EurOpen Quarterly

EurOpen — The European Federation of Open Systems User Groups — November 1994, Issue 1

New chairman

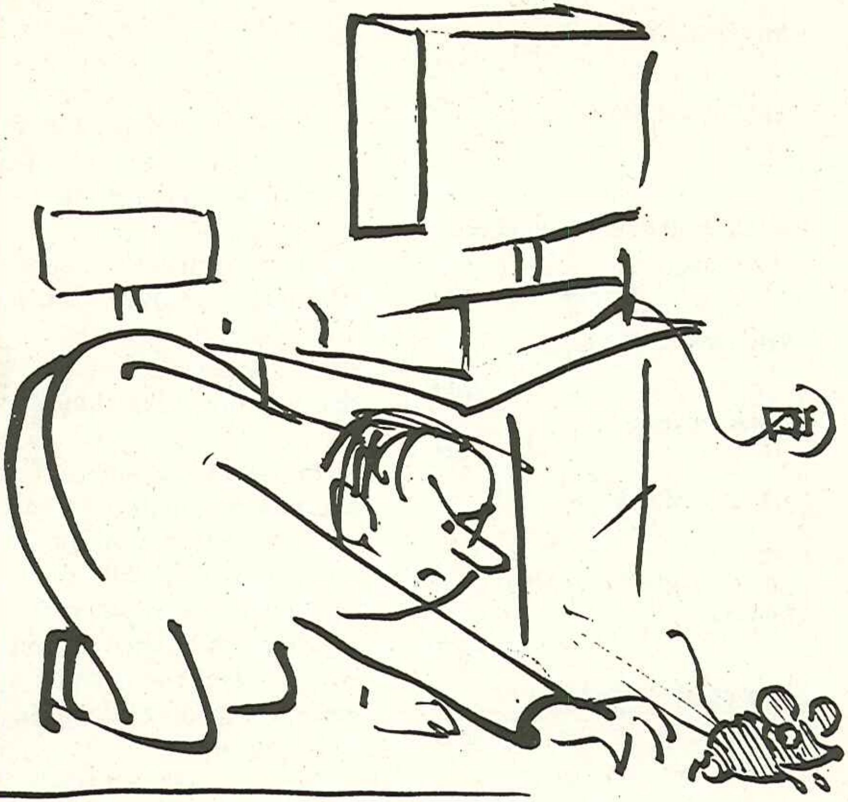
Kim Biel-Nielsen is the new chairman of EurOpen. He gives his views on EurOpens future.

The need for privacy

Philip Zimmermann, author of the PGP software, gives his views on why cryptography is necessary.

System administration models

Local system administrators or a central datacenter?



Contents

Welcome

Welcome to the first real issue of EurOpen´s new magazine, EurOpen Quarterly. Some of the readers have seen issue 0 of Open Quarterly — the time inbetween the two issues has been spent trying to find a better name for the publication (we hope we succeeded) and collecting articles.
The idea behind EurOpen Quarterly is to collect articles from the national user groups publications and publish them to a wider audience.

In this first issue we mainly bring material from our American counterparts ";login" (published by the USENIX association) and UniNews (published by UniForum). We hope to bring more European material in future issues.

In this issue we bring a portrait of the new EurOpen chairman **Kim Biel-Nielsen.**

A testimony by the author of **PGP, Philip Zimmerman**, about the need for a sane American policy on **cryptography technology**, adressed to a US Congress subcommittee.

The president of the System Administrators Guild, Elizabeth Zwicky presents the two **system adminstration models**: centralized vs. local.

The EurOpen treasurer Marten van Gelderen presents the **financial statement** for 1993.

And if you ever wondered why you only need **backups** that you for some reason haven´t got — well, Greg Rose has a theory.

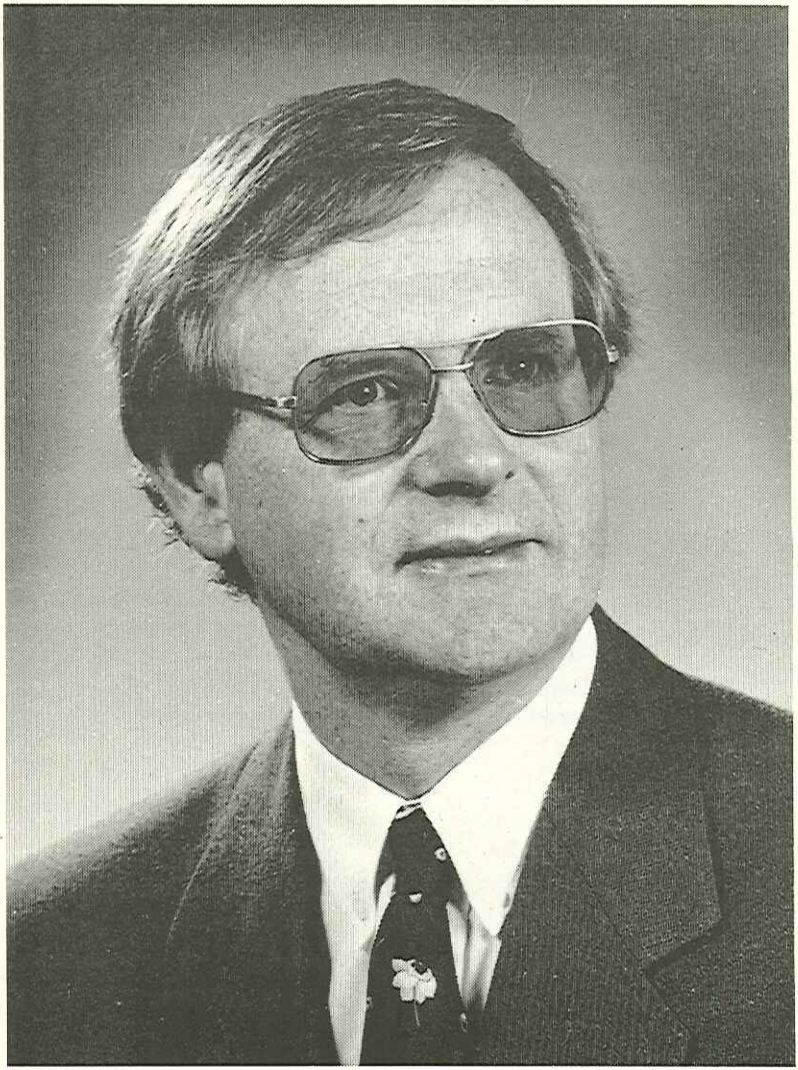
We are very interested in submissions from our readers, preferably in English, or at least with an abstract in English.

Comments and suggestions are very welcome as well.

❑

Out of Denmark: An Open Systems Unifier

The new chairman of EurOpen



If the task of bringing the open systems world together through associations can be seen as a cause, Kim Biel-Nielsen is one of its foremost evangelists. One of the founders of the Danish UNIX Users' Group and the new chairman of EurOpen, Biel-Nielsen preaches the value of group action and cooperation to anyone who will listen. And he does it with a distinct Danish flair.

Biel-Nielsen was born in Copenhagen in 1949 and his parents immigrated to the United States in the early '50s. After about five years, they moved to Sweden, where Biel-Nielsen got his education through high school. In 1970, he moved once more with his family, this time back to Denmark, where he attended the University of Copenhagen. His attempt to become a chemical engineer ended when "I failed horribly in math, several times." Then, by accident, he discovered a course in computers and changed his course of study.

In 1976 Biel-Nielsen, now married, got his first job in computers with IBM in Copenhagen. Later he took a position with S.C. Metric, a Danish distributor of other companies' hardware and software. In 1991 the company spun off its UNIX software division, which became Uniware Denmark. Biel-Nielsen was named the new company's managing director, a position he still holds.

Biel-Nielsen's first experience with the concept of open systems came in 1982 when his company was distributing computers from the U.S. company Zilog. That company had developed a commercial UNIX system called the Zilog System 8000. "From 1982 to 1985 or '86, when Zilog discontinued manufacture of these systems, S.C. Metric had become the dominant Danish supplier of UNIX hardware," Biel-Nielsen remembers. "We

Name: Kim Biel-Nielsen

Age: 45

Birthplace: Copenhagen, Denmark

Position: Managing director, Uniware Denmark

Years in Current Position: 3

Years in the Industry: 18

Association Leadership: Chairman, EurOpen, Vice chairman, Danish UNIX Users' Group (DKUUG)

Pet Open Systems Peeve: "That people believe Microsoft is open. We got rid of the "B" in IBM and we are about to go into a new proprietary world controlled by Intel and Microsoft."

Management Philosophy: "Delegate as much as possible, preferably everything. Give individuals the power to make the decisions that are necessary for their jobs and for their lives. It's astonishing to find that if you give people the power to make the decisions, how large a percentage of right decisions they make."

had a very large installed base when they decided to discontinue building the systems. In order the sell the systems, we had gained the distribution rights of a number of software products, including Informix and Uniplex. We were then approached by other software companies in the market, who said they had almost lost out to us, and couldn't we sell the software products for them instead? Then we said that rather than find a new hardware product, why not become a distributor of software? We did that and it's proven to be a successful strategy."

Biel-Nielsen likens his current job as managing director of Uniware to walking a tightrope. "Whenever you deal with somebody, you have to be good enough that they don't find somebody else. On the other hand, you shouldn't be so good that they decide the business is lucrative enough that they should go into it themselves. What you always need to do is get new products so that you can follow the market. If you don't get new products as the market changes, you will eventually find yourself behind the market." On the other hand, Uniplex and Informix, the products his company started with, are still its best sellers.

Although Uniware has purposely restricted itself to the Danish market, it's toying with expanding its horizons, but cautiously. "In a relatively small market, you are operating under a kind of geographic and cultural protection," Biel-Nielsen notes. "You are probably not totally geared to compete in the larger markets. If we were to go into another market, I think we ought to go into a small market because we understand how a small market works. I don't think we really understand how a big market works."

Denmark's UNIX Club

A year or so after that introduction to UNIX, Biel-Nielsen was approached by a group of students who wanted to establish a UNIX club in Denmark. "I felt that it was a wonderful idea," he remembers. "We sat together, 20 people or so, and decided to form the Danish UNIX User Group, DKUUG. We just had our 10-year anniversary. Keld Simonsen, the chairman, and myself were among the first board members." Both are still on the board and Simonsen is still chairman, Biel-Nielsen has been vice chairman for the past three years.

"Where Keld is a tremendously technical university and academic type, I am much more business oriented. So from the very first day we managed to get the Danish user group to be wide enough to provide a home for both the "suits" and the "techies." And I believe that by having that span of interest, we have managed to grow the DKUUG to be the most successful UNIX association in the world." As evidence for that claim, Biel-Nielsen cites his group's membership of 1,100 out of the Danish population of five million. We've never come across an association that had the same percentage of the total population."

Why so many? One reason is Denmark's cultural climate. "It is natural for people to be members of associations. People like to do it and they get very much involved. They come to the meetings and put up proposals and are willing to do a lot of voluntary work." The other reason is that the association has carefully made room for both technical and commercial UNIX people. "We said we wanted to provide services which are of interest to everybody," he says. The group provides a professionally written newsletter, as well as 10 to 12 meetings a year on technical topics, as well as marketing and executive-level topics. In addition, more informal "club meetings" give members a chance to socialize and discuss the latest industry news.

The DKUUG pioneered expansion of the Internet in Northern Europe, providing gateways to Norway, Finland, and Estonia. Those areas now have a direct connection to Amsterdam and use the Danish lines for backup. The Danish Internet hub, DKnet, is a wholly owned subsidiary of the DKUUG, employs 10 persons and turns over $1 million to $2 million a year. "Every six months we have to double the line capability, just because of the explosion in traffic."

Currently, the DKUUG is campaigning worldwide for the right to use the three Danish national alphabetic characters in computer systems.

Getting Europe Together

Biel-Nielsen's association with EurOpen began eight years ago when he joined the board of directors. As the umbrella organization for Europe's open systems associations, EurOpen has had trouble finding its niche. The original concept called for a head tax on members of all the European open systems groups, so that EurOpen would get part of their membership dues. In turn, EurOpen provided a number of services, including a technical newsletter, technical conferences and public domain software. That system worked fine until some of the larger associations began to get so big that they became self-sufficient. Then the head tax concept no longer seemed fair to the larger groups. "We were adding national groups from developing Eastern European countries which were unable to pay for the services, but they had high requirements for the services. The taxes were imposed on the large associations, which didn't need the services because they were providing for themselves. So we had a rapidly deteriorating system. EurOpen declined very much."

Biel-Nielsen was then voted out of the executive leadership and an attempt was made to rescue the situation by adding expensive central services and staff. However, about two years ago the national groups rebelled and voted in a new executive, in which Biel-Nielsen was included. They implemented a new structure that they called Eurocheap, meaning that "everything that cost money was slashed." And instead of paying a head tax based on the number of members, the national groups had the option several categories of membership. The EurOpen newsletter and conferences were discontinued, and EUNet, the European Internet, was spun off.

However, a realization began to grow that the cost-cutting had gone too far. "We had managed to remove the reason for EurOpen to exist by really removing every service," Biel-Nielsen says. "At the last governing board meeting I proposed a change of direction, and at the same time decided to run for chairman. I got elected as chair for two years and we got to re-launch central services, but in a new and different way." Although the process hasn't been formally agreed to, EurOpen plans to join with UniForum, USENIX and other national groups into a world citizenship of UNIX user groups. "The idea behind this is that if you are a member of any open systems user group, you have the right to use the services of another group when you visit that territory."

EurOpen also is building a new European newsletter, taking the best articles from other association newsletters. In a test launch recently, the new EurOpen Quarterly secured 5,000 commitments for subscriptions. "Without a publication at the EurOpen level, we don't have a common vehicle to speak to the members, or to the members of the member associations."

Biel-Nielsen also hopes to launch a pilot program for EurOpen value-added network services, involving use of the World Wide Web to spread information about the services and activities of all the European associations. "And we hope that by 1995 we will be able to re-launch conferences or specialized workshops at the European level. What we have to do for the next two years is to make the association visible and make it something that the members may be proud of. Once we've done that, we want to extend the range of this so that people understand the concept of joint citizenship between groups. I see the synergy of the World Wide Web and the global citizenship of open systems groups making people understand what happens in other parts of the world. In the end, they may feel they have been enriched by this." ❑

This article was originally published in the UniForum publication UniNews, July 6th, 1994.

EurOpen Financial Statements over 1993

Marten van Gelderen
EurOpen Treasurer

Having been elected as Treasurer of EurOpen on the last Governing Board meeting, which was held on April 16-17, 1994 in London, it seems appropriate to report on the financial status of EurOpen as at December 31st, 1993 in this first issue of the new EurOpen newsletter.

The report is based on records as provided by our office in Owles Hall. The figures were audited by Price Bailey and reported to the Treasurer. That report was distributed to the Governing Board meeting. The actual presentation differed only in the layout of the figures: in my system the layout is in the classic Italian style, in Price Bailey's system the layout is in the Anglo-Saxon style.

As a start, the balance sheet over 1992 was recalled. That served, of course, as the opening balance for 1993.

1993 EurOpen Opening Balance in ECU

Balance 1993		Activa	Passiva
0100	Fixed Assets	39375.00	
1200	Current Assets	187094.00	
1400	Liquid Assets	271094.00	
0500	Capital & Reserves		305802.00
1600	Short Term Obligations		191761.00
Total		**497563.00**	**497563.00**

1993 EurOpen Closing Balance in ECU

Balance 1993		Activa	Passiva
0100	Fixed Assets	10430.00	
0300	Financial Assets	84674.00	
1200	Current Assets	46652.00	
1400	Liquid Assets	90280.00	
0500	Capital & Reserves		208731.00
1600	Short Term Obligations		23305.00
Total		**232036.00**	**232036.00**

All figures, by the way, are given in ECU, the European Currency Unit.

Next, the records for the operation of EurOpen in 1993 were appended, which then provided the closing balance for 1993.

The obvious conclusion from the figures is that EurOpen took the full burden of the restructure in

1993 as planned. This restructure also included the cancellation of the contract of the executive director as decided by the Governing Board Meeting on November 21-22, 1992 in London.

The deficit over 1993 amounts to 116,154 ECU.

This is more than the projected figure for 1993 which was estimated to be 79,793 ECU.

However, the Currency Reserve position in the balance sheet (part of the Capital & Reserves position, not shown separately in this report) was decreased from 37,240 ECU to 18,157 ECU, which led to a drop in Capital & Reserves that can be calculated in two ways: `305,802 - 208,731 = 116,154 - (37,240 - 18,157) = 97,071.`

The difference between projected and actual deficit can be traced back to a misunderstanding of how EUnet should be split off from EurOpen.

Everybody agreed that there was 42,000 ECU as profitability of EUnet in previous years in the books of EurOpen that somehow "belonged to" EUnet. Originally that amount was accounted for in various "loans", booked against "Liquid Assets". I should have realised that those loans cannot remain in the books of both parties (EurOpen and EUnet) indefinitely. That would not be called "good business practice" by Her Majesty's tax office and by Price Bailey.

So the loans had to be transformed into a real burden (unfortunately). EurOpen arranged with EUnet to let the burden materialise gradually during 1993 and the first quarter of 1994. Therefore in the final figures for 1993 three quarters of that burden is taken as a real deficit. If we add the 31,500 ECU to my estimation of 79,793 ECU we arrive at 111,293 ECU for the deficit, which is in my view within margins when compared to the actual deficit of 116,154 ECU.

Another unforseen liquid burden was the fact that the participation into EUnet equity proved to be so successfull that EurOpen had to buy more shares than anticipated to maintain their 25.1% blocking minority.

If EurOpen decides to let go of their 25.1% in favour of some percentage in the range of the big groups (AFUU and GUUG) money will flow back to EurOpen.

In the official balance for 1993 the money that was spent on the EUnet shares shows up as a "financial asset", which hopefully will generate some dividend in the (near) future.

In summary, the results over 1993 are not good but they were anticipated indeed.

The financial position of EurOpen cannot be called "very good" but on the other hand not "very bad" either.

The Capital&Reserves dropped from 305802 ECU to 208731 ECU.

We still can take some risks, but not very big ones.

❑

X/Open Set To Begin UNIX Branding

Program will coincide with release of products later this year

X/Open Co., owner of the UNIX brand name, is gearing up to begin a formal branding process for UNIX products. Although a schedule has not been announced, indications are that the branding process will coincide with the release of new UNIX-based products by system vendors later in 1994.

"We are absolutely on schedule" for awarding of the UNIX brand, X/Open's chief technical officer, Mike Lambert, told an audience at the recent Xhibition conference in San Jose, CA. "The X/Open fast track is done. It's all over except for the final editing process. You are going to see unified UNIX."

No major changes in the branding plans have been made since the announcement by all major UNIX vendors of the Spec 1170 UNIX unification plan in September 1993, Lambert said. Spec 1170 will allow programmers to write applications to a common set of application programming interfaces (APIs) for all UNIX systems. Novell, owner of the source code to System V release 4 of UNIX, agreed to transfer the UNIX brand to X/Open's control last October. Lambert said development of a test suite for UNIX brand candidates is also on schedule.

Spec 1170 was initiated because the core APIs of the various UNIX implementations contained a number of what Lambert calls gratuitous differences that do not add value to the systems but do increase cost, especially on the part of application developers.

UNIX vendors needed a standard specification in order to reduce development costs and complete with newer integrated operating systems packages, namely Microsoft's Windows NT. Originally there were 1,170 separate APIs that were part of the Spec 1170 project.

Vendors hope that the acceptance of Spec 1170 and implementation of UNIX branding will further the acceptance of open systems. "Incompatibility between versions of UNIX has been the biggest barrier to the adoption of open systems," Lambert said. "That is what's standing in the way, particularly of small-to-medium sized companies that want to change."

Publication of the X/Open specification for Spec 1170 is expected during the current quarter, and branded products are expected to be available by the end of the year. Sponsors of X/Open's unified UNIX project are Hewlett-Packard, IBM, Novell's UNIX Systems Group, the Open Software Foundation, and SunSoft.

"What we are doing is realigning the trademark to what the majority of people think UNIX is," Lambert said. "It's a technology rather than a few thousand lines of code developed by AT&T. It's a conformance mark that applies to any product that conforms to Spec 1170."

Four Conformance Areas

Products to be branded will have to conform in four areas: the X/Open Portability Guide (XPG4), which lays down basic system interfaces, commands and C language requirements; the Spec 1170 system interfaces; a set of internationalized terminal interfaces; and the network APIs, consisting of the sockets interface originated in Berkeley UNIX and since adopted by major vendors, and the X/Open Transport Interface (XTI), version 2.

The set of internationalized terminal interfaces, designed to give UNIX a way of communicating with character terminals, which are not X Window-capable, is known as Curses. Curses was included in the branding scheme in part because independent software vendors frequently use Curses functions. Many applications either use Curses as their main display vehicle or as an alternate if an X-Window display device is not available, according to Seth Rosenthal, Novell software engineer.

The sockets interface is included for standardization because of the large body of existing socket-based applications and because it is already supported by most UNIX vendors, Rosenthal said. Sockets provides an interface to transport layer network protocols such as the transmission control protocol (TCP) used on the Internet. The version to be used is 4.3 BSD Reno, the most recent.

Three Stages

The UNIX branding scheme contains three stages: interim branding, soft UNIX branding and hard UNIX branding. Interim branding is available now as a step to make UNIX apply to more products before full branding is implemented. To comply, the product must conform to XPG3 or XPG4, comply with the System V Interface Definition (SVID2 or SVID3), be subject to a Novell license, and be committed to move to hard UNIX branding within a year.

Soft branding mandates full conformance to Spec 1170 but not necessarily to internationalized Curses, whose specification has not been submitted to X/Open yet. Vendors also need to commit to moving these products to hard branding.

When products are hard branded, they must conform to Spec 1170 version 1, internationalized Curses and undergo full testing.

Some products that are branded may be operating system neutral or operating system independent, Lambert said. The products that are operating system neutral will use the XPG trademark instead of the UNIX trademark and will provide the broadest possible portability. ❑

This article was originally published in UniNews, July 20th, 1994

The God of Backup

Greg Rose
ggr@acci.com.au

There is a God whose prerogatives include backups. I don´t know this God´s name, but I know He (or She, or perhaps It, after all I wouldn´t want to get sexist when talking to this God...) is definitely a vengeful God. Vengeful, angry, full of wrath, innovative in devising punishments and with a warped sense of humor. Altogether, He (She,It) is not a fun Guy (Gal, Goo) to have around.

Case in point

Take a case in point. This is a true story. I know the names of the individuals and companies involved, but I´m not going to tell you. Anyway, there is this computer vendor, let´s call them Vendor Inc., who sold a big, expensive computer to The Customer Corporation (say). This computer runs Customer Corp.´s absolutely vital, not to mention huge, corporate-everything database.

But Backup is no kind and loving god! He´s one of the OLD gods! He demands sacrifice!

This system and database had been installed for over ten years, and the Data Processing department of Customer Corp. had been doing its job quietly and happily for that time. Every six months, in addition to Customer Corp.´s regular backup schedule, they took a full-system image dump, ending up with more than 10 tapes. Then, being the professionals that they are, Customer Corp.´s Data Processing people sent the tapes to Vendor Inc. and paid a lot of money to have them loaded and verified. Vendor Inc. actually had to assemble a big enough machine and restore and run the system on it. Then the tapes were locked into a fireproof safe at Vendor Inc.´s headquarters in case they were needed.

Well, late in December, Customer Corp.´s mainframe had lost a cabinet full of drives to a small fire. "No worries," said the D.P. manager, a Mr. Lamb. "We´ll just get new drives under maintenance and reload from the backups!"

The replacement drives were installed within a day; after all, Customer Corp. was big and important, and they paid a lot for maintenance too. The tapes were retrieved from Vendor Inc.´s safe, and the reload commenced. As it happened, the major backup had been done in november, only a couple of weeks earlier.

Tape 7 was the problem. Tape 7 couldn´t be read. To be slightly more precise, what was there could be read, but there wasn´t anything there. Nothing at all. It had been a brand new tape before the backup was done, of course, no expenses were spared, and it had all the caracteristics of a brand new tape now. It looked like some sort of procedural error had occured, and one of the other tapes had been written twice, or some such irrelevant thing.

It was, of course, recrimination time. Poor Mr. Lamb was called up before the Board of Customer Corp., and asked to explain why the system had been down for two weeks. Fortunately, he was able to point the finger: Vendor Inc. was supposed to ensure that the backups were all there. The CEO of Customer Corp. called the CEO of Vendor Inc., and after the conversation had settled down a bit, asked why the backups had been useless after Customer Corp. had spent the last 13 years paying (a lot) for them to be verified? "I´ll get back to you," said Vendor Inc.´s CEO, with a sort of quaver in his voice.

Vendor Inc.´s CEO was noticeably more confident when he called back. "I have some bad news for you — I hope you´re sitting down," he said to Customer Corp.´s Head Honcho. "When the tapes came last month there was a note attached. It said that you were fed up with paying so much to have the backups verified, after all they were never used, and you just wanted us to store them. It was signed by a Mr. B. Counter. Of course we did as requested. I´m sorry."

Mr. Lamb was fired for failing to verify that the verification had happened. Somewhere, I´m sure, there was the sound of Hysterical Laughter.

Religious rite

Many people think that "backup" is a noun, an object that you refer back to when you need to. Others think that "backup" is a verb: the act of copying data. Any noun can be used as a verb. That´s close, but here is the Truth.

A backup is a religeous rite which propitiates the God of Backups.

It´s obvious really, Everyone knows that if you take a good backup it will never be used. Even Murphy knew that. (Archives get used a lot. They are not backups. If you ever let your users know how easily you can restore files, they will delete important files whenever they need temporary storage, then just ask you for them back. That´s an archive, not a backup.)

The converse is also true. If you forget to take a backup, it isn´t so bad, the God has other people he can Hassle, for a while anyway. But if you take a backup onto a bad media, or have a power outage in the middle of one, or take a backup with a script that must be run in "/"

when your current directory is "*/tmp*", or any of those sorts of things, well, you asked for it. Kerpow! The God of Backups wants his rituals done right, Or Else.

Those were the days

Just to establish my credentials (and show you how old I am), I´ll give you another example. We´d been running Version 5 UNIX (no, that is not UNIX System V) for about six months when Version 6 came in. Doing a disk-to-disk copy of an RK05 using the block device took about 15 minutes. But V6 introduced raw devices!

We had three drives, not surprisingly numbered 0, 1, and 2. No tape, but removable packs. All backups were disk-to-disk. Well, we went to single user mode, put the system backup in drive 1, and started to *dd* from */dev/rk0* to */dev/rk1*. (I warned you about nouns and verbs, didn´t I?) About halfway, our administrator stopped the copying, and said, "I´ll just use the raw devices to make it faster", the moment the copying was interrupted, the God´s beeper went off, and He began watching in fascination.

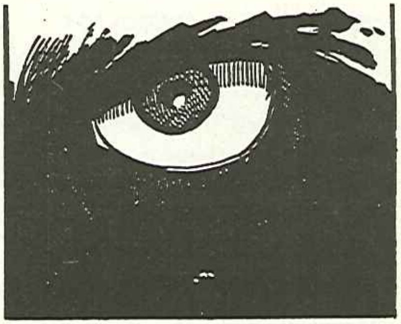
Our administrator quickly mknoded three times to create the raw devices. When the dd was restarted, this time on the raw devices, the lights on drives 0 and 2 (!) came on, and stayed on for a satisfying amount of time as entire tracks were copied. It took about thirty seconds before we noticed that the wrong drive was ligthing up. The DecWriter console still showed the typo that mixed up the drive minor numbers, but it was too late. The system disk backup contained the beginning of the current system disk, but the end of the old one. The end of the actual system disk was intact, but the beginning of it was clobbered by the front of the user disk. The situation might have been recovered at this point, since the whole system disk image existed, but in two pieces, but in two places.

Of course, since the system was running off that system disk, it promptly crashed. Maniacal Laughter.

So when you are performing a backup, remember the proper sense of gravity in the situation. Your backup ceremony should be systematic. Label the tapes neatly, immediately after they come out of the drive. Store them properly. Don´t interrupt a backup, and don´t let anything stop you from finishing one. Establish a schedule of Worship, and stick to it.

And don´t ever start giggling during a backup, or tell backup jokes. ❑

Backup is always watching... and waiting!



The article originates in ;login March/April 1994

A Quarter Century of UNIX

by Peter Salus. Published 1994 by Addison Wesley

Reviewed by Rob Kolstad <kolstad@usenix.org>

For the first time in my life, I read a substantial book in a single sitting. I really read the whole thing, not just scanned and looked at the pictures and interesting subparagraphs. It was a different way for me to absorb information; usually, I nibble at books instead of gobbling them whole. It was a fascinating way to spend 3.5 hours.

Peter Salus, the official UNIX and USENIX gadfly (and Bookworm), has completed his sociological study of the first 25 years of UNIX. It features a terrific timeline of UNIX development and the events that brought it to its present state.

After an entertaining dual-chapter introduction that ranges from spacewar to Multics, the history moves to a formal note (surely due to the lack of direct interviews) that covers Babbage, Hollerith, mechanical computers, electronic computers, and an interesting slice through the tree of computer architectural development (straight from ENIAC to the PDP series; with few branches off the direct path).

Peter Salus "knows just about everybody,", says one ;login: book reviewer. "He should have quotes in there from dozens of luminaries." And so he does!

Quotes from Bell Labs luminaries, BSD aces, and industry stars are sprinkled liberally through the text. I found the chapters on UNIX´s early evolution to be particularly instructive: we now have a definitive source against which to check folklore and hold the legends in check. I was surprised at how muddy were the early details of UNIX evolution as held in my mind.

The book also covers evolution of the various user groups. Peter has collected stories and comments from 20 years ago that help put the current user group politics into a fine perspective.

In its final third, Peter discusses the UNIX industry, from startups through current industry "UNIX wars." It seemed quite complete to me.

Who should read this book? Anyone who wants to be sure they have an idea of the background of how UNIX came to be what it is today. It was good reading for me, because it clarified much of the folklore that I thought I knew (but about which I was occasionally confused). It's a fine idea for those moving into UNIX guru-hood, as they can hear the definitive folklore (from the actual horses' mouths, as it were) and be immediately caught up with six years of attending USENIX conferences. It's also a fine idea for spouses (parents, relatives, close friends) of UNIX gurus who are trying to figure out the culture. Corporate managers might enjoy reading this, as its clear text gives the background of the operating system and the essence of its social context in a way no marketing prose can.

❑

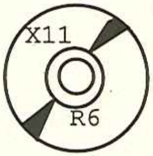
The review was first published in ;login June 1994.

X11R6 on CD

The UKUUG is pleased to offer a new CD service to EurOpen members; X Window System, Version 11 Release 6 - X11R6 was released on Monday 2nd May at 16.00 GMT (17.00 BST). It is freely available from several archives around the world, including SunSITE Northern Europe: <src.doc.ic.ac.uk:/packages/X11R6/>

It is also available on CD via the UKUUG Software Distribution Service. The CD will be in ISO 9660 with Rockridge Extensions so will work fine with most UNIX CD systems e.g. SunOS 4.1.3, Linux.

These CD's are produced to order on a frequent basis (weekly), rather than being mass produced at a pressing plant in 1,000's, so they will be very up to date and will contain the very latest contributions as and when they become available.



Costs:

X11R6Members Others

1 CD (UK post)45.00 GBP 55.00 GBP

1 CD (UK express post) 50.0060.00

1 CD (Europe post50.00 60.00

Please send orders to the EurOpen Secretariat. All orders must be accompanied by payment. VISA/MASTERCARD/ACCESS details or cheque drawn on a UK bank in Pounds sterling.

❑

System Administration Models

Elizabeth Zwicky
zwicky@corp.sgi.com

The most popular system administration model is none whatsoever. You have computers, some of which have system administrators. Which ones have system administrators is determined entirely at the whim of whoever purchases the computer. This model has the advantage of extreme simplicity, requiring no thought and no agreement to implement. On the other hand, it has severe disadvantages. It maximizes the extent to which decisions about computing are made on an ad-hoc-basis to meet short term needs. People buy computers that they can´t use because there´s nobody to help them set them up; people buy computers without buying backup systems or using them, and important projects are lost; resources are duplicated unnecessarily. This constitutes a major drain on corporate resources — most obviously money, but more importantly the time and energy of people who are fighting computers instead of using them.

It is therefore in the corporate interest to actually ensure that there are system administrators and that those system administrators are effective. To that end, there should be some vision as to how those system administrators are distributed.

Datacenters

For some reason, the model that leaps to people´s mind first is a purely centralized model based on the datacenters that became common in the days when IBM was still revising their estimate of the total number of computers the world needed from 6 to a few thousand. This inspires fear and loathing, and well it should; centralized datacenters were a neccessary evil, not a desirable solution, even when they were standard. In a world of workstations and personal computers, they are not merely inadvisable as a complete solution, they´re impossible. If you attempt to centralize control of all the company´s computing resources, issues of resource contention and local custonizations will drive people to go back to buying their own unsupported computers, leaving you somewhat worse off than if you had just let them do it in the first place, since the new computers will be actively hidden. Nobody creates new purely centralized facilities, and the old ones discovered this problem with a vengeance when personal computers first became popular. This is therefore a straw-man argument, frequently mentioned, but only to be discredited.

An act of balance

In reality, a reasonable model will balance out a number of confliction needs. You need to achive economics of scale, by putting resources as high up in the organizationas practical. You also want to standardize across groups in order to maximize your ability to move information and people within the company. You need to custom fit the computers to their users as much as possible — one-size-fits-all works no better for computers than for clothes. You need to provide effective assistance to people, which means both having people who know what their particular circumstances and needs are and having people who are always available. You need system administrators who are responsible to the people they support, but those system administrators also need specialized management and support.

The end result is going to be some combination of centralized and local support. The centralized support is going to specialize in consistency, availability, and deep understanding of system administration issues, including explaining managers to system administrators and vice versa. The local support is going to specialize in local adaptation, user support, and representing the special needs of their community to the centralized support. Within this basic theme, there are many possible variations, mostly representing different solutions to two main problems: who is the line manager for the local system administrators, and what organizational level do they work for?

The local system administrators can either work for the central organization and be assigned to areas, or they can work for the local groups and be advised by the central organization. I admit that theoretically they could work for both simultaneously, resulting in an organizational directed graph rather than an organizational tree, but I sincerely hope that most businesses will reject this solution on the grounds that it is widely known to be a quick route to managerial disasters.

Pros and cons

Having the local system administrators work for the central organization adds flexibility, helps to ensure consistency in both technical and managerial procedures, and ensures a support structure for the system administrators. On the other hand, it loosens the connection between the system administrators and the people they support, by making the system administrators into effectively internal contractors. (This is a special problem in companies that don't already have people in this sort of position.) In a company that is currently relatively strongly centralized, it may serve to increase local control; in a company that is currently very distributed, it will increase central control, which is likely to be a political and social problem. Whatever the organizational chart says, it will also give the system administrators a strong sense of having two managers, since they are trying to please both their manager, and the people in the local area they support. Again, this problem is likely to be most acute in companies where this sort of situation is rare.

Having the local system administrators work for the groups that they support avoids many managerial and political problems, at the expense of putting hiring and managerial decisions for system administrators in the hands of people who may not have the expertise in the area that the central group has. This tends to lead to inconsistent management, and encourages inconsistent technical decisions as well, by loosening the connections between the local groups. It will also leave most system administrators in very small groups (often consisting of lone system administrators). Some things cannot be managed at that level - networks, for instance - and must be provided as central services. Some things, like backups and security, are so crucial to the company that they must be monitored by a central group. Some things, like news and electronic mail, only provide costeffective and user-friendly service if there is some centralized service available for them. Users need coverage when their system administrators are ill or otherwise absent; they need a reliable and easy-to-remember way to contact the correct people when something doesn't work, which almost certainly means a central dispatching service which can provide answers to routine queries, route problems to the appropriate person, and cover more hours than the local system administrators. Small system administration groups cannot be reasonably expected to be expert in everything and will need technical support in some areas.

All of this means that there will be a large number of problems and processes that involve both central system administrators and local system administrators, often in multiple parts of the central group and multiple local groups. These situations are extremely failure-prone, because of the number of people and hand-offs involved, and very hard to resolve when they fail, because there is rarely a single person at fault and a single place to fix things. This is by no means unique to the situation where local system administrators work for the local group, but it is significantly worsened there, because it increases the number of handoffs between different management trees. Handing a process off to someone with a different set of priorities and a different manager involves more risk of failure that handing it off within the same organization.

It is not unusual for companies to choose to combine these methods by leaving local system administrators managed by local groups where there are existing pools of administrators and expertise, and putting system administrators with central managers into the remaining groups. This is an effective solution for places that either want central control, or have groups that don't want to put the effort into hiring their own system administrators. Moving system administrators that are currently in local groups where they are well-integrated and effective is spectacularly difficult and unpopular. The opposite case — where the company wants to put in local system administrators but not everybody wants them is less frequent and usually easier to fix. It usually results from a group that doesn't really want any system administrators at all, and the issues surrounding that will have to be dealt with under either method. Mixing the two methods gives both sets of advantages, but it also provides both sets of disadvantages, and while each local group gets one set of advantages or the other, the central group gets to deal with both sets of disadvantages simultaneously.

The question of numbers

All of this discussion has conveniently ignored the question of exactly what a local group is and exactly where the central group is. A local group needs to be a set of people with a strong common goal and culture, that already works as a reasonably cohesive unit. It needs to be large enough to support at least one system administrator, which leads inexorably into discussions of how many users a single system administrator should support. Most companies will want the largest possible number of people covered per administrator, which is partly a technical issue and partly a social issue. The technical issue can be roughly summed up by saying that the number of administrators you need rises with the complexity of the site and with the amount of support the users need. It is a mistake to assume that technically oriented users like engineers automatically need less support than non-technical users like secretaries; it is more accurate to say that they need different sorts of support The social issue involves familiarity. The point of putting system administrators in local groups is to make them a working part of the group. This is not going to work unless the people who're being supported all know the system administrator. As a generalization, a local group should be no larger than a building, to encourage this sort of familiarity.

Picking local group sizes is extremely dependent on the corporate culture, and usually on the internal structure of individual pieces of the company. It's rarely possible to pick a single level of the organizational chart and declare it to be the right place to put the system administrators; not only does this usually leave local groups of extremely uneven size, it also leaves everybody above that level unsupported. This process should be regarded as an art, not a science, and left to fall out of the natural way the company works to the maximum extent possible.

The central group will generally be at the corporate level (although there is nothing stopping an individual part of the company from adopting this sort of model internally, when the company as a whole has no model at all, in which case the "central" group will be at the top level available). This is appropriate because issues of security, backups, and consistent electronic interface to the outside world should be corporate priorities, and because it leads to the maximum possible economies of scale. On the other hand, it may turn out to be reasonable to have sub-centers in smaller pieces of the company (at the risk of increasing all the communications problems). In particular, it's important to arrange financial matters so that purchases can be made where they are sensible. For instance, it may be reasonable for a number of local groups to share a file server that is not large enough for the whole company to share, and there should in that case be a mechanism for buying and supporting that machine. A programming division will probably have multiple local groups that share a need for the same compilers and tools, making it reasonable to buy and support those at the division level. It is in the best interest of the company to make it as easy as possible for groups to band together for site licenses of software and support; many companies either overpurchase software because this isn't possible, or end up wasting most of their savings in paying employees to argue about the financials. Ideally, these sub-groups can be handled in the center, but if that is not effective, putting in small amounts of intermediate organization may well be worth the effort.

No single answer

All of this falls short of suggesting a particular solution for everybody's company. This is because there is no one right answer for the general case, although there may be a right answer for some specific cases. Almost any answer is better than ignoring the issue altogether, however, a traditional company large enough to have more than one building is going to need both local and central administrators, and they are going to need to work closely together.

Elizabeth Zwicky is president of SAGE, the System Administrators Guild

❑

Originally published in ;login October 1994

The need for privacy

Testimony of Philip Zimmermann to Subcommittee for Economic Policy, Trade, and the Environment US House of Representatives 12 Oct 1993

Mr. Chairman and members of the committee, my name is Philip Zimmermann, and I am a software engineer who specializes in cryptography and data security. I'm here to talk to you today about the need to change US export control policy for cryptographic software. I want to thank you for the opportunity to be here and commend you for your attention to this important issue.

I am the author of PGP (Pretty Good Privacy), a public-key encryption software package for the protection of electronic mail. Since PGP was published domestically as freeware in June of 1991, it has spread organically all over the world and has since become the de facto worldwide standard for encryption of E-mail. The US Customs Service is investigating how PGP spread outside the US. Because I am a target of this ongoing criminal investigation, my lawyer has advised me not to answer any questions related to the investigation.

The information age is here

Computers were developed in secret back in World War II mainly to break codes. Ordinary people did not have access to computers, because they were few in number and too expensive. Some people postulated that there would never be a need for more than half a dozen computers in the country. Governments formed their attitudes toward cryptographic technology during this period. And these attitudes persist today. Why would ordinary people need to have access to good cryptography?

Another problem with cryptography in those days was that cryptographic keys had to be distributed over secure channels so that both parties could send encrypted traffic over insecure channels. Governments solved that problem by dispatching key couriers with satchels handcuffed to their wrists. Governments could afford to send guys like these to their embassies overseas But the great masses of ordinary people would never have access to practical cryptography if keys had to be distributed this way. No matter how cheap and powerful personal computers might someday become, you just can't send the keys electronically without the risk of interception. This widened the feasibility gap between Government and personal access to cryptography.

Today, we live in a new world that has had two major breakthroughs that have an impact on this state of affairs. The first is the coming of the personal computer and the information age. The second breakthrough is public-key cryptography.

With the first breakthrough comes cheap ubiquitous personal computers, modems, FAX machines, the Internet, E-mail, digital cellular phones, personal digital assistants (PDAs), wireless digital networks, ISDN, cable TV, and the data superhighway. This information revolution is catalyzing the emergence of a global economy.

But this renaissance in electronic digital communication brings with it a disturbing erosion of our privacy. In the past, if the Government wanted to violate the privacy of ordinary citizens, it had to expend a certain amount of effort to intercept and steam open and read paper mail, and listen to and possibly transcribe spoken telephone conversation. This is analogous to catching fish with a hook and a line, one fish at a time. Fortunately for freedom and democracy, this kind of labor-intensive monitoring is not practical on a large scale.

Today, electronic mail is gradually replacing conventional paper mail, and is soon to be the norm for everyone, not the novelty it is today. Unlike paper mail, E-mail messages are just too easy to intercept and scan for interesting keywords. This can be done easily, routinely, automatically, and undetectably on a grand scale. This is analogous to driftnet fishing — making a quantitative and qualitative Orwellian difference to the health of democracy.

The second breakthrough came in the late 1970s, with the mathematics of public key cryptography. This allows people to communicate securely and conveniently with people they´ve never met, with no prior exchange of keys over secure channels. No more special key couriers with black bags. This, coupled with the trappings of the information age, means the great masses of people can at last use cryptography. This new technology also provides digital signatures to authenticate transactions and messages, and allows for digital money, with all the implications that has for an electronic digital economy. (See appendix)

. This convergence of technology — cheap ubiquitous PCs, modems, FAX, digital phones, information superhighways, et cetera — is all part of the information revolution. Encryption is just simple arithmetic to all this digital hardware. All these devices will be using encryption. The rest of the world uses it. and they laugh at the US because we are railing against nature, trying to stop it. Trying to stop this is like trying to legislate the tides and the weather. It's like the buggy whip manufacturers trying to stop the cars — even with the NSA on their side, it's still impossible. The information revolution is good for democracy — good for a free market and trade. It contributed to the fall of the Soviet empire. They couldn´t stop it either

Soon, every off-the-shelf multimedia PC will become a secure voice telephone, through the use of freely available software. What does this mean for the Government's Clipper chip and key escrow systems?

Like every new technology, this comes at some cost. Cars pollute the air. Cryptography can help criminals hide their activities. People in the law enforcement and intelligence communities are going to look at this only in their own terms. But even with these costs, we still can´t stop this from happening in a free market global economy. Most people I talk to outside of Government feel that the net result of providing privacy will be positive.

President Clinton is fond of saying that we should "make change our friend". These sweeping technological changes have big implications, but are unstoppable. Are we going to make change our friend? Or are we going to criminalize cryptography? Are we going to incarcerate our honest, well-intentioned software engineers?

Law enforcement and intelligence interests in the Government have attempted many times to suppress the availability of strong domestic encryption technology. The most recent examples are Senate Bill 266 which mandated back doors in crypto systems, the FBI Digital Telephony bill, and the Clipper chip key escrow initiative. All of these have met with strong opposition from industry and civil liberties groups. It is impossible to obtain real privacy in the information age without good cryptography.

The Clinton Administration has made it a major policy priority to help build the National Information Infrastructure (NII). Yet, some elements of the Government seems intent on deploying and entrenching a communications infrastructure that would deny the citizenry the ability to protect its privacy. This is unsettling because in a democracy, it is possible for bad people to occasionally get elected — sometimes very bad people. Normally, a well-functioning democracy has ways to remove these people from power. But the wrong technology infrastructure could allow such a future government to watch every move anyone makes to oppose it. It could very well be the last government we ever elect.

When making public policy decisions about new technologies for the Government, I think one should ask oneself which technologies would best stengthen the hand of a police state. Then, do not allow the Government to deploy those technologies. This is simply a matter of good civic hygiene.

Export controls are outdated and are a threat to privacy and economic competitiveness

The current export control regime makes no sense anymore, given advances in technology

There has been considerable debate about allowing the export of implementations of the full 56-bit Data Encryption Standard (DES). At a recent academic cryptography conference, Michael Wiener of Bell Northern Research in Ottawa presented a paper on how to crack the DES with a special machine. He has fully designed and tested a chip that guesses DES keys at high speed until it finds the right one. Although he has refrained from building the real chips so far, he can get these chips manufactured for $10.50 each, and can build 57000 of them into a special machine for $1 million that can try every DES key in 7 hours, averaging a solution in 3.5 hours. $1 million can be hidden in the budget of many companies For $10 million, it takes 21 minutes to crack, and for $100 million, just two minutes. That´s full 56-bit DES cracked in just two minutes. I'm sure the NSA can do it in seconds, with their budget. This means that DES is now effectively dead for purposes of serious data security applications. If Congress acts now to enable the export of full DES products, it will be a day late and a dollar short.

If a Boeing executive who carries his notebook computer to the Paris airshow wants to use PGP to send email to his home office in Seattle, are we helping American competitiveness by arguing that he has even potentially committed a federal crime?

Knowledge of cryptography is becoming so widespread, that export controls are no longer effective at controlling the spread of this technology. People everywhere can and do write good cryptographic software, and we import it here but cannot export it, to the detriment of our indigenous software industry.

I wrote PGP from information in the open literature, putting it into a convenient package that everyone can use in a desktop or palmtop computer. Then I gave it away for free, for the good of our democracy. This could have popped up anywhere, and spread. Other people could have and would have done it. And are doing it. Again and again. All over the planet. This technology belongs to everybody.

People want their privacy very badly

PGP has spread like a prairie fire, fanned by countless people who fervently want their privacy restored in the information age.

Today, human rights organizations are using PGP to protect their people overseas. Amnesty International uses it. The human rights group in the American Association for the Advancement of Science uses it.

Some Americans don't understand why I should be this concerned about the power of Government. But talking to people in Eastern Europe, you don´t have to explain it to them. They already get it — and they don't understand why we don't.

I want to read you a quote from some E-mail l got last week from someone in Latvia, on the day that Boris Yeltsin was going to war with his Parliament:

"Phil I wish you to know: let it never be, but if dictatorship takes over Russia your

PGP is widespread from Baltic to Far East now and will help democratic people if necessary. Thanks."

Appendix — How Public-Key Cryptography Works

In conventional cryptosystems, such as the US Federal Data Encryption Standard (DES), a single key is used for both encryption and decryption. This means that a key must be initially transmitted via secure channels so that both parties have it before encrypted messages can be sent over insecure channels. This may be inconvenient. If you have a secure channel for exchanging keys, then why do you need cryptography in the first place?

In public key cryptosystems, everyone has two related complementary keys, a publicly revealed key and a secret key. Each key unlocks the code that the other key makes. Knowing the public key does not help you deduce the corresponding secret key. The public key can be published and widely disseminated across a communications network. This protocol provides privacy without the need for the same kind of secure channels that a conventional cryptosystem requires.

Anyone can use a recipient's public key to encrypt a message to that person, and that recipient uses her own corresponding secret key to decrypt that message. No one but the recipient can decrypt it. because no one else has access to that secret key. Not even the person who encrypted the message can decrypt it.

Message authentication is also provided. The sender's own secret key can be used to encrypt a message, thereby "signing" it. This creates a digital signature of a message which the recipient (or anyone else) can check by using the sender's public key to decrypt it. This proves that the sender was the true originator of the message, and that the message has not been subsequently altered by anyone else, because the sender alone possesses the secret key that made that signature. Forgery of a signed message is infeasible, and the sender cannot later disavow his signature.

These two processes can be combined to provide both privacy and authentication by first signing a message with your own secret key, then encrypting the signed message with the recipient's public kcy. The recipient reverses these steps by first decrypting the message with her own secret key, then checking the enclosed signature with your public key. These steps are done automatically by the recipient's software.

Philip Zimmermann is a software consultant specializing in cryptography, data security, and authentication, and is the author of Pretty Good Privacy (PGP), the most widely used software package in thc world for email encryption He can be reached via email at prz@acm.org.

❑

The article was published in "Usenix summer 1994 Invited Talks."

NEW HONORARY MEMBERS FOR EUROPEN

It was decided at the recent Executive meeting that Honorary Membership of EurOpen should be offered to Mr. George Schild, EurOpen Chair November 1992 - May 1993 and Zdravko Podolski, EurOpen Chair, May 1993 - April, 1994, in recognition of their efforts and time given to the Group. The Secretariat has written to offer the invitation for Honorary membership and awaits confirmation of acceptance.

□

EurOpen Quarterly

EurOpen Quaterly is published by EurOpen

EurOpen Secretariat
Owles Hall
Buntingford
Herts. SG9 9PL
United Kingdom

Editor

Søren Oskar Jensen

EurOpen Quarterly
C/O Søren O. Jensen
Vesterbrogade 65, 2.th.
DK-1620 Copenhagen V
Tlf. +45 31 22 84 43
Fax +45 39 17 98 97
Email: dkuugnyt@dkuug.dk

□

Forthcoming EurOpen Events

November:

1	FUUG	SNMP meeting - Finland
3-4	GURU	ROSE'94 - Open Systems Conference & Exhibition - Bucharest, Romania (arot@guru.ro)
14-18	USENIX	First Symposium on Operating Systems Design and Implementation (OSDI) - Monterey, CA, USA
14-18	SUG	Sun User Group Technical Workshop - Austin, TX, USA
17	CSUUG	Autum Conference - Czech Republic
18	EurOpen.SE	Annual meeting - Stockholm, Sweden
24	DKUUG	POSIX in Praxis & DKUUG's Annual meeting - Denmark

December:

8-9	USENIX	IEEE Mobile Computing Systems & Applications - Santa Cruz, CA, USA
10-15		DECUS - Anaheim, CA, USA
13	FUUG	Christmas party and perl programming - Finland

1995:

January:

?	FUUG	Processing, Interfaces architectures, symmetrical multiprocessing - Finland
9-13		IEEE 1003 - USA
16-20	USENIX	Winter Conference - New Orleans, LA, USA