You may register online at

http://www.usenix.org/networking99/

Conference on Network Administration

Program Committee

PROGRAM CO-CHAIRS:
David Williamson, *Global Networking and Computing*
Paul Ebersman, *Vixie Enterprises*

Fuat Baran, *Columbia University*
Brent Chapman, *Covad Communications Company*
Phil Draughon, *RMS Business Systems*
Paul Ferguson, *Cisco Systems*
Jeff Jensen, *WebTV Networks, Inc.*
Bill LeFebvre, *Group sys Consulting*
Bryan McDonald, *Global Networking and Computing*
Hal Pomeranz, *Deer Run Associates*
Wade Warner, *Georgia State University*

Workshop on Intrusion Detection and Network Monitoring

Program Committee

CHAIR: Marcus J. Ranum, *Network Flight Recorder, Inc.*

Charles Antonelli, *University of Michigan*
Frederick Avolio, *Avolio Consulting*
Tina Darmohray, *SystemExperts, Corp.*
Rik Farrow, *Consultant*
Dan Geer, *CERTCO*
Norm Laudermilch, *UUNet/Worldcom*

Table of Contents

Program-at-a-Glance

1st Conference on Network Administration — NETA

Tuesday, April 6

6:00 pm – 9:00 pm	On-Site Registration
6:00 pm – 9:00 pm	Welcome Reception

Wednesday, April 7

7:30 am – 5:00 pm	On-Site Registration
9:00 am – 10:30 pm	Opening Remarks and Keynote
11:00 am – 5:30 pm	Technical Program
6:00 pm – 8:00 pm	Conference Reception
8:00 pm – 11:00 pm	Birds-of-a-Feather Sessions

Thursday, April 8

7:30 am – 5:00 pm	On-Site Registration
9:00 am – 5:30 pm	Technical Program
12:30 pm – 2:00 pm	Hosted Luncheon

Combined Tutorial Program — NETA & ID

Friday, April 9 Tutorials

7:30 am – 5:00 pm	On-Site Registration
9:00 am – 5:30 pm	Tutorial Program
12:30 pm – 2:00 pm	Tutorial Luncheon

Saturday, April 10 Tutorials

7:30 am – 5:00 pm	On-Site Registration
9:00 am – 5:30 pm	Tutorial Program
12:30 pm – 2:00 pm	Tutorial Luncheon

1st Workshop on Intrusion Detection and Network Monitoring — ID

Sunday, April 11

7:30 am – 5:00 pm	On-Site Registration
9:00 am – 10:30 pm	Opening Remarks and Keynote
11:00 am – 5:30 pm	Technical Program
6:00 pm – 8:00 pm	Reception
8:00 pm – 10:00 pm	Birds-of-a-Feather Sessions

Monday, April 12

7:30 am – 5:00 pm	On-Site Registration
9:00 am – 5:30 pm	Technical Program
12:30 pm – 2:00 pm	Hosted Luncheon

Important Dates to Remember:

Registration Savings Deadline: ***Tuesday, March 16, 1999***

Hotel Discount Deadline: ***Tuesday, March 16, 1999***

Special Co-Located USENIX Events

1st Conference on Network Administration

NETA

April 7–10, 1999, Santa Clara, California

Sponsored by USENIX and Co-Sponsored by SAGE

Dear Networker:

For the first time, the USENIX Association and SAGE, the System Administrators Guild, have convened a conference just for the professional network administration community. Join us for an opportunity to interact with fellow network administrators working in sites of all sizes. Take advantage of expertise gained by years of varied and innovative work throughout the world.

The program committee has worked hard to provide outstanding speakers selected for their expertise and experience. Please come to Santa Clara for learning, presentations, and fun.

The Conference on Network Administration (NETA) Refereed Paper sessions feature topics ranging from the latest in tools for the network manager to presentations on integrating voice and video services into a data network. The Invited Talks sessions contain something for everyone, including discussions of some of the latest network technologies and case studies of real networks. We will also have Birds-of-a-Feather sessions to help you answer all the questions you may have.

The tutorial track offers a full spectrum of courses tailored to all levels of experience and spanning a wide range of interests. Attend these two days of tutorials and take home new skill you can use immediately.

On behalf of the 1999 Conference on Network Administration Committee,

Program Co-Chairs
David Williamson,
Global Networking and Computing
Paul Ebersman,
Vixie Enterprises

1st Workshop on Intrusion Detection and Network Monitoring

ID

April 9–12, 1999, Santa Clara, California

Sponsored by USENIX, the Advanced Computing Systems Technical Association

Dear Networker:

Security is a concern for anyone who runs a network. Unfortunately, most of us don't have enough hours in the day to worry about fending off hackers instead of getting useful work done. Intrusion detection techniques and technologies offer the hope of being able to learn about attacks or misuses of the network with a minimum of human intervention. As the level of connectivity between networks increases, and the networks' vulnerability to hacking increases, intrusion detection and monitoring are going to play a more important role as we build the networks of the future.

USENIX has always served as a forum for disseminating ideas in advanced computing research and practical system management. The Workshop on Intrusion Detection and Network Monitoring is another such forum: an opportunity for those interested in this field to meet and learn from the researchers who are pushing the envelope and from the practitioners who are building the next state of the art.

Please join us in Santa Clara for a workshop that will continue the USENIX tradition of excellence, communication, and education.

On behalf of the 1999 Workshop on Intrusion Detection and Network Monitoring Committee,

Program Chair
Marcus J. Ranum,
Network Flight Recorder, Inc.

Six Days of Sharing Networking Solutions Including Two Days of Tutorials

Master the newest technology

Stay on top of the latest technology. Register now for tutorials.

Tutorial fees include
- Admission to the tutorial(s) you select
- Printed and bound tutorial materials from your session(s)
- Lunch

Technology is changing more rapidly than ever before. As a network administrator, you are expected to stay up to the minute on the latest technology and techniques, and do your job.

USENIX tutorials aim to provide the critical information you need. Delivered by experts with hands-on experience, tutorials are practical, intensive, and essential to your professional development.

Our guarantee: 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

USENIX provides Continuing Education Units (CEUs) for a small additional administrative fee. The CEU is a nationally recognized standard unit of measure for continuing education and training, and is used by thousands of organizations. Each full-day USENIX 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 credits. Consult your employer or school to determine their applicability.*

Register now to guarantee your first choice. Seating is limited.

Select From These Quality Tutorials

Each tutorial runs from 9:00 AM to 5:00 PM. Lunch is included with your tutorial fees. Please select only one per day.

Friday, April 9

F1 Configuring Cisco Routers on an IP Network
William LeFebvre, *Group sys Consulting*

F2 Intrusion Detection and Network Forensics
Marcus J. Ranum, *Network Flight Recorder, Inc.*

F3 Handling Computer and Network Security Incidents
Jim Duncan, *Penn State University,* and Rik Farrow, *Consultant*

F4 How Networks Work: The Limits of Modern Internetworking
Dr. Vincent C. Jones, *PE*

Saturday, April 10

S1 Secure Communications over Open Networks
Marcus J. Ranum, *Network Flight Recorder, Inc.*

S2 Computer Attacks: Trends and Countermeasures
Tina Darmohray, *SystemExperts, Corp.;* Phil Cox, *Networking Technology Solutions*

S3 Internet Security for UNIX System Administrators
Ed DeHart, *Pittsburgh OnLine, Inc.*

S4 Topics in Network Administration
PART 1: IP Addressing for Surviving in the Global Internet
Howard C. Berkowitz, *Network Architecture Consultant*
PART 2: Faster and Faster—Gigabit Ethernet Networks, File Servers, and Users
Stuart McRobert, *Imperial College, London*

NETA & ID Tutorial Program


William LeFebvre


Marcus J. Ranum

Friday, April 9, 1999

F1 Configuring Cisco Routers on an IP Network

William LeFebvre, *Group sys Consulting*

Who should attend: System administrators who are or anticipate being responsible for router configuration and maintenance on their Inter- or Intranet site. Attendees are expected to have a solid knowledge of general networking concepts, data encapsulation, the ISO seven-layer model, the Internet Protocols, IP addressing, and subnetting. Knowledge of routing protocols, especially distance vector versus link state, is also recommended. This class is not intended to teach networking concepts, but to apply those concepts to the configuration of a router.

Routers are the glue that holds the Internet together by providing the direct connectivity between adjacent networks. Cisco routers dominate the router marketplace, and they are an extremely popular choice among sites with high networking demands. But configuring and maintaining Cisco routers is unlike anything else in the industry. The command-oriented interface is unique and difficult to master.

This course introduces the attendees to the essentials of Cisco router configuration. After completing this course, participants will feel comfortable at a router's console and will be able to interpret output from more common router commands. They will understand the various modes of the Internetwork Operating System (IOS), and how to read and alter a basic configuration.

Topics to be covered include:

- Router modes (user, privileged, and configuration)
- Configuration file syntax
- Command-line editing
- On-line help
- Configuration statements essential to IP
- Configuring routing protocols: RIP, IGRP, EIGRP, OSPF
- Serial lines: ISDN and Frame Relay (if time permits)

The class size will not permit any hands-on work, but live demonstrations will be provided throughout the lecture. Although this class is not part of the Cisco curriculum, William is a Certified Cisco Systems Instructor.

William LeFebvre is an author, programmer, teacher, and systems administration expert. William has been using UNIX and Internet technologies since 1983 and teaching tutorials since 1989. He has written many articles on UNIX, networking and systems administration issues. Currently he is a columnist for *UNIX Review,* writing the monthly "Daemons & Dragons" column. William is also the editor for the SAGE series Short Topics in System Administration. William has contributed to several widely used UNIX packages, including Wietse Venema's logdaemon package.

F2 Intrusion Detection and Network Forensics

Marcus J. Ranum, *Network Flight Recorder, Inc.*

Who should attend: Network and system managers, security managers, and auditors. This tutorial will assume some knowledge of TCP/IP networking and client/server computing.

What can intrusion detection do for you? Intrusion detection systems are designed to alert network managers to the presence of unusual or possibly hostile events within the network. Once you've found traces of a hacker, what should you do? What kind of tools can you deploy to determine what happened, how they got in, and how to keep them out? This tutorial provides a highly technical overview of the state of intrusion detection software and the types of products that are available, as well as the basic principles to apply for building your own intrusion detection alarms. Methods of recording events during an intrusion are also covered.

Course outline:

- What is IDS?
  - Principles
  - Prior art
- Can IDS help?
  - What IDS can and can't do for you
  - IDS and the WWW
  - IDS and firewalls
  - IDS and VPNs
- Types and trends in IDS design
  - Anomaly detection
  - Misuse detection
  - Traps
  - Future avenues of research
- Concepts for building your IDS
  - What you need to know first
  - Performance issues
- Tools for building your IDS
  - Sniffers and suckers
  - Host logging tools
  - Log recorders
- Reporting and recording
  - Managing alerts
  - What to throw away
  - What to keep
- Network Forensics
  - So you've been hacked
  - Forensic tools
  - Brief overview of evidence handling
  - Who can help you
- Resources and References

Marcus J. Ranum is CEO and founder of Network Flight Recorder, Inc. He is the principal author of several major Internet firewall products, including the DEC SEAL, the TIS Gauntlet, and the TIS Internet Firewall Toolkit. Marcus has been managing UNIX systems and network security for over 13 years, including configuring and managing whitehouse.gov. Marcus is a frequent lecturer and conference speaker on computer security topics.

NETA & ID Tutorial Program

F3 Handling Computer and Network Security Incidents

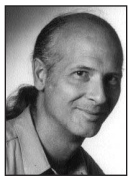
Jim Duncan, *Penn State University,* and
Rik Farrow, *Consultant*

Who should attend: System and network administrators, security staff, and their management who have responsibility for the security of networks and connected systems. Basic knowledge of modern operating systems and networking is recommended because it will help in understanding the example incidents, procedures, and countermeasures.

Are you prepared to handle a security incident at your site? Responding to computer security incidents is a requirement for any organization in which computers and networks are an important part of the infrastructure. This course provides the knowledge necessary to prepare for and handle computer and network security incidents with step-by-step information and examples from real-world incidents.

Incident handling ranges from the mundane, yet critical details of preparing your management and modifying policy to working with an incident in progress and correctly handling evidence. The instructors will explain the types of incidents and how to gain management support in building an incident response team. This course provides examples of actual incident handling and the steps involved in recovering from an incident, since incident handling impinges on all aspects of effective system administration.


Jim Duncan


Rik Farrow

You will learn about the need for comprehensive computer security incident handling capability, how to communicate that need to management and the user community, how to investigate an incident (as a handler, not as law enforcement), and how to build and maintain that capability. You will also learn how to adapt policy and the incident handling capability to each other, how to staff an incident response team, and how to establish links and communicate with other teams and law enforcement agencies. Even if you are the only person tasked with security, this tutorial will help you prepare yourself and your organization for an inevitable computer security incident.

Jim Duncan is Manager of Network and Information Systems and Principal Systems Administrator for The Pennsylvania State University's Applied Research Laboratory, a multi-disciplinary research facility for the U.S. Navy and other sponsors. He is a contributor to RFC 1244, The Site Security Policy Handbook, and has developed numerous policies, guidelines, and presentations on systems and network administration, computer security, incident handling, and ethics. He has over ten years' experience in UNIX systems.

Rik Farrow 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, US West, Canadian RCMP, Swedish Navy, and for many US and European user groups. He is the author of UNIX System Security and System Administrator's Guide to System V. Farrow writes columns for *;login:* and *Network Magazine.*

WANTED: Ideas, Papers, Authors

LISA '99
13th System Administration Conference

November 7–12, 1999
Seattle Convention Center, Seattle, WA

Sponsored by USENIX, and co-sponsored by SAGE

Be a part of LISA and play a role in shaping the program.

See the call for Papers at:
http://www.usenix.org/events/lisa99/
Deadline for submissions: May 25, 1999.

Send inquiries to:

Program Chair:
David Parter, *University of Wisconsin*
lisa99chair@usenix.org

Invited Talks Coordinators:
Phil Scarr, *Global Networking and Computer, Inc.;*
Jennifer Katinsky, *Silicon Graphics, Inc.*
itlisa@usenix.org

LISA'99 is put together by a volunteer committee of experienced sys admins. The Program Committee welcomes your submissions by May 25, 1999.

NETA & ID Tutorial Program

Marcus J. Ranum

F4 How Networks Work: The Limits of Modern Internetworking

Dr. Vincent C. Jones, *PE*

Who should attend: This tutorial is targeted at those technical individuals, regardless of title, who are responsible for the design and upkeep of extended LAN and LAN/WAN networks supporting multiple protocol architectures. A working knowledge of TCP/IP, Ethernet, and the OSI reference model is assumed.

This tutorial explores the theoretical underpinnings of modern network technology, probing the current limits of performance and distinguishing between those limits which are fundamental and those which are temporary. Along the way, we'll separate the hype from the reality on a wide range of critical technologies, from cell relay (ATM) and virtual LANs to IPv6 and link state routing.

The bottom line is that every networking protocol and technology is a compromise among competing needs and the better you understand the underlying theory, the better able you are to make appropriate choices that best meet the needs of your users and their applications.

Among the many topics we'll address are:

- Speed and distance limits of twisted-pair and fiber-optic cable
- Switching versus bridging and routing
- What is wrong with RIP and why is it so popular regardless
- Topology considerations in OSPF routed networks
- Common pitfalls when adding redundancy
- Why some protocols, such as NFS and NetWare, are particularly challenging when moving from a LAN to a LAN/WAN enterprise network (and how to make them behave)

The focus at all times is on practical knowledge—how the theory applies to real world networks. But rather than just presenting rules of thumb, we will delve into the theory behind the rules so you can understand which rules must be strictly obeyed and which can be safely stretched.

Vincent C. Jones is an independent consultant providing advice on network planning, design, and analysis to business and government clients. Specializing in the design, analysis and management of integrated local and wide area networks for cooperative, distributed processing in multivendor environments, Dr. Jones has over twenty-five years of experience finding practical, cost-effective solutions to complex networking issues.

Saturday, April 10, 1999

S1 Secure Communications over Open Networks

Marcus J. Ranum, *Network Flight Recorder, Inc.*

Who should attend: Programmers, network managers, and individuals who need to develop or deploy secure communication systems. Some experience with TCP/IP and UNIX is assumed.

People increasingly rely on electronic communications as a daily part of their private lives. Corporations rely on Internet services as essential tools for their business. At the same time, many of the tools being used lack even basic protections against snooping and tampering. To make matters more interesting, governments are becoming concerned that civilian use of secure communications may threaten national security, and are pushing for various degrees of regulation.

This tutorial is intended to teach the experienced network and system manager how to build and deploy a wide range of secure communication tools. Tools are discussed within the overall context of communication security and appropriateness. Topics will range from the highly paranoid, including basic spycraft and covert channels, to the practical, such as building your own VPN router or operating PGP. We will cover actual configurations, set-up procedures, and command lines for software packages on BSD UNIX. Debugging and verifying operation will also be discussed.

Topics include:

- The communications security environment
- Covert operations: introductory spycraft
- Absolute security: one-time-pads
- DES encryption
- Mail security: PGP
- Hiding communications: steganography
- Virtual Private Networks: using SSH and IPSEC
- Privacy: anonymous remailers, anonymizer servers, and crowds
- Up and coming technologies
- The regulatory environment
- Where to get crypto-munitions

Marcus J. Ranum is CEO and founder of Network Flight Recorder, Inc. He is the principal author of several major Internet firewall products, including the DEC SEAL, the TIS Gauntlet, and the TIS Internet Firewall Toolkit. Marcus has been managing UNIX systems and network security for over 13 years, including configuring and managing whitehouse.gov. Marcus is a frequent lecturer and conference speaker on computer security topics.

NETA & ID Tutorial Program


Phil Cox


Tina Darmohray


Ed DeHart

S2 Computer Attacks: Trends and Countermeasures

Tina Darmohray, *SystemExperts, Corp.;*
Phil Cox, *Networking Technology Solutions*

Who should attend: System and network administrators who implement or maintain networks and site managers charged with selecting and setting site security requirements. Familiarity with TCP/IP networking is a plus.

Many classic security problems, such as perimeter and host security, have become well defined and are routinely addressed by a wide range of product offerings; however, computer and network attacks are still on the rise. Effectively combating these attacks is a network and security management discipline with emerging strategies and solutions. This tutorial will cover the latest trends in computer attacks and the security precautions you can take against them, including defensive penetration analysis, host auditing, network logging solutions, and intrusion detection.

After this tutorial, attendees will understand the important areas of security management. They will be able to defensively assess their system and network security. Additionally they will have an appreciation for auditing and monitoring hosts and networks for intrusions and storing critical information required for network forensics.

Topics include:

- Trends in computer attacks
- Defensive penetration analysis
- Host and network auditing tools
- Intrusion detection
- Network forensics
- Ethics, policies, and legal concerns of auditing computer communications

Phil Cox is a consultant for Networking Technology Solutions, and is a member of a government incident response team. Phil frequently writes and lectures on issues bridging the gap between UNIX and Windows NT. He is a featured columnist in *;login:* and is on this year's LISA Conference program committee.

Tina Darmohray is a network and security consultant with over a decade of experience in administration and programming of UNIX/TCP-based computers. She specializes in firewalls, Internet connections, Sendmail/DNS configurations and defensive intrusion management. Previously she was the lead for the UNIX support team at Lawrence Livermore National Laboratory. Tina was a founding board member of the System Administrators Guild, SAGE. She is also the editor of the popular SAGE short topics booklet Job Descriptions for System Administrators, editor of "SAGE News and Features" for *;login:,* and co-chair of the USENIX LISA IX Conference.

S3 Internet Security for UNIX System Administrators

Ed DeHart, *Pittsburgh OnLine, Inc.*

Who should attend: UNIX system administrators, network managers, operations and support staff. You should have a good working knowledge of UNIX system administration, and be an experienced Internet user.

In this tutorial you will learn strategies and techniques to help eliminate the threat of Internet intrusions and to improve the security of UNIX systems connected to the Internet.

This tutorial will also help you understand, set up, and manage a number of Internet services appropriate to your site's mission.

At the end of the day, you will be able to establish and maintain a secure Internet site that allows the benefits of Internet connectivity while protecting the organization's information.

Topics will include:

- Latest information on security problems
- UNIX system security
- TCP/IP network security
- Site security policies

Ed DeHart is a former member of the CERT Coordination Center, which he helped found in 1988. The CERT was formed by the Defense Advanced Research Projects Agency (DARPA) to serve as a focal point for the computer security concerns of Internet users. Today, Ed is the president of Pittsburgh OnLine, Inc., an ISP that operates several UNIX servers.

S4 Topics in Network Administration

Part 1: IP Addressing for Surviving in the Global Internet

Howard C. Berkowitz, *Network Architecture Consultant*

(Sorry: Part 1 & 2 are not sold individually)

Who should attend: Planners and network administrators who have set up IP addresses and subnets for private networks, but now have to operate on the Internet, connecting to it with users, Internet Service Providers, and application servers potentially at different sites. Students should be proficient with basic IP addressing and subnetting, probably using class A/B/C structures, and should have a general sense of CIDR addressing. Suggested pre-tutorial reading will be available.

The Internet's success has been one of its biggest problems, as techniques originally developed for a small research network have been inadequate for today's demands. To maintain backwards compatibility, many hacks to the original technology have been needed, in no area more than routing and addressing.

NETA & ID Tutorial Program

Howard C. Berkowitz

Stuart McRobert

This course identifies a wide range of techniques introduced to scale the Internet, and which need to be considered by network planners and administrators who want to work in the Internet environment. The course will begin with guidelines for systematic problem analysis to determine the application-level justification for address space and advanced connectivity, such as "multihoming." We will move into a quick review of the notation for modern addressing, and then review some of the issues of using traditional class A/B/C issues in a modern classless network—and workarounds for some of the problems, including tunneling and virtual private network methods. Roles and limitations of network address translators and proxies will also be identified. Additional addressing and naming considerations necessary to operate in the global Internet will then be reviewed, including autonomous system numbers and IP address aggregation. The course concludes with guidance about preparing the justifications for obtaining address space, and for internally administering your address space.

Howard C. Berkowitz has been helping computers talk to people and people talk to computers, occasionally muttering to computers himself, since 1969. He built networks before we knew to call them networks, and now deals with mission-critical and Internet routing involving thousands of routers. An active participant in the Internet Engineering Task Force (IETF), he authored or coauthored several RFCs on addressing, including RFC2072, "Router Renumbering Guide." He recently published the book *Designing Address Architectures for Routing and Switching,* and will have another out shortly, *Designing Routing and Switching Architectures for Enterprise Networks.* Active in the North American Network Operators' Group (NANOG), he has given several talks on operationally critical aspects of addressing.

Part 2: Faster and Faster—Gigabit Ethernet Networks, File Servers, and Users

Stuart McRobert, *Imperial College, London*

Who should attend: System and network administrators responsible for designing or upgrading computer networks and file servers supporting a wide variety of applications, along with managers seeking a better understanding of this rapidly advancing technology.

With the increasing speed of CPUs and rising numbers of desktop and laptop systems fully utilizing Fast Ethernet bandwidth, many network backbones and central servers have been left behind with yesteryear's technology. Although the need to upgrade is often well understood, just where do you begin?

This tutorial is intended for people facing just such a challenge and looks at two key areas, high performance networking with Gigabit Ethernet (1000 Mbps) and faster file serving. By the end of this tutorial you should have a sound understanding of both Gigabit Ethernet and ways of providing high performance fileserving for various applications.

Key topics include:

- Faster Networking
  - Gigabit Ethernet: What is it? How does it work? The standards
  - Hardware: Fiber Channel, media types, link lengths
  - 802.3x full/half duplex links, flow control
  - 802.1p, 802.1Q Virtual LANs (VLANs), Tagging
  - Wire speed switching and hardware IP routing
  - Product examples, Extreme Networks
  - Packet filtering
  - Trunking or link aggregation
  - Quality of service, management issues
- Faster File Servers
  - UNIX and Veritas File Systems, logging
  - File server platforms, disks, I/O requirements
  - RAID: levels, performance issues, hardware vs. software, system management
  - Volume Managers, Sun Solstice DiskSuite and Veritas
  - Fault tolerance: fail-over, backups, storage replication, HSM

Stuart McRobert is the Network Systems analyst in the Department of Computing at Imperial College in London, where he has recently designed and installed a multi-Gigabit Ethernet backbone, and along with his colleagues manages SunSITE Northern Europe, a 300+GB mirror archive. Stuart has spoken at several USENIX conferences and user group meetings in the USA, Australia, and Europe.

Wednesday, April 7, 1999

9:00am – 10:30am Opening Session

Opening Remarks & Awards
Paul Ebersman and David Williamson, *Program Co-Chairs*

Keynote Address
Norm Schryer, *AT&T Research Labs*

"Home, Road and Work Have Merged Via the Internet"

Folks work all the time, everywhere: at home, on the road and at work. The network is everywhere, both wired and wireless. Provisioning, operating and maintaining such distributed systems opens new universes of services and disasters.

EXAMPLES: Folks listen to music over the data network and don't want it disturbed; if your VPN/IPSEC vendor flunks certificate handling then folks at home and on the road are dead—and so are you.

Standards, interoperability and vendor management are the keys to success and continued survival. Norm's talk will cover the modern world's neat functionality, distributed responsibility and central fragility.

NORM SCHRYER received a Ph.D. in Mathematics from the University of Michigan in 1969 and then joined the Computing Science Research Center of AT&T Bell Laboratories. In 1996, at the AT&T/Lucent/NCR trivestiture, he moved to AT&T Labs Research, where he is presently Division Manager of Broadband Services Research: cable modem and optical fiber links to homes and the wireless remote piloting of vehicles/telepresences.

10:30am – 11:00am Break

11:00am – 12:30pm Monitoring and Video

Session Chair: Jeff Jensen, *WebTV Networks, Inc.*

Driving via the Rearview Mirror: Managing a Network with Super MRTG
Jeff Allen, *WebTV Networks, Inc.*

Don't Just Talk About the Weather—Manage It! A System for Measuring, Monitoring, and Managing Internet Performance and Connectivity
Cindy Bickerstaff, Ken True, Charles Smothers, Tod Oace, Jeff Sedayao, *Intel Corporation;* and Clinton Wong, *@Home Networks*

Supporting H.323 Video and Voice in an Enterprise Network
Randal Abler and Gail Wells, *Georgia Institute of Technology*

12:30pm – 2:00pm Lunch (on your own)

2:00pm – 3:30pm Configuration Management and Security

Session Chair: William LeFebvre, *Group sys Consulting*

Network Documentation: A Web-Based Relational Database Approach
Wade Warner and Rajshekhar Sunderraman, *Georgia State University*

Just Type Make! Managing Internet Firewalls, Including Router Access Control Lists, Sendmail Configurations, DNS Databases, and OS Upgrades, Using Make and Other Publicly Available Utilities
Sally Hambridge, Charles Smothers, Tod Oace, and Jeff Sedayao, *Intel Corporation*

Tricks You Can Do If Your Firewall Is a Bridge
Thomas A. Limoncelli, *Lucent Technologies*

3:30pm – 4:00pm **Break**

4:00pm – 5:30pm

New Challenges and Dangers for the DNS

Jim Reid, *Origin b.v.*

New and probably unavoidable developments including IPv6, Secure DNS, SRV records and dynamic updates are soon going to have a major impact on DNS administration. Each of these developments poses its own set of problems. Jim will describe these challenges and examine likely solutions and strategies for dealing with them.

8:00pm – 11:00pm **Birds-of-a-Feather Sessions**

Thursday, April 8, 1999

9:00am – 10:30am

Problems with World-Wide Networking

Holly Brackett Pease, *Digital Isle*

Administering a worldwide network presents unique routing and logistics problems. Routing policies set by some country's Internet exchanges, by Tier-1 ISPs, and by in-country providers can sometimes be arbitrary and impossible to predict. In this talk Holly will discuss these policies and offer suggestions for navigating them. She will also cover some less-than-glamorous logistics problems presented by the nature of a global network such as: government carriers, interface standards, and taxes.

The Little NIC That Could

Christopher J. Wargaski, *RMS Business Systems*

Usually the creation and operation of a Network Information Center (NIC) is a costly endeavor requiring vast personnel and equipment resources. This can be a difficult task, especially in a large politically charged environment undertaking cost-cutting measures. Using another model, however, a NIC can be created and run in an efficient manner using only a modest amount of new hardware and software resources, and without additional personnel resources.

10:30am – 11:00am **Break**

11:00am – 12:30pm

Splitting IP Networks: The 1999 Update

Thomas Limoncelli, *Lucent Technologies*

Thomas Limoncelli will discuss techniques for renumbering and splitting IP networks. These techniques were perfected when splitting AT&T's Bell Labs networks in Holmdel, NJ during the AT&T/Lucent split. Renumbering isn't fun, but it is more common every day. He will focus on their trials and tribulations but emphasize techniques that can be used anywhere. Find out what has been learned since the original presentation at LISA '97.

Network Management on the Cheap

Rob Wargaski, *RMS Business Systems*

This presentation discusses the need and utility of a network management system, and recognizes that many organizations are not willing (for a variety of reasons) to invest in one of the "big" systems. Useful tools can be freely obtained, and run on a Linux system. Rob will describe some tactical and strategic tools and show how they can be used to improve the health of a network.

12:30pm – 2:00pm **Hosted Luncheon**

2:00pm – 3:30pm

Evolution of VLAN/ELAN Architecture at Vanderbilt University

John Brassil, *Vanderbilt University*

John Brassil will examine the design and implementation of VLAN architecture at Vanderbilt University that began as part of the Backbone Reengineering Project (1995-98) and the subsequent changes to that design. Since the backbone is ATM-based and edge networks are Ethernet LANs, the parallel Emulated LAN (ELAN) architecture and its evolution will also be described.

The talk is intended primarily as a case study of VLAN/ELAN implementation in a large university or corporate environment. It will describe the factors which influence design decisions, and the tradeoffs/pitfalls that accompany a particular choice. Design considerations for an MPOA (Multi-Protocol Over ATM) architecture will also be discussed.

Interoperable Virtual Private Networks (VPNs), Directory Services, and Security

Eric Greenberg, *Seine Dynamics*

In order to achieve an organization's network application performance and functional objectives, and make for more manageable and effective deployments, an integrated "Network Application Framework" design approach must be taken. Eric Greenberg will address key areas of framework integration: Virtual Private Networks (VPN) including IPSEC, PPTP, and L2TP; Directory Services including LDAP, NDS, and X.500; Single sign-on and network/application security services including Certificates, Kerberos, and SSL/TLS; and integration of disparate networking architectures including TCP/IP, IBM SNA, and NetWare.

3:30pm – 4:00pm **Break**

4:00pm – 5:30pm **Closing Session**

Internet Measurements

Evi Nemeth, *University of Colorado, Boulder;* k. claffy, *Cooperative Association for Internet Data Analysis at the San Diego Supercomputer Center, UCSD*

MCI and CAIDA (Cooperative Association for Internet Data Analysis) have dedicated passive measurement boxes (OXcMONS's) on the MCI backbone and at key exchange points. This talk will summarize the data seen on these networks including protocol distributions, packet sizes, flow characteristics, network and AS matrices, etc. We will also present data from an active measurement tool, skitter, that has been used to probe the Internet at about 30,000 key server hosts. Attendees will get a feel for the traffic on the Internet and changes in that traffic over the last couple of years.

Sunday, April 11, 1999

9:00am – 10:30am

Opening Remarks

Marcus Ranum, *Program Chair*

Keynote Address

Peter G. Neumann, Principal Scientist
Computer Science Laboratory, SRI International

Challenges for Anomaly and Misuse Detection

The field somewhat mistakenly called "intrusion detection" needs to broaden its scope of endeavor in various respects, and overcome some of the characteristic difficulties that have slowed its progress. This talk will address several such approaches:

- Generalizing the domains of detectability to include other aspects such as reliability, survivability, and financial stability
- Providing unprecedented flexibility and interoperability among different analysis systems
- Integrating with other computer-communication technologies such as heterogeneous network management and the Web
- Incorporating robust tamperproofing and modern software engineering into future systems for analysis and response
- Enabling sound dynamic reconfigurability based on analysis results
- Research directions
- The need for robust open-source systems and ongoing testbed environments
- Greater forcing functions needed on developers of operating system components and applications.

Peter G. Neumann has worked on survivability since the mid-1950s, on system security starting with Multics in 1965, on intrusion detection since 1983, and on reliability, safety and risks more recently. He is author of the Addison-Wesley book Computer-Related Risks *and moderates the RISKS Forum newsgroup (comp.risks). He also is a Fellow of ACM, IEEE, and AAAS. He holds a 1961 PhD from Harvard and a 1960 Dr. rerum naturarum Technische Hochschule from Darmstadt. See his Web site at* http://www.csl.sri.com/neumann/ *for Congressional testimonies, RISKS information, and further background.*

10:30am – 11:00am **Break**

11:00am - 12:30am

Analysis and Large Networks

Session Chair: Fred Avolio, *Avolio Consulting*

Analysis Techniques for Detecting Coordinated Attacks and Probes
Tim Aldrich, Stephen Northcutt, Bill Ralph, *Naval Surface Warfare Center Dahlgren Division*

Intrusion Detection and Intrusion Prevention on a Large Network: A Case Study
Tom Dunigan, Greg Hinkel, *Oak Ridge National Laboratory*

An Eye on Network Intruder-Administrator Shootouts
Luc Girardin, *UBS, Ubilab*

12:30pm – 2:00pm **Lunch (on your own)**

2:00pm – 3:30pm **Invited Talks**

Session Chair: Marcus Ranum, *Network Flight Recorder, Inc.*

Why Monitoring Mobile Code Is Harder Than It Sounds

Gary McGraw, *Reliable Software Technologies*

Mobile code is code that traverses a network during its lifetime and is able to execute at the destination machine. The idea behind mobile code is actually quite simple—sending around data that can be automatically executed wherever it arrives, anywhere on the network. The problem is this: running someone else's code on your computer is a risky activity. Who is to say what the code might try to do and whether or not its activities will be malicious? This is not a new problem by any stretch of the imagination. In fact, it's really an old problem with a new twist. There are many well-known systems for creating and using mobile code. From a security perspective, Java clearly leads the pack. Monitoring mobile code presents some interesting challenges. First and foremost is the problem of identifying mobile code before it runs. Naive approaches, which include scanning port 80 traffic for the <APPLET> tag, are known not to work. Another problem is determining which resources mobile code should and should not be allowed to access, and making sure the policy is enforced. Complex policy-oriented systems like JDK 1.2 (based on code signing and access control lists) may actually make things harder.

3:30pm – 4:00pm **Break**

4:00pm – 5:30pm **Software and Processes**

Session Chair: Tina Darmohray, *SystemExperts, Corp.*

On Preventing Intrusions by Process Behavior Monitoring
R. Sekar, *Iowa State University;* Thomas Bowen, Mark Seagal, *Bellcore*

Intrusion Detection Through Dynamic Software Measurement
Sebastian Elbaum, John C. Munson, *University of Idaho*

Learning Program Behavior Profiles for Intrusion Detection
Anup Ghosh, Aaron Schwartzbard, Michael Schatz, *Reliable Software Technologies*

7:00pm – 9:00pm **Birds-of-a-Feather Sessions (BoFs)**

Do you have a topic that you'd like to discuss with others? Our Birds-of-a-Feather sessions may be perfect for you. BoFs are very interactive and informal gatherings for attendees interested in a particular topic. BoFs may be scheduled in advance or on-site at the symposium. Schedule your BoF in advance by telephoning the USENIX Conference Office at 1.949.588.8649, or sending email to: *conference@usenix.org*

Monday, April 12, 1999

9:00am – 10:30am **IDS Systems**

Session Chair: Charles Antonelli, *University of Michigan*

Automated Intrusion Detection Methods Using NFR
Wenke Lee, Christopher Park, Salvatore J. Stolfo, *Columbia University*

Experience with EMERALD Thus Far
Phillip A. Porras, Peter G. Neumann, Teresa Lunt, *SRI International*

Defending Against the Wily Surfer—Web-Based Attacks and Defenses
Dan Klein, *LoneWolf Systems*

10:30am – 11:00am **Break**

11:00am – 12:30pm **Network Data Processing and Storage**

Session Chair: Dan Geer, *CERTCO*

Preprocessor Algorithm for Network Management Codebook
Minaxi Gupta, Mani Subramanian, *Georgia Institute of Technology*

The Packet Vault: Secure Storage of Network Data
Charles J. Antonelli, Matthew Undy, Peter Honeyman, *Center for Information Technology Integration, University of Michigan*

Real-Time Intrusion Detection and Suppression in ATM Networks
Ricardo Bettati, Wei Zhao, Dan Teodor, *Texas A&M University*

12:30pm – 2:00pm **Hosted Luncheon**

2:00pm – 3:30pm **Invited Talks**

Session Chair: Norm Laudermilch, *UUNet/Worldcom*

Design and Integration Principles for Large-Scale Infrastructure Protection
Edward Amoroso, *AT&T*

Basic intrusion detection design and integration principles are outlined for practical large-scale infrastructure protection schemes. Issues in the development of middleware for multi-vendor interoperability, algorithms for high-volume alarm processing, and visualization techniques for intrusion display are included.

Experiences Learned from Bro
Vern Paxson, *Network Research Group, Lawrence Berkeley National Labs*

Bro is a system for detecting network intruders in realtime by passively monitoring a network link. Its design emphasizes high-speed (FDDI-rate) monitoring, real-time notification, clear separation between mechanism and policy, and extensibility. To achieve these ends, Bro is divided into an "event engine" that reduces a kernel-filtered network traffic stream into a series of higher-level events, and a "policy script interpreter" that interprets event handlers written in a specialized language used to express a site's security policy. Bro has been in production use since early 1996. We discuss the structure of the system and the lessons learned from our experiences, with an emphasis on some of the key challenges for future intrusion detection systems.

3:30pm – 4:00pm **Break**

4:00pm – 5:00pm **Statistics and Anomalies**

Session Chair: Marcus Ranum, *Network Flight Recorder, Inc.*

A Statistical Method for Profiling Network Traffic
David Marchette, *Naval Surface Warfare Center, Dahlgren Division*

Transaction-Based Anomaly Detection
Roland Buschkes, Mark Borning, *Aachen University of Technology*

5:00pm - 5:30pm **Works-in-Progress Reports (WIPs)**

Session Chair: Marcus Ranum, *Network Flight Recorder, Inc.*

Do you have interesting work you would like to share, or a cool idea that is not yet ready to be published? The USENIX audience provides valuable discussion and feedback. Short, pithy, and fun, Works-in-Progress Reports (WIPs) introduce interesting new or ongoing work. We are particularly interested in presentation of student work. Prospective speakers should send a short one- or two-paragraph report, to *idwips@usenix.org.*

A schedule of presentations will be posted at the conference and the speakers will be notified in advance. Works-in-Progress Reports are five-minute presentations; the time limit will be strictly enforced.

USENIX & SAGE Membership Information and Events

About USENIX

Since 1975, the USENIX Association has brought together the community of engineers, system administrators, scientists, and technicians working on the cutting edge of computing. USENIX and its members are engaged in problem-solving, in innovation, and in research that works.

USENIX conferences are the essential meeting grounds for the presentation and discussion of the newest information on the technical developments in computing.

USENIX and its members are dedicated to:

- Problem-solving with a practical bias
- Fostering innovation that works
- Communicating rapidly the results of both research and innovation
- Providing a neutral forum for the exercise of critical thought and the airing of technical issues

USENIX Website: *www.usenix.org*

About SAGE

SAGE, the System Administrators Guild, is the largest membership society for system managers and is dedicated to the advancement and recognition of system administration as a profession. SAGE is a special technical group within USENIX. To join SAGE, you must be a member of USENIX.

SAGE Website: *www.usenix.org/sage/*

The USENIX Association
2560 Ninth Street, Suite 215
Berkeley, CA 94710
Phone: 1.510.528.8649
Fax: 1.510.548.5738
Email: *office@usenix.org*
Web: *http://www.usenix.org/*

Upcoming USENIX Events

5th Conference on Object-Oriented Technologies and Systems (COOTS)
May 3–7, 1999, San Diego, CA
http://www.usenix.org/events/coots99/

USENIX Workshop on SmartCard Technology
May 10–11, 1999, Chicago, IL
http://www.usenix.org/events/smartcard99/

USENIX Annual Technical Conference
June 6–11, 1999, Monterey, CA
http://www.usenix.org/events/usenix99/

3rd USENIX Windows NT Symposium
July 12–14, 1999, Seattle, WA
Paper submissions due: February 23, 1999
http://www.usenix.org/events/usenix-nt99/

2nd Large Installation System Administration of Windows NT Conference (LISA-NT)
Sponsored by USENIX, Co-sponsored by SAGE
July 14–16, 1999, Seattle, WA
Paper submissions due: February 23, 1999
http://www.usenix.org/events/lisa-nt99/

8th USENIX Security Symposium
Sponsored by USENIX in cooperation with The CERT Coordination Center
August 23–26, 1999, Washington, D.C.
Paper submissions due: March 9, 1999
http://www.usenix.org/events/sec99/

2nd Conference on Domain-Specific Languages
Sponsored by USENIX in cooperation with ACM SIGPLAN and SIGSOFT
October 3–6, 1999, Austin, TX
Paper submissions due: March 22, 1999
http://www.usenix.org/events/dsl99/

2nd USENIX Symposium on Internet Technologies and Systems (USITS)
Sponsored by USENIX, Co-Sponsored by IEEE Computer Society Task Force on Internetworking
October 11–14, 1999, Boulder, CO
Extended abstracts due: April 15, 1999
http://www.usenix.org/events/usits99/

13th Systems Administration Conference (LISA '99)
Sponsored by USENIX and SAGE
November 7–12, 1999, Seattle, WA
Paper submissions due: May 25, 1999
http://www.usenix.org/events/lisa99/

7th Tcl/Tk Conference
February 14–18, 2000, Austin, TX
http://www.usenix.org/events/tcl00/

USENIX Annual Technical Conference
June 19–23, 2000, San Diego, CA
http://www.usenix.org/events/usenix00/

9th USENIX Security Symposium
August 14–17, 2000, Denver, CO
http://www.usenix.org/events/sec00/

4th Symposium on Operating Systems Design & Implementation
November 2000, San Diego, CA
http://www.usenix.org/events/osdi00/

USENIX AND SAGE THANK THEIR SUPPORTING MEMBERS

USENIX Supporting Members: Apunix Computer Services • Auspex Systems, Inc. • Cirrus Technologies • CISCO Systems, Inc. • Compaq Computer Corporation • CyberSource Corporation • Deer Run Associates • Earthlink Network, Inc • Hewlett-Packard India Software Operation • Internet Security Systems, Inc. • Lucent Technologies, Bell Labs • Microsoft Research • Neosoft, Inc. • New Rider Press • Nimrod AS • O'Reilly & Associates • Performance Computing • Questra Consulting • Sendmail, Inc. • TeamQuest Corporation • UUNET Technologies, Inc. • Windows NT Systems Magazine • WITSEC, Inc.

SAGE Supporting Members: Atlantic Systems Group • Collective Technologies • Compaq Computer Corporation • Deer Run Associates • D.E. Shaw & Co. • ESM Services, Inc. • Global Networking & Computing Inc. • Microsoft Research • New Riders Press • O'Reilly & Associates • Remedy Corporation • SysAdmin Magazine • Taos Mountain • Transquest Technologies, Inc. • Unix Guru Universe (UGU)

Thank you

Hotel and Travel Information

Hotel Discount Reservation Deadline:

Tuesday, March 16, 1999

USENIX has negotiated special rates for conference attendees at the Santa Clara Marriott Hotel. Contact the hotel directly to make your reservation. Please mention USENIX to get our special group rate. A one-night's room deposit must be guaranteed on a major credit card. To cancel your reservation, you must notify the hotel at least 24 hours before your planned arrival date.

Santa Clara Marriott Hotel
2700 Mission College Blvd.
Santa Clara, CA 95052
Toll Free: 1.800.228.9290
Local Phone: 1.408.988.1500
Reservation Fax: 1.408.567-0391

Single/Double Occupancy $169.00
(*Plus local tax, currently 9.5%)*

PARKING Self-parking is complimentary.

Discount Airfares

Special airline discounts will be available for USENIX attendees. Please call for details:

JNR, Inc.
Toll Free: 1.800.343.4546 (USA and Canada)
Telephone: 1.949.476.2788

Airport-to-Hotel Transportation

The San Jose International Airport is 5 miles from the Santa Clara Marriott. Taxi service is approximately $13 one way. Shuttle service is not available.

The San Francisco International Airport is approximately 33 miles from the Santa Clara Marriott. V.I.P. Shuttle offers van transportation to the Santa Clara Marriott. Reservations are required at least 24 hr. in advance. Call 1.408.577.1800 to make arrangements. Current shuttle cost is $24 one way. If you are renting a car, take Highway 101 South approximately 33 miles. Exit at Great America Parkway, turning right. Take right turn on Mission College Blvd. to hotel.

Activities & Services

QUESTIONS?

USENIX Conference Office
22672 Lambert Street, Suite 613
Lake Forest, CA 92630
Phone: 1.949.588.8649
Fax: 1.949.588.9706
Email: *conference@usenix.org*
URL: *http://www.usenix.org*
Office hours:
8:30 am – 5:00 pm Pacific Time

Conference Proceedings

One copy of the proceedings is included with your Technical Sessions registration fee. To order additional copies, contact the USENIX Association at 1.510.528.8649, or send email to *office@usenix.org*

Birds-of-a-Feather Sessions (BoFs)

Wednesday and Sunday evenings

Do you have a topic that you'd like to discuss with others? Our Birds-of-a-Feather sessions may be perfect for you. BoFs are very interactive and informal gatherings for attendees interested in a particular topic. Schedule your BoF in advance by telephoning the USENIX Conference Office at 1.949.588.8649, or email to *conference@usenix.org*

BoFs may also be scheduled on-site and will be announced at the conference.

Social Activities

Meet the conference speakers and connect with your peers in the community.

Conference on Network Administration

Tuesday
6:00 pm – 9:00 pm Welcome Reception

Wednesday
6:00 pm – 8:00 pm Conference Reception
8:00 pm – 11:00 pm Birds-of-a-Feather Sessions

Thursday
12:30 pm – 2:00 pm Hosted Luncheon

Workshop on Intrusion Detection and Networking Monitoring

Sunday
6:00 pm – 8:00 pm Conference Reception
8:00 pm – 10:00 pm Birds-of-a-Feather Sessions

Monday
12:30 pm – 2:00 pm Hosted Luncheon

Registration Information and Fees

Early Registration Discount Deadline:

Tuesday, March 16, 1999

NON-MEMBERS

If attending both Technical Sessions, pay non-member fee for the Conference on Network Administration and check the membership box. Then pay the member fee for the Workshop on Intrusion Detection and Network Monitoring. You save on the second registration and become a USENIX member.

Pay an additional $30 to also join SAGE.

1st Conference on Network Administration

Technical Sessions Fees (April 7–8, 1999)

Technical Sessions registration fees include:

- Admission to all NETA Technical Sessions
- Copy of Conference Proceedings
- Admission to the NETA Conference Functions

Early registration fee (until March 16, 1999)

Member*	$360
Non-member or Renewing Member**	$440
Full-time student	$ 75
(Must provide copy of current student I.D. Card)	

After March 16, add $50 to the Technical Sessions fee.

** The member fee applies to current members of USENIX, ACM, IEEE, EurOpen National Groups, JUS or AUUG*

*** Join USENIX or renew your membership at no additional charge. Pay the non-member technical sessions fee and check the USENIX membership box on the registration form and your existing membership will be renewed or you will receive a new one-year individual association membership.*

Tutorial Fees (April 9–10, 1999)

Tutorial registration fees include:

- Admission to the tutorial(s) you select
- Printed and bound tutorial materials for selected session(s)
- Lunch on the day(s) of your tutorial(s)

Early registration fee (until March 16, 1999)

Tutorial Program for one day	$395
CEU credit (optional)	$ 15
Tutorial Program for two days	$690
CEU credit (optional)	$ 30

After March 16, add $50 to the tutorial fee.

1st Workshop on Intrusion Detection and Network Monitoring

Technical Sessions Fees (April 11–12, 1999)

Technical Sessions registration fees include:

- Admission to all ID Technical Sessions
- Copy of Conference Proceedings
- Admission to the ID Conference Functions

Early registration fee (until March 16, 1999)

Member*	$360
Non-member or Renewing Member**	$440
Full-time student	$ 75
(Must provide copy of current student I.D. Card)	

After March 16, add $50 to the Technical Sessions fee.

** The member fee applies to current members of USENIX, ACM, IEEE, EurOpen National Groups, JUS or AUUG*

*** Join USENIX or renew your membership at no additional charge. Pay the non-member technical sessions fee and check the USENIX membership box on the registration form and your existing membership will be renewed or you will receive a new one-year individual association membership.*

REFUND/CANCELLATION POLICY

If you must cancel, all refund requests must be in writing and postmarked no later than March 29, 1999. Telephone/email cancellations cannot be accepted. You may substitute another in your place. Contact the Conference Office for details.

Payment

Payment by check or credit card MUST accompany the registration form. Purchase orders, vouchers and telephone reservations cannot be accepted.

Student Stipends and Discounts

Technical Sessions: USENIX offers a special discount rate of $75 for its technical sessions for full-time students. You must include a copy of your current student I.D. card with your registration. This special fee is not transferable. A separate fee is requested for NETA and ID.

Student Stipends: A limited number of student stipends are available to pay for travel, living expenses, and registration fees to enable full-time students to attend the conference. To apply for a stipend, read ***comp.org.usenix*** 6 to 8 weeks before the conference, visit our Web site, ***www.usenix.org/students/*** or email ***students@usenix.org*** for more information.

Copy this form as needed. Type or print clearly.

Registration Form 1st NETA Conference / ID Workshop, April 7–12, 1999

The address you provide will be used for all future USENIX mailings unless you notify us in writing.

Name First Last

First Name for Badge Member Number

Company / Institution

Mail Stop Mail Address

City State Zip Country

( ) ( )

Telephone No. Fax

Email Address (1 only please) **A B U V W X**

Attendee Profile

Please help us meet you needs by answering the following questions. All information is confidential.

❑ *I do not want to be on the Attendee list.*
❑ *I do not want my address made available except for USENIX mailings.*
❑ *I do not want USENIX to email me notices of Association activities.*

What is your affiliation (check one):
❑ academic ❑ commercial ❑ gov't ❑ R&D

What is your role in the purchase decision (check one):
1. ❑ final **2.** ❑ specify **3.** ❑ recommend **4.** ❑ influence **5.** ❑ no role

What is your primary job function (check one):
1. ❑ system/network administrator **2.** ❑ consultant **3.** ❑ academic/researcher
4. ❑ developer/programmer/architect **5.** ❑ system engineer
6. ❑ technical manager **7.** ❑ student **8.** ❑ security **9.** ❑ webmaster

How did you first hear about this meeting (check one):
1. ❑ USENIX brochure **2.** ❑ newsgroup/bulletin board **3.** ❑ *;login:*
4. ❑ WWW **5.** ❑ from a colleague **6.** ❑ magazine

What publications or newsgroups do you read related to Network Administration and/or Intrusion Detection? _____

Payment Must Accompany This Form

Payment (U.S. dollars only) must accompany this form. ***Purchase orders, vouchers, email, and telephone registrations cannot be accepted.***

❑ **Payment enclosed.** Make check payable to **USENIX Conference.**

Charge to my: ❑ VISA ❑ MasterCard ❑ American Express ❑ Discover

Account No. _____ / Exp. Date

Print Cardholder's Name

Cardholder's Signature

Please complete this registration form and return it along with full payment to:
USENIX Conference Office, 22672 Lambert St., Suite 613,
Lake Forest, CA USA 92630 Phone: 1.949.588.8649 Fax: 1.949.588.9706

You may FAX your registration form to 1.949.588.9706 if paying by credit card. To avoid duplicate billing, please DO NOT mail an additional copy.

Tutorial Program Select one full-day tutorial per day.

Friday, April 9, 1999 (9 am – 5 pm)
❑ F1 Configuring Cisco Routers on an IP Network
❑ F2 Intrusion Detection and Network Forensics
❑ F3 Handling Computer and Network Security Incidents
❑ F4 How Networks Work: The Limits of Modern Internetworking

Saturday, April 10, 1999 (9 am – 5 pm)
❑ S1 Secure Communications over Open Networks
❑ S2 Computer Attacks: Trends and Countermeasures
❑ S3 Internet Security for UNIX System Administrators
❑ S4 Topics in Network Administration

REFUND/CANCELLATION POLICY **If you must cancel, all refund requests must be in writing with your signature, and postmarked no later than March 29, 1999. Telephone cancellations cannot be accepted. You may substitute another in your place. Call the conference office for details: 1.949.588.8649.**

Tutorial Program Fees (April 9–10, 1999)

One full-day tutorial ..... $395.00 $ _____
CEU credit (optional) ..... $15.00 $ _____
Two full-day tutorials ..... $690.00 $ _____
CEU credit (optional) ..... $30.00 $ _____
Late fee applies if postmarked after Tuesday, March 16, 1999 ..... Add $50.00 $ _____

Conference on Network Administration

Technical Session Fees (April 7–8, 1999)

Current member fee ..... $360.00 $ _____
(Applies to individual members of USENIX, EurOpen national groups, JUS, AUUG, and SAGE-AU.)

Non-member or renewing member fee* ..... $440.00 $ _____
Join or renew your USENIX membership, for no additional fee, AND attend the conference. **Check here:** ❑

NOTE: **If attending both Technical Sessions, pay non-member fee for the Network Administration Conference and check the membership box above. Then pay member fee for the Workshop on Intrusion Detection & Network Monitoring.**

Join or renew your SAGE membership (you must be a current member of USENIX) Add $30.00 $ _____
Late fee applies if postmarked after *Tuesday, March 16, 1999* ..... Add $50.00 $ _____
Full-time student** fee, pre-registered or on-site ..... $75.00 $ _____
Full-time student** fee including USENIX membership fee ..... $100.00 $ _____
***Students: attach a photocopy of current student I.D.*

Workshop on Intrusion Detection and Network Monitoring

Technical Session Fees (April 11–12, 1999)

Current member fee ..... $360.00 $ _____
(Applies to individual members of USENIX, EurOpen national groups, JUS, and AUUG.)

Non-member or renewing member fee* ..... $440.00 $ _____
Join or renew your USENIX membership, for no additional fee, AND attend the conference. **Check here:** ❑

Late fee applies if postmarked after *Tuesday, March 16, 1999* ..... Add $50.00 $ _____
Full-time student** fee, pre-registered or on-site ..... $75.00 $ _____
Full-time student** fee including USENIX membership fee ..... $100.00 $ _____
***Students: attach a photocopy of current student I.D.*

TOTAL DUE $_____