EurOpen Quarterly

EurOpen — The European Federation of Open Systems User Groups — May 1995, Issue 2

PGP

The US Government is trying to stop "data encryption for the masses" by launching a legal battle against PGP's creator Phillip Zimmermann.

Hooking up to the Internet

There's a lot more to putting your company on the Internet than just deciding which Internet provider you will use.

What good is a gigabyte?

What are we actually going to use all that space for?

Contents

Schedules...

The name of this magazine — "EurOpen Quarterly" — indicates that four issues are published a year and one would — still based on the name — assume that one issue is published in each quarter of the year.

Well that was actually the plan, but the editor has since come to regret the name many times. Microsoft was at least smart enough *not* to choose the name "Windows February 95".

It has been more difficult than expected to gather the material for this issue — the main problem is that the newsletters published by the national groups in EurOpen falls in two categories: either in a "Usenix Computing Systems"-like style with very technical and long articles, or in a more newsletter-like style, i.e. mainly containing information from the group to its members. So the number of articles judged to be of broad interest to European providers and users of Open Systems has been few — especially when we try to keep the ratio of American articles at max. 50%.

So it took longer than anticipated but we believe that the time has been spent well, and the result will be appealing to our readers. Some of the highlights are:

- We follow up on the article from issue 1 about Phillip Zimmermann (the author of the PGP encryption package) and his legal battle with the US Government.
- It´s no longer a battle about who´s the first kid on the block with a WWW homepage, it´s a battle about not being the *last*! We have some sound advice on how to introduce your company to the Internet.
- Software is a product — its manufacture take a lot of skilled manpower, so in an attempt to reduce costs companies are beginning to look at the Indian software industry.

❑

Inviting Internet Inside

Connecting your company to The Internet is not just a technical matter — there are many other consequences to be considered.

Frank Neergaard.
DKnet

Everybody is talking about Internet at the moment — from your systems manager to the taxi-driver who gets you home after a night on the town.

Of course you need to be on Internet — not having an Internet address is worse than not having a fax number.

This is why many are thinking about connecting their companies to Internet. Some jump straight into it without considering the possible consequences, others are hesitating — there is, after all, so much to be wary of.

Let´s be realistic — getting on Internet is about a lot more than just establishing a permanent link to DKnet and setting up a WWW-server on the nearest UNIX computer. There are a great deal of questions you should ask yourself (and each other), and when the employees get on Internet, they´re going to become different people.

> *"when the employees get on Internet, they´re going to become different people"*

The first question (after the technical details of line type, etc., have been settled) is what you want to do with your Internet link. Do you wish to offer information? Are all employees going to have access to it? Which newsgroups should be accessible?

Offering information

If you want to offer information on Internet, it is important to decide what you want to offer, and who you want to reach.

Companies often want to offer information about themselves and their products through WWW, but precisely what should it be? Should it be just an advertisement, or should technical support be available?

If you just want to advertise, there are few problems, especially if your catalogue rarely changes. If, on the other hand, you are interested in technical support, or

something similar, you should be aware that maintaining such a service can be very demanding.

It may be worth considering letting an agency take care of your WWW-service. This is especially relevant if there are no qualified employees, or if you don´t want to dedicate someone to the job.

Internet for employees

Which employees should have access to Internet?

If the link is purely for marketing purposes, it is hardly neccessary to grant everybody access, but other parts of the company can often benefit from using Internet.

The question is what you want. Some choose to make Internet freely available. This is fine if everybody has sufficient self-control, but unfortunately this is not always the case, and then what do you do?

The risk is that an employee will be smitten by the possibilities on Internet, and end up spending most of his day on WWW or MUD. The employees satisfaction with the company will probably be great, but productivity will probably not be.

> *"The risk is that an employee will be smitten by the possibilities on Internet"*

It is of course possible, in such a situation, to get the employee back on the right track, but how do you prevent the situation from arising at all?

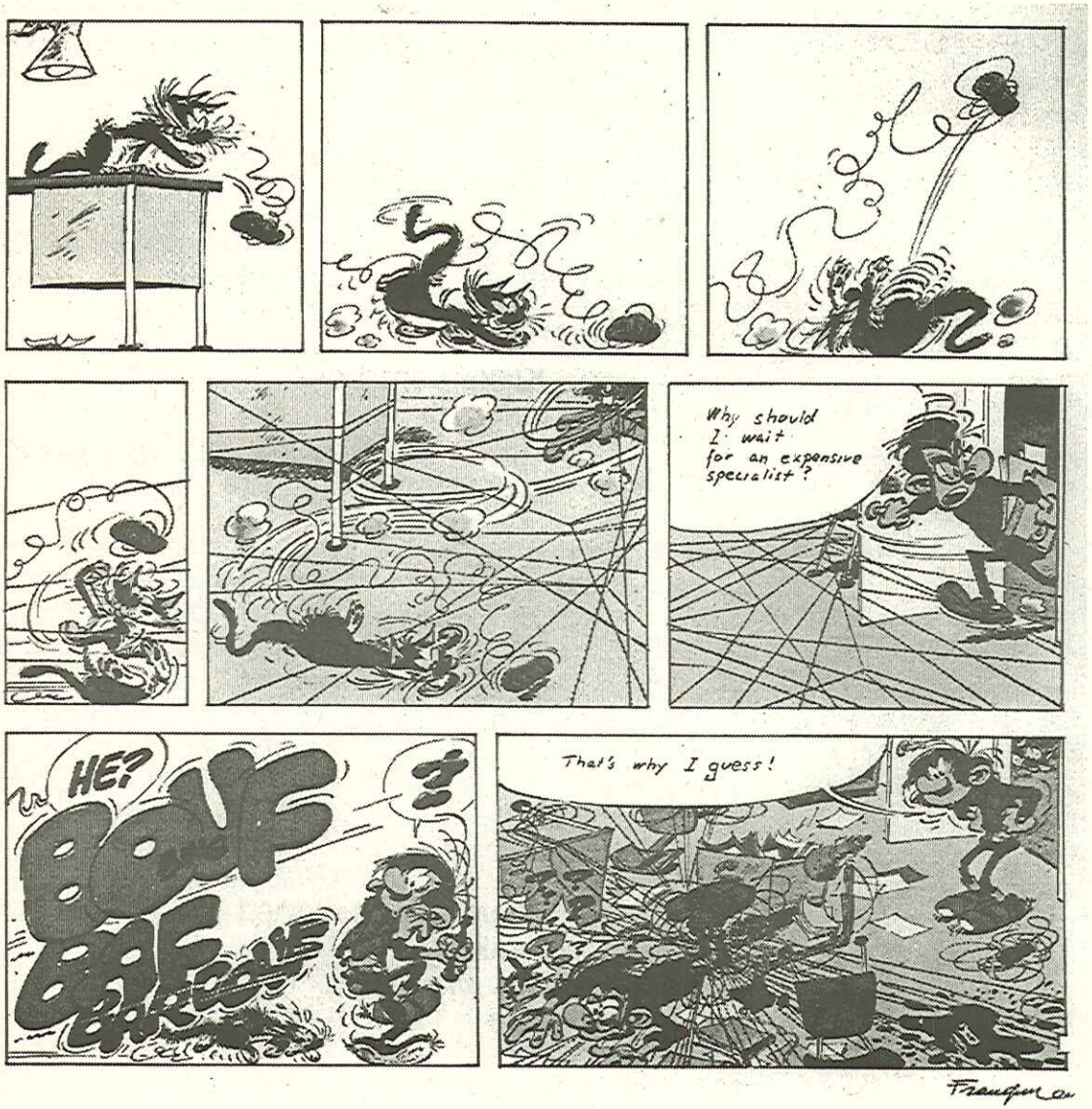
One possibility is to prevent everybody from using Internet, but this is hardly desirable. Drawing up a set of rules and regulations regarding the use of Internet is a much better solution.

Exactly how restrictive these rules should be depends on the company and its employees. If everybody is reasonable there is no reason for strict rules, and in principle there is nothing wrong with a little private use of Internet, as long as it doesn´t interfere with the work at hand. Other companies are forced to create very strict rules, and may even need penalties against infringements.

Another problem is defining what use of Internet is work-related. If a developer has a specific problem that can be solved by looking at comp.sys.sun.hardware then there is no problem, but in many situations it can be difficult to distinguish.

Many companies compromise and allow Internet to be used for both work and more private matters — but during working hours the link is strictly for work-related use. Browsing through the film database on WWW or reading alt.fan.sandra-bullock is for after hours.

In fact, a comparison could be made to the use of company telephones. Most companies do not have problems with employees spending their entire day chatting


Why should I wait for an expensive specialist?
HE?
BOAF
That's why I guess!

instead of doing their job. Internet is not quite the same thing, but the comparison is relevant.

There is no need to exaggerate the problem, but it is important to know where you stand, and to make sure your employees know it.

Newsgroups — the daily newspaper

Newsgroups are an excellent source of information and are used by many as a supplementary to the daily newspaper.

If the company has chosen to receive news, a policy should be implemented for their use.

If there is a newsgroup that, directly or indirectly, concerns company products, a single employee can be given the responsibility of following it. This will often be a good idea.

The next level of newsgroups are those that are directly related to production. In this category, a company that produces S-bus cards for Sun computers, would probably find comp.sys.sun.-hardware to be very relevant.

How do you use these newsgroups?

> *"If the company has chosen to receive news, a policy should be implemented for their use"*

There is no point in having every employee reading every article in these groups every day. A much better solution is to have one employee read all the letters and have him select any that are of interest. Another possibility is to restrict the use of the group to those that have a specific problem they need an answer to. The third level is all the other newsgroups — i.e. groups that have no relation to production, but are of interest to one or more employees. Again, this is a question of discipline — if the employees possess it, these newsgroups are not a problem. As long as they do not spend half the day reading alt.music.soundgarden.

Again, a comparison can be made to something we already know, such as the newspapers and magazines a company subscribes to. This works fine in most companies, although abuse is limited if there is only one newspaper (several employees can read news at the same time).

Internal communication

Can Internet-access benefit internal communication? Yes, actually it can. Perhaps not directly, but when access is granted to Internet, people quickly learn to use the facilities that are made available through electronic post, newsgroups, WWW, etc.

When they have realized what possibilities these facilities hold globally, they will often become interested in using the same facilities internally, and, used correctly, this can be an extremely effective tool.

Training

If you just open up the Internet and tell everybody they can use it, you are making a big mistake. The result will be that some employees immediatly throw themselves at it, and spend the next three weeks surfing around and trying things out. Yes, they will learn to use it, but it may not be the best time to tear three weeks out of the calendar. On the other hand, there will be employees who never learn to use Internet, either because they are not computer-literate, or because their first attempts failed.

> ***"Inviting Internet inside your house is not a matter to be taken lightly"***

Once you have decided what you want from Internet — preferably in collaboration with representatives from different groups of employees — you need to arrange training.

If there are employees who can take care of this, internal courses can be arranged, perhaps working with an Internet consultant. An alternative is to make use of one of the many Internet courses that are becoming available.

Note that an external course should be followed up by an internal course or seminar, so that the specific situation of the company is covered.

Conclusion

Inviting Internet inside your house is not a matter to be taken lightly — there are problems that should be adressed first.

Many of these problems are not all that different from those connected with telephones and newspapers, etc. — but Internet is still new and exciting, and reactions to it will neccessarily be different.

There is no doubt that this will change, when Internet has become less unusual. But until that time comes, you should be aware of the questions it raises.

One shouldn´t, on the other hand, be afraid of Internet, just because problems can occur. If preventive steps are taken, and one is prepared for the problems, there is no reason why things should not run smoothly.

❑

This article was originally published in "DKUUG-Nyt May 1995"

Who Are My Peers?

Elizabeth Zwicky
<zwicky@corp.sgi.com>

System administrators are frequently exhorted to think of the people they support as colleagues, but it doesn´t happen often, in either direction: system administrators think of the people they support as users, or "lusers", and other people think of the system administrators as office help or fascists, despite all attempts to encourage other attitudes. (It doesn't help that such attempts usually are aiming for "necessary evil" as an improved attitude.)

The fact is, if you are a Nobel-prize-winning physicist, and you have a brilliant idea about physics, you call a physicist. If you are a Nobel-prize-winning physicist, and you spill your coffee into your keyboard, forget your password, or unplug your computer by mistake, you call a system administrator. The system administrator may have been told that really, as a physicist, you're top notch, but the evidence to hand is going to suggest that you are not really fully in contact with the world around you. This is all very well for a Nobel-prize-winning physicist — nobody expects them to be completely normal — but the same effect holds for lesser mortals like computer programmers, and is likely to be taken as proof that they are not all that bright. If the physicist does happen to call up the system administrator to share the news of his brilliant idea about physics, the system administrator is rarely able to make much sense of it, which doesn´t advance the cause of mutual respect, either.

In turn, system administrators are generally apparent to the people as bearers or receivers of bad news. When the IRS calls, your first thought isn´t "Gee, my refund must be larger than I expected," it´s "AUDIT! AUDIT! AUDIT!" When you see mail from a system administrator, your first thought is not "I wonder how my life has been improved now?" it´s "What died?" You are also apt to be a little uncomfortable around someone who generally sees you at your worst, particularly when you have a strong feeling that they laugh about it.

More fundamentally, the sense of team membership that people are looking for depends on working together towards common goals. While system administrators and the people they support do have common goals, these tend to be large and abstract; everybody wants the company to succeed, for instance. In day-to-day life, people spend most of their time

thinking about and working on smaller, more immediate goals, and those goals rarely involve system administrators and other employees as partners. System administrators generally interact with too many people to be real team members; a system administrator normally supports a number of different teams, and you can't be a sixth of a team member.

So what can you do about it? First, you can try to improve communication in several different directions. Arrange things so you're talking to people when they are not already frustrated and upset. Find out what other people really do, so that you can think of them mentally as "the algorithms expert" instead of "the guy with the sticky keyboard." If people are willing to listen, explain things to them — most of them have no idea about things that we think are intuitive, as evidenced by the person who wanted a five minute explanation of the procedure for installing a device under UNIX. Any device. Under any version of UNIX. He thought there was exactly one procedure, the same for terminals, printers, disks, and so on; after all, devices are files, right? No wonder he thought system administration was easy!

Second, you can redefine the target. You're not going to achieve a situation where the system administrators are team members on every team they support, and you're unlikely to get a ratio where each system administrator supports exactly one team. Stop trying; aim for mutual respect and communication. Look for peers among other system administrators, and work at being a respected and respectful outsider among the people you support. Realize that this doesn't come automatically, and base your attempts to communicate on an understanding that you and the people you support come from different backgrounds and have different sets of expertise and knowledge.

Admittedly, this is widely regarded as terrible advice, and for good reason. "Separate but equal" has never been a highly successful theory. On the other hand, failure to acknowledge reality is not a highly successful theory either, and the reality is that system administrators are more like umpires than team members. It is therefore going to take real work to achieve a good relationship, and that work is not simplified by attempts to claim that system administrators and the people they support are peers — they're just too dense to notice it.

❑

This article was originally published in ";login: August 1994"

The Global Workforce

Jøns Dalum
marketing consultant
The Danish Chamber of Commerce

If Danish software companies wish to maintain their competitive edge, they have to look beyond the borders of their country. India is now a possibility.

India is normally associated with mass poverty and holy cows. During recent years, however, India has become a producer of high technology. Not many people in Denmark — or in Europe, for that matter — have noticed that India is moving towards becoming a major force in the exportation of computer services and software technology.

61% of the Indian software is exported to the USA — Europe purchases only 17%. What is it the Americans have discovered, and Europe is only just waking up to?

"During recent years India has become a producer of high technology"

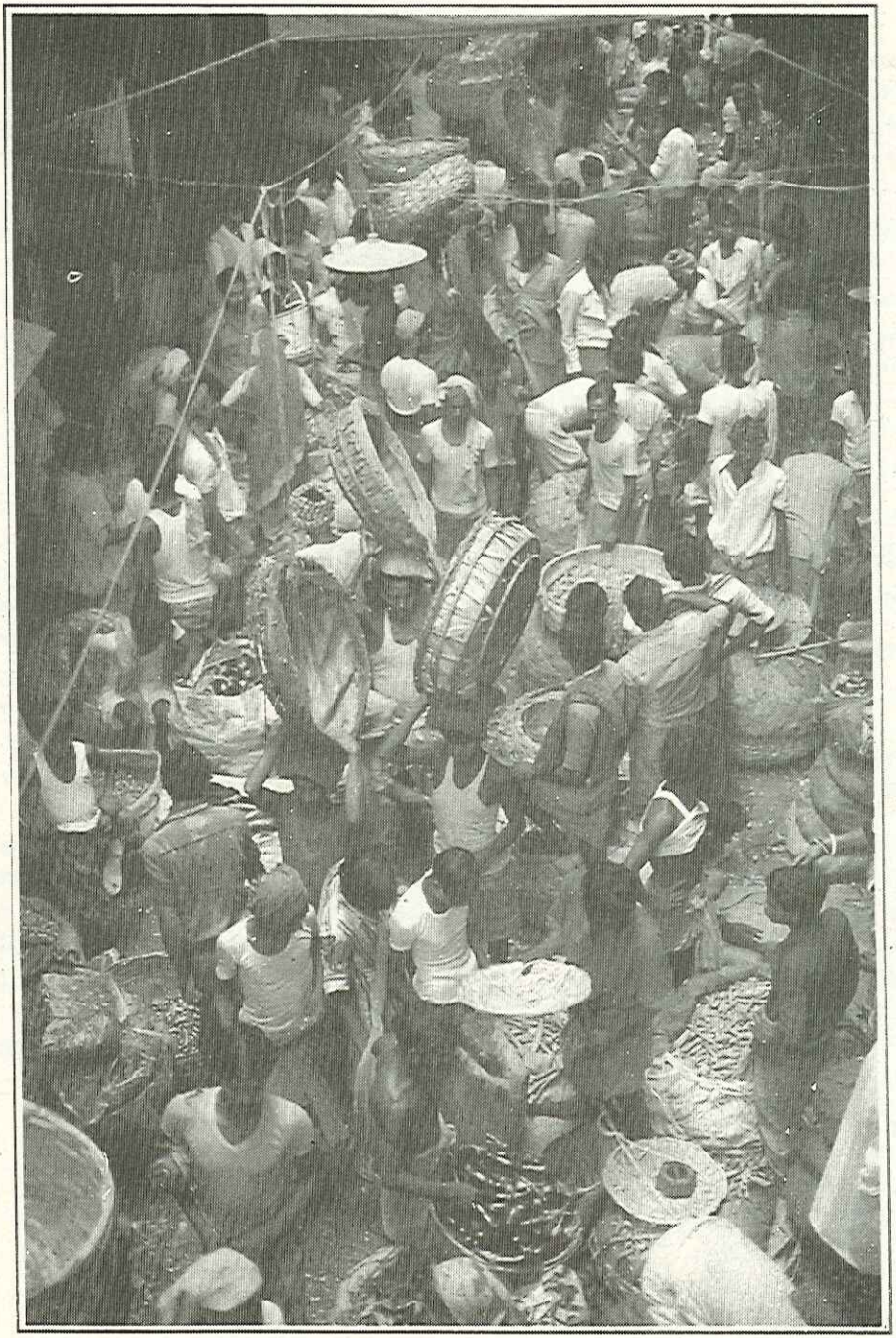
Good business for Danish companies

In order to shed some light on this, organizations, such as the Danish Chamber of Commerce, have worked on informing Danish companies about the Indian software industry. Most recently, the Chamber of Commerce sent a trade delegation to India, and the general impression among the companies was that Danish companies, with interests in information technology, would stand to gain considerable advantages on the international market by collaborating with suitable Indian companies.

The Chamber´s activities have produced results and, measured on a European scale, Danish software houses are well represented in India. 4 or 5 Danish information technology companies, including CRI International, DDE and Seven Technologies are represented in India. Most recently the Agricultural Computer-Center in Aarhus has established a subsidiary in Bangalore — the software-Mekka of India. It is expected that this 100% Danish-owned company will have 20-30 employees by the end of 1995.

The information technology scheme

India´s success in the field is due to a special relationship to the USA. During the 1980´s, when computer technology was almost nonexistent in India, prime minister



and computer enthusiast Rajiv Gandhi decided to make software a matter of strategic importance. Information technology was given very attractive business terms, and a scheme was set in motion to bring Indian computer programmers living in USA back to India. Rajiv Gandhi´s idea was extremely expensive, but it has succeeded to an astonishing degree.

"61% of the Indian software is exported to USA — Europe purchases only 17%"

Indian software production — and exportation — has exploded in the last decade. In the mid-eighties India exported for 24 million US dollars. This amount has today been increased to 450 million dollars, making software the fastest growing industry in India. Exports are expected to reach a billion dollars in 1997/98 — and all indicators point towards continued growth.

Difficulties with labour permits

The Indian software export was originally realized through so-called "body-shopping," meaning that Indian programmers worked for weeks or months on projects in the customers company, typically in USA. In Denmark, Girobank has recently been reported in the news as having a number of Indians working on a large conversion project, which is to be carried out in India. This "on-site" method is, however, being fased out, partly because it is expensive, and partly because of the difficulty in obtaining labour permits abroad, especially in USA.

Information technology by satellite

Today the Indian companies are predominantly aiming at acquiring so-called "off-shore" projects, where the work is carried out by employees in India. This is feasible, because many companies have bought access to satellite links, which allow them to work around the clock with the customer in USA or Europe. For example, the Patni Computer company in Bombay has over 400 employees, but no mainframe computers. The company uses a high-speed satellite link to hook up with the customers hardware when an assignment is under way.

The Indian domestic market has also developed significantly, and sales in India are expected to exceed the exports within a few years. The growth in the domestic market is partly due to India having introduced tough copyright regulations and lower tariffs on application and system software. With this in mind, India is an interesting market for European software-exporters.

10,000 new computer specialists a year

The growth described above has only been possible because India has a well trained workforce in the software domain. This growth has gathered further momentum, because of the relatively low wages paid to Indian programmers, compared to their western counterparts. There are 120,000 employees in the Indian software industry today, and every year 10,000 new specialists are trained. The monthly pay for a well educated programmer is Dkr 6,000 (about 830 ECUs).

Indian software companies are generally open to the idea of collaborating with western companies. However, a Danish company looking for an Indian partner would be well advised in examining possible partners very carefully. This should be professionally, as well as technically, economically and organizationally. As an example, Indian companies often have very professional management at the top. In the middle echelons of the company, however, the management is often very lacking, and it is through these people that communication will flow in any joint-venture.

"Rajiv Gandhi's idea was extremely expensive, but it has succeeded to an astonishing degree"

Global workforce

So far the Americans have been more successful than the Europeans in benefitting from the Indian possibilities on the software market. Danish information technology companies are only just beginning to show interest in international opportunities. In this regard, it has been said that no software will be produced in Denmark, 10 years from now, unless collaborations are undertaken with companies from the "cheaper countries." We will simply not be competitive. This is surely exaggerated, but this is not the last time we will be hearing the term "Global workforce" in the software domain.

❑

This article was originally published in the Danish magazine "PROSA-bladet May 1995."

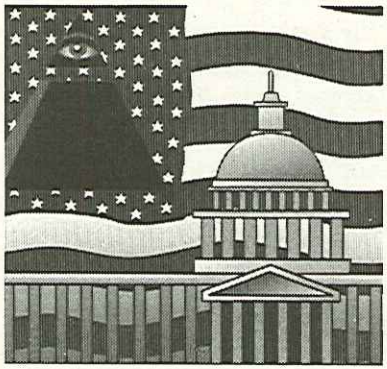
PGP, Phil Zimmermann, Life, the Universe, and so on ...

Greg Rose
PGP key ID: 09D3E64D
1994/11/30
<Greg_Rose@sydney.sterling.com>

[Author's Note: I´m preparing this article for ;login: in a very short time, mostly due to sickness, so I hereby state that in places I'm using (and modifying) words written by Hugh Miller of Loyola University Chicago. Hugh didn´t assert copyright on the material I´ve used, and it is in a good cause, so I hope he doesn't mind too much.

This article is presented for the information of members, in accordance with the Board of Directors´ desire to keep the membership informed, but the opinions expressed in it are not the opinions of USENIX or its Board of Directors. Other contributions and points of view are, of course, welcome.]

It´s funny that the resident Australian on the USENIX Board of Directors would write an article like this, but I sort of volunteered by being the one to bring this to their attention. Anyway, to cut a long story short, There Is Something Funny Going On, and if you aren´t aware of it, we think you might want to be. If you already know about the Grand Jury indictment proceedings involving Phil Zimmermann (prz@acm.org) then you can stop now, but if you don´t, please read on.



First, you need to know why I´m writing this. The combination of some fairly abstract mathematics, some archaic laws in the United States, and some "Pretty Good" software, has caused a situation with interesting ramifications.

Background: Public Key Cryptography

In 1976, Whitfield Diffie and Martin Hellman wrote a paper about asymmetric cryptography. If you imagine locks with keys to be analogous to conventional or symmetric cryptography, then public key or asymmetric cryptography is about a different kind of lock — where you have two keys, and one can secure the lock, but not open it, and the other can open the lock but not secure it. You keep the one that can open the lock in your pocket,

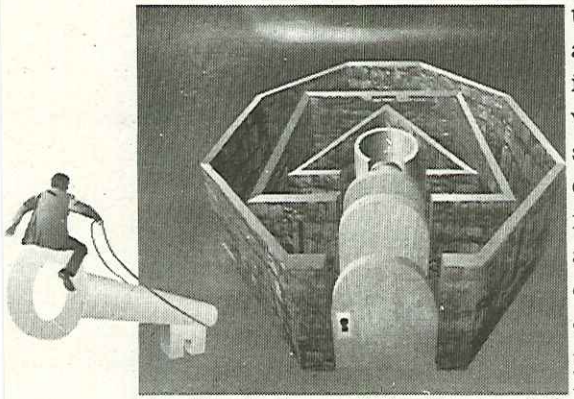
"Round up the usual suspects" — from another tale of spies and scapegoats

but you make as many copies as you like of the other one, and give them to your friends. Now, if you want to send a secret message to your friend Alice, you can lock it away using the copy of Alice's "locking" key, and only Alice can unlock it to read it. But there is another benefit (which stretches the analogy a bit): Alice could use her key to "lock" something away, and if you can use a copy of Alice's other key to "unlock" it successfully, you know that Alice must have "locked" it. This is the essence of digital signatures.

Ron Rivest, Adi Shamir, and Len Adelman invented what is called the RSA system a few years later. It is the only currently known system in which the keys used for "locking" and "unlocking" are interchangeable, the only difference being which one you keep secret. A careful reader will have noticed that I interchanged the meanings of "locking" and "unlocking" at the end of the last paragraph.

Phil Zimmermann, in 1990, used the RSA system in a program called "Pretty Good Privacy," or PGP for short, which enables people

to send secret messages to each other, or verify the authenticity of who sent it, or both. PGP is, in some sense, too good. According to the state of the art, messages encoded or signed with PGP are uncrackable and unforgeable.



(Side note: RSA is patented in the US, and some people think that Phil may have done something wrong in using a patented algorithm in PGP. However, that issue is completely irrelevant to the rest of this article, and if you think that it matters you may as well stop reading.)

This is Pretty Serious technology. It enables freedom fighters in southeast Asia to communicate securely. It may also allow terrorists in the US to communicate securely. The US has laws, under which PGP is classed as a "munition" in the same category as tanks and napalm, which prevent its export from the US. It is worth noting that, in the same sense a people in other countries can easily manufacture tanks and napalm, any decent programmer could implement RSA encryption knowing only the published algorithm. In fact, my own interest in this issue started in 1990 when I was doing exactly that in Sydney, Australia.

So what is the problem?

Somehow, PGP was illegally exported from the US, and it was almost certainly without Phil Zimmermann's knowledge. Phil is currently engaged with a US Federal Grand Jury considering his indictment.

Note that the indictment is not for actually exporting PGP himself, which the government freely admits he did not do, but for making it available in such a manner that it might get exported by someone else! The government clearly wishes to crush Phil and send a strong message about making software available on networks, especially software they don't like, even if the author takes significant care to discourage or prevent export. They wish to establish that the author is responsible for potentially illegal acts committed by others even without his knowledge or control.

This is the issue that is important and of interest to USENIX members.

Phil Zimmermann Legal Defense Fund Appeal

[Note: This section was originally written by Hugh Miller of Loyola University Chica-

go, but edited by me mostly to give up-to-the minute information, so blame me for any mistakes — Greg Rose]

> ***"The government clearly wishes to crush Phil and send a strong message about making software available on networks"***

In November, 1976, Martin Hellman and Whitfield Diffie announced their discovery of public-key cryptography by beginning their paper with the sentence: "We stand today on the brink of a revolution in cryptography."

We stand today on the brink of an important battle in the revolution they unleashed. Philip Zimmermann, who encoded and released the most popular and successful program to flow from that discovery, may be about to go to court.

It has been over fourteen months now since Phil was first informed that he was the subject of a grand jury investigation being mounted by the San Jose, CA, office of US Customs into the international distribution, over the Internet, of the original version of the program. [On January 12th, Phil's legal team met for the first time with William Keane, Assistant US Attorney for the Northern District of California, who is in charge of the grand jury investigation, in San Jose. The aim of this meeting was, I believe, to try and get the indictment proceedings stopped, but that failed, and the grinding process continues. An indictment, if one is pursued by the government after this meeting, could be handed down shortly. — Greg Rose]

If indicted, Phil would likely be charged with violating statute 22 USC 2778 of the US Code, "Control of arms exports and imports." This is the federal statute behind the regulation known as ITAR, "International Traffic in Arms Regulations," 22 CFR 120.1 et seq. of the Code of Federal Regulations. Specifically, the indictment would allege that Phil violated 22 USC 2778 by exporting an item listed as a "munition" in 22 CFR 120.1 et seq. without having a license to do so. That item is cryptographic software — PGP.

At stake, of course, is far more than establishing whether Phil violated federal law or not. The case presents significant issues and will establish legal precedent, a fact known to everyone involved. According to his lead counsel, Phil Dubois, the US government hopes to establish the proposition that anyone having anything at all to do with an illegal export — even someone like Phil, whose only involvement was writing the program and making it available to US citizens and who has no idea who actually exported it — has committed a federal felony offense.

The government also hopes to establish the proposition that posting a "muni-

tion" on a BBS or on the Internet is exportation. If the government wins its case, the judgment will have a profound chilling effect on the US software industry, on the free flow of information on the emerging global networks, and in particular upon the grassroots movement to put effective cryptography in the hands of ordinary citizens. The US government will, in effect, resurrect Checkpoint Charlie — on the Information Superhighway.

We may not all know the price Phil has had to pay for his courage and willingness to challenge the crypto status quo. For years now Phil has been the point man in the ongoing campaign for freely available effective cryptography for the everyday computer user. The costs, personal and professional, to him have been great. He wrote the original code for PGP 1.0 by sacrificing months of valuable time from his consulting career and exhausting his savings. He continues to devote large amounts of his time testifying before Congress, speaking at engagements around the world , and agitating for "cryptography for the masses," largely at his own expense.

> *"The US government will, in effect, resurrect Checkpoint Charlie — on the Information Superhighway"*

Phil´s legal team consists of his lead counsel, Philip Dubois of Boulder, CO; Kenneth Bass of Venable, Baetjer, Howard & Civiletti, in Washington, DC, first counsel for intelligence policy for the Justice Department under President Carter, Eben Moglen, professor of law at Columbia and Harvard Universities; Curt Karnow, a former assistant US attorney and intellectual property law specialist at Landels, Ripley & Diamond in San Francisco; and Thomas Nolan, noted criminal defense attorney in Menlo Park.

While this is a stellar legal team, what makes it even more extraordinary is that several of its members have given their time for free to Phil´s case. Still, while their time has been donated so far, other expenses — travel, lodging, telephone, and other costs — have fallen to Phil. If the indictment is handed down, time and costs will soar, and the members of the team currently working pro bono may no longer be able to. Justice does not come cheap in the US, but Phil deserves the best justice money can buy him.

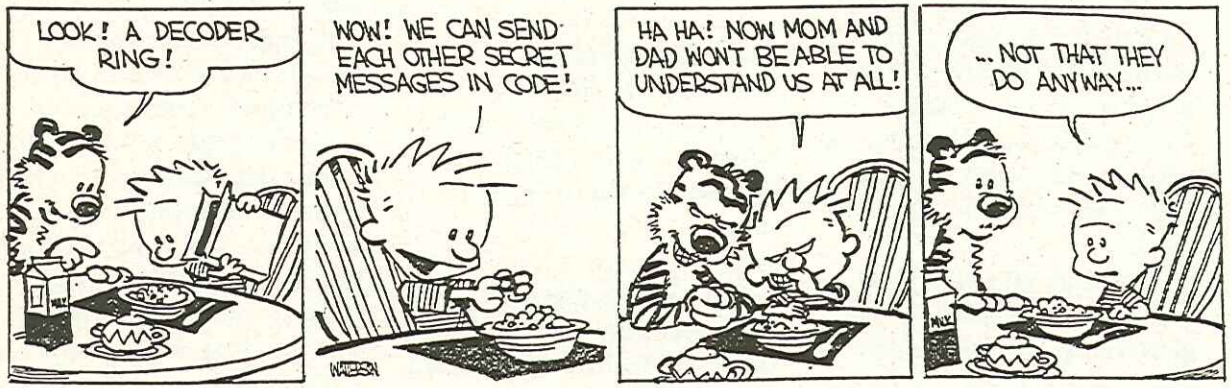
> *"Justice does not come cheap in the US, but Phil deserves the best justice money can buy him"*

This is where you and I come in. Phil Dubois estimates that the costs of the

case will run from US$100,000 - $150,000 [if an indictment is handed down], leaving aside the lawyers' fees. If Phil's team must charge for their services, the total cost of the litigation may range as high as $300,000. The legal defense fund is already several thousand dollars in the red.

Phil has assumed the burden and risk of being the first to develop truly effective tools with which we all might secure our communications against prying eyes, in a political environment increasingly hostile to such an idea — an environment in which Clipper chips and digital telephony bills are the government's answer to our concerns. Now is the time for us all to step forward and help shoulder that burden with him.

It is time more than ever. I call on all of us, both here in the US and abroad, to help defend Phil and perhaps establish a groundbreaking legal precedent. PGP now has an installed base of hundreds of thousands of users. PGP works. It must — no



other "crypto" package, of the hundreds available on the Internet and BBS's worldwide, has ever been subjected to the governmental attention PGP has. How much is PGP worth to you? How much is the complete security of your thoughts, writings, ideas, communications, your life´s work, worth to you? The price of a retail application package? Send it. More? Send it. Whatever you can spare: send it.

A legal trust fund, the Philip Zimmermann Defense Fund (PZDF), has been established with Phil Dubois in Boulder. Donations will be accepted in any reliable form, check, money order, or wire transfer, and in any currency, as well as by credit card.

You may give anonymously or not, but please — give generously. If you admire PGP, what it was intended to do and the ideals which animated its creation, express your support with a contribution to this fund.

How to donate

To send a check or money order by mail, make it payable to "Philip L. Dubois, Attorney Trust Account." Mail the check or money order to the following address:

Philip Dubois
2305 Broadway
Boulder, CO USA 80304
(Phone #: +1-303-444-3885)

To send a wire transfer, your bank will need the following information:

Bank: VectraBank
Routing #: 107004365
Account#: 0113830
Account Name: "Philip L. Dubois, Attorney Trust Account"

Now here´s the neat bit. You can make a donation to the PZDF by Internet mail on your VISA or MasterCard. Worried about snoopers intercepting your e-mail? Don´t worry: use PGP.

Simply compose a message in plain ASCII text giving the following: the recipient ("Philip L. Dubois, Attorney Trust Account"); the bank name of your VISA or MasterCard; the name which appears on it; a phone number at which you can be reached in case of problems; the card number; date of expiry; and, most important, the amount you wish to donate. (Make this last item as large as possible.) Then use PGP to encrypt and ASCII-armor the message using Phil Dubois's public key. (You can also sign the message if you like.) Email the output file to Phil Dubois (dubois@csn.org). Please be sure to use a "Subject:" line reading something like "Phil Zimmermann Defense Fund" so he'll know to decrypt it right away. You can easily find out how to get PGP and Phil Dubois´ public key if you want to, just see the various FAQs in sci.crypt and alt.security.pgp

❑

This article was originally published in ";login: April 1995"

What Good is a Gig?

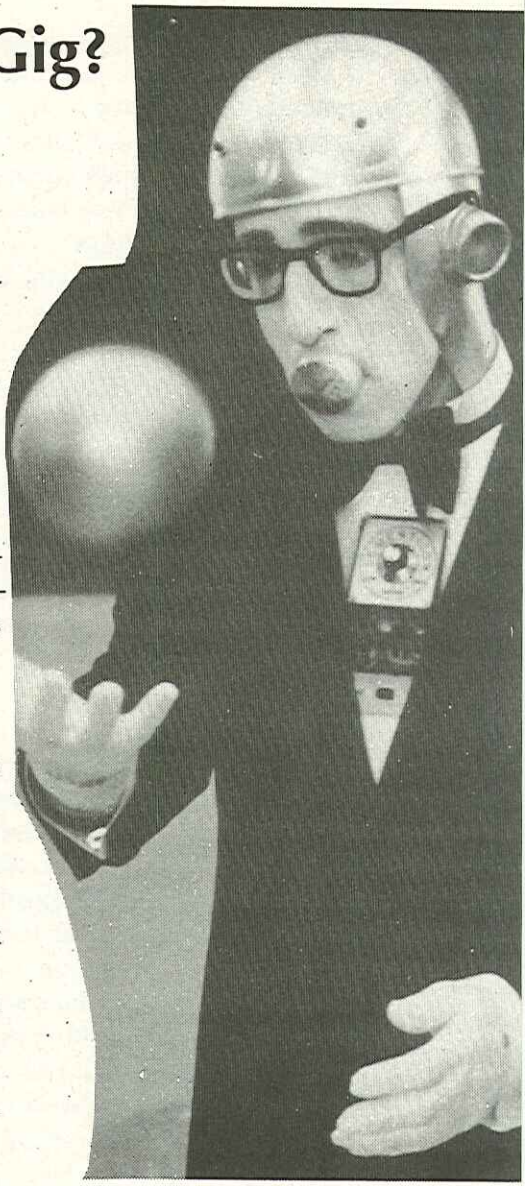
Scott Hazen Mueller
<scott@zorch.sf-bay.org>

I was telling my wife about the gigabit RAMs that are due out in the year 2000, and she asked me, "What can you do with a gigabyte of memory? Especially if you can only use 640K at a time?"

Now maybe that 640K limit will soon be as relevant as handcranks on cars, but the question still stands. What sorts of things become possible? What becomes easy? What becomes more difficult? Furthermore, what about gigabytes of disk? Gigapixels of display? And gigabits of bandwidth? What will they enable in the future?

If the only differences new technologies bring are in terms of quantity, then I'm not interested. I don't care that much about running window systems faster, or having 100 applications resident at the same time, or whatever. Likewise, a 32k x 32k pixel display, while marginally mind-boggling, is not all that exciting if it's just one big screen that I run my Window system on. The future needs to be about new functionality, if it is going to be fun and interesting, and more importantly, if computers are to really penetrate society and become useful tools for everyone. New technologies should be used to unleash new capabilities, not just make the same old ones run faster.

Take, for example, the user interface. The most common user interface, the teletype, basically dates back to middle of the century. Some work has been done in the area of penbased input, but that is a niche market and is likely to stay that way. Speech input has been around for a few years, but the current implementations



The future might not look like this.

have many drawbacks. This is definitely an area in which technological advances can make a difference. As computer power becomes cheaper, it becomes more reasonable to use brute-force algorithms, such as really large lookup tables, to decode speech input. I think that speech input will have a definite place in the user interface of the future.

The keyboard will likely be with us for some time to come. It is just too hard to beat a keyboard for bulk entry of text. Various firms are already doing work in new methods of attaching the keyboard. Remote control units for consumer electronics are already so ubiquitous that there are firms making programmable units that can replace several device specific units. Converge these two trends, and you come up with remote keyboards, portable units that interface via infrared or digital radio to computers. I would like one right now, so I can do away with that annoying cable.

What about output methods? Larger memories is one enabling technology for larger displays, but I seriously doubt that we'll actually see monolithic gigapixel displays anytime soon. What I do consider possible is the multi-headed paradigm, with several physical devices sharing one virtual display space. That display space will contain more than just computer applications. Consider for a moment the effects of the convergence of television, telephony, and computing. AT&T hopes to make the television into a device to access information via the telephone. Computer companies want to integrate telephone and television access into your desktop system. Cable television companies want to start delivering telephone service over your lines, and give you information services over those same lines.

One way to look at this is as a conflict, in which one model (and side) wins, and the other falls by the wayside. Another way to look at this is to focus on the convergence, the melding of the three technologies. If you take a system with gigabits of bandwidth, several gigabytes of secondary storage, and a few gigabytes of physical memory, there is no reason whatsoever it cannot fill all roles at once.

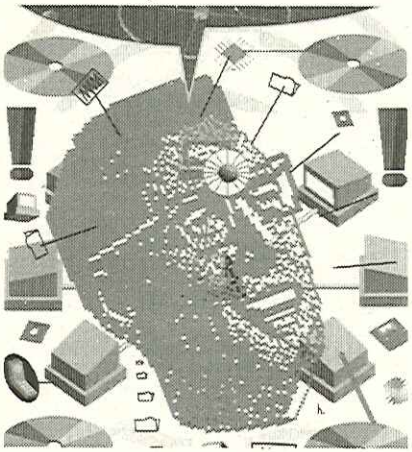
Taking that premise, it begins to make sense to view physical display devices as windows into a private virtual information world, all sharing a common space, but from different points of view. Looking at it that way, then any one of multiple screens can be used in any of the roles, as a viewing device for text and graphical information (computer), as a point-to-point communication channel (video phone), or as a terminal for pre-programmed video (television).

Think of the virtual world as a sort-of virtual desktop. Instead of just a bunch of glass teletypes, the worldscape can have live video, several kinds of communications gateways, local applications, and who knows what else, all existing in parallel, and viewable from any dis-

play on the system. Instead of having a screen saver that has to monitor activity and then become active, have a virtual fish-tank somewhere in the world, and have the displays pan to it when they are not being used for something else.

Also, the portable keyboards I mentioned above could be used in conjunction with any of the display devices. If you want to work in a different room, simply carry your keyboard to a new place, pan the display to the area you were working in, and there you are. If the keyboards use digital radio to interface to the computer, the system could even track you as you moved around the building, and have your workspace ready for you.

What are some of the possibilities that are enabled by massive local storage? Right now, I can buy about half a gigabyte for a little over $200. That's a nice amount, but it's quite easy to fill that up just with a fully-featured system, not to mention the applications and interfaces I've been talking about. Even halving the cost per megabyte is not going to make much difference; a gigabyte of disk just isn't that much. However, the cost will probably drop around 10x by the end of the century. That may well be enough to make a difference. For example, my wife's vinyl record collection



takes about 11 linear feet of space. My first-order estimate is that it constitutes 10 gigabytes of audio data. At today's prices, it would run about $3500 to buy enough disk space to digitize all of that data. In a few years, the cost would fall to $350, certainly well within the reach of a computer-literate middle-class couple. At that point, not only does massive local storage become practical, but it also becomes desirable, because you can do things with the data on-line that you simply cannot do in the original format. For example, we could categorize every song from the collection by artist, title, type, enjoyment factor, date, mood, or whatever. Then, we could arrange to play them by any of those categories, at any time, without having to shuffle media. On top of that, we could buy new songs as they came out and add them to the collection, at a low incremental cost.

It probably wouldn't be practical to do the same with our videotape library but we could certainly reprocess them to newer media, e.g. 8mm or 4mm tape, in digital format, and archive them for future use. Instead of needing a dedicated device (the VCR) to view them, we could just load the archive tape into a drive used also for routine backups, and view them on any of the system

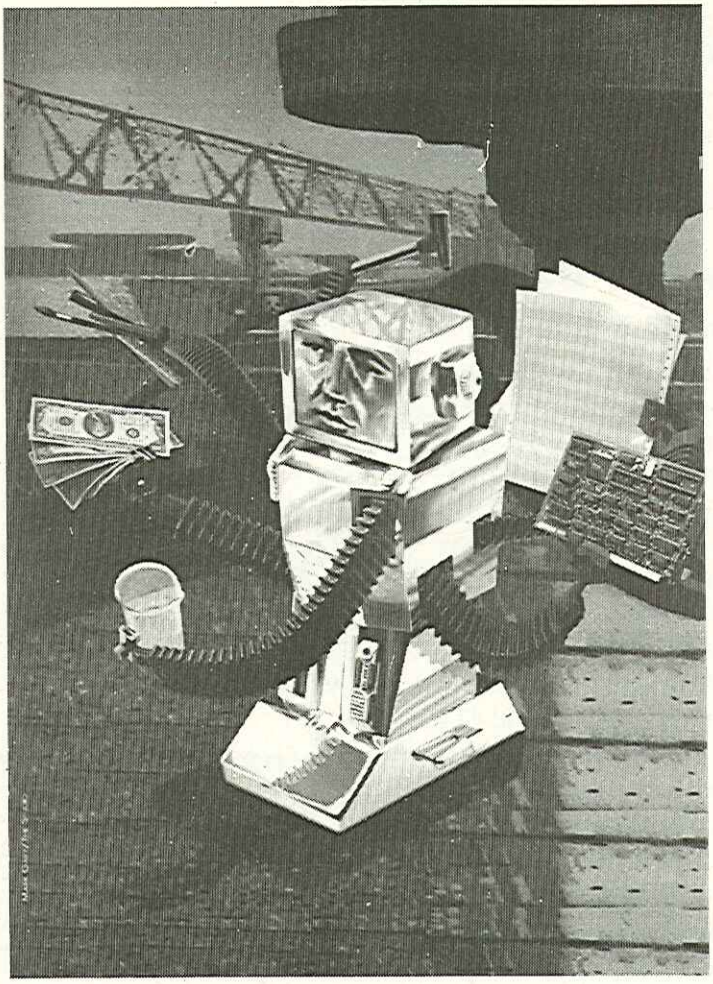
displays.

I can't see handling our books in this way; they have physical properties that we find attractive. We do own plenty of paperbacks that frankly, I would archive, since they have a limited lifetime. For a lot of textual material, it would make sense to scan and archive it. I would do the same with our various paper records; even an 8mm tape takes much less room than a moderate-sized file.

There is a downside, of course, to having this much on-line capacity. It would be quite difficult to ensure good backups. This would create a tension between the distributed and centralized model. If the bandwidth from the providers could be put into place, it would become much more convenient to merely access data over the network, and let the provider worry about backup. However, if the cost for network access is too steep, then people will want more of their data on their own local system, so that they can access it for free. In the final analysis, the communications channels are going to be the glue that holds everything together. Without sufficient bandwidth, video-on-demand becomes impractical. Without bandwidth as a driver, the convergence of television into the computer/telephone complex becomes much less likely. Without the convergence of television, I don't believe that the display technology will be driven into the shared mode I've envisioned. Without shared displays, the computer will be just a box that sits in the corner and processes text information at the paltry 112 kilobits/second available over ISDN.

The wide bandwidth channels will enable everything to happen all at once, and this is going to be the key factor in converging all of the current computer and communication technologies into one bundle. The networking will have to enable seamless interface between technologies. For example, my wife and I have two computers, two displays, keyboards and mice, two televisions in the house, and several telephone, including two in the office. All of these are basically unshared resources, even though we have the computers networked together. Tying the computers together at 10 Megabits/second enables some sharing, and we can exchange files and the like, but that is about all.

In order to share memory, I/O devices and peripherals, and generate the virtual world, it will be necessary to network systems at gigabit rates. Likewise, general-purpose video will require the same high data rates. Voice telephony does not require the high data rates, but establishing the in-building network makes it possible to attach phone sets as access points. Furthermore, if the phone sets are connected to the network, they can be used as voice-input terminals. For some functions this will most likely be more convenient than keyboard entry. As an example, a phone set in a family room could be



used to order up video on the display (formerly television) there.

These technologies are exciting, and I look forward to seeing computers handle more and more communication tasks for everyone. What I really want to know is what sort of social changes these tools will bring about. Some changes are already here. There are many more great changes coming, and — like the person trying to envision the world today after seeing a car for the first time — what is visible now is just the very beginning.

❑

This article was originally published in ";login: April 1995"

Linux grows

René Seindal
(seindal@diku.dk)

It is well known that Linux started as the hobby project of a Finnish computer science student, and has developed from there.

It now seems that Linux is maturing. The steadily increasing number of Linux users are making it hard to ignore, and commercial software has started to appear — something that was unthinkable when Linux was just a hacker-system.

The amount of commercial software for Linux will soon increase even further, when Linux changes to the ELF object format, which it will share with several commercial UNIX-versions. Work is also progressing on converting Linux to other types of hardware than the 80386 based PC. When this happens the numbers of Linux users can be expected to increase again.

The ELF Object Format

It has been possible for some time to run programs on an experimental basis in the ELF format under Linux. Many have wished to use WordPerfect under Linux, since there is no other WYSIWYG word-processor for the system.

Several other UNIX systems for PCs use the ELF object format. It is already possible to use most program files for these systems under Linux. It is a requirement that the programs are statically linked. If dynamically linked libraries are used, problems of compatibility will arise.

In this way, WordPerfect for Linux is a reality without WordPerfect having created a version especially for Linux. Since most suppliers offer versions of their products for systems such as Unixware and SCO, these can also be expected to be available for Linux. How this will influence the demand for Linux is impossible to say, but it will surely not lessen it.

Coming editions of the Ygdrasil Linux on CD-ROM will exclusively utilise the ELF format, which is expected to become the standard format within a few months.

Linux on new hardware

Linux has always been confined to the PC, because the kernel was only available in a single edition, and this edition wasn't particularly portable. This will soon change. Work is under progress on moving the system from the Intel 80386 processor to the Motorola 68K processor, to Digitals ALPHA processor, to

MIPS, to Sparc 4 and to Power PCs.

The Motorola edition is the one nearest to completion. The conversion is being done on Amiga and Atari computers, and looks very promising. The developers have a functioning kernel, and are able to bring up a system that is capable of compiling itself. They still need X-windows and a number of hardware-specific drivers. This will in all likelyhood be the first non-PC edition of Linux to be released. Whether it will run on Macintosh computers remains to be seen.

Linux for Digitals ALPHA risc processor is also progressing. The System can be brought up, but is still rather limited. The developers have stated that only a hacker could love the project as it is now. The conversion is being done with cross-compilers, which can run on Linux/386 or OSF/1 on the ALPHA processors.

The other three conversions are still in the very early stages, and it will be some time before they are functioning.

An important matter, which all Linux developers are working on, is the gathering of all these branches of the system into a unified source hiearchy. Linus Torvalds is personally coordinating these efforts. Anybody who has installed a recent edition of Linux will have noticed that there have been some relocations in the kernel source. For the moment only the Intel 80386 and Motorola 68K editions' sources have been unified, but more will be done as work progresses on the other conversions.

❑

This article was originally published in the Danish magazine "PROSA-bladet April 1995."

Linux

Calendar of Open Systems Events

Jan Sæll
YASK SystemKonsult AB
<jan@ask.se>

I have made this calender from different sources (newgroups, Usenix papers and so on). Contact persons with Email stated where available.

If you think that I have missed something, or if you have an event that should be in the calendar, mail me and I will include it next month. My Email address is jan@ask.se.

June

5-7	USENIX	UNIX Security	Salt Lake City, UT, USA
8-23	ACM	ACM SIGPLAN Conference	La Jolla, CA, USA
26-29	USENIX	Conference on Object-Oriented Technology	Monterey, CA, USA

July

6-11	USENIX	Tcl/Tk Workshop	Toronto, Canada
4-5		1st IEEE International On-Line Testing Workshop (nic@verdon.imag.fr)	Novotel Nice Centre Nice, France
10-14		IEEE 1003	USA
17-21	IETF	IETF	Stockholm, Sweden
17-21		NetWorld+Interop 95	Tokyo, Japan
31-4		Technology of Object-Oriented Languages and Systems (tools-info@scs.fiu.edu)	Santa Barbara, California, USA

August

6-11	ACM	ACM Siggraph	Los Angeles, CA - USA

13-18		Interex 95	Toronto, Canada
14-18		Computers in Context: Joining Forces in Design (bodker@daimi.aau.dk)	Århus, Denmark
25-27		9th Nordic Symposium on Computer Simulations of Liquids and Solids (nscs95@fy.chalmers.se)	Gothenburg, Sweden
30-1	ACM	ACM SIGCOMM '95	Cambridge, MA, USA

September

5-9		Media Vision	Stockholm, Sweden
6-8	EurOpen	Internet Security Seminar	Budapest, Hungary
11-13	EurOpen	Internet Security Seminar	Stockholm, Sweden
11-15		High performance networking, HPN'95	Palma de Mallorca, Spain
12-14	GUUG	GUUG'95 Annual meeting and congress	Wiesbaden, Germany
18-21	AUUG	AUUG	Sydney, Australia
18-22	USENIX	LISA '95	Monterey, CA, USA
19-21		UNIX Expo	New York, USA
25-29		NetWorld+Interop '95	New York City, USA
26-29		Networks, Data Telecom - Stockholm, Sweden	
29-1		MAXIDATA Explosion - Stockholm, Sweden	

October

9-13		IEEE 1003	USA
12-15		SIGSOFT '95	Washington, DC, USA
15-19		Object-oriented Programming, Systems, Languages and Applications	Austin, TX, USA

23-24	EurOpen	Publishing on the Internet	Amsterdam, Holland
25-26	EurOpen	Publishing on the Internet	Stockholm, Sweden
25-28	IEEE	Parallel & Distributed Processing Symposium	San Antonio, TX, USA

November

1-4	GURU	ROSE'95 (rose@guru.ro)	Bucharest, Romania
2-8		DECUS	San Francisco, CA, USA
3-5		Computers At Home 95	Stockholm, Sweden
5-9	ACM	ACM Multimedia '95	San Francisco, CA, USA
6-8		Mac World Expo 95	Stockholm, Sweden
6-10		NetWorld + InterOpen '95	Paris, France
21-24		Scanautomatic	Gothenburg & Stockholm, Sweden

December

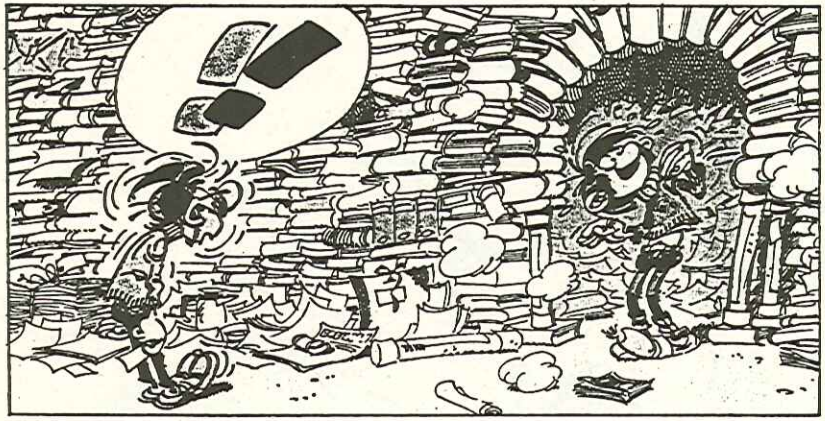
2-7		DECUS	San Francisco, CA, USA
3-6		SOSP	Colorado, USA
4-8		IETF	Dallas, TX, USA
11-14		4th World Wide Web Conference	Boston, MA, USA

EurOpen Book Scheme

EurOpen has negotiated special rates for its members on books from O´Reilly & Associates, typically at three quarters of the list price.

The special EurOpen discount prices **do not** include postage and packing.

Please contact the Secretariat for a listing of the books.



EurOpen Quarterly

EurOpen Quarterly 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

❑