.–5:00 P.M.)

S9	Mark-Jason Dominus	Perl Program Repair Shop and Red Flags
S10	Jacob Farmer	***New!*** Next-Generation Storage Networking and Data Protection
S11	David N. Blank-Edelman	***New!*** Over the Edge System Administration, Volume 1
S12	Mike Ciavarella	***New!*** Documentation Techniques for SysAdmins
S13	Geoff Halprin	***New!*** Troubleshooting: A Basic Skill

MONDAY, APRIL 11, 2005 FULL DAY (9:00 A.M.–5:00 P.M.)

M1	Rik Farrow	Hands-on Linux Security Class: Learn How to Defend Linux/UNIX Systems by Learning to Think Like a Hacker *(Day 2 of 2)*
M2	Radia Perlman and Charlie Kaufman	Network Security Protocols: Theory and Current Standards
M3	Peter Baer Galvin	Advanced Solaris System Administration Topics
M4	David Blank-Edelman	Perl for System Administration: The Power and the Praxis
M5	Theodore Ts'o	Inside the Linux Kernel (Updated for v. 2.6)
M6	Heison Chak	***New!*** VoIP Principles and Practice
M7	Mike Ciavarella and Lee Damon	***New!*** Seven Habits of the Highly Effective System Administrator
M8	Marcus Ranum	System Log Aggregation, Statistics, and Analysis

TUESDAY, APRIL 12, 2005 FULL DAY (9:00 A.M.–5:00 P.M.)

T1	David Rhoades	Network Security Assessments Workshop—Hands-on *(Day 1 of 2)*
T2	James Mauro and Richard McDougall	***New!*** Solaris Kernel Performance, Observability, and Debugging *(Day 1 of 2)*
T3	Peter Baer Galvin	***New!*** Solaris 10 Security Features Workshop
T4	Tom Christiansen	Advanced Perl Programming
T5	Joshua Jensen	***New!*** RPM Package Management
T6	Gerald Carter	Managing Samba 3.0
T7	John Sellens	Practical System and Network Monitoring
T8	Lee Damon and Geoff Halprin	***New!*** Release Engineering and Project Lifecycle

WEDNESDAY, APRIL 13, 2005 FULL DAY (9:00 A.M.–5:00 P.M.)

W1	David Rhoades	Network Security Assessments Workshop—Hands-on *(Day 2 of 2)*
W2	James Mauro and Richard McDougall	***New!*** Solaris Kernel Performance, Observability, and Debugging *(Day 2 of 2)*
W3	Gerald Carter	Implementing LDAP Directories
W4	John Sellens	System and Network Monitoring: Tools in Depth
W5	Æleen Frisch	Administering Linux in Production Environments

THURSDAY, APRIL 14, 2005 FULL DAY (9:00 A.M.–5:00 P.M.)

R1	David Rhoades	Hacking & Securing Web-based Applications
R2	Richard Bejtlich	***New!*** Network Security Monitoring with Open Source Tools
R3	Mark Burgess	***New!*** Configuration Management with Cfengine
R4	Steve Acheson and Laura Kuiper	***New!*** Cisco Device Configuration Basics—Live!
R5	John Sellens	***New!*** Databases: What You Need to Know

S1 Hands-on Linux Security Class: Learn How to Defend Linux/UNIX Systems by Learning to Think Like a Hacker *(Day 1 of 2)*

Rik Farrow, *Security Consultant*

9:00 a.m.–5:00 p.m.

Who should attend: System administrators of Linux and other UNIX systems; anyone who runs a public UNIX server.

Few people enjoy learning how to swim by being tossed into the ocean, but that's what happens if a system you manage gets hacked. You often have little choice other than to reload that system, patch it, and get it running again. This two-day class gives you a chance to work with systems that have been "hacked," letting you search for hidden files or services or other evidence of the intrusion. Examples are taken from real, recent attacks on Linux systems. You will perform hands-on exercises with dual-use tools to replicate what intruders do as well as with tools dedicated to security. The tools vary from the ordinary, such as find and strings, to less familiar but very important ones, such as lsof, scanners, sniffers, and the Sleuth Kit.

The lecture portion of this class covers the background you need to understand UNIX security principles, TCP/IP, scanning, and popular attack strategies.

Day Two will explore the defenses for networks and individual systems. The class will end with a discussion of the use of patching tools for Linux, including cfengine.

Class exercises will require that you have an x86-based laptop computer that can be booted from a KNOPPIX CD. Students will receive a version of Linux on CD that includes the tools, files, and exercises used in the course. Please download a copy of KNOPPIX (http://www.knoppix.org), burn it, and try it out.

Exercises include:

Day One:

- Finding hidden files and evidence of intrusion
- TCP/IP and its abuses
- hping2 probes, or xprobe with ethereal again
- nmap while watching with ethereal or tcpdump (connect and SYN scans)
- Working with buffer-overflow exploit examples
- Apache servers and finding bugs in scripts
- John the Ripper, password cracking

For the description of Day 2, see p. 8.

S2 Bridges, Routers, Switches, and Internetworking Protocols

Radia Perlman, *Sun Microsystems*

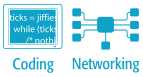
9:00 a.m.–5:00 p.m.

Who should attend: Anyone who might need to design a protocol, implement a protocol, write network-based applications, or plan or manage a network. Anyone who is just curious about what is really going on under the covers in a network, and how things got the way they are. Anyone with the courage to see things from different angles, and not just parrot orthodoxy. Paradoxically, this tutorial is good as an introduction to people who are incredibly confused by all the terms and don't know where to start, as well as people who have been using this stuff for years, assumed they understood it, and want to see how all the pieces fit.

The concepts of IP addresses, masks, MAC addresses, routing algorithms, domains, switches, bridges, are pervasive when dealing with networks. We all use these terms, and configure these things, but what is really going on? What are the implications of choosing a switch vs. a router? What kinds of things can go wrong in a protocol that is misdesigned, misimplemented, or mismanaged? This tutorial describes the major protocols involved in the network infrastructure. It describes conceptually what goes on in the packet switches (both layer 2/bridges and layer 3/routers), as well as the implications on endnodes. It contrasts connection-oriented approaches such as ATM and MPLS with connectionless approaches such as IPv4 and IPv6. It covers the endnode-visible pieces of layer 3, such as neighbor-discovery and address autoconfiguration. It covers intradomain routing algorithms (distance vector such as RIP and link state such as OSPF or IS-IS) and interdomain (BGP). It describes the spanning tree algorithm used by bridges/switches.

Topics include:

- Layer 2 (MAC) addresses
  - Why 6 bytes?
  - Relation to layer 3 addresses (IP)
- Bridges
  - Basic idea
  - Why it's more powerful than a repeater
  - Station address learning and forwarding
  - Spanning tree
- What are switches? "switched Ethernet"
- Connection-oriented networks: ATM, MPLS
- Connectionless protocols: IPv4, IPv6, and comparison with others
- Neighbor discovery (ARP, DHCP)
- Routing (distance vector vs link state, interdomain vs intradomain)
- IP Multicast
- NAT



S3 *New!* Hot Topics in System Administration

Ned McClain,
Applied Trust Engineering

9:00 a.m.–5:00 p.m.

Who should attend: System and network administrators who are interested in picking up several new technologies quickly.

From a stand-alone client attached to the Internet to a distributed network of Web servers, systems administrators are being tasked with bringing their office environments online. The network services that need to be configured in order to do this can be daunting to administrators who aren't familiar with the required applications. Configuration examples as well as overviews of the underlying protocols will give attendees the tools to implement services on their own systems. The following areas will be covered (with a special emphasis on security):

Topics include:

- BIND9 Tips and Tricks: A Better DNS
  Learn about powerful new functionality such as split views, remote management, and even DNSSEC. This topic is a must for every modern administrator.
- Rapid Linux Disaster Recovery
  We evaluate Mondo, an open source disaster recovery tool that can create bootable recovery CDs from any Linux server. When used in tandem with a solid tape backup system, Mondo recovery CDs can reduce "bare metal" recovery time from hours to minutes.
- Linux Kernel Tuning
  Whether it's performance, security, or functionality you're looking to cajole your system into, we'll give you the "what to's" and the "how to's," and even the "what you can'ts" of this rare art.
- Practical Integration of UNIX and Active Directory
  We'll not only explore the standard integration tools, such as OpenLDAP, PAM, and NSS, but will show you how to create custom scripts to manage Active Directory from UNIX.
- Performance Crises Case Studies #4
  Don't miss the latest episode of this incredibly popular segment! We've taken a new set of real-life system administration performance crises and dissected them, providing insight on how to diagnose and remedy situations that you may someday face. This is a great way to gain practical knowledge in the performance arena.
- Custom Open Source Performance Monitoring
  We provide practical examples of extending a monitoring system to collect historical performance trends. We'll use examples specific to Nagios and RRDtool, but the lessons and gotchas discussed here will prove useful to anyone looking to implement a new monitoring system.

S4 Regular Expression Mastery

Mark-Jason Dominus,
Consultant and Author
9:00 a.m.–12:30 p.m.

Who should attend: System administrators and users who use Perl, grep, sed, awk, procmail, vi, or emacs. Attendees should have prior experience using regexes in UNIX utilities such as grep, sed, Perl, Python, vi, or emacs.

Have you ever written a regex that produced unexpected results? Do your regexes ever appear to hang forever? Can't figure out why they behave differently in different utilities for no apparent reason? Then this is the class for you.

The first section of the class will explore the matching algorithms used internally by common utilities such as grep and Perl. Understanding these algorithms will allow us to predict whether a regex will match, which of several matches will be found, and which regexes are likely to be faster than others, and to understand why all of these behaviors occur. We'll learn why commonly used regex symbols such as ".", "$", and "\1" may not mean what you thought they did.

In the second section, we'll look at common matching disasters, a few practical parsing applications, and some advanced Perl features. We'll finish with a discussion of optimizations that were added to Perl 5.6, and why you should avoid using "/i".

Topics include:

- Inside the regex engine
  - Regular expressions are programs
  - Backtracking
  - NFA vs. DFA
  - POSIX and Perl
  - Quantifiers
  - Greed and anti-greed
  - Anchors and assertions
  - Backreferences
- Disasters and optimizations
  - Where machines come from
  - Disaster examples
  - Tokenizing
  - New optimizations
  - Matching strings with balanced parentheses

Coding Sysadmin

S5 *New!* Eliminating Backup System Bottlenecks Using Disk-to-Disk and Other Methods

Jacob Farmer, *Cambridge Computer Services*
9:00 a.m.–12:30 p.m.

Who should attend: System administrators and policy-makers responsible for protecting their organization's data. A general familiarity with server and storage hardware is assumed. The class focuses on architectures and core technologies and is relevant regardless of what backup hardware and software you currently use. Students will leave this lecture with immediate ideas for effective, inexpensive improvements to their backup systems.

Topics include:

- Identifying and eliminating backup system bottlenecks
- Conventional disk staging
- Virtual tape libraries
- "Incremental forever" and "synthetic full" backup strategies
- Information life cycle management, nearline archiving
- Data replication
- Continuous backup
- Snapshots
- The current and future tape drives
- Zero duplication file systems
- iSCSI


Sysadmin

S6 *New!* Kerberos 5—Revenge of the Three-Headed Dog

Gerald Carter, *Samba Team/HP*
9:00 a.m.–12:30 p.m.

Who should attend: Administrators who want to understand Kerberos 5 implementations on both UNIX/Linux and Windows clients and servers.

Kerberos is an an old technology that has been driven to the forefront by deployments of Microsoft Active Directory domains. The introduction of a standard authentication protocol into Windows domains has caused many network administrators to reexamine ways to integrate UNIX/Linux and Windows clients in a single authentication model.

Topics include:

- Key concepts of the Kerberos 5 protocol
- Related authentication interfaces (e.g., SASL, GSSAPI)
- The specifics of implementing of Krb5 realms
- Implementations of Krb5 cross-realm trusts
- Integrating Windows and UNIX/Linux clients into Krb5 realms
- Possible pitfalls of using popular Krb5 implementations such as MIT, Heimdal, and Windows 200x


Networking Security

S7 *New!* Advanced Shell Programming

Mike Ciavarella,
University of Melbourne
9:00 a.m.–12:30 p.m.

Who should attend: Junior or intermediate system administrators or anyone with a basic knowledge of programming, preferably with some experience in Bourne/Korn shells (or their derivatives).

The humble shell script is still a mainstay of UNIX/Linux system administration, despite the wide availability of other scripting languages. This tutorial details techniques that move beyond the quick-and-dirty shell script.

Topics include:

- Common mistakes and unsafe practices
- Modular shell script programming
- Building blocks: awk, sed, etc.
- Writing secure shell scripts
- Performance tuning
- Choosing the right utilities for the job
- Addressing portability at the design stage
- When not to use shell scripts

Coding Sysadmin

S8 *New!* Next-Generation Security Tools

Peter Baer Galvin,
Corporate Technologies
9:00 a.m.–12:30 p.m.

Who should attend: Systems managers and security managers interested in current security problems and the new generation of tools designed to solve those problems.

Are you looking for the latest security solutions for your installations? This course begins by reviewing the nasty world of current security threats and the many problems sites have to fix. It then talks about what is solvable and what still has no solution. Finally, it covers each of the possible solutions in detail. (Note: Most of these solutions are commercial products.)

Topics include:

- A security methodology
- Firewalls: Why don't they work?
- Protecting Web servers
- Reducing spam
- Patch management and avoiding patching
- Network snooping
- Gaining status knowledge of your facility
- Content filtering and antivirus software
- Weak and strong authentication
- Spyware and peer-to-peer networks


Security

S9 Perl Program Repair Shop and Red Flags

Mark-Jason Dominus,
Consultant and Author
1:30 p.m.–5:00 p.m.

Who should attend: Anyone who writes Perl programs regularly. Participants should have at least three months' experience programming in Perl.

Write better code, faster. This class will show you how to improve your own code and the code of others, making it cleaner, more readable, more reusable, and more efficient, while at the same time making it 30–50% smaller. Smaller code contains fewer bugs and takes less time to maintain.

We will examine several real code examples in detail and see how to improve them. We'll focus on red flags–warning signs in your code that are plainly visible once ou know what to look for–and on techniques that require little complex thought or ingenuity. All the bad code in this class is guaranteed 100% genuine and typical. Participants are encouraged to submit their own code for anonymous review in the class. (Email submissions to mjd-usenix-2005@plover.com by March 1.)

Topics include:

- Families of variables
- Making relationships explicit
- Refactoring
- Programming by convention
- Conciseness
- Why you should avoid the "." operator
- Elimination of global variables
- Superstition
- The "use strict" zombies
- The cardinal rule of computer programming
- The psychology of repeated code
- Techniques for eliminating repeated code
- What can go wrong with "if" and "else"
- The Condition That Ate Michigan
- Resisting "Holy Doctrine"
- Trying it both ways
- Structural vs. functional code
- Elimination of structure
- Boolean values
- Programs that take two steps forward and one step back
- Programs that are 10% backslashes
- 'print print print print print '
- C-style "for" loops
- Loop counter variables
- Array length variables
- Unnecessary shell calls
- How (and why) to let "undef" be the special value
- Confusing internal and external representations of data
- Tool use
- Eliminating repeated code with higher-order functions
- The "swswsw" problem
- Avoiding special cases
- Using uniform data representations

Coding

S10 *New!* Next-Generation Storage Networking and Data Protection

Jacob Farmer, *Cambridge Computer Services*
1:30 p.m.–5:00 p.m.

Who should attend: Sysadmins running day-to-day operations and those who set or enforce budgets. This lecture is technical in nature, but it does not address command-line syntax or the operation of specific products or technologies. Rather, the focus is on general architectures and various approaches to scaling in both performance and capacity. Since storage technologies tend to be expensive, there is some discussion of the relative cost of different technologies and of strategies for managing cost and achieving results on a limited budget.

There has been tremendous innovation in the data storage industry in the past few years, and this year the pace has quickened. Proprietary monolithic SAN and NAS subsystems are giving way to open-system and distributed architectures. Data-transfer protocols such as SCSI, NFS, and CIFS are facing competition from VI and DAFS. Fibre-channel and parallel SCSI interfaces are challenged by Gigabit Ethernet, iSCSI, and serial ATA. Bottlenecks imposed by I/O buses and stacks stand to be eliminated by Infiniband and RDMA.

This tutorial describes the latest technologies to hit the market for storage networking: SAN and NAS architectures, virtual storage, parallel file systems, storage interfaces, etc.

Topics include:

- Fundamentals of storage networking
- Shortcomings of conventional SAN and NAS architectures
- Comparison of storage interfaces: fibre channel, SCSI, serial ATA, Infiniband, Ethernet
- Comparison of storage protocols: CIFS, NFS, SCSI, VI, DAFS
- Open systems storage virtualization
- The convergence of SAN and NAS
- High-performance file sharing (NAS on steroids)
- SAN-enabled file systems
- Wide-area file systems
- Parallel file systems
- Content-addressable storage


Networking Sysadmin

S11 *New!* Over the Edge System Administration, Volume 1

David N. Blank-Edelman,
Northeastern University
1:30 p.m.–5:00 p.m.

Who should attend: Old-timers who think they've already seen it all, and those who want to develop inventive thinking early in their career. Join us and be prepared to be delighted, disgusted, and amazed. Most of all, be ready to enrich your network and system adminstration by learning to be different.

Can you think "out of the box" about system administration? One of the things that distinguishes the really great sysadmins from the good ones is their ability to be creative in their approach to problems and solutions. It's time to learn how to break the rules, abuse the tools, and generally turn your system administration knowledge inside out. This class is a cornucopia of ideas for creative ways to take the standard (and sometimes not-so-standard) system administration tools and techniques and use them in ways no one would expect. We'll also cover some tools you may have missed.

Topics include:

- How to (ab)use perfectly good network transports by using them for purposes never dreamed of by their authors
- How to increase user satisfaction during downtimes with 6 lines of Perl
- How to improve your network services by intentionally throwing away data
- How to drive annoying Web-only applications that don't have a command line interface–without lifting a finger
- How to use ordinary objects you have lying around the house, such as Silly Putty, to make your life easier (seriously!)


Sysadmin

S12 *New!* Documentation Techniques for SysAdmins

Mike Ciavarella,
University of Melbourne
1:30 p.m.–5:00 p.m.

Who should attend: System administrators who need to produce documention for the systems they manage or who want to improve their documentation skills.

Attendees should leave this tutorial with the ability to make immediate, practical use of the techniques presented in this tutorial in their day-to-day tasks. Particular emphasis is placed on documentation as a time-saving tool rather than a workload imposition.

Topics include:

- Why system administrators need to document
- The document life cycle
- Targeting your audience
- An adaptable document framework
- Common mistakes
- Tools to assist the documentation process


Sysadmin

S13 *New!* Troubleshooting: A Basic Skill

Geoff Halprin, *The SysAdmin Group*
1:30 p.m.–5:00 p.m.

Who should attend: System administrators wishing to hone their ability to troubleshoot a problem under pressure, on a system of which their knowledge may be limited.

One of the most basic skills a system administrator must be able to call upon is that of problem diagnosis and resolution, that is, troubleshooting. It doesn't matter what else you do; if the system is broken, your priority is to fix it.

Topics include:

- A general process for troubleshooting
- Specific techniques that will help you get to the root of the problem
- Ways to identify candidate solutions with confidence


Sysadmin

Hands-on Training at USENIX '05

In addition to our excellent slate of lecture and seminar-based tutorials, USENIX '05 also offers you the chance to get up close and personal with the code through hands-on tutorials.

Tutorials presented in this format include:

- S1, M1: Hands-on Linux Security Class: Learn How to Defend Linux/UNIX Systems by Learning to Think Like a Hacker
- T1, W1: Network Security Assessments Workshop–Hands-on

These sessions require you to bring your own laptop–please see the detailed course descriptions for complete information on system requirements.

Training Program Registration

Every USENIX '05 training program registration includes:

- Admission to the tutorials you select
- Lunch on the day of your tutorial
- Training program CD-ROM, including all available tutorial presentations and materials
- Printed tutorial materials for your courses
- Admission to the Conference Reception
- Conference T-shirt
- Wireless connectivity in conference session area
- Optional discount on a one-year subscription to *Dr. Dobb's Journal*

Our Guarantee

If you're not happy, we're not happy. If you feel a tutorial does not meet the high standards you have come to expect from USENIX, let us know by the first break and we will change you to any other available tutorial immediately.

Continuing Education Units (CEUs)

USENIX provides Continuing Education Units for a small additional administrative fee. The CEU is a nationally recognized standard unit of measurement for continuing education and training and is used by thousands of organizations.

Each full-day tutorial qualifies for 0.6 CEUs. You can request CEU credit by completing the CEU section on the registration form. USENIX provides a certificate for each attendee taking a tutorial for CEU credit and maintains transcripts for all CEU students.

CEUs are not the same as college credit. Consult your employer or school to determine their applicability.

M1 Hands-on Linux Security Class: Learn How to Defend Linux/UNIX Systems by Learning to Think Like a Hacker *(Day 2 of 2)*

Rik Farrow, *Security Consultant*
9:00 a.m.–5:00 p.m.

Day two of this class focuses on practical forensics, that is, how to analyze a possibly hacked Linux or UNIX system from a system administrator's perspective. As a system administrator, you will not be acting as law enforcement, trying to find the perpetrator, but instead will be working as quickly as possible with the goal of uncovering what went wrong. Finding rootkits and backdoors on a sample hacked system gives you an idea of what you might find on other similar systems. You can also get clues about the nature of the attack by discovering the tools left behind on a system by an attacker.

The final portion of this class focuses on patching, with a discussion of cfengine. As this is the second day of a two-day, hands-on course, we will not repeat material covered on the first day (including getting the CD working with your laptop). If you plan on attending the course only the second day, you might want to contact the instructor before the class and get a test CD to ensure that your laptop will work in the classroom environment.

Exercises include:

Day Two:

- Elevation of privilege and suid shells
- Rootkits, and finding rootkits (chkrootkit)
- Sleuth Kit (looking at intrusion timelines)
- iptables and netfilter
- Tracking down DoS floods
- Cfengine configuration
- Vulnerability scanning with nessus

For the description of Day 1, see p. 4.

M2 Network Security Protocols: Theory and Current Standards

Radia Perlman, *Sun Microsystems,*
and Charlie Kaufman, *Microsoft*
9:00 a.m.–5:00 p.m.

Who should attend: Anyone who wants to understand the theory behind network security protocol design, with an overview of the alphabet soup of standards and cryptography. This tutorial is especially useful for anyone who needs to design or implement a network security solution, but it is also useful to anyone who needs to understand existing offerings in order to deploy and manage them. Although the tutorial is technically deep, no background other than intellectual curiosity and a good night's sleep in the recent past is required.

First, without worrying about the details of particular standards, we discuss the pieces out of which all these protocols are built.

We then cover subtle design issues, such as how secure email interacts with distribution lists, how designs maximize security in the face of export laws, and the kinds of mistakes people generally make when designing protocols.

Armed with this conceptual knowledge of the toolkit of tricks, we describe and critique current standards.

Topics include:

- What problems are we trying to solve?
- Cryptography
- Key distribution
  - Trust hierarchies
  - Public key (PKI) vs. secret key solutions
  - Handshake issues
  - Diffie-Hellman
  - Man-in-middle defense
  - Perfect forward secrecy
  - Reflection attacks
- PKI standards
  - X.509
  - PKIX
- Real-time protocols
  - SSL/TLS
  - IPsec (including AH, ESP, and IKE)
- Secure email
- Web security
  - URLs
  - HTTP, HTTPs
  - Cookies

M3 Advanced Solaris System Administration Topics

Peter Baer Galvin,
Corporate Technologies, Inc.
9:00 a.m.–5:00 p.m.

Who should attend: UNIX administrators who need more knowledge of Solaris administration, especially the next-generation features of Solaris 10.

We will discuss the major new features of recent Solaris releases, including which to use (and how) and which to avoid. This in-depth course will provide the information you need to run a Solaris installation effectively. This tutorial has been updated to include Solaris 10 and several other new topics.

Topics include:

- Installing and upgrading
  - Planning your installation, filesystem layout, post-installation steps
  - Installing (and removing) patches and packages
- Advanced features of Solaris
  - Filesystems and their uses
  - The /proc filesystem and commands
  - ZFS
- The Kernel
  - Kernel and performance tuning: new features, adding devices, tuning, debugging commands
  - DTrace
- Enhancing Solaris
  - Virtual IP: configuration and uses
  - Performance: how to track down and resolve bottlenecks
  - Tools: useful free tools, tool use strategies
  - Security: locking down Solaris, system modifications, tools, zones, privileges
  - Resource management: fair share scheduler
  - Resources and references

M4 Perl for System Administration: The Power and the Praxis

David N. Blank-Edelman,
Northeastern University
9:00 a.m.–5:00 p.m.

Who should attend: System and network administrators with at least advanced-beginner to intermediate Perl skills, who would like to make their jobs easier and less stressful in times of sysadmin crisis.

Perl was originally created to help with system administration, so it is a wonder there isn't more instructional material available to help people in our field use Perl to their advantage. This tutorial hopes to begin to remedy this situation by presenting six solid hours of instruction on using Perl for system administration.

The morning section, based on the instructor's O'Reilly book, will concentrate on the power of Perl for sysadmin tasks. This jam-packed survey will take a multi-platform look at using Perl in cutting-edge and old-standby system administration domains.

Topics include:

- Secure Perl scripting
- Dealing with files and filesystems
  - Source control
  - XML
  - Databases
  - Log files
- Dealing with SQL databases via DBI and ODBC
- Email as a sysadmin tool (including spam analysis)
- Network directory services: NIS, DNS, LDAP, ADSI
- Network management: SNMP and WBEM

In the afternoon, we'll look at ways to use short Perl programs to solve time-critical sysadmin problems. Focusing on a set of battle stories, we'll discuss various approaches to dealing with crises with the help of Perl.

You'll walk away from this class with Perl approaches and techniques that can help you solve your daily system administration problems. You'll have new ideas for writing small Perl programs to get you out of big sysadmin pinches. On top of all this, you are likely to have deepened your knowledge of Perl.

Coding


Sysadmin

M5 Inside the Linux Kernel (Updated for Version 2.6)

Theodore Ts'o, *IBM*
9:00 a.m.–5:00 p.m.

Who should attend: Application programmers and kernel developers. You should be reasonably familiar with C programming in the UNIX environment, but no prior experience with the UNIX or Linux kernel code is assumed.

This tutorial will give you an introduction to the structure of the Linux kernel, the basic features it provides, and the most important algorithms it employs.

The Linux kernel aims to achieve conformance with existing standards and compatibility with existing operating systems; however, it is not a reworking of existing UNIX kernel code. The Linux kernel was written from scratch to provide both standard and novel features, and it takes advantage of the best practice of existing UNIX kernel designs.

Although the material will focus on the latest release version of the Linux kernel (v. 2.6), it will also address aspects of the development kernel codebase (v. 2.7) where its substance differs from 2.6. It will not contain any detailed examination of the source code but will, rather, offer an overview and roadmap of the kernel's design and functionality.

Topics include:

- How the kernel is organized (scheduler, virtual memory system, filesystem layers, device driver layers, networking stacks)
  - The interface between each module and the rest of the kernel
  - Kernel support functions and algorithms used by each module
  - How modules provide for multiple implementations of similar functionality
- Ground rules of kernel programming (races, deadlock conditions)
- Implementation and properties of the most important algorithms
  - Portability
  - Performance
  - Functionality
- Comparison between Linux and UNIX kernels, with emphasis on differences in algorithms
- Details of the Linux scheduler
  - Its VM system
  - The ext2fs filesystem
- The requirements for portability between architectures

Coding


Open Source

M6 *New!* VoIP Principles and Practice

Heison Chak, *SOMA Networks*
9:00 a.m.–5:00 p.m.

Who should attend: Managers and system administrators involved in the evaluation, design, implementation, and deployment of VoIP infrastructures. Participants do not need prior exposure to VoIP but should be familiar with network principles. Attendees will come away from this tutorial with a foundation in VoIP, enabling strategic and cost-effective VoIP deployments in a varierty of environments.

This tutorial will cover VoIP principles and their interaction and interface with the PSTN and IP networks. While CODECs, protocols, quality, and some IETF standards are being discussed, this tutorial is also filled with practical examples. Asterisk, which is open-source PBX software, will be used to demonstrate some of the unique features of VoIP.

Topics include:

- Toll bypass
- Interactive Voice Response System
- Text-to-speech applications
- Analog telephone adapter provisioning
- Call detail recording and blacklisting
- Echo training


Networking

Our Guarantee: If you're not happy, we're not happy. If you feel a tutorial does not meet the high standards you have come to expect from USENIX, let us know by the first break and we will change you to any other available tutorial immediately.

Continuing Education Units (CEUs): USENIX provides Continuing Education Units for a small additional administrative fee. The CEU is a nationally recognized standard unit of measurement for continuing education and training and is used by thousands of organizations.

Each full-day tutorial qualifies for 0.6 CEUs. You can request CEU credit by completing the CEU section on the registration form. USENIX provides a certificate for each attendee taking a tutorial for CEU credit and maintains transcripts for all CEU students.

CEUs are not the same as college credit. Consult your employer or school to determine their applicability.

M7 Seven Habits of the Highly Effective System Administrator

Mike Ciavarella, *University of Melbourne,* **and Lee Damon,** *University of Washington*

9:00 a.m.–5:00 p.m.

Who should attend: Junior system administrators with anywhere from little to 3+ years of experience in computer system administration. We will focus on enabling the junior system administrator to "do it right the first time." Some topics will use UNIX-specific tools as examples, but the class is applicable to any sysadmin and any OS. Most of the material covered is "the other 90%" of system administration—things every sysadmin needs to do and to know, but which aren't details of specific technical implementation.

We aim to accelerate the experience curve for junior system administrators by teaching them the time-honored tricks (and effective coping strategies) that experienced administrators take for granted and which are necessary for successful growth of both the administrator and the site.

The class covers many of the best practices that senior administrators have long incorporated into their work. We will touch on tools you should use, as well as tools you should try to avoid. We will touch on things that come up frequently, as well as those which happen only once or twice a year. We will look at a basic security approach.

Topics include:

- Why your computers should all agree on what time it is
- Why root passwords should not be the same on every computer
- Why backing up every filesystem on every computer is not always a good idea
- Policies: where you want them and where you might want to avoid them
- Ethical issues
- Growth and success as a solo sysadmin and as part of small, medium, and large teams
- Training, mentoring, and personal growth planning
- Site planning, budgeting, and logistics
- Books that can help you and your users

Sysadmin

M8 System Log Aggregation, Statistics, and Analysis

Marcus Ranum, *Tenable Security, Inc.*

9:00 a.m.–5:00 p.m.

Who should attend: System and network administrators who are interested in learning what's going on in their firewalls, servers, network, and systems; anyone responsible for security and audit or forensic analysis.

This tutorial covers techniques and software tools for building your own log analysis system, from aggregating all your data in a single place, through normalizing it, searching, and summarizing, to generating statistics and alerts and warehousing it. We will focus primarily on open source tools for the UNIX environment, but will also describe tools for dealing with Windows systems and various devices such as routers and firewalls.

Topics include:

- Estimating log quantities and log system requirements
- Syslog: mediocre but pervasive logging protocol
- Back-hauling your logs
- Building a central loghost
- Dealing with Windows logs
- Logging on Windows loghosts
- Parsing and normalizing
- Finding needles in haystacks: searching logs
- I'm dumb, but it works: artificial ignorance
- Bayesian spam filters for logging
- Storage and rotation
- Databases and logs
- Leveraging the human eyeball: graphing log data
- Alerting
- Legalities of logs as evidence

Networking Sysadmin

T1 Network Security Assessments Workshop—Hands-On *(Day 1 of 2)*

David Rhoades,
Maven Security Consulting, Inc.
9:00 a.m.–5:00 p.m.

Who should attend: Anyone who needs to understand how to perform an effective and safe network assessment.

How do you test a network for security vulnerabilities? Just plug some IP addresses into a network-scanning tool and click SCAN, right? Not quite. Numerous commercial and freeware tools assist in locating network-level security vulnerabilities. However, these tools are fraught with dangers. Performing a security assessment (a.k.a. vulnerability assessment or penetration test) against a network environment requires preparation, the right tools, methodology, knowledge, and more. This hands-on workshop will cover the essential topics for performing an effective and safe network assessment.

Class exercises will require that students have an x86-based notebook computer with a CD-ROM drive and a 10/100 Ethernet network card. Students must follow the instructions at http://www.mavensecurity.com/bootdisk prior to attending the workshop. All software provided will be publicly available freeware.

Students will perform selected steps of a general network assessment against a target network consisting of several Windows and UNIX-based servers, as well as various routing components.

Topics include:

Day One:

- Lab setup and preparation
- Security assessment overview
- Assessment preparation
- Assessment safety
- Documentation and audit trail
- Assessment phase 1: network inventory

For the description of Day 2, see p. 14.


Networking Security

T2 *New!* Solaris Kernel Performance, Observability, and Debugging *(Day 1 of 2)*

James Mauro and Richard McDougall, *Sun Microsystems*
9:00 a.m.–5:00 p.m.

Who should attend: System and database administrators, software architects, developers and programmers, performance and systems analysts, and IT architects wanting to obtain a deeper understanding of the key Solaris subsystems, as well as the tools and facilities that can be used to:

- Observe, trace, and debug to optimize performance
- Observe, trace and debug to root-cause aberrant behavior
- Observe and trace to understand how the application workload interacts with the operating system
- Better understand the system as a whole

Attendees should have some basic understanding of operating system principles and application performance analysis. Students choosing to attend only Day Two should be familiar with Solaris kernel subsystems and have at least rudimentary knowledge of the bundled tools and utilities and their use.

Applications are becoming more complex every day, and many of the new Solaris features significantly reduce the effort required to administer and anazlyze performance of the entire application and operating system stack.

You may take this class as either a one-day experts class or a two-day complete class. On Day One, we provide an architectual overview of the major Solaris subsystems and an introduction to Solaris performance analysis. On Day Two, we cover advanced topics and spend significant time with hands-on case studies, using the latest tools, including dtrace, mdb, memtool, mdb, trapstat, and the Solaris process "ptools."

Topics include:

Day One:

- Solaris overview with performance monitoring and tuning
- Memory
- Process management & scheduling
- Filesystems
- Networking and I/O

For the description of Day 2, see p. 14.

Coding Sysadmin

T3 *New!* Solaris 10 Security Features Workshop

Peter Baer Galvin,
Corporate Technologies, Inc.
9:00 a.m.–5:00 p.m.

Who should attend: Solaris systems managers and administrators interested in the new security features in Solaris 10 (and features in previous Solaris releases that they may not be using).

This course covers a variety of topics surrounding Solaris 10 and security. Solaris 10 includes many new features, and there are new issues to consider when deploying, implementing, and managing Solaris 10. This will be a workshop featuring instruction and practice/exploration. Each student should have a laptop with wireless access for remote access into a Solaris 10 machine.

Topics include:

- Solaris cryptographic framework
- NFSv4
- Solaris privileges
- Solaris Flash archives and live upgrade
- Moving from NIS to LDAP
- Dtrace
- WBEM
- Smartcard interfaces and APIs
- Kerberos enhancements
- Zones
- FTP client and server enhancements
- PAM enhancements
- Auditing enhancements
- Password history checking
- ipfilters


Security Sysadmin

T4 Advanced Perl Programming

Tom Christiansen,
Consultant
9:00 a.m.–5:00 p.m.

Who should attend: Anyone with a journeyman-level knowledge of Perl programming who wants to hone Perl skills. This class will cover a wide variety of advanced topics in Perl, including many insights and tricks for using these features effectively. After completing this class, attendees will have a much richer understanding of Perl and will be better able to make it part of their daily routine.

Topics include:

- Symbol tables and typeglobs
- Modules
- References
  - Implications of reference counting
  - Using weak references for self-referential data structures
  - Autovivification
  - Data structure management, including serialization and persistence
  - Closures
- Fancy object-oriented programming
  - Using closures and other peculiar referents as objects
  - Overloading of operators, literals, and more
  - Tied objects
- Managing exceptions and warnings
  - When die and eval are too primitive for your taste
  - The use warnings pragma
  - Creating your own warnings classes for modules and objects
- Regular expressions
  - Debugging regexes
  - qr// operator
  - Backtracking avoidance
  - Interpolation subtleties
  - Embedding code in regexes
- Programming with multiple processes or threads
  - The thread model
  - The fork model
  - Shared memory controls
- Unicode and I/O layers
  - Unicode named characters and combined characters
  - Accessing Unicode properties
  - I/O layers for encoding translation
  - Upgrading legacy text files to Unicode
  - Unicode display tips
- What's new in Perl lately
  - Switch statement
  - Defined-or operators
  - Pre-compiled modules
  - Dynamic handles
  - Virtual I/O through strings

Coding

T5 *New!* RPM Package Management

Joshua Jensen, *IBM*
9:00 a.m.–5:00 p.m.

Who should attend: System administrators deploying, or interested in deploying, RPM-based Linux systems in a production environment. Attendees should be familiar with the basics of system administration in a UNIX/Linux environment, user-level commands, and TCP/IP networking. Novice administrators and gurus alike should leave the tutorial having learned something.

Whether your environment is a single server or a network with thousands of desktops, workstations, and servers, Linux application deployment, upgrades, and errata policy can be effectively managed with RPM packages. From simple command-line queries to source build environments, from networked package management solutions such as Novell's Zenworks for Linux and Red Hat's RHN to the simple but effective Yum, this course emphasizes real-world solutions, covering everything you need to know to use, create, and manage RPM packages and systems.

Topics include:

- Introduction to RPM: What's a package and what isn't
- Working with RPMs: Basic functionality explored
- Advanced RPM use: Auto dependency aid, rollback, and more
- Building RPMs: Source RPMs, spec files, RPM macros
- Special considerations for dual architecture systems
- Advanced functionality: Triggers and pre/post scripting
- RPM security: Build signing and pre-installation verification
- Package management systems: APT, RHN, RCE/Zenworks, Yum


Open Source Sysadmin

T6 Managing Samba 3.0

Gerald Carter,
Samba Team/Hewlett-Packard
9:00 a.m.–5:00 p.m.

Who should attend: System administrators who are currently managing Samba servers or are planning to deploy new servers this year. This course will outline the new features of Samba 3.0, including working demonstrations throughout the course session.

Topics include:

- Providing basic file and print services
- Centrally managing printer drivers for Windows clients
- Configure Samba's support for Access Control Lists and the Microsoft Distributed File System
- Making use of Samba VFS modules for features such as virus scanning and a network recycle bin
- Integrating with Windows NT 4.0 and Active Directory authentication services
- Implementing a Samba primary domain controller along with Samba backup domain controllers
- Migrating from a Windows NT 4.0 domain to a Samba domain
- Utilizing account storage alternatives to smbpasswd such as LDAP


Networking Open Source Sysadmin

Please see **http://www.usenix.org/usenix05/training** for full tutorial descriptions and program updates.

T7 Practical System and Network Monitoring

John Sellens, *SYONEX*
9:00 a.m.–5:00 p.m.

Who should attend: Network and system administrators interested in real-life, practical, host- and network-based monitoring of their systems and networks. Participants should have an understanding of the fundamentals of networking, basic familiarity with computing and network components, and some familiarity with UNIX and scripting languages.

Participants will leave this tutorial able to immediately start using a number of monitoring systems and techniques that will improve their ability to manage and maintain their systems and networks.

Topics include:

- Monitoring: goals, techniques, reporting
- SNMP: the protocol, reference materials, relevant RFCs
- Introduction to SNMP MIBs (Management Information Bases)
- SNMP tools and libraries
- Other (non-SNMP) tools
- Security concerns when using SNMP and other tools on the network
- Monitoring applications: introductions, use, benefits and complications, installation and configuration (Big Brother, Nagios, SNIPS, MRTG, Cricket, etc.)
- Special situations: remote locations, firewalls, etc.
- Monitoring implementation roadmap: policies, practices, notifications, escalations, reporting

T8 *New!* Release Engineering and Project Lifecycle

Geoff Halprin, *The Sysadmin Group,*
and Lee Damon, *University of Washington*
9:00 a.m.–5:00 p.m.

Who should attend: Software developers, system administrators, and managers who deal with internal or external project/product lifecycles and quality.

We will look at projects varying in scope from "Here's a new product we just bought; roll it out," through "We need an internal _foo_ server; make it happen," to "Here's this new thing we are developing; let's do it right so we can ship it." We will cover matters from quick projects to "This will take a year and 20 people to deploy."

The focus of this class will be on internally developed projects for internal use with some extrapolation to sold or shipped products. Large and small projects alike can benefit from proper planning and roll-outs. We will prove that the old adage, "There is never time to do it right, but there is always time to do it over," is never a good answer or a good philosophy. We will also examine the phenomenon of "Shoot the engineer and ship the product" in light of the reality most of us face: "The first 90% of the project takes 10% of the time; the remaining 10% takes 90% of the time."

This is not intended to replace formal training for project planners. It is intended to make life better for people who deal with projects on a day-to-day basis. We will provide you with the ideas and some of the tools to take your projects from "We need this quick" to a supportable and released project–or even product.

Topics include:

- Test planning and implementation
- Project release planning
- Project lifecycles
- Replacement planning and updating

"[USENIX has] very useful tutorials—they're well worth it and will help me do my job better."

—Steve McEntyre, *Plasmon Data*

"USENIX Annual Tech has always been a place to stay current on the interesting work that interesting people are doing."

—Eric Allman, *original author of Sendmail and CTO of Sendmail, Inc.*

W1 Network Security Assessments Workshop—Hands-On *(Day 2 of 2)*

David Rhoades,
Maven Security Consulting, Inc.
9:00 a.m.–5:00 p.m.

Who should attend: Anyone who needs to understand how to perform an effective and safe network assessment.

How do you test a network for security vulnerabilities? Just plug some IP addresses into a network-scanning tool and click SCAN, right? Not quite. Numerous commercial and freeware tools assist in locating network-level security vulnerabilities. However, these tools are fraught with dangers. Performing a security assessment (a.k.a. vulnerability assessment or penetration test) against a network environment requires preparation, the right tools, methodology, knowledge, and more. This hands-on workshop will cover the essential topics for performing an effective and safe network assessment.

Class exercises will require that students have an x86-based notebook computer with a CD-ROM drive and a 10/100 Ethernet network card. Students must follow the instructions at http://www.mavensecurity.com/bootdisk prior to attending the workshop. All software provided will be publicly available freeware.

Students will perform selected steps of a general network assessment against a target network consisting of several Windows and UNIX-based servers, as well as various routing components.

Topics include:

Day Two:

- Assessment phase 2: target analysis
  - TCP port scanning
  - UDP port scanning
  - SNMP
- Assessment phase 3: exploitation and confirmation
  - Automated vulnerability scanning tools
  - (Online) brute-force attacks
  - (Offline) password cracking
  - Manual testing
- Special consideration testing
  - Firewalls and routers
  - Auditing email servers
  - Web servers
  - Stealth technique summary
- Vulnerability scanning tools
  - Automated scanning tools
  - Commercial scanners
- Nessus
  - Nessus Clients
  - Using Nessus

For the description of Day 1, see p. 11.


Networking Security

W2 *New!* Solaris Kernel Performance, Observability, and Debugging *(Day 2 of 2)*

James Mauro and Richard McDougall, *Sun Microsystems*
9:00 a.m.–5:00 p.m.

Who should attend: System and database administrators, software architects, developers and programmers, performance and systems analysts, and IT architects wanting to obtain a deeper understanding of the key Solaris subsystems, as well as the tools and facilities that can be used to:

- Observe, trace, and debug to optimize performance
- Observe, trace and debug to root-cause aberrant behavior
- Observe and trace to understand how the application workload interacts with the operating system
- Better understand the system as a whole

Attendees should have some basic understanding of operating system principles and application performance analysis. Students choosing to attend only Day Two should be familiar with Solaris kernel subsystems and have at least rudimentary knowledge of the bundled tools and utilities and their use.

Applications are becoming more complex every day, and many of the new Solaris features significantly reduce the effort required to administer and anazlyze performance of the entire application and operating system stack.

You may take this class as either a one-day experts class or a two day complete class. On Day One, we provide an architectual overview of the major Solaris subsystems and an introduction to Solaris performance analysis. On Day Two, we cover advanced topics and spend significant time with hands-on case studies, using the latest tools, including dtrace, mdb, memtool, mdb, trapstat, and the Solaris process "ptools."

Topics include:

Day Two:

- Solaris observability and debugging tools
- Advanced memory architecture and tuning
- Filesystem performance
- Advanced thread scheduling and tools
- Advanced dtrace
- Workload consolidation and resource management

For the description of Day 1, see p. 11.

Coding Sysadmin

W3 Implementing LDAP Directories

Gerald Carter,
Samba Team/Hewlett-Packard
9:00 a.m.–5:00 p.m.

Who should attend: Both LDAP directory administrators and architects.

System administrators today run a variety of directory services, although these are referred to by names such as DNS and NIS. The Lightweight Directory Access Protocol (LDAP) is the up-and-coming successor to the X500 directory and has the promise of allowing administrators to consolidate multiple existing directories into one. The course will focus on integrating standard network services with LDAP directories. The examples are based on UNIX hosts and the OpenLDAP directory server and will include actual working demonstrations throughout the course.

Topics include:

- Replacing NIS domains
- Integrating Samba user accounts
- Integrating MTAs such as Sendmail, Qmail, or Postfix
- Creating address books for mail clients
- Managing user access to HTTP and FTP services
- Integrating with DHCP & DNS servers
- Scripting with the Net::LDAP Perl module
- Defining custom attributes and object classes


Networking Sysadmin

"There are lots of places to go to get talked at by smart people. USENIX is the one place to go to talk *with* them"

—Dan Geer, *Chief Scientist, Verdaysys Inc.*

Meet people with interests similar to yours! Organize your own BoF. See p. 29 for details.

W4 System and Network Monitoring: Tools in Depth

John Sellens, *SYONEX*
9:00 a.m.–5:00 p.m.

Who should attend: Network and system administrators ready to implement comprehensive monitoring of their systems and networks using the best of the freely available tools. Participants should have an understanding of the fundamentals of networking, familiarity with computing and network components, UNIX system administration experience, and some understanding of UNIX programming and scripting languages.

Are you looking for the latest and greatest in system and network monitoring tools? This tutorial will provide in-depth instruction in the installation and configuration of some of the most popular and effective system and network monitoring tools, including Nagios, Cricket, MRTG, and Orca.

Participants should expect to leave the tutorial with the information needed to immediately implement, extend, and manage popular monitoring tools on their systems and networks.

Topics include, for each of Nagios, Cricket, MRTG, and Orca:

- Installation–Basic steps, prerequisites, common problems, and solutions
- Configuration, setup options, and how to manage larger and non-trivial configurations
- Reporting and notifications–proactive and reactive
- Special cases–how to deal with interesting problems
- Extending the tools–how to write scripts or programs to extend the functionality of the basic package
- Dealing effectively with network boundaries and remote sites
- Security concerns and access control
- Ongoing operation

W5 Administering Linux in Production Environments

Æleen Frisch, *Exponential Consulting*
9:00 a.m.–5:00 p.m.

Who should attend: Both current Linux system administrators and administrators from sites considering converting to Linux or adding Linux systems to their current computing resources.

The course will focus on the administrative issues that arise when Linux systems are deployed to address a variety of real-world tasks, by covering problems arising from both commercial and research-and-development contexts.

Topics include:

- Recent kernel developments
- High-performance I/O
  - Advanced filesystems and logical volumes
  - Disk striping
  - Optimizing I/O performance
- Advanced compute-server environments
  - Beowulf
  - Clustering
  - Parallelization environments/facilities
  - CPU performance optimization
- High availability Linux: fault tolerance options
- Enterprise-wide authentication
- Fixing the security problems you didn't know you had (or, what's good enough for the researcher/hobbyist won't do for you)
- Automating installations and other mass operations
- Linux in the office environment

Every USENIX '05 training program registration includes:

- Admission to the tutorials you select
- Lunch on the day of your tutorial
- Training program CD-ROM, including all available tutorial presentations and materials
- Printed tutorial materials for your courses
- Admission to the Conference Reception
- Conference T-shirt
- Wireless connectivity in conference session area
- Optional discount on a one-year subscription to *Dr. Dobb's Journal*

See p. 33 for additional registration information, then check out http://www.usenix.org/anaheim05 today!

Please see **http://www.usenix.org/usenix05/training** for full tutorial descriptions and program updates.

R1 Hacking & Securing Web-based Applications

David Rhoades,
Maven Security Consulting, Inc.
9:00 a.m.–5:00 p.m.

Who should attend: People who are auditing Web application security, developing Web applications, or managing the development of a Web application.

Is your Web application secure? Sites such as CD Universe, CreditCard.com, and others have found out the hard way: encryption and firewalls are not enough. Numerous commercial and freeware tools assist in locating network-level security vulnerabilities. However, these tools are incapable of locating security issues for Web-based applications.

With numerous real-world examples from the instructor's years of experience with security assessments, this informative and entertaining course is based on fact, not theory. The course material is presented in a step-by-step approach and will apply to Web portals, e-commerce (B2B or B2C), online banking, shopping, subscription-based services, or any Web-enabled application.

Students will learn:

- The primary risks facing Web applications
- Exposures and vulnerabilities in HTML and JavaScript, authentication, and session tracking
- Tools, techniques, and methodologies required to locate weaknesses
- Recommendations for mitigating exposures found
- Best practices for Web application security

Topics include:

- Foundational security
- Web server and Web application output
- Authentication
- Sign-on
- Sesssion issues
- Transaction issues
- Third-party products
- Testing procedures
- Methodology and safety

Coding Security

R2 *New!* Network Security Monitoring with Open Source Tools

Richard Bejtlich, *TaoSecurity.com*
9:00 a.m.–5:00 p.m.

Who should attend: Engineers and analysts who detect and respond to security incidents. Participants should be familiar with TCP/IP. Command-line knowledge of BSD, Linux, or another UNIX-like operating system is a plus. A general knowledge of offensive and defensive security principles is helpful.

This tutorial will equip participants with the theory, tools, and techniques to detect and respond to security incidents. Network Security Monitoring (NSM) is the collection, analysis, and escalation of indications and warnings to detect and respond to intrusions. NSM relies upon alert data, session data, full content data, and statistical data to provide analysts with the information needed to achieve network awareness. Whereas intrusion detection cares more about identifying successful and usually known attack methods, NSM is more concerned with providing evidence to scope the extent of an intrusion, assess its impact, and propose efficient, effective remediation steps.

NSM theory will help participants understand the various sorts of data that must be collected. This tutorial will bring theory to life by introducing numerous open source tools for each category of NSM data. Attendees will be able to deploy these tools alongside existing commercial or open source systems to augment their network awareness and defensive posture.

Topics include:

- NSM theory
- Building and deploying NSM sensors
- Accessing wired and wireless traffic
- Full content tools: Tcpdump, Ethereal/Tethereal, Snort as packet logger
- Additional data analysis tools: Tcpreplay, Tcpflow, Ngrep, Netdude
- Session data tools: Cisco NetFlow, Fprobe, Flow-tools, Argus, SANCP
- Statistical data tools: Ipcad, Trafshow, Tcpdstat, Cisco accounting records
- Sguil (sguil.sf.net)
- Case studies, personal war stories, and attendee participation

Material in the class is supported by the author's book *The Tao of Network Security Monitoring: Beyond Intrusion Detection* (Addison-Wesley, 2005).


Networking Open Source Security

R3 *New!* Configuration Management with Cfengine

Mark Burgess, *Oslo University College*
9:00 a.m.–5:00 p.m.

Who should attend: System administrators with a basic knowledge of scripting who wish to get to grips with cfengine to automate the maintenance and security of their systems. UNIX administrators will be most at home in this tutorial, but cfengine can also be used on Windows 2000 and above. This tutorial works as a guide to the extensive documentation, focusing pragmatically on the key issues and filtering out details.

Cfengine is a tool for setting up and maintaining a configuration across a network of hosts. It is sometimes called a tool for "Computer Immunology"–your computer's own immune system. You can think of cfengine as a very high-level language, much higher-level than Perl or shell, together with a smart agent. The idea behind cfengine is to create a single "policy" or set of configuration files that describes the setup of every host on your network, without sacrificing their autonomy.

Cfengine runs on every host and makes sure that it is in a policy-conformant state; if necessary, any deviations from policy rules are fixed automatically. Unlike tools such as rdist, cfengine does not require hosts to open themselves to any central authority nor to subscribe to a fixed image of files. It is a modern tool, supporting state-of-the-art encryption and IPv6 transport, that can handle distribution and customization of system resources in huge networks (tens of thousands of hosts). Cfengine runs on hundreds of thousands of computers all over the world.

Topics include:

- The components of cfengine and how they are used
- How to get the system running
- How to develop a suitable policy, step by step
- Security
- Organizing configuration files (updating and configuring)
- Ordering issues in configuration management
- Cfservd security and key deployment
- Searching for data with filters
- Special functions and arrays
- Alerts and persistent classes
- Multi-homed host issues
- IPv6 issues
- Methods and modules and when to use them
- Host monitoring with FriendStatus
- Anomaly detection and response with cfenvd
- What is coming in cfengine?

Coding Sysadmin

R4 *New!* Cisco Device Configuration Basics—Live!

Steve Acheson and Laura Kuiper, *Cisco Systems*
9:00 a.m.–5:00 p.m.

Who should attend: Administrators who want to know how to configure and manage Cisco routers and switches for business or home. The tutorial will include a live demonstration of how to configure your devices and get all the parts working together.

This class covers the basics of what needs to be done to get the router working, additional configurations for the switch, and some basic security configuration for the devices.

Topics include:

- Introduction to IOS and its naming
- Stepping through the configuration basics (both the script and via the Command line)
- Using the IOS CLI
- Setting up Network Time Protocol (NTP)
- Security: Access Control List basics
- CDP (Cisco Discovery Protocol)
- Setting up SNMP monitoring
- SSH (secure access)
- Local authentication
- RADIUS authentication
- Making your router a DHCP server
- Doing NAT/PAT with your router
- Configuring routing basics
- Using your router as a VPN gateway
- Using the SDM (Security Device Manager) GUI to configure your router
- Differences between CatOS- and IOS-based switches
- Spanning tree
- Trunking
- PVLAN edge (protected port)
- Troubleshooting
- "show" commands
- "debug" commands


Networking

R5 *New!* Databases: What You Need to Know

John Sellens, *SYONEX*
9:00 a.m.–5:00 p.m.

Who should attend: System and application administrators who need to support databases and database-backed applications.

Databases used to run almost exclusively on dedicated database servers, with one or more database administrators (DBAs) assigned exclusively to their care. These days, with the easy availability of database software such as MySQL and PostgreSQL, databases are popping up in many more places and are used by many more applications.

As a system administrator you need to understand databases, their care and feeding. Attendees will leave the tutorial with a better understanding of databases and their uses and will be ready to deploy and support common database software and database-backed applications.

Topics include:

- An introduction to database concepts
- The basics of SQL (Structured Query Language)
- Common applications of databases
- BerkeleyDB and its applications
- MySQL installation, configuration, and management
- PostgreSQL installation, configuration, and management
- Security, user management, and access controls
- Ad-hoc queries with standard interfaces
- ODBC and other access methods
- Database access using other tools: Perl, PHP, sqsh, etc.
- Basic database-backed application development


Sysadmin

Steve Acheson (R4) is currently an Information Security Architect at Cisco Systems, Inc., where he is a senior member of the Corporate Information Security Department, responsible for network and system security, including designing internal security architecture and external/firewall access. Before working for Cisco, Steve managed security for NASA's Numerical Aerospace Simulations facility at Ames Research Center. He has worked in the field for over 15 years as a system administrator, network engineer, and security analyst.

Richard Bejtlich (R2) is technical director for specialized security monitoring in ManTech International Corporation's Computer Forensics and Intrusion Analysis division. He was previously a principal consultant at Foundstone, performing incident response, emergency network security monitoring, and security research. Prior to joining Foundstone in 2002, Richard served as senior engineer for managed network security operations at Ball Aerospace & Technologies Corporation. From 1998 to 2001 Richard defended global American information assets as a captain in the Air Force Computer Emergency Response Team (AFCERT). He led the AFCERT's real time intrusion detection mission, supervising 60 civilian and military analysts. He is the author of *The Tao of Network Security Monitoring: Beyond Intrusion Detection* and the co-author of the forthcoming *Real Digital Forensics*, both published by Addison-Wesley. He also wrote original material for *Hacking Exposed*, 4th Edition, and *Incident Response*, 2nd Edition, both published by McGraw-Hill/Osborne. He acquired his CISSP certification in 2001 and CIFI credentials in 2004. His home page is http://www.taosecurity.com and his popular Web log resides at http://taosecurity.blogspot.com.

David N. Blank-Edelman (S11, M4) is the Director of Technology at the Northeastern University College of Computer and Information Science and the author of the O'Reilly book *Perl for System Administration*. He has spent the last 19 years as a system/network administrator in large multi-platform environments, including Brandeis University, Cambridge Technology Group, and the MIT Media Laboratory. He has given several successful invited talks off the beaten path at LISA and is the LISA '05 Program Chair.

Mark Burgess (R3) is a professor at Oslo University College and is the author of cfengine. He has been researching the principles of network and system administration for over ten years and is the author of *Principles of Network and System Administration* (John Wiley & Sons). He is frequently invited to speak at conferences.

Gerald Carter (S6, T6, W3) has been a member of the Samba Development Team since 1998. He has published articles with various Web-based magazines and teaches courses as a consultant for several companies. Currently employed by Hewlett-Packard as a Samba developer, Gerald has written books for SAMS Publishing and is the author of the recent *LDAP System Administration* for O'Reilly Publishing.

Heison Chak (M6) is a system and network administrator who works for SOMA Networks, focusing on network management and performance analysis of data and voice networks. Heison has been an active member of the Asterisk community. He started delivering tutorials at USENIX conferences and contributing articles to *;login:* in 2004.

Tom Christiansen (T4) has been involved with Perl since day zero of its initial public release in 1987. Author of several books on Perl, including *The Perl Cookbook* and *Programming Perl* from O'Reilly, Tom is also a major contributor to Perl's online documentation. He holds undergraduate degrees in computer science and Spanish and a Master's in computer science. He now lives in Boulder, Colorado.

Mike Ciavarella (S7, S12, M7) has been producing and editing technical documentation since he naively agreed to write application manuals for his first employer in the early 1980s. He has been a technical editor for MacMillan Press and has been teaching system administrators about documentation for the past eight years. After a number of years working as Senior Partner and head of the Security Practice for Cybersource Pty Ltd, Mike returned to his alma mater, the University of Melbourne. He now divides his time between teaching software engineering and providing expert testimony in computer security matters.

Lee Damon (M7, T8) has a B.S. in Speech Communication from Oregon State University. He has been a UNIX system administrator since 1985 and has been active in SAGE since its inception. He assisted in developing a mixed AIX/SunOS environment at IBM Watson Research and has developed mixed environments for Gulfstream Aerospace and QUALCOMM. He is currently leading the development effort for the Nikola project at the University of Washington Electrical Engineering Department. He is past chair of the SAGE Ethics and Policies Working Groups.

Mark-Jason Dominus (S4, S9) has been programming in Perl since 1992. He is a moderator of the comp.lang.perl.moderated newsgroup, the author of the Text::Template, Tie::File, and Memoize modules, a contributor to the Perl core, and author of the perlreftut man page. His work on the Rx regular expression debugger won the 2001 Larry Wall Award for Practical Utility. He lives in Philadelphia with his wife, daughter, and several plush octopuses.

Jacob Farmer (S5, S10) is the CTO of Cambridge Computer Services, a specialized integrator of backup systems and storage networks. He has over 15 years of experience with storage technologies and writes an expert advice column for *InfoStor* magazine. He is currently writing a book on storage networking.

Rik Farrow (S1, M1) provides UNIX and Internet security consulting and training. He has been working with UNIX system security since 1984 and with TCP/IP networks since 1988. He has taught at the IRS, Department of Justice, NSA, NASA, US West, Canadian RCMP, Swedish Navy, and for many US and European user groups. He is the author of *UNIX System Security*, published by Addison-Wesley in 1991, and *System Administrator's Guide to System V* (Prentice Hall, 1989). Farrow writes a column for *;login:* and a network security column for *Network* magazine. Rik lives with his family in the high desert of northern Arizona and enjoys hiking and mountain biking when time permits.

Æleen Frisch (W5) has been a system administrator for over 20 years. She currently looks after a pathologically heterogeneous network of UNIX and Windows systems. She is the author of several books, including *Essential System Administration* (now in its 3rd edition).

Peter Baer Galvin (S8, M3, T3), is the Chief Technologist for Corporate Technologies, Inc., a systems integrator and VAR, and was the Systems Manager for Brown University's Computer Science Department. He has written articles for *Byte* and other magazines. He wrote the "Pete's Wicked World" and "Pete's Super Systems" columns at *SunWorld*. He is currently contributing editor for *Sys Admin*, where he manages the Solaris Corner. Peter is co-author of the *Operating Systems Concepts* and *Applied Operating Systems Concepts* textbooks. As a consultant and trainer, Peter has taught tutorials on security and system administration and has given talks at many conferences and institutions on such topics as Web services, performance tuning, and high availability.

Geoff Halprin (S13, T8) has spent over 25 years as a software developer, system administrator, consultant, and troubleshooter. He has written software from system management tools to mission-critical billing systems, has built and run networks for enterprises of all sizes, and has been called upon to diagnose problems in every aspect of computing infrastructure and software. He has spent more years troubleshooting other people's systems and programs than he cares to remember. Geoff was on the board of the System Administrators Guild (SAGE) and is now a member of the USENIX board of directors.

Joshua Jensen (T5) has worked for IBM and Cisco Systems and was Red Hat's first instructor, examiner, and RHCE. At Red Hat, he wrote and maintained large parts of the Red Hat curriculum: Networking Services and Security, System Administration, Apache and Secure Web Server Administration, and the Red Hat Certified Engineer course and exam. Joshua has been working with Linux since 1996 and finds himself having come full circle—he is now employed by IBM while working with Red Hat Linux onsite at Cisco Systems. In his spare time he dabbles in cats, fish, boats, and frequent flyer miles.

Charlie Kaufman (M2) is Security Architect for the Common Language Runtime group at Microsoft. He is editor of the new Internet Key Exchange (IKEv2) protocol for the IPsec working group of IETF. He has contributed to a number of IETF standards efforts, including chairing the Web Transaction Security WG and serving as a member of the Internet Architecture Board (IAB). He served on the National Academy of Sciences expert panel that wrote the book *Trust in Cyberspace*. He was previously a Distinguished Engineer at IBM, where he was Chief Security Architect for Lotus Notes and Domino, and before that Network Security Architect for Digital. He holds over 25 patents in the fields of computer security and computer networking. He is coauthor of *Network Security: Private Communication in a Public World* (Prentice Hall, 2002).

Laura Kuiper (R4) is currently a Computer Security Architect at Cisco Systems, Inc., where she is a senior member of the Computer Information Security Department, responsible for network and system security, including designing internal security architecture and external/firewall access. Before working for Cisco, Laura managed the network at SAIC. She has worked in the field as a network engineer and security analyst for over 9 years.

James Mauro (T2, W2) is a Senior Staff Engineer in the Performance and Availability Engineering group at Sun Microsystems. Jim's current projects are focused on quantifying and improving enterprise platform availability, including minimizing recovery times for data services and Solaris. Jim co-developed a framework for system availability measurement and benchmarking and is working on implementing this framework within Sun.

Ned McClain (S3) co-founder and CTO of Applied Trust Engineering, lectures around the globe on applying cutting-edge technology in production computing environments. Ned holds a B.S. in Computer Science from Cornell University and is a contributing author of both the *UNIX Systems Administration Handbook* and the *Linux Administration Handbook*.

Richard McDougall (T2, W2) is a Sun Microsystems Distinguished Engineer who specializes in operating systems technology and system performance. He is based at the Menlo Park Performance and Availability Engineering group, where he drives development of performance and behavior enhancements to the Solaris operating system and Sun's hardware architectures. He has led the development of resource management principles, has contributed to the development of virtual memory and file systems within the Solaris operating system, and has architected many tools for analysis, monitoring, and capacity planning. He is the lead author of *Resource Management* (Prentice Hall). He has written numerous articles and papers on measurement, monitoring, and capacity planning of Solaris systems and frequently speaks at industry and customer technical conferences on the topics of system performance and resource management.

Radia Perlman (S2, M2) is a Distinguished Engineer at Sun Microsystems. She is known for her contributions to bridging (spanning tree algorithm) and routing (link state routing), as well as security (sabotage-proof networks). She is the author of *Interconnections: Bridges, Routers, Switches, and Internetworking Protocols* and co-author of *Network Security: Private Communication in a Public World*, two of the top ten networking reference books, according to *Network Magazine*. She is one of the twenty-five people whose work has most influenced the networking industry, according to *Data Communications Magazine*. She has about 50 issued patents, an S.B. and S.M. in mathematics and a Ph.D. in computer science from MIT, and an honorary doctorate from KTH, the Royal Institute of Technology in Sweden.

Marcus Ranum (M8) is Chief Security Officer at Tenable Security, Inc., and a world-renowned expert on security system design and implementation. He is recognized as the inventor of the proxy firewall and the implementer of the first commercial firewall product. He has designed a number of groundbreaking security products, including the DEC SEAL, the TIS firewall toolkit, the Gauntlet firewall, and NFR's Network Flight Recorder intrusion detection system. He has been involved in every level of operations of a security product business, from developer to founder and CEO of NFR. Marcus has served as a consultant to many FORTUNE 500 firms and national governments, as well as serving as a guest lecturer and instructor at numerous high-tech conferences. In 2001, he was awarded the TISC Clue award for service to the security community, and he holds the ISSA lifetime achievement award.

David Rhoades (T1, W1, R1) is a principal consultant with Maven Security Consulting, Inc. Since 1996, David has provided information protection services for various FORTUNE 500 customers. His work has taken him across the US and abroad to Europe and Asia, where he has lectured and consulted in various areas of information security. David has a B.S. in computer engineering from the Pennsylvania State University and has taught for the SANS Institute, the MIS Training Institute, and ISACA.

John Sellens (T7, W4, R5) has been involved in system and network administration since 1986 and is the author of several related USENIX papers, a number of *;login:* articles, and the SAGE Short Topics in System Administration booklet #7, *System and Network Administration for Higher Reliability*. He holds an M.Math. in computer science from the University of Waterloo and is a chartered accountant. He is the proprietor of SYONEX, a systems and networks consultancy. From 1999 to 2004, he was the General Manager for Certainty Solutions in Toronto. Prior to joining Certainty, John was the Director of Network Engineering at UUNET Canada and was a staff member in computing and information technology at the University of Waterloo for 11 years.

Theodore Ts'o (M5) has been a Linux kernel developer since almost the very beginnings of Linux: he implemented POSIX job control in the 0.10 Linux kernel. He is the maintainer and author of the Linux COM serial port driver and the Comtrol Rocketport driver, and he architected and implemented Linux's tty layer. Outside of the kernel, he is the maintainer of the e2fsck filesystem consistency checker. Ted is currently employed by IBM Linux Technology Center.

9:00 A.M.–10:30 A.M.

Opening Remarks, Awards, and Keynote

KEYNOTE ADDRESS

Von Neumann's Universe: Digital Computing at the Institute for Advanced Study, 1945-1958

George Dyson, *historian and author of* Darwin Among the Machines

The digital universe consists of two kinds of bits: differences in space and differences in time. Digital computers translate between these two forms of information—structure and sequence—according to definite rules. Exactly 60 years ago, John von Neumann and a small group of nonconformists launched a project to do this at electronic speed. The resulting architecture and coding has descended directly to almost all computers now in use.

Von Neumann succeeded in jump-starting the computer revolution by bringing engineers into the den of the mathematicians, rather than by bringing mathematicians into a den of engineers. The stored-program computer, as delivered by von Neumann, broke the distinction between numbers that mean things and numbers that do things. Our universe would never be the same.

With a bare 5 kilobytes of high-speed storage, von Neumann and his colleagues tackled previously intractable problems ranging from thermonuclear explosions, stellar evolution, and long-range weather forecasting to cellular automata, genetic coding, and the origins of life. Programs were small enough to be completely debugged, but hardware could not be counted on to perform consistently from one kilocycle to the next. Although this situation is now reversed, many of the lessons learned on the von Neumann project remain directly applicable today.

George Dyson is a historian of technology whose interests have ranged from the development (and redevelopment) of the Aleut kayak (*Baidarka*, 1986) to the evolution of digital computing and telecommunications (*Darwin Among the Machines*, 1997) and nuclear bomb-propelled space exploration (*Project Orion*, 2002). Dyson, who lives in Bellingham, Washington, divides his time between building boats and writing books. He is currently compiling an account of the confluence of people, technology, and ideas surrounding John von Neumann's Electronic Computer Project at the Institute for Advanced Study, 1945–1958.

11:00 A.M.–12:30 P.M.

GENERAL SESSION

DEBUGGING

Coding

Debugging Operating Systems with Time-traveling Virtual Machines
Samuel T. King, George W. Dunlap, and Peter M. Chen, *University of Michigan*

Using Valgrind to Detect Undefined Value Errors with Bit-precision
Julian Seward, *OpenWorks LLP;* Nicholas Nethercote, *University of Cambridge*

Pulse: A Dynamic Deadlock Detection Mechanism Using Speculative Execution
Tong Li, Carla S. Ellis, Alvin R. Lebeck, and Daniel J. Sorin, *Duke University*

FREENIX SESSION

SOFTWARE TOOLS

Coding

Build Buddy for Fun and Profit
Dan Mills, *Novell, Inc.*


Open Source

Scmbug: Policy-based Integration of Software Configuration Management with Bug-tracking
Kristis Makris, *Arizona State University;* Kyung Dong Ryu, *IBM T.J. Watson Research Center*

Linux Physical Memory Analysis
Paul Movall, Ward Nelson, and Shaun Wetzstein, *IBM*

INVITED TALK

Computer Simulations of Thermal Convection and Magnetic Field Generation in Stars and Planets
Gary Glatzmaier, *University of California, Santa Cruz*

Coding

Global 3D computer models have produced numerical simulations of convection and magnetic field generation in the liquid interiors of terrestrial planets like the Earth and giant planets like Jupiter. The structure and time-dependence of the large-scale magnetic fields outside the core in Earth simulations resemble the Earth's field to first order, and the surface zonal wind profiles in giant planet simulations are beginning to resemble Jupiter's banded zonal wind profile. Examples of such 3D simulations will be presented together with much higher-resolution 2D turbulent simulations, which suggest we are still far from having a robust understanding of the internal dynamics of planets.

GURU IS IN

Please see www.usenix.org/usenix05/tech for updates.

2:00 P.M.–3:30 P.M.

GENERAL SESSION

PLANNING & MANAGEMENT


Sysadmin

Surviving Internet Catastrophes
Flavio Junqueira, Ranjita Bhagwan, Alejandro Hevia, Keith Marzullo, and Geoffrey M. Voelker, *University of California, San Diego*

Making Scheduling "Cool": Temperature-Aware Workload Placement in Data Centers
Justin Moore and Jeff Chase, *Duke University;* Parthasarathy Ranganathan and Ratnesh Sharma, *Hewlett-Packard Labs*

CHAMELEON: A Self-evolving, Fully-adaptive Resource Arbitrator for Storage Systems
Sandeep Uttamchandani, Li Yin, Guillermo A. Alvarez, John Palmer, and Gul Agha, *IBM Almaden Research Center*

FREENIX SESSION

EMULATION

Coding


Open Source

Running Virtualized Native Drivers in User Mode Linux
V. Guffens and G. Bastin, *Université Catholique de Louvain*

QEMU, a Fast and Portable Dynamic Translator
Fabrice Bellard

USB/IP–A Peripheral Bus Extension for Device Sharing over IP Network
Takahiro Hirofuchi, Eiji Kawai, Kazutoshi Fujikawa, and Hideki Sunahara, *Nara Institute of Science and Technology*

INVITED TALK

DDoS Defense in Practice and Theory
Eddie Kohler, *University of California, Los Angeles, and Mazu Networks*


Networking

Depending on whom you ask, distributed denial of service attacks are either a nuisance, or avoidable today using commercial tools, or so fundamental as to require rearchitecting the Internet. So how serious is the problem, and what can we do? This talk will attempt to answer these questions with a tour of the current DDoS landscape, including commercial and research-grade solutions and experiences from the trenches.


Security


Sysadmin

GURU IS IN

Clustering
Greg Bruno, *San Diego Supercomputer Center*

4:00 P.M.–5:30 P.M.

GENERAL SESSION

IMPROVING FILESYSTEMS

Coding

A Transactional Flash File System for Microcontrollers
Eran Gal and Sivan Toledo, *Tel-Aviv University*

Analysis and Evolution of Journaling File Systems
Vijayan Prabhakaran, Andrea C. Arpaci-Dusseau, and Remzi H. Arpaci-Dusseau, *University of Wisconsin, Madison*

Comparison Based File System Verification
Yuen-Lin Tan, Terrence Wong, John D. Strunk, Gregory R. Ganger, *Carnegie Mellon University*

FREENIX SESSION

NETWORKING


Networking

Trickle: A Userland Bandwidth Shaper for Unix-like Systems
Marius A. Eriksen


Open Source

A Tool for Automated IPtables Firewall Analysis
Robert Marmorstein and Phil Kearns, *College of William and Mary*


Sysadmin

Grave Robbers from Outer Space: Using 9P2000 Under Linux
Eric Van Hensbergen, *IBM Austin Research Lab;* Ron Minnich, *Los Alamos National Labs*

INVITED TALK

Online Gaming
Mark Wirt, *Butterfly.net*

Coding

Please see www.usenix.org/usenix05/tech for updates.


Networking

GURU IS IN

Databases
John Sellens, *SYONEX*

9:00 A.M.–10:30 A.M.

GENERAL SESSION

DEFENDING AGAINST ATTACKS


Networking

Active Internet Traffic Filtering: Real-Time Response to Denial-of-Service Attacks
Katerina Argyraki and David R. Cheriton, *Stanford University*


Security

Building a Reactive Immune System for Software Services
Stelios Sidiroglou, Michael E. Locasto, Stephen W. Boyd, and Angelos D. Keromytis, *Columbia University*


Sysadmin

Attrition Defenses for a Peer-to-Peer Digital Preservation System
T.J. Giuli, *Stanford University;* Petros Maniatis, *Intel Research;* Mary Baker, *Hewlett-Packard Labs;* David S. H. Rosenthal, *Stanford University;* Mema Roussopoulos, *Harvard University*

FREENIX SESSION

INVITED TALK

Under the Hood: Open Source Business Models in Context
Stephen R. Walli, *Consultant*


Open Source

People debate regularly about whether or not open source software is "good for business," and how one makes money on something given away "for free." They raise concerns over the commoditization effects and portray a gloomy future where open source software will "eat its way" up a stack of functionality until software is valueless.

This talk looks at historical open source companies, then steps back to look under the hood at a broader business context for the dynamics at work to provide a business model for open source software. Part of the story behind Microsoft's community projects will be told along the way.

INVITED TALK

NFSv4
Spencer Shepler, *Sun Microsystems*


Networking


Sysadmin

With NFS version 4, the IETF has provided the first openly defined filesystem protocol. NFSv4 draws upon previous versions of NFS along with characteristics of other distributed filesystems to provide a useful, flexible framework for today's client and server environments. NFSv4 provides strong security through the use of either Kerberos V5, SPKM-3, or LIPKEY. NFSv4 combines the previously disparate set of protocols surrounding NFS into a single protocol. NFSv4 also allows for adaptation to future needs via minor versioning. The details of these features and the rest of the protocol will be reviewed as well as the performance characteristics of today's NFSv4 environment.

GURU IS IN

Kerberos 5, LDAP, and Samba
Gerald Carter, *Samba Team/Hewlett-Packard*

11:00 A.M.–12:30 P.M.

GENERAL SESSION

IMPROVING DATA MOVEMENT


Networking

Peer-to-Peer Communication Across Network Address Translators
Bryan Ford, *Massachusetts Institute of Technology;* Pyda Srisuresh, *Caymas Systems, Inc.;* Dan Kegel

Maintaining High-Bandwidth Under Dynamic Network Conditions
Dejan Kostic, Ryan Braud, Charles Killian, Erik Vandekieft, James W. Anderson, Alex C. Snoeren, and Amin Vahdat, *University of California, San Diego*

Server Scalability and TCP Offload
Doug Freimuth, Elbert Hu, Jason LaVoie, Ronald Mraz, Erich Nahum, Prashant Pradhan, and John Tracey, *IBM T.J. Watson Research Center*

FREENIX SESSION

SECURITY VISUALIZATION


Networking

Ourmon and Network Monitoring Performance
James R. Binkley and Bart Massey, *Portland State University*


Open Source

Brooery: A Graphical Environment for Analysis of Security-Relevant Network Activity
Christian Kreibich, *University of Cambridge*


Security

NetState: A Network Version Tracking System
Nancy Durgin, Yuqing Mai, and Jamie Van Randwyk, *Sandia National Laboratories*

INVITED TALK

10–20x Faster Software Builds
John Ousterhout, *Electric Cloud, Inc.*

Coding

Almost all software projects with more than a few dozen developers are plagued by slow builds that sap productivity, extend release schedules, and impact product quality. Parallel builds offer the potential of significant speedups, but previous attempts at parallelizing builds have had only modest success, primarily due to the lack of complete dependency information. In this talk I will present the architecture of Electric Cloud, a gmake-compatible build system that uses clusters of inexpensive servers to run massively parallel builds. The key to the Electric Cloud approach is that it deduces dependencies on the fly by monitoring file accesses during the build, so that it knows when it is or isn't safe to run build steps in parallel. I will also describe other aspects of the system, such as its versioning network file system and its use of peer-to-peer protocols for moving file data efficiently. Finally, I will compare Electric Cloud to other approaches such as distcc.

GURU IS IN

Please see www.usenix.org/usenix05/tech for updates.

2:00 P.M.–3:30 P.M.

GENERAL SESSION

SHORT PAPERS I


Networking

A Hierarchical Semantic Overlay Approach to Peer-to-Peer Similarity Search
Duc A. Tran, *University of Dayton*


Security

A Parts-of-file File System
Yoann Padioleau and Olivier Ridoux, *Campus Universitaire de Beaulieu*


Sysadmin

BINDER: An Extrusion-based Break-In Detector for Personal Computers
Weidong Cui and Randy H. Katz, *University of California, Berkeley;* Wai-tian Tan, *Hewlett-Packard Laboratories*

Proper: Privileged Operations in a Virtualised System Environment
Steve Muir, Larry Peterson, and Marc Fiuczynski, *Princeton University;* Justin Cappos and John Hartman, *University of Arizona*

AMP: Program Context Specific Buffer Caching
Feng Zhou, Rob von Behren, and Eric Brewer, *University of California, Berkeley*

Automatic Synthesis of Filters to Discard Buffer Overflow Attacks: A Step Towards Realizing Self-Healing Systems
Zhenkai Liang, R. Sekar, and Daniel C. DuVarney, *Stony Brook University*

FREENIX SESSION

INVITED TALK–Mac OS X Tiger: What's New for UNIX Users?
Dave Zarzycki, Senior Engineer, BSD Technology Group, Apple Computer


Open Source

Mac OS X "Tiger" contains hundreds of new features, many of them in the open-source UNIX "underpinnings" of the system. This talk will discuss new features in the Kernel, new support for rapid indexing and searching of filesystem data, extended file attribute management, strategies for increased performance and 64 bit application support, various software development tool updates, and Tiger's new subsystems for application logging and daemon/service control.

INVITED TALK

Thin Clients: Past, Present, and Future
Jason Nieh, *Columbia University*


Security


Sysadmin

Exponential improvements in networking and the management cost and complexity of PCs are driving the reemergence of thin clients. But this is not a return to the past of dumbed-down terminal interfaces and limited functionality. Modern thin clients can provide rich PC application functionality and enable new application services while simplifying system administration and improving system security. These benefits arise from a model of running all application logic on servers which then simply send display updates to the clients. I will examine how thin clients can address today's IT infrastructure problems and I will then discuss challenges and opportunities.

GURU IS IN

Startups
Stephen Walli, *Consultant*

4:00 P.M.–5:30 P.M.

GENERAL SESSION

SHORT PAPERS II

Coding

Facilitating the Development of Soft Devices
Andrew Warfield, Keir Fraser, and Steven Hand, *University of Cambridge*


Networking

Implementing Transparent Shared Memory on Clusters Using Virtual Machines
Matthew Chapman, *University of New South Wales;* Gernot Heiser, *National ICT Australia*


Sysadmin

Measuring CPU Overhead for I/O Processing in the Xen Virtual Machine Monitor
Ludmila Cherkasova and Rob Gardner, *Hewlett-Packard Laboratories*

Fast Transparent Migration for Virtual Machines
Michael Nelson, Beng-Hong Lim, and Greg Hutchins, *VMware, Inc.*

Performance of Multithreaded Chip Multiprocessors and Implications for Operating System Design
Alexandra Fedorova, *Harvard University and Sun Microsystems;* Margo Seltzer, *Harvard University;* Christopher Small and Daniel Nussbaum, *Sun Microsystems*

Hyper-Threading Aware Process Scheduling Heuristics
James R. Bulpin and Ian A. Pratt, *University of Cambridge*

WORK-IN-PROGRESS REPORTS (WIPS)

Short, pithy, and fun, Work-in-Progress reports introduce interesting new or ongoing work. If you have work you would like to share or a cool idea that's not quite ready for publication, send a one- or two-paragraph summary to usenix05wips@usenix.org. We are particularly interested in presenting students' work. A schedule of presentations will be posted at the conference, and the speakers will be notified in advance. Work-in-Progress reports are five-minute presentations; the time limit will be strictly enforced.

GURU IS IN

Please see www.usenix.org/usenix05/tech for updates.

9:00 A.M.–10:30 A.M.

GENERAL SESSION

SPEEDING UP THINGS

Coding

A Portable Kernel Abstraction for Low-Overhead Ephemeral Mapping Management
Khaled Elmeleegy, Anupam Chanda, and Alan L. Cox, *Rice University;* Willy Zwaenepoel, *EPFL*

Adaptive Main Memory Compression
Irina Chihaia and Thomas Gross, *ETH Zurich*

Drive-Thru: Fast, Accurate Evaluation of Storage Power Management
Daniel Peek and Jason Flinn, *University of Michigan*

INVITED TALK/FREENIX SESSION

Linux and JPL's Mars Exploration Rover Project: Earth-based Planning, Simulation, and *Really* Remote Scheduling
Scott Maxwell and Frank Hartman, *NASA JPL*


Open Source

NASA/JPL's Mars Exploration Rover project is the first time a JPL flight project has used Linux systems for critical mission operations. Scott Maxwell and Frank Hartman, two of MER's rover drivers, also wrote the Rover Sequencing and Visualization Program (RSVP), the Linux-based software used on Earth to drive Spirit and Opportunity. Scott and Frank will discuss the software they developed, as well as their experiences using Linux to drive two vehicles across the Martian terrain, a hundred million miles from Earth.

GURU IS IN

Open Source vs. Corporate Intellectual Property
Stormy Peters, *Hewlett-Packard*

11:00 A.M.–12:30 P.M.

GENERAL SESSION

LARGE SYSTEMS

Coding


Sysadmin

Itanium–A System Implementor's Tale
Charles Gray and Matthew Chapman, *University of New South Wales;* Peter Chubb, *University of New South Wales and National ICT Australia;* David Mosberger-Tang, *Hewlett-Packard Labs;* Gernot Heiser, *University of New South Wales and National ICT Australia*

Providing Dynamic Update in an Operating System
Andrew Baumann and Gernot Heiser, *University of New South Wales and National ICT Australia;* Jonathan Appavoo, Dilma Da Silva, Orran Krieger, and Robert W. Wisniewski, *IBM T.J. Watson Research Center;* Jeremy Kerr, *IBM Linux Technology Center*

SARC: Sequential Prefetching in Adaptive Replacement Cache
Binny S. Gill and Dharmendra S. Modha, *IBM Almaden Research Center*

FREENIX SESSION

MULTIMEDIA


Open Source

OpenCSG: A Library for Image-Based CSG Rendering
Florian Kirsch and Jürgen Döllner, *University of Potsdam*

FreeVGA: Architecture Independent Video Graphics Initialization for LinuxBIOS
Li-Ta Lo, Gregory R. Watson, and Ronald G. Minnich, *Los Alamos National Laboratory*

The Ethernet Speaker System
David Michael Turner and Vassilis Prevelakis, *Drexel University*

INVITED TALK

Possible Futures for Software
Vernor Vinge, *Hugo award-winning sci-fi author of the* Across Real Time *series,* The Witling, True Names, *and* A Fire Upon the Deep

Coding


Security

No one knows what software technology will be in twenty years. However, there are variables that will probably drive the outcome, for example, hardware improvements, success at managing large projects, and demand for "secure computing." In this talk, I consider four scenarios for the software future, based on different values for these drivers. There are things to love and things to loathe in these scenarios, but consideration of their various onset symptoms could be helpful in adapting to (or affecting) what really happens in our future.

GURU IS IN

Please see www.usenix.org/usenix05/tech for updates.

Paying by check? Use our online reservation system! See p. 33 for details.

2:00 P.M.–3:30 P.M.

GENERAL SESSION

IMPROVING OS COMPONENTS

Coding

Slinky: Static Linking Reloaded
Christian Collberg, John H. Hartman, Sridivya Babu, and Sharath K. Udupa, *University of Arizona*

CLOCK-Pro: An Effective Improvement of the CLOCK Replacement
Song Jiang, *Los Alamos National Laboratory;* Feng Chen and Xiaodong Zhang, *College of William and Mary*

Group Ratio Round-Robin: O(1) Proportional Share Scheduling for Uniprocessor and Multiprocessor Systems
Bogdan Caprita, Wong Chun Chan, Jason Nieh, Clifford Stein, and Haoqiang Zheng, *Columbia University*

FREENIX SESSION

MEASUREMENT

Coding

A PC-Based Open-Source Voting Machine with an Accessible Voter-Verified Paper Ballot
Arthur M. Keller, *UC Santa Cruz and Open Voting Consortium;* Alan Dechert, *Open Voting Consortium;* Karl Auerbach, *InterWorking Labs;* David Mertz, *Gnosis Software, Inc.;* Amy Pearl, *Software Innovations;* Joseph Lorenzo Hall, *UC Berkeley*


Open Source

Auto-pilot: A Platform for System Software Benchmarking
Charles P. Wright, Nikolai Joukov, Devaki Kulkarni, Yevgeniy Miretskiy, and Erez Zadok, *Stony Brook University*

Interactive Performance Measurement with VNCPlay
Nickolai Zeldovich and Ramesh Chandra, *Stanford University*

INVITED TALK

Flying Linux
Dan Klein, *USENIX*


Open Source

How good is Linux, really? When your life is at stake, your attitudes change considerably. This talk will look at what it takes to make software truly mission critical and man-rated. We'll go back to the earliest fly-by-wire systems–Mercury, Gemini, and Apollo–and look at such diverse (but critical!) issues as compartmentalization, trojans and terrorism, auditing and accountability, bugs and boundary conditions, distributed authoring, and revision control. At the end of this talk, what you thought might be an easy answer will be seen to be not so easy.

GURU IS IN

Security
Rik Farrow, *Security Consultant*

4:00 P.M.–5:30 P.M.

USENIX GAME SHOW

Closing out this year's conference, the USENIX Game Show will pit attendees against each other in a test of technical knowledge and cultural trivia. Host Rob Kolstad and sidekick Dan Klein will provide the questions and color commentary for this always memorable event.

Will You Be the Next Game Show Champion?
Here's a sample of the kinds of questions you'll be asked to qualify as a contestant for the USENIX Game Show. Host Rob Kolstad culls trivia from every imaginable category, from woodworking tools through calculus to prehistoric animals. Hit the books now so you'll be ready for your chance to showcase your knowledge and win fabulous prizes.

Category: Animal Adjectives
Q: "Lupine" pertains to what animal?
A: Wolves

Category: Before and After
Q: "Crocodile Rock" meets "Rocky Mountain High"
A: Elton John Denver

Category: Mythical Beasts
Q: Name the three headed-dog that guards the gates of the underworld.
A: Cerberus

Category: Network Services
Q: What daemon does the "biff" service use?
A: comsat

Category: Professions
Q: What does a wainwright do?
A: Make wagons

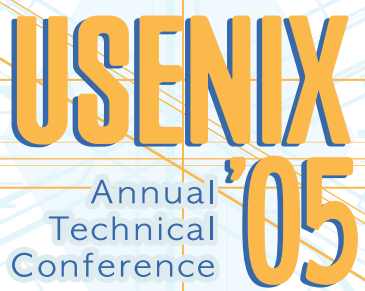
Category: "Three"
Q: Who was the richest person on Gilligan's Island?
A: Thurston J. Howell, III

Sponsorships & Vendor Sessions Now Available!

We are actively seeking corporate support for USENIX '05.

A range of sponsorships are available, including hosted evening sessions where you can present your products and services, recruit, host a users group, or enlist beta testers. All sponsorships provide you with the opportunity to put your company or organization in front of an internationally renowned community of academics, engineers, systems administrators, developers, and students.

See http://www.usenix.org/usenix05/sponsors to learn more, or contact Cat Allman, USENIX Sales Director, at 510-528-8649 x32 or sales@usenix.org for more information.



About USENIX

USENIX: The Advanced Computing Systems Association

Since 1975, USENIX has brought together the community of innovators, engineers, system administrators, scientists, and technicians working on the cutting edge of the computing world. Its mission is to support research and technical training for this dynamic community and its over 6,000 active members.

A complimentary USENIX membership is part of every non–USENIX-member technical sessions registration. The benefits of this membership include:

- Free subscription to *;login:*, the magazine of USENIX, both in print and online
- Online access to all Conference Proceedings from 1993 to the present
- The right to vote in USENIX Association elections
- Discounts on technical session registration fees for all USENIX-sponsored and co-sponsored events
- Discounts on purchasing printed Proceedings, CD-ROMs, and other Association publications
- Discounts on industry-related publications such as *Sys Admin*, *Linux Journal*, and O'Reilly and No Starch Press books

USENIX and Email: Mutual Benefits for Subscribing

As valued USENIX members and conference attendees, you have a choice about whether to receive email from USENIX. Below is a brief list of reasons why you should.

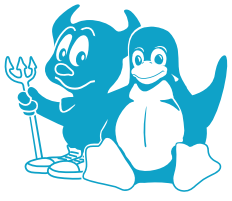
- It's the best way to receive the most up-to-date conference info and important organizational news.
- It saves you money: The more people USENIX reaches via email, the less money it spends on promotional efforts. This translates to lower registration fees for you.
- USENIX never shares, sells, rents, or exchanges its email address. The only email you'll get from USENIX is about USENIX.

When registering for USENIX '05, please mark "yes, send me USENIX announcements via email." It's the best choice for getting the latest USENIX conference information, discounts, and news.

At USENIX '05 you can combine days of training with days of technical session content to build the conference that meets your needs. Pick and choose the sessions that best fit your interest–focus on just one topic or mix and match themes.

- Enhance your skills with the in-depth Training Program.
- Join industry luminaries as they discuss important and timely topics in the Invited Talks sessions.
- Check out the latest developments and interesting applications in the General Session and FREENIX Refereed Papers.
- Bring your most difficult questions to the experts in the Guru Is In Sessions.

Whether your focus is coding, networking, open source, security, or system administration, USENIX '05 has the advanced content you're looking for.



Open Source

Is open source your life? Linux your passion? USENIX '05 offers you content to hone your skills and fire your imagination–from speakers who know what they're talking about.

Here is a list of Training Sessions, Refereed Papers, and Invited Talks related to open source software. Create an open source conference just for you.

TRAINING SESSIONS

S1/M1: Hands-on Linux Security Class: Learn How to Defend Linux/UNIX Systems by Learning to Think Like a Hacker

M5: Inside the Linux Kernel (Updated for v. 2.6)

T5: RPM Package Management

T6: Managing Samba 3.0

W4: System and Network Monitoring: Tools in Depth

W5: Administering Linux in Production Environments

R2: Network Security Monitoring with Open Source Tools

INVITED TALKS

Under the Hood: Open Source Business Models in Context

Linux and JPL's Mars Exploration Rover Project: Earth-based Planning, Simulation, and *Really* Remote Scheduling

Mac OS X Tiger: What's New for UNIX Users?

Flying Linux

REFEREED PAPER SESSIONS

Software Tools

Emulation

Networking

Security Visualization

Multimedia

Measurement

Security

Calling all security researchers and practitioners: USENIX '05 offers a variety of programs to meet your needs.

Here is a list of Training Sessions, Refereed Papers, and Invited Talks related to security. Mix and match from the lists of sessions to design the security-focused conference you need!

TRAINING SESSIONS

S1/M1: Hands-on Linux Security Class: Learn How to Defend Linux/UNIX Systems by Learning to Think Like a Hacker

S6: Kerberos 5–Revenge of the Three-Headed Dog

S8: Next-Generation Security Tools

M2: Network Security Protocols: Theory and Current Standards

T1/W1: Network Security Assessments Workshop–Hands-on

T3: Solaris 10 Security Features Workshop

R1: Hacking & Securing Web-based Applications

R2: Network Security Monitoring with Open Source Tools

INVITED TALKS

DDoS Defense in Practice and Theory

Thin Clients: Past, Present, and Future

Possible Futures for Software

REFEREED PAPER SESSIONS

Defending Against Attacks

Security Visualization

Short Papers I

Coding

All code all the time: USENIX '05 has what you're looking for.

Here is a list of Training Sessions, Refereed Papers, and Invited Talks related to coding. Mix and match to create the coding-centric conference you need.

TRAINING SESSIONS

- **S2:** Bridges, Routers, Switches, and Internetworking Protocols
- **S4:** Regular Expression Mastery
- **S7:** Advanced Shell Programming
- **S9:** Perl Program Repair Shop and Red Flags
- **M4:** Perl for System Administration: The Power and the Praxis
- **M5:** Inside the Linux Kernel (Updated for v. 2.6)
- **T2/W2:** Solaris Kernel Performance, Observability, and Debugging
- **T4:** Advanced Perl Programming
- **T8:** Release Engineering and Project Lifecycle
- **R1:** Hacking & Securing Web-based Applications
- **R3:** Configuration Management with Cfengine

INVITED TALKS

Computer Simulations of Thermal Convection and Magnetic Field Generation in Stars and Planets

Online Gaming

10–20x Faster Software Builds

Possible Futures for Software

REFEREED PAPER SESSIONS

Debugging

Software Tools

Emulation

Improving Filesystems

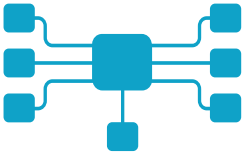
Short Papers II

Speeding Up Things

Large Systems

Improving OS Components

Measurement



Networking

Is networking your life? USENIX '05 offers a wide variety of sessions on the latest topics in networking—theoretical and practical, Linux and UNIX.

Here is a list of Training Sessions, Refereed Papers, and Invited Talks related to networking. Mix and match to create the networking-focused conference you need.

TRAINING SESSIONS

- **S2:** Bridges, Routers, Switches, and Internetworking Protocols
- **S3:** Hot Topics in System Administration
- **S6:** Kerberos 5—Revenge of the Three-Headed Dog
- **S10:** Next-Generation Storage Networking and Data Protection
- **M2:** Network Security Protocols: Theory and Current Standards
- **M6:** VoIP Principles and Practice
- **M8:** System Log Aggregation, Statistics, and Analysis
- **T1/W1:** Network Security Assessments Workshop—Hands-on
- **T6:** Managing Samba 3.0
- **T7:** Practical System and Network Monitoring
- **W3:** Implementing LDAP Directories
- **W4:** System and Network Monitoring: Tools in Depth
- **R2:** Network Security Monitoring with Open Source Tools
- **R4:** Cisco Device Configuration Basics—Live!

INVITED TALKS

DDoS Defense in Practice and Theory

Online Gaming

NFSv4

REFEREED PAPER SESSIONS

Networking

Defending Against Attacks

Improving Data Movement

Security Visualization

Short Papers I

Short Papers II

Sysadmin

Interested in all things related to system administration? USENIX '05 is the place to get your questions answered.

Here is a list of Training Sessions, Refereed Papers, and Invited Talks related to system administration. Pick and choose sessions to create the conference you need.

TRAINING SESSIONS

S1/M1: Hands-on Linux Security Class: Learn How to Defend Linux/UNIX Systems by Learning to Think Like a Hacker

S3: Hot Topics in System Administration

S4: Regular Expression Mastery

S5: Eliminating Backup System Bottlenecks Using Disk-to-Disk and Other Methods

S7: Advanced Shell Programming

S10: Next-Generation Storage Networking and Data Protection

S11: Over the Edge System Administration, Volume 1

TRAINING SESSIONS (CONTINUED)

S12: Documentation Techniques for SysAdmins

S13: Troubleshooting: A Basic Skill

M3: Advanced Solaris System Administration Topics

M4: Perl for System Administration: The Power and the Praxis

M7: Seven Habits of the Highly Effective System Administrator

M8: System Log Aggregation, Statistics, and Analysis

T2/W2: Solaris Kernel Performance, Observability, and Debugging

T3: Solaris 10 Security Features Workshop

T5: RPM Package Management

T6: Managing Samba 3.0

T7: Practical System and Network Monitoring

T8: Release Engineering and Project Lifecycle

W3: Implementing LDAP Directories

W4: System and Network Monitoring: Tools in Depth

W5: Administering Linux in Production Environments

R3: Configuration Management with Cfengine

R5: Databases: What You Need to Know

INVITED TALKS

DDoS Defense in Practice and Theory

NFSv4

Thin Clients: Past, Present, and Future

REFEREED PAPER SESSIONS

Planning & Management

Networking

Defending Against Attacks

Short Papers I

Short Papers II

Large Systems

HOST YOUR OWN BIRDS-OF-A-FEATHER (BOF) SESSION

Looking for another opportunity to meet people with interests similar to yours? Want to share your knowledge and enthusiasm with your peers? Organize your own Birds-of-a-Feather Session. BoFs are casual, 1–3 hour sessions that take place in the evening so they don't conflict with daytime sessions. BoFs can be about anything: open source projects, specific platforms or tools, professional topics, etc. They can also be purely social activities. However, commercial BoFs, such as product demos or discussions of proprietary technologies by companies, will be charged a sponsorship fee.

BoFs may be scheduled during the conference at the registration desk or in advance by contacting bofs@usenix.org. Interested in sponsoring a commercial BoF? Email sales@usenix.org.

Make the most of your USENIX experience by pursuing your interests–set up a BoF at USENIX '05.

CONFERENCE ACTIVITIES

Welcome Reception

Sunday, April 10, 6:00 p.m.–7:00 p.m.

Join fellow attendees at the opening night Welcome Reception. Refreshments and snacks provided.

Conference Orientation

Sunday, April 10, 6:30 p.m.–7:00 p.m.

Whether this is your first time at Annual Tech or your tenth, stop by the Conference Orientation to learn how to get the most out of the conference in its new, expanded format. The orientation includes an overview of Anaheim, an introduction to USENIX, and an added opportunity to meet your peers.

Poster Reception

Wednesday, April 13, 6:00 p.m.–7:30 p.m.

Don't miss the cool new ideas and the latest preliminary research on display at the Poster Reception. Take part in challenging discussions and enjoy great food.

USENIX 30th Anniversary Reception

Thursday, April 14, 7:00 p.m.–8:30 p.m.

Join USENIX in celebrating our 30th anniversary at the conference reception, yet another opportunity to mingle with colleagues and enjoy food and drinks.

Birds-of-a-Feather Sessions (BoFs)

Monday, April 11–Thursday, April 14, 8:30 p.m.–11:30 p.m.

Lead or attend a BoF! Meet with your peers! Present new work! Don't miss these special activities designed to maximize the value of your time at the conference. The always popular evening Birds-of-a-Feather sessions are very informal gatherings of persons interested in a particular topic. BoFs may be scheduled during the conference at the registration desk or in advance by contacting bofs@usenix.org.

Work-in-Progress Reports (WiPs)

Thursday, April 14, 4:00 p.m.–5:30 p.m

Short, pithy, and fun, Work-in-Progress reports introduce interesting new or ongoing work. If you have work you would like to share or a cool idea that's not quite ready for publication, send a one- or two-paragraph summary to usenix05wips@usenix.org. We are particularly interested in presenting students' work. A schedule of presentations will be posted at the conference, and the speakers will be notified in advance. Work-in-Progress reports are five-minute presentations; the time limit will be strictly enforced.

USENIX Game Show

Friday, April 15, 4:00 p.m.–5:30 p.m.

Closing out this year's conference, the USENIX Game Show will pit attendees against each other in a test of technical knowledge and cultural trivia. Host Rob Kolstad and sidekick Dan Klein will provide the questions and color commentary for this always memorable event.

SPECIAL CONFERENCE FEATURES

Conference Services

Bring Your Laptop!

USENIX is pleased to offer 802.11b wireless Internet connectivity and a conference wiki at USENIX '05. The network issues NAT'd addresses via DHCP and is open and insecure. Although traffic monitoring is prohibited, use of crypto is nonetheless highly recommended. A laptop drop room with power, Ethernet connections, and a few computers with Web browsers and *NIX shell will be available. The conference wiki and other network service information will be available at http://conference.usenix.org. If you have questions, please send email to wireless@usenix.org.

Conference Proceedings

Those registered for the technical sessions will receive a complimentary copy of the Proceedings, either in print or on CD-ROM. Additional copies of the Proceedings and the CD-ROM will be available for purchase at the conference. To order copies after the conference, see http://www.usenix.org/publications/ordering.

Student Discounts and Stipends

Training

A limited number of tutorial seats are reserved for full-time students at the very special rate of $200 for one full-day tutorial (if you plan to take half-day tutorials, you must take both half-days to qualify for the student rate). You must email the Conference Department, conference@usenix.org, to confirm availability and make a reservation. In your email, please specify which tutorials you wish to attend. You will be given a code number to use when you register. The Conference Department must receive your registration form, with the code number, full payment, and a photocopy of your current student I.D. card, within 14 days from the date you make your reservation, or your reservation will be canceled. This special fee is nontransferable.

Technical Sessions

USENIX offers full-time students the deeply discounted rate of $90 per day for Student technical sessions. students who are not USENIX members, add $40 to your technical sessions fees. You must fax a copy of your current student I.D. card to the USENIX Conference Department when you register. This special fee is not transferable.

Student Stipends for Conference Attendence

A limited number of student stipends are available to pay for travel, accommodations, and registration fees to enable full-time students to attend the conference. To apply for a stipend, visit our student stipend Web page: http://www.usenix.org/students/stipend.html.

Please note that if you intend to apply for a student stipend, you should not register for the conference until you hear whether you have been awarded a stipend. Sorry, faxes will not be accepted for student stipend applications.

MARRIOTT ANAHEIM

700 West Convention Way
Anaheim, CA, 92802-3483
(714) 750-8000

USENIX has negotiated special rates for conference attendees at the Marriott Anaheim. Please make your reservation as soon as possible, by contacting the hotel directly and mentioning USENIX to get the special group rate.

Hotel Discount Reservation Deadline

Monday, March 21, 2005

Room Rates

Single/Double/Triple/Quad: $169

Note: When the rooms in the USENIX block have sold out, requests will be handled on a space-available basis at the hotel's standard rate. Please make your reservation early!

Online Reservations

See the USENIX '05 Web site for details:
http://www.usenix.org/events/usenix05/hotel.html

STAYING AT THE MARRIOTT ANAHEIM? GET DISCOUNTS ON DISNEY TICKETS!

Want to experience the "happiest place on Earth"? USENIX can get you there for less! USENIX '05 conference attendees who stay at the headquarters hotel have the opportunity to purchase Disneyland park tickets at a discounted price. This offer includes both Disneyland and Disney's California Adventure. Check out http://www.usenix.org/events/usenix05/hotel.html for more information.

TRANSPORTATION

Airports

Anaheim's location in the Los Angeles metropolitan area makes it easily accessible by air. The three closest airports are Orange County/John Wayne (15 miles SE), Long Beach (20 miles N), and Los Angeles (35 miles NW), all of which are served by major airlines. Shuttle service to the hotels is easily accessible from LAX and Orange County. Other airports serving the region include Ontario (35 miles NE) and Burbank/Bob Hope (40 miles NW).

Traveling to USENIX '05 from Outside the U.S.A.?

See detailed advice from the National Academies about visiting the United States, at www7.nationalacademies.org/visas/Traveling_to_US.html.

ABOUT ANAHEIM

USENIX is pleased to bring USENIX '05 to Anaheim. Anaheim offers a wealth of activities for the entire family, a wide array of restaurants to suit every taste and budget, and the beautiful weather of Southern California. There are many attractions that will be of interest to USENIX '05 attendees, many of which are within a few miles of the hotel. Here are just a few:

- What better reason to visit Anaheim—besides attending USENIX '05—than to discover the magic of Disneyland? If you stay at the Marriott Anaheim, you'll receive valuable discounts on tickets!
  - Disneyland Park
  - Disney's California Adventure
  - Downtown Disney
- Board the Queen Mary in nearby Long Beach for a tour of the floating palace, a fine meal, or even a glimpse of a ghost.
- Explore the world's largest ocean at the Aquarium of the Pacific in Long Beach.
- View classic examples of "Space Age Modern" architecture along Beach Boulevard and Katella Avenue. See http://www.anaheimcolony.com/googie.htm to learn more.

For more ideas, visit the Anaheim/Orange County Visitor & Convention Bureau's Web site: www.anaheimoc.org.

WHY SHOULD YOU STAY IN THE HEADQUARTERS HOTEL?

We strongly encourage you to stay in the conference hotel and when making your reservation to identify yourself as a USENIX conference attendee. By staying at the headquarters hotel, you not only help us keep registration fees low, but you also get valuable discounts on local attractions.

By contracting rooms for our attendees, we significantly reduce hotel charges for meeting room rental. When those sleeping rooms are not occupied, we face significant financial penalties. Those penalties ultimately force us to raise registration fees.

With costs going higher and higher, we are working hard to negotiate the very best hotel rates for you and to keep other conference expenses down, in order to keep registration fees as low as possible. We appreciate your help in this endeavor.

THANKS TO USENIX SUPPORTING MEMBERS

Addison-Wesley/Prentice Hall PTR
Ajava Systems, Inc.
AMD
Asian Development Bank
Atos Origin BV
Cambridge Computer Services, Inc.
Delmar Learning
DoCoMo Communications Laboratories USA, Inc.
Electronic Frontier Foundation
Hewlett-Packard
IBM
Intel
Interhack
MacConnection
The Measurement Factory
Microsoft Research
Oracle
OSDL
Perfect Order
Portlock Software
Raytheon
Sun Microsystems, Inc.
Taos
Tellme Networks
UUNET Technologies, Inc.
Veritas Software

THANKS TO USENIX '05 MEDIA SPONSORS

Addison-Wesley/Prentice Hall PTR
C/C++ Users Journal
Dr. Dobb's Journal
DSstar
GRIDtoday
Homeland Defense Journal
HPCwire
ITtoolbox
Linux Journal
No Starch Press
OSTG
Queue
SNIA
StorageNetworking.org
Sys Admin
UserFriendly.org

USENIX Annual Technical Conference '05

Paying by check? Use our online reservation system! See p. 33 for details.

REGISTRATION INFORMATION

Register or make a reservation on the Web today at http://www.usenix.org/usenix05/registration.

Pay today with a credit card, or make a reservation online and then pay by check, phone, or fax. Have the best of both worlds: the convenience of online registration without the hassle of hand-written forms, and the ability to pay as you want, when you want!

Early Bird Registration Deadline:
March 21, 2005

Training Program Fees Include:
- Admission to the tutorials you select
- Lunch on the day of your tutorial
- Training program CD-ROM, including all available tutorial presentations and materials
- Printed tutorial materials for your courses
- Admission to the Conference Reception
- Conference T-shirt
- Wireless connectivity in conference session area
- Optional discount on a one-year subscription to *Dr. Dobb's Journal*

Technical Sessions Fees Include:
- Admission to all technical sessions on the days you attend
- Copy of the Conference Proceedings (printed or on CD-ROM)
- Admission to the Conference Reception
- Conference T-shirt
- Wireless connectivity in conference session area
- Optional discount on a one-year subscription to *Dr. Dobb's Journal*

Multiple Employee Discount
We offer discounts for organizations sending 5 or more employees to USENIX '05. Please email usenix05_reg@usenix.org for more details.

The group discount cannot be used in conjunction with any other discounts, and it cannot be applied retroactively–that is, refunds will not be issued to those meeting the discount requirement after they have already registered.

Refund/Cancellation Date:
Friday, April 1, 2005

All refund requests must be emailed to conference@usenix.org by Friday, April 1, 2005. You may substitute another in your place.

Questions? Email conference@usenix.org

REGISTRATION FEES

Daily Rates
- 1 day of technical sessions: $250
- 1 day of training: $625
- 1 half-day of training: $325 (second half-day only $300)

SAVE! Choose One of Our Special Discount Packages

Package A.	3 Days of Technical Sessions	$650	*Save $100!*
Package B.	2 Days of Training	$1200	*Save $50!*
Package C.	3 Days of Training	$1775	*Save $100!*
Package D.	4 Days of Training	$2300	*Save $200!*
Package E.	5 Days of Training	$2825	*Save $300!*

For maximum savings, combine Package A with Package B or C.

If you are *not* a member of USENIX, EurOpen.SE, or NUUG, add $115 to your technical sessions fees.

Late Fees
- After March 21, members and nonmembers (not students), add $150 to your technical sessions fees.
- After March 21, members and nonmembers (not students), add $150 to your training program fees.

Optional Costs
- Continuing Education Units (CEUs): $15 per training day

Full-Time Students
A limited number of tutorial seats are reserved for full-time students at the very special rate of $200 per day. Students must reserve their tutorial seats before registering; see p. 30 for more information.

Full-time students may attend technical sessions for only $90 per day. Students who are *not* members of USENIX, add $40 to your technical sessions fees.

PLEASE READ: This is *not* a registration form. Please use our online form to register or make a reservation. If you choose to make a reservation and pay later by check or credit card, you will receive a printable summary of your session selections, the cost breakdown, and the total amount due. Please submit a copy of this summary along with your payment or have it with you when you call. Tutorial bookings cannot be confirmed until payment has been received. Purchase orders, vouchers, and telephone reservations cannot be accepted.

Join leading researchers and practitioners for 6 full days of the latest in cutting-edge technology.

MEDIA SPONSORS

Addison-Wesley/Prentice Hall PTR
C/C++ Users Journal
Dr. Dobb's Journal
DSstar
GRIDtoday
Homeland Defense Journal
HPCwire
ITtoolbox
Linux Journal
No Starch Press
OSTG
Queue
SNIA
StorageNetworking.org
Sys Admin
UserFriendly.org

Register by March 21 and save! • www.usenix.org/anaheim05

USENIX

USENIX 30th ANNIVERSARY

USENIX Association
2560 Ninth St, Suite 215
Berkeley, CA 94710

Phone: 510-528-8649
Fax: 510-548-5738

www.usenix.org/anaheim05

Register with the priority code on your mailing label to receive a $25 discount!

NON-PROFIT ORGANIZATION
US POSTAGE
PAID
PERMIT #110
HOPKINS, MN