EurOpen Quarterly

EurOpen — The European Federation of Open Systems User Groups — November 1995, Issue 3

Yahoo

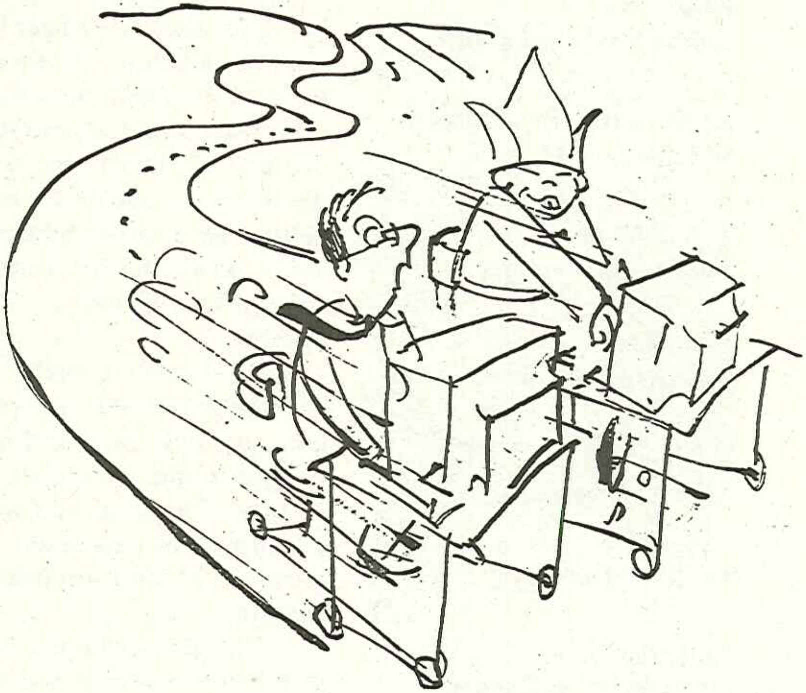
From homegrown to fullblown — Yahoo started as a private tool for two students, less than two years later they recieve more than two million hits per day and are about to turn into a business for its two founders.

Zen and Internet

Brian Eberhardt has (inspired byWinnie The Pooh) contemplated the relations between Internet and the philosophy of Tao).

IP - Next Generation

The Internet is running out of IP adresses — IPng is the chosen solution.



Contents

Three-quarters

There is an English expression: “to add insult to injury”. That is a pretty apt describtion of what happened with the second issue of EurOpen Quarterly. After finally being finished, well past the original deadline, all the copies ended up collecting dust on a shelf at the distributing center. The distributor simply forgot to distribute the copies! By a rather bizarre set of accidents this wasn´t noticed for well over a month.

This shouldn´t really have been possible, all we can say is: Sorry! It will not happen again — ever! At least not like that, and we promise to be extremely paranoid about everything this time.

Still, this third issue is delayed as well. The reasons are more or less the same as those that caused the original delay of the last issue: lack of material. We have ended up using a lot of material from the DKUUG-Nyt. The alternative would have been to use more US material, but it really ought to be possible to make a European magazine consisting of, at least primarily, European material.

But aside from all these excuses and complaints we still think that this issue is a pretty good one. We have tried to balance the hard technical material in “IPng”, “FreeBSD”, “Everest”, and “PGP, the Book” with more “soft” material about “Yahoo” and “The Birth of an Internet Newspaper”. We have even tried to add some philosophy with “Zen and the Art of Internet Understanding” — it may sound somewhat frightening but do not despair: the main inspiration for the article came from Winnie The Pooh!

❑

ZEN and the Art of Internet Understanding

Brian Eberhardt has engaged in some philosophical thinking on the relations between the Internet and our daily lives, and the connections between Eastern Taoism and his activities on the great Internet.

Brian Eberhardt
SuperUsers A/S

Always getting there, the Present & the Little Things

The Internet and Taoism has something in common. Tao means "The Way" in the sense that the important thing is the journey — getting there, being in transit, not the actual arrival at the goal. Once you have reached any given goal this is no longer a goal as one has already defined a new goal. Exactly thus is the nature of the Internet, in any given moment (the Present) one always finds oneself somewhere on the Information Highway.

Another important concept in Taoism is "The Little Things" and their great importance. This is the very na-

"It is hard to be brave," said Piglet, sniffing slightly, "when you´re only a Very Small Animal."

Rabbit, who had begun to write very busily, looked up and said:

"It is because you are a very small animal that you will be Useful in the adventure before us."

Quoted from Benjamin Hoff's "The Tao Of Pooh" ture of the Internet with its great number of small computers adding up to the Internet. Each unit on its own has no significance, but all of them combined become the wholeness of the Internet.

The Tao of Geography

"The Way", getting there, has always had great importance in our daily lives. Since the first means of transport were introduced, slowly mankind has become more and more dependent on being able to transport itself from one place to another. Today one can attend meetings and conferences anywhere on Earth without any great sacrifice of neither money nor time. The concept of geographical distance has lost its essence, due to the ease with which we can move across the planet and our society is very much based on this fact. We are always getting there, but often the transport is "offline", we travel a great distance to reach a given destination only then to go "online", i.e., participate or meet in the context desired. In a similar way, information received is often "offline" (past, obsolete). Once we are reading it, it has been updated (latest issue, latest revision, latest edition, latest plan, etc.).

Experiencing the Present, here and now is important also when travelling. On a journey of experience this is the very experience. But during business travel and when dealing with "snail-mail", many experiences are offline.

The Tao of the Internet

The Internet is eliminating the concept of distance in a new sense; now it is often unnecessary or uninteresting to move geographically by traditional means of transport.

Where once travelling and physical transport of goods was necessary, today more and more information is being exchanged via the Internet.

When you are browsing/surfing the Internet via WWW you are always online. You are in the Present as defined by Taoism. This is one of the important elements of WWW — the information received is "here and now information". It is not an old issue of some department store catalogue you are browsing, but always the very latest. The Internet is more intense, more Present than the heap of mail gathering, waiting to be read.

The meaning of The Little Things

Another basic concept in Taoism is "the meaning of the Little Things". That which forms the experience in the Present is the sum of our environment. Everyday things are what makes us experience joy. The art of understanding this is Taoism in a nutshell.

The structure of the Internet is consisting of 50.000 networks again consisting of 4 million computers, which in turn are operated by more than 50 million users (1995-

I can see my watch, without taking my hand from the left grip of the cycle, that it is eight-thirty in the morning. The wind, evne at sixty miles an hour, is warm and humid.

I´m happy to be riding back into this country. It is a kind of nowhere, famous for nothing at all and has an appeal because of just that. Tensions disappear along old roads like this. We bump along the beat-up concrete between the cattails and stretches of meadow and then more cattails and marsh grass. Here and there is a stretch of open water and if you look closely you can see wild ducks at the edge of the cattails. And turtles... There´s a red-winged blackbird.

I whack Chris´s knee and point to it.

"What!" he hollers.

"Blackbird!"

He says something I don´t hear. "What!" I holler back.

He grabs the back of my helmet and hollers up, "I´ve seen *lots* of those, Dad!".

"Oh!" I holler back. Then I nod. At age eleven you don´t get very impressed with red-winged balckbirds. You have to get older for that.

Quoted from Robert Pirsig´s "Zen And The Art Of Motorcycle Maintenance" figures) is the very example of all the little things combined to create a wholeness.

Past and Present

Traditional means of transport such as ships, trains, cars, aeroplanes, etc. have influenced our daily lives greatly. Our whole way of life both private and in business is based on geographical mobility. Not so long ago, a person might never once in his entire life leave his home town and consequently would not be able to understand any other dialect than his own. Today we are spinning around, spending a lot of time on offline transport (the movement from X to Y itself is without any importance, only the destination counts). We have become dependent on geographical mobility to get to work, to go shopping, to visit friends and aquaintances, etc.. Our entire society is made for and based on transporting ourselves and things, things, things, from one place to another. The invention of different means of transport has become the foundation of functioning in the western world of the 1990´s.

Present and Future

The Internet is changing this way of life. With the Internet a lot of our offline transport will disappear. In many situations we will choose to avoid unnecessary transport, using the Internet instead when sending/receiving information, renewing bus-passes, checking out library books, reading newspapers, having video-conferences for secondary meetings, shopping, etc., etc. — the list is endless. This development of the Internet will influence our daily lives greatly in the next few years. We technicians have a very limited imagination in this area. We can hardly grasp the immense changes in society (and our own lives!) that this will bring about.

New basic technologies have proven themselves to change first our way of doing things, then what we are doing, and in the end our environment.

This may sound both good and bad. It is bad having to mope in front of our monitors all day long and good to rid oneself of offline transport and offline information. Only God knows the answers to how our future and how our surroundings will change.

Take care of each other!

❑

This article was originally published in DKUUG-Nyt No. 78, May 1995

IP — The Next Generation

The Internet is about to run out of address space. What seemed a "more than adequate number of addresses for all future use" back in the ´70s have turned out to be too few even for the near future. Jens Fallesen describes **IPng** — the solution that hopefully will allow the Internet to keep expanding.

Jens Fallesen
DKnet

Once back in the 1970´s some visionary people came up with the idea that IP should have 32-bit addresses so "you wouldn´t run out of addresses for a while". It has probably dawned on most of us that the truth of the matter is a different one, and there are two major problems: Firstly we are running out of addresses -- there are different theories as to when this will happen — and furthermore routing tables are becoming too big and complicated in the central routers on the Internet.

How are we to solve these problems?

Either we create a new IP-protocol with improved longevity or we prolong the lifespan of the existing one.

Both solutions are very problematic — the first demands new software in everything that runs IP, and that is a great deal of gadgets worldwide — and the other solution is no solution, really, but simply a question of postponing the problem.

Still there is a major interest in prolonging the life of IP. This is due partly to the time it takes to define a new standard, and partly to the fact that once the standard is agreed upon, a great deal of time passes before the equipment is adequate.

Saving Proposals

One of the prolongations is "private address space", as defined in RFC 1597. Here a series of addresses is reserved for internal use in networks which will never connect to the Internet, any-way. This could be firms which are not hooked up to the Internet, or a matter of having all hosts behind a Firewall. This may also be used on a routing-net, as addresses on the internal nets normally never go out onto the Internet. This reduces the demand for officially registrated IP-numbers.

Another prolongation is Classless Inter-Domain Routing (CIDR). CIDR means that the netmask could have any length, not depending on classtype (A, B, or C) when routing IP-addresses. Then you can route an entire block of C-classes in one entry — for example, 193.88.0.0-193.88.7.255 might be routed with the mask 255.255.248.0. This routing would often be defined as 193.88.0.0/21, i.e. 21-bit. Thus the routing tables have been reduced considerably.

Both of these methods may postpone the problem, but it is still only a matter of time before the problem arises once more.

New Protocol

The solution must be creating a new protocol, and since the middle of 1994 a lot of very competent people have spent a great amount of time doing this. They have been very busy, as there are many requests to consider.

It all started back in 1992. A series of suggestions were made to replace the current IP-protocol:

- CNAT
- IP Encaps
- Nimrod
- Simple CLNP
- PIP
- SIP
- TP/IX

Some of these evolved, so that IP Encaps became IPAE and Simple CLNP became TUBA. Then IPAE and SIP were united as SIP, and ultimately, the new SIP was united with PIP to become SIPP. This coincided with TP/IX becoming CAT-NIP.

I shall not go into the different protocols, but in mid-1994 it was agreed to proceed with IPng (IP next generation), based mainly on a 128-bit version of SIPP.

IP next generation

A set of criteria was made for IPng, including that the problems of IPv4 (the present version) was to be solved:

- 32 bit in IP-addresses are not enough. We are running out of addresses.
- Routing tables in backbones grow too quickly.
- The hierachy of net, subnet and host in IP is too simple.
- The classification (A, B, C, D, E) is impractical, and lacks specific classes, e.g. mobile computers.

Another important problem to be addressed was the transition from IPv4 to IPng. And if that was not enough, new facilities were required, for example real-time flow, built-in security, and automatic configuration.

As it happens all of these problems have been solved in IPng! An address-space of 128 bits equals 665.570.-793.348.866.943.898.599 addresses per square meter of the face of the Earth. Even the most pessimistical hierarchal division of the addresses still leaves 1564 addresses per square meter. It is plausible, then, that the addresssection will be big enough well into the future.

There are three types of IPng addresses:

- Unicast — single node
- Cluster — a group of nodes sharing a common address where packages to the cluster-address goes to one of the nodes.
- Multicast — a group of nodes, where a package sent to one address goes to all nodes in the group.

Routing in IPng is much like the present routing with CIDR, only on a 128-bit level. There are a few differences, such as better possibilities for hierarchal and more efficient routing. It will be easier to pre-select one of several possible routes. Mobile computers can be moved worldwide and automatically be assigned a local IP-number, as well as re-addressing, so that routing for some nodes can be altogether avoided.

In addition to solving the problems, IPng includes a number of novelties, flow control, for example. This is something which benefits applications such as live video or sound — it takes a certain consistency to ensure fluency in the pictures and sound transfered. This problem is solved by giving different types of flow control to different types of packages. A live quality video session must be put through continually, while a newsfeed, for example, is mere excess capacity traffic.

Security

Another novelty — maybe the most important — is security. Security is an integral part of IPng, not something you have to add yourself on top of IPng. There are two security functions in IPng:

IPng Authentication Header

This is a facility proving only that the package is authentical and originates from the party posing as sender. The method itself is independent of algorithm, but the use of Keyed MD5 as signature has been suggested. With this function in IPng, packet spoofing and the like becomes very difficult, as a package can only have a valid Authentication Header if it originates from the right source.

IPng Encapsulating Security Header

This concerns encryption of the data transfered. Using DES has been suggested.

The seperation of these two functions has been made to avoid legal problems in countries that restrict the use of encryption.

It is often the case that encrypted identification is allowed in these coutries, while actual encryption of data is not allowed. With this classification it is possible to at least use identification when sending to or from these countries.

Another important novelty in IPng is Automatic Network Configuration. This is known from Apple-Talk, among others; once you turn on your machine it finds a free IPng-address by itself. This makes network installing easier — your router needs only to know which net you have, then addresses in this net is assigned dynamically. We have already seen initiatives towards this in IP through DHCP; now it becomes a part of basic protocol.

Headers

In spite of all these new features and the bigger address space (which is four times the size used in IPng), the IPng-header is only twice as big as the one in IPv4. The header is more simple and thus more efficient. The header in IPng consists of a series of standard sections:

- Version
  4-bit version number — in IPng, this is 6.
- Flow Label
  28-bit label for the above mentioned possibilities for flow control.
- Payload Length
  16-bit section containing the remaining lenght of package (after header).
- Next Header
  Stating the type of the following header, for example a TCP or UDP header.
- Hop Limit
  A value counted down for every component (typically one router), a package passes on its way. If the value reaches 0 before the package reaches its destination, the package is discarded. This replaces Time To Live in IPv4 to prevent looping packages, among other things.

This replacement is easier to administrate than TTL, also TTL was often implemented simply by counting down the TTL value by a fixed value.

- Source Address
- Destination address
  Two 128-bit IPng-addresses

Also, there are some extra headers that may follow the primary header.

Each of these special headers have different purposes:

- Routing
- Fragmenting
- Identification
- Encrytion
- Special point-to-point options

The Protocol contains a wide variety of functions centered on a relatively simple basic header. This helps to make routing of IPng more efficient.

IPng is designed for the ATM-based high-speed net of the future and other similar technologies, but runs efficiently on low-bandwidth nets like GSM.

The Transition

Actually, there is only one problem: How to make the transition from IPv4 to IPng?

A solution might be defining "The Big Changeover", however, this is to be considered as pretty unrealistic. It would mean that all machines had to be converted in one day. The ultimate conclusion would be that the Internet never saw so little action in any one day (or week).

Let us face it, the solution is to run both systems simultaneously for a limited period of time. This has been addressed by the people behind IPng. The transition runs in two phases — in phase one both protocols run, in phase two only IPng runs.

The Simple IPv6 Transition — SIT has been defined. To make this possible the following requirements must be met:

- IPv4 and IPng hosts must be compatible.
- IPv6 routers and hosts must be installable along the way without any communication problems with the existing IPv4 hosts.
- The transition must be as easy as possible to implement for users and systemworkers alike.

To make SIT possible, it will be necessary for traffic between two IPng-hosts to run through IPv4-routers, making necessary some sort of definition for IPng-via-IPv4 tunnelling. Suggestions for both automatic and manual tunnelling have been made.

During the transitional phase routers capable of managing both IPng and IPv4 will be necessary. These routers may also support making IPng over IPv4 tunnelling transparent. There will also be routers capable of converting between IPv4 and IPng.

There is little doubt that this transitional phase may become very chaotic indeed, however, we must recognize that there is no other way.

As of now the standard is still just a proposal, but no major changes are likely to be made before the standard is adopted, leaving only the question of when phase one and two, respectively, are to be implemented.

Certain criticisms have already been made, primarily concerning the problems of transition from IPv4 to IPng, however, some people consider the 128-bit address section a potential problem.

Lastly, some people question whether the immense effort of a complete conversion of the net is justified by the improvements made in IPng.

I shall not be the judge of these things, but if you are interested in further information on this subject, I refer to the following URL which contains a very good run-through of IPng, including the pros and cons:

`http://ganges.cs.tcd.ie/4ba2/ipng/`

But for now — watch out for your IP-numbers. They are soon to become an endangered species.

❑

This article was originally published in DKUUG-Nyt No. 82, October 1995

Yahoo: From Homegrown to Full-Blown

On the World-Wide Web, it seems everyone is looking to strike pay dirt even organizations that became popular because of their quirky, homegrown appeal. Take Yahoo, for instance.

Mary Margaret Peterson

You´ve probably heard of Yahoo even if you haven´t used it. But plenty of people are: The system gets more than two million hits per day. Those anxious to join the action make electronic requests to be listed on Yahoo´s broad-based hierarchical Web index. One of the two company founders, Stanford University Ph.D. candidates in electrical engineering David Filo and Jerry Yang, or someone they´ve trained looks at that Web page and decides where to place the entry in the hierarchy. Within a few weeks, the home page is listed for anyone to search.

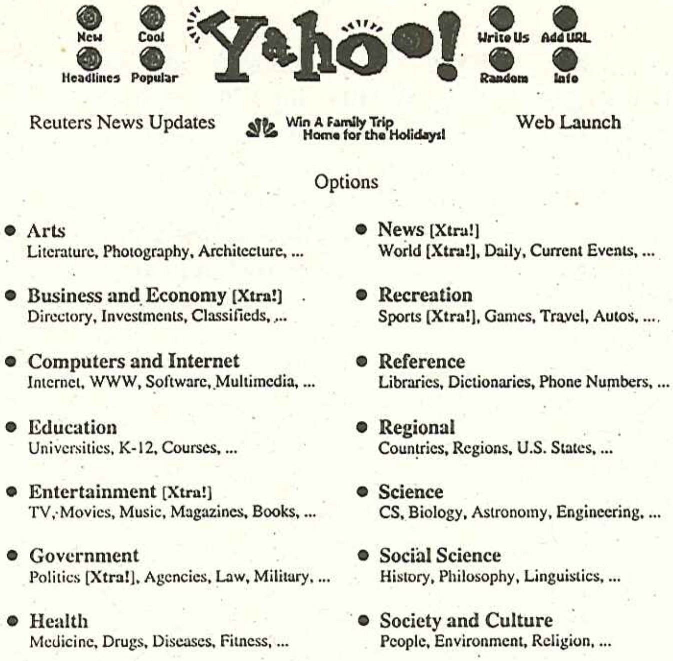
Yahoo users can search the list for free, and although it isn´t currently set up for entertainment browsing, plenty of intriguing items can be found there. The "Talk to My Cat" home page, for instance, connects you to a home in Los Angeles where a computer is hookeel up (with its sound digitizer on) in the room where the home page owner´s cat sleeps. You type a message into your computer, and the sleepy feline at the other end hears a digitized reading of it. Those who log in may read all the witty messages sent to the cat.

Another Web page listed in Yahoo had been put up asking for a stay of execution for a death-row prisoner in Chicago. "We put everything up there that has content," says Yang. "We haven´t denied requests to date."

At least some of this freewheeling outlook could change as Yahoo moves into the future. It has acquired venture capital from Sequoia Capital of Menlo Park, CA, and made a deal with the Web browser provider Netscape of nearby Mountain View.

Growing Beyond the Roots

The Yahoo indexing system began about a year and a half ago as a way for Yang and Filo to share their Web hot lists. Over time it grew into something a lot bigger than a collection of Web sites. It first evolved into "Jerry and Dave´s Guide to the Internet" and then into Yahoo. Yang says they found the exuberant name while doing a search for names that began with "ya," to stay within the yacc Unix tradition. (Yacc is a Unix compiler whose name stands for "yet another compiler compiler.") The pair quickly adapted the name into its own acronym, which Yang says stands for "yet another hierarchical officious oracle."



Reuters News Updates

Win A Family Trip Home for the Holidays!

Web Launch

Options

- **Arts**
  Literature, Photography, Architecture, ...
- **Business and Economy** [Xtra!]
  Directory, Investments, Classifieds, ...
- **Computers and Internet**
  Internet, WWW, Software, Multimedia, ...
- **Education**
  Universities, K-12, Courses, ...
- **Entertainment** [Xtra!]
  TV, Movies, Music, Magazines, Books, ...
- **Government**
  Politics [Xtra!], Agencies, Law, Military, ...
- **Health**
  Medicine, Drugs, Diseases, Fitness, ...
- **News** [Xtra!]
  World [Xtra!], Daily, Current Events, ...
- **Recreation**
  Sports [Xtra!], Games, Travel, Autos, ...
- **Reference**
  Libraries, Dictionaries, Phone Numbers, ...
- **Regional**
  Countries, Regions, U.S. States, ...
- **Science**
  CS, Biology, Astronomy, Engineering, ...
- **Social Science**
  History, Philosophy, Linguistics, ...
- **Society and Culture**
  People, Environment, Religion, ...

Officious or not, this “hierarchical oracle” showed early on that it had the power to grow. Between the time Yang and Filo started the system in April 1994 and December of the same year, they´d seen requests to access documents listed on Yahoo double monthly. Since then growth has ieveled off to 30 to 40 percent per month. “It´s quite a chore to develop and maintain a system with that many users,” says Yang.

So late last year, the pair decided to move the Yahoo system off campus, where Stanford had let them host it on one of the university´s servers. Hence the deals with Netscape and Sequoia Capital. According to Yang, the fledgling company´s arrangement with Netscape is a co-marketing relationship. Netscape will house the Yahoo system on its T-3 backbone and provide some hardware to the company, while Yahoo will commit not to move to Netscape´s competitors. But in some ways, the infusion of venture capital that Yahoo has received poses more far-reaching possibilities.

Attracting the Wily Advertiser

The question of how to take a basic homegrown World-Wide Web service and turn it into a profit-making enterprise — without alienating a loyal user base — faces many companies as they plow the fertile fields of the Web looking for their own cash crop. Companies taking a Web service from free to for-a-fee; companies with existing for-a-fee Web services; and companies just tackling the Web as a marketplace all confront the same sort of issues.

Yang and Filo have ruled out, at least initially, the two obvious ways of making money on the Web: charging users and charging for listings. That leaves just one avenue: Advertising.

But how do you entice advertisers as well as users into what is for them uncharted territory? And how much cost will the new market bear?

Yang makes no bones that much of making a business work on the Web is virgin territory. "We think the Internet market on the whole is going to be like the Wild West," he says. it´s uncharted in its unpredictability. It's impossible to project revenues or forecasts of what money you´ll make, because there are no established pricing models. Models for advertising and subscriptions haven´t been established."

Still, companies are making their businesses work on the World-Wide Web — some of them offering indexing, and search and retrieval services. InfoSeek of Santa Clara, CA, offers a free Web search service with ads and an advertising-free commercial Web indexing service. Users on InfoSeek´s commercial Web search service pay 10 cents per search, users on the free service see ads each time they log in.

Steve Kirsch, founder and president of InfoSeek, claims that advertising on the Web "is less iffy" than other types of advertising, because on the Web you can track the number of hits that come into the server. "Based on that [advertisers] can make a determination of whether the number of hits an ad receivced was worth their money," he says.

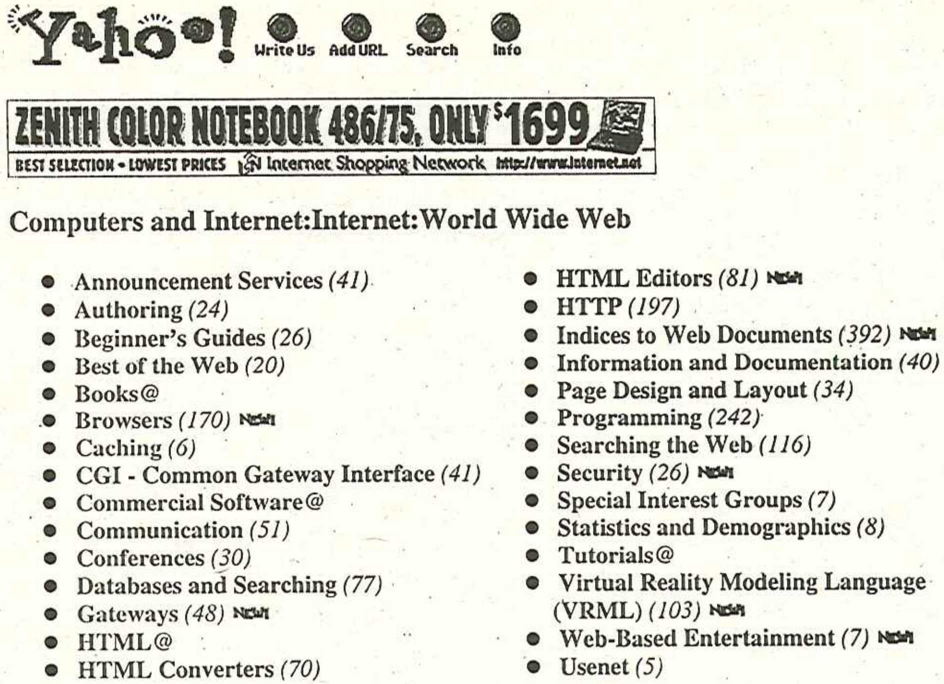
Yet Kirsch adds that selling advertising is probably the higgest challenge Yahoo will face in going commercial. "It´s a new area. It's an unproven media. People are experimenting. There´s no consistency in the pricing. The demographics are unclear. The effictiveness is unproven."

And he admits that even though InfoSeek runs ads from non-high-tech vendors such as the airline Cathay Pacific, the bulk of its ads come from vendors that are familiar with the World-Wide Web and have their own sites.

Yang and Filo are hoping to find a formula that will bring in both high-tech and low-tech industries, which raises the bar. "High-tech companies don´t care much whether you have the right qualifications, in terms of set models, like how much it costs to advertise to 1000 people." Yang said. "Proctor and Gamble may need more proof that people are accessing the system."

Qualifying Users

Counting hits is another issue that has to be solved in order to attract quality advertising. You can track how many hits per day your site receives, but how convincing will that number be to a po-



ZENITH COLOR NOTEBOOK 486/75, ONLY $1699
BEST SELECTION • LOWEST PRICES Internet Shopping Network http://www.internet.net

Computers and Internet:Internet:World Wide Web

- Announcement Services *(41)*
- Authoring *(24)*
- Beginner's Guides *(26)*
- Best of the Web *(20)*
- Books@
- Browsers *(170)* New!
- Caching *(6)*
- CGI - Common Gateway Interface *(41)*
- Commercial Software@
- Communication *(51)*
- Conferences *(30)*
- Databases and Searching *(77)*
- Gateways *(48)* New!
- HTML@
- HTML Converters *(70)*
- HTML Editors *(81)* New!
- HTTP *(197)*
- Indices to Web Documents *(392)* New!
- Information and Documentation *(40)*
- Page Design and Layout *(34)*
- Programming *(242)*
- Searching the Web *(116)*
- Security *(26)* New!
- Special Interest Groups *(7)*
- Statistics and Demographics *(8)*
- Tutorials@
- Virtual Reality Modeling Language (VRML) *(103)* New!
- Web-Based Entertainment *(7)* New!
- Usenet *(5)*

tential advertiser? The number of hits doesn´t necessarily indicate the number of users who loggcd on to a particular system. For one thing, graphic elements in a file or home page cause more hits-per-user to be created. For instance, if one person logs in to a home page with five graphic elements that produces a count of six hits; one for access to the page and one for each of the graphics. Yahoo contains no graphics, so all of its hits are text-based.

But even if you provide accurate raw numbers. chances are that the advertiser will he looking for more information, such as the quality of those numbers. That means demographics. Advertisers live by them. but the Web can´t do much to provide them.

"You can tell what machine a user comes from," says Yang, "but not [who] the individual [is]. It´s very difficult to determine the number of people accessing a site. When we talk about not being able to project revenues, it´s because the whole advertising theme is based on the number of people."

Even if it were easier to provide accurate demographics, Yang and Filo are determined not to create the impression of giving away demographic information on their users. "It is important to know how users perceive us," says Yang. "We don´t want to invade people´s privacy or even to lend the impression that we´re invading privacy."

Then there is the age-old question of control. Once Yahoo or any other company begins accepting advertising space on its service, how much control will that advertiser assert over the content of the service? In the case of Yahoo, the key question is, will those who are paying for advertising be listed more prominently in the hierarchy? Will the advertiser´s competitors be listed in a less important position or worse yet, fall off the list?

Yang and Filo insist this isn´t likely to happen. The pair plans to maintain control of their indexing hierarchy and make it as unobtrusive as possible for the user. "We want to say, this is where the ad will go, are you interested?" said Yang. "We lean toward putting ads in a delineated area, not according to how much the advertiser paid."

Daniel Dern, an independent Internet analyst based in Newton Center, MA, takes a tempered approach to advertising on the Web. "The beauty of advertising-based funding is it gets the project going without requiring the users to throw their quarters in," he says. "The danger is whether we like what we get and whether it stays around."

A Flashier look

Soon Yahoo users will see more than ads. They´ll also see the start of a new look for the system. "We´re going to improve the search engine, throw in some graphics to make it better looking, offer people some alternatives," says Yang. "Right now it's minimalist. People like that because it´s fast. There will still be ways to get the system speed."

Filo says that over time the system should become easier to use. "We´re not real user-friendly right now, because we built Yahoo for our own needs. but eventually we might move in that direction."

"Hopefully it will be something that´s fun and cool," says Yang, talking about the new model for Yahoo. "David and I hope people will not have to see the ads [unless they wish to]. We´ll make it look good."

Even though there are changes in the wind, you should still be able to find everything under the Web on Yahoo. As much as anything else, the quirky and unexpected have built Yahoo's loyal user base. So when the new, improved Yahoo irons out the wrinkles in its business plan and steps out with a crisp new look this summer, users will be watching, many of them hoping that at least some of the rumples remain.

❑

This article was originally published in UniForum Monthly, September 1995.

The Birth of an Internet Newspaper

"The Danish News" started as a few Danish news clippings typed in by Leif Andersen and sent to a friend living in California, who wanted to keep in touch with the happenings in Denmark. Now, three years later, close to 2000 Danes living outside Denmark subscribe to the news service. The service is financed through donations and is run by Leif Andersen and his wife Bodil.

Leif Andersen
*BLA*net*
leander@blanet.dk

bla*net

It was a beautiful spring day in 1992 — or maybe it was grey and drab. But it was in March, a few weeks after Bodil Andersen (who prefers the name Dille) had decided to add the Danish business paper "Børsen" to our daily supplies.

On that day the paper´s U.S. correspondent wrote about a Danish society of computer people in Silicon Valley. At that time the president was Bent Torp Jensen. An long-lost old friend happened to have the same name and had actually been spotted in California seven years earlier. In the article his name was just mentioned in a passing remark, but so was the e-mail-address.

The Wedding

Many may know this already: On saturday afternoon [November 18th] Miss Alexandra Manley of Hong Kong was married to Prince Joachim in the chapel of Frederiksborg Palace. The ceremony went perfect apart from a single uninvited guest.

After the exchange of "Are-you-who-I-think-you-are?" and "Yes-hello-how-are-you-doing?" he asked me whether I knew anybody who would write e-mails once in a while and tell something about what was going on in Denmark in general. "I can do that", I replied — and this is where the story begins:

"The Story about Danish News, Denmarks first worldwide news service on the Internet.", to be told with an emphasis on the technical aspects by the pen-pusher throughout the years, Leif Andersen.

In those days, back in 1992, the Danish newspaper Politiken had a summary of the articles that they found the most important. I copied that and sent it off to Bent. It took me only 15-20 minutes and went well for a couple of days. Then Bent wrote that he had distributed the summary through the Danish e-mailing list in California. "Oops" I thought, "what about copyright?" Well, it was for private use and no money changed hands, so I continued for another couple of months. But after a while Politiken pulled out, or rather, the summary became increasingly inadequate and in the end it disappeared. I tried copying articles, but each news item grew longer and longer and the job took up an awful lot of time. It was (and is) so much easier to watch the news on TV, scribble down a few key words and then write a short report.

Meanwhile, mail started to arrived from people who were not on the list, just as there was some talking about collecting funds for us. By the end of 1992 most news items were originally from the newspapers and then came:

January 2nd, 1993

This particular day I distributed the first news written solely by me. It was such a relief. I continued to refer to a single source of information (e.g. an article in Politiken or a feature on the news), but now I could use my own words which was less time-consuming (then I added more items and ended up using too much time again).

During the year of 1993 news appeared on the two gopher-servers (DKnet and DENet). The number of "subscribers" to the Danish List increased gradually from about 50 in the beginning to 500 by April 1994. Just as the administrator of the Danish List had announced this, the list server broke down.

June 1st, 1994

By the end of 1993 Bent started the initial collection for the "Leif Foundation" and shortly before the breakdown, a Dane working at Amdahl in USA started another collection. Soon it was clear that the incoming amount of money would be considerable. I had turned 40 and in my earlier years, when I was more naive, I had once paid a small amount into an account and according to the rules I had to empty the account before the end of 1994. This amount, which had increased considerably, made me able to buy quite a few machines to fascilitate the work and reduce the costs of communication. By June 1st 1994 the BLA*net (B. & L. Andersen´s Network) was established as a one-man sideline business. The same month I purchased the first machine, Mille, and with great help from DKnet, the blanet.dk domain took off shortly after with a UUCP-connection to the world and the Internet.

Apart from a few times where the sysadmin.com was down due to overload (every newsletter carries 10-15 Mb of data!) the number of subscribers has increased. After the breakdown the news has been distributed via a special list (the News List) so that those who want only the news, do not have to take part in the discussions that are going on between the subscribers to the Danish List.

Dille has always been a gifted researcher and a "databank" because of her photographic memory with people and names. When the blanet.dk was set up she got her own address and was now able to keep up. Soon DilleSport was a reality with a, almost, daily article almost ever since.

March 13th, 1995

This monday the listadmin sent out a message to all the subscribers of the two lists saying that the News List had reached the magical number of 1000 subscribers. The Danish List "only" has 787. Twenty-nine countries are represented. The readers are to be found mainly in the U.S. and Canada, but also in countries like Jordan, Bermuda and Kazakhstan.

A typical day with the Andersen Family

At breakfast we split the paper as Dille takes the sports section with her to work, and I take what is left of the first section. On the trains we both take notes. Dille´s Psion can be used on the bus, but my sub-notebook has turned out to be too difficult to handle there. Today we are both employees at Datacentralen A/S, but in geographically seperate divisions. During the day we listen to the news on the radio. When we get home we take some time off until the first tele-newscast at 6.30 pm. Then we write the last news items and I do the editing while watching the second newscast. These days we usually wait until the news at 9 pm and the following sports programme before I add Dille's sports news. In the end I add key figures from the business news, go through it all, and send it off. Saturday and Sunday the Andersen Family is off duty!

The concept of the newsletter is that every piece of

bla*net

An uninvited guest

There were room for 330 guests in the chapel of Frederiksborg Palace but the tabloid paper "Ekstra Bladet" found it amusing to "expose" a breach in the security surrounding the wedding by inviting the famous French "party crasher", 64 year old, Claude Khazizian.

[...]

By posing as another guest he managed to get through the security check at the entrance to the chapel. A police officer later became suspicious and had "Claude X", as he names himself, arrested. After being questioned by the police he was released without charges. He has performed the same stunt at a ceremony at the French Elysee Palace where he managed to have his photo taken with, among others, Helmut Kohl.

news is made up of a very short summary, usually 5-10 lines. Oddly enough it is not that difficult to shorten newspaper articles from half a page to just a few lines. Another requirement is that it should not take long to write each news item. We are both acceptable ten-finger typists, but we have an old house and friendships to maintain, and not all cultural activities can be postponed to the weekend. At the moment we are close to three hours of work which is too much, but a few manual routines can be automated. The problem is that we do not have time for that.

While we aim at keeping the actual news reports as objective as possible the DilleSport is far more engaging. Here you can find sports that do not receive adequate attention in the Danish media, such as women's sports and sports for the disabled. Perhaps not suprisingly this has been popular with the readers.

The Leif Foundation

Money is essential. Bent voluntarily introduced the collection by the end of 1993. "Give whatever you want" — that gave us just enough to cover the subscription fee to the newspaper. In spring, when another collection started it amounted to almost 10.000 DKR. In the fall of 1994 we raised almost 14.000 DKR. Without taking into account the extraordinary expenses for hardware and the fact that none of us gets paid, we ended the year of 1994 with decent working profits on the BLA*net. This way the operation of blanet.dk (which is just a UUCP-connection to the DKnet) was guaranteed throughout a great part of 1995.

The Funding For This Programme...

The news, at least in its present concise form, is free. Straight from the heart: I do not believe in the electronic newspaper, neither as an electronic version of the paper edition nor as some interactive variant. It will not happen until it is cheaper and faster to read than the paper in the mailbox every morning. The only way to preserve the Danish News and to keep it coming out on a daily basis is by means of sponsoring, as is practised by the Public Broadcasting System in the U.S.: PBS is financed by a combination of public funds, company sponsors and viewer´s contributions. But until we have found an acceptable model (acceptable for the readers — whom we, in this case, can ask without any real expenses) we will continue as a user-financed news service.

Distribution Is Faceted

We reserve the copyright and all other rights. You can freely redistribute the news through e-mail and put it on the free and publicly accessible BBSs. Commercial providers need to obtain a licence from us beforehand

and may have to pay a fee (this has not happened yet, though). We also have licence holders who use the news for their newspaper columns or redistribute it by telefax.

Home Technology

In a corner of the living-room "The Big Computer", Mille, is placed. It´s a 486DX2 with 8 Mb RAM and a 420 Mb HD in a tower cabinet. Inside is a 6 port serial card and the OS is Linux (v. 1.0.9). It works as a modem server, UUCP gateway (to DKnet), list server (for Danish OSS, among other things), info server, fax server etc. On my desk is Carina, who also runs Linux. It is an old 386DX. It is my mailbox and information database (the tools are there as well). Mille has a UUCP connection through a dedicated line. At the moment the writing and the editing of the news take place on Quark, by now an unfortunately outdated Olivetti Quaderno sub-notebook, running MS-DOS. Quark goes with me to and from work, and around the world.

On the other side of my desk is Dille´s desk, where she writes the sports news on her small Psion 3a palmtop, DilleDok. Benji, our "graphical workstation" which is going to run both OS/2 Warp and Linux, is not yet in operation. Technically it is larger than Mille (486DX2, 16 Mb Ram, 512 Mb HD) but has only a desktop cabinet. In the future we will try to produce WWW versions of the news including pictures and drawings. We just need a cheap WWW server that we can update automatically. Short term plans are that we will upgrade all the Linux/OS2 machines to LAN (cheapernet) and move Mille down into the basement.

❑

bla*net

Critical ombudsman

On Friday the ombudsman of the Parliament, Hans Gammeltoft-Hansen, presented his critical examination of the two reports on the riots in Copenhagen on the 18th and 19th of May 1993. The reports were made by the current Supreme Court judge Asbjørn Jensen.

...

Hans Gammeltoft-Hansen especially criticizes the fact that Asbjørn Jensen let the actions of the Copenhagen Police be investigated by — the Copenhagen Police — not the Special Branch of the National Police. There were raised charges against three police officers after the riots but no senior officers were ever questioned.

This article was originally published in DKUUG-Nyt No. 77, April 1995. The news clippings are from November 20th 1995.

FreeBSD, The Inside Story

For more than 10 years Poul-Henning has ravaged the Danish world of UNIX. He has his own little company which, among other things, offers security audits and counseling concerning UNIX/LAN/WAN-installations. It also provides FreeBSD-based servers for Internet purposes and of course all kinds of UNIX sorcery.

Poul-Henning Kamp
The FreeBSD Core Team
<phk@FreeBSD.org>

My intention is to give a general view of what is going on and to go deeper into a couple of interesting details.

At the moment we are working with two versions; "2.1" (also named "stable") which will be released this fall and "2.2" (also named "current") which points towards the future. Having two parallel versions helps us in satisfying both the users who need great stability to run production on FreeBSD and the users who want to try out the new stuff.

Both versions originate from the "2.0.5" version released this spring but the difference between them is that the "2.1"-tree only contains error correction and well-tested changes while the "2.2"-tree contains some "fresh code". David Greenman, our Chief Architect, very carefully filters the patches from "2.2" that he finds adequate. Both versions are available through the "sup"-protocol at the Internet.

Ports

I think that our ports deserve to be mentioned. Thanks to Satoshi Asami, our "portsmeister", we now have about 320 ports of software from the Internet. Having a port of a piece of software means that the user can install the software without any problems. We supply a Makefile and other files, patches and scripts neccesary to install the software in the machine. If I want "elm" installed I just use the command:

```
cd/usr/ports/mail/elm
make all install
```

If my machine is connected to the Internet it will automatically fetch the source file from the right site. If my machine is not connected to the Internet it can get the file from a CD-ROM or something similar.

Wherever it is technically and legally possible we have made a binary package of the existing packages. In that case the command:

```
pkg_add elm.pkz
```

should do it.

I could fill the rest of my article with a list of the 320 ports but that would not be sporting behaviour. Let me just add that everything I have ever heard about is available here, plus a whole lot more.

Devfs

By looking at the mknod(8) command you see at once that there is something unreliable about it. You use the mknod to tie knowledge about the configuration of the kernel into the file system by making device nodes in /dev. I consider that cheating!

If my serial port driver finds 64 ports why do I have to tell that to the kernel? That is what the devfs is supposed to clean out. The devfs is a kernel module which partly functions as a file system being fitted to /dev and partly as a database for the device drivers. When a driver detects a device it now tells the devfs module that it has found e.g. /dev/rfd0. The devfs then makes a pseudo inode appearing in /dev. Curiously enough it simplifies everything. All device drivers contain a lot of code dealing with major/minor numbers that can now be made in a much easier way. Likewise the special cases existing in all file systems can be removed. The devfs was implemented as prototype in "2.0.5" by Mr. Julian Elischer <julian@tfs.com>.

FreeBSD vs. Linux

You have all read about Linux, magazine by magazine, and I am sure that many of you have asked the question: "What is the difference between FreeBSD and Linux?". There are many differences. Too many for anybody to judge with any credibility which one is best. The most essential difference is which Copyright/Copyleft covers the code. Many people get small uncontrollable nervous breakdowns when they consider using a "Copylefted" piece of code in "commercial" environments. Nobody really knows where you are at legally if you mix Copyleft software with your own — the scenario simply has not been tried by any court yet. Most people simply avoid using Copyleft code, "just to play safe".

To eliminate this restriction the FreeBSD project

FreeBSD

has introduced the "BSD"-copyright. It offers the same privileges but the paranoid passages about the supplying of source code in N years or about the "infectious" GPL has been omitted. If a company delivers a FreeBSD as OS in a system, the company´s programs or/and device driver will not automatically go through GPL or otherwise be compromised. This does not mean that you can not use GPL code with FreeBSD, just that you will find the source distinctly seperated from other FreeBSD sources. Secondarily FreeBSD is geared for "real" UNIX jobs, unlike Linux.

From what I have heard and seen it looks like the producers of Linux focus exclusively on workstations without paying much attention to the scaling of N*100 processors/TCP-connections. In that way the FreeBSD has become quite popular as WWW-server, FTP-server, InterNet firewall, mailserver, NFS-server, DNS-server and so on, besides, of course, as X-server or workstation. We have a lot of ISPs (Internet Service Provider) as well, using FreeBSD machines as server for their modems, offering their customers either PPP, SLIP or /bin/sh-entry.

A good example of such a machine is "wcarhive.cdrom.com", a Pentium 100 sitting at the backbone network of BARRnet with an ethernet routinely pulling 300 ftp clients — plus incidentals...

FreeBSD can be downloaded from the Internet or purchased on CD-rom.

If you want further information

```
http://www.freebsd.org/
```

If you want to try FreeBSD

```
ftp ftp.freebsd.org
cd pub/FreeBSD
```

❑

This article was originally published in DKUUG-Nyt No. 81, September 1995

Everest — SCO´s New Flagship

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

I have been working with Unix and its different dialects for a number of years and, in my opinion, nothing new has happened for a long time. The most recent development was SUN releasing Solaris and SCO releasing SCO Unix. However, SCO has just released its latest version of their operating system — Everest.

Test Equipment

An AST PowerExec 4/25 (486 with 25 Mhz) with 20Mb RAM and 700Mb harddisc was used for the test.

Installation Procedure

You discover right away that SCO has planned ahead, working with the flexible installing which was used already in SCO ODT 3.0. Now the system is delivered on only one disc and one CD. No more changing of discs, you just boot up on the boot disc and answer some questions, such as serial number, which net card you have and so on. Then the machine runs the entire installation. This makes it possible to work during installation, and we all agree that waiting during installation to answer a few simple questions or to change discs is completely meaningless, making this a pleasant installation procedure. Let us then move on to the features tested.

File System

With Everest, SCO introduces several new types of file systems, such as HTFS (High Throughput File System) and DTFS (Desktop File System).

HTFS is a completely new type of file system which includes Journaling. According to the information from SCO, this is a very fast file system and I did detect a considerable increase in speed when processing. Unlike the old system (SCO ODT 3.0), the starting up of the X-server and so on was noticeably faster. I did some testing of discs and in spite of the sluggishness common to discs, copying to these was up to 15% faster than in the old EAFS file system. HFTS (and DTFS) also includes Version Management, making the system capable of storing more (configurably) older copies in the files and you can call up older and even deleted files. In addition to a faster and better file system the number of inodes in the system has been increased, with HFTS having more than 130,000,000 inodes and DTFS even more.

DTFS is made specifically for managing the small memory storage space in desktop computers, as it includes compression of disc data.

In addition to the new file system, Virtual Disc Management is included, making SCO Unix capable of managing RAID systems (RAID 0 — Stripping, RAID 1 — Mirroring, RAID 4 and RAID 5 — Stripping with parity). This is managed with the new administrative tool (more on this in the following), making it relatively easy to handle. The system in its present form cannot handle Hot Swap (changing discs on the fly), to change discs you must shut down the system. However, it does include Hot Standby (meaning that if a disc has been introduced and configurated, but not used, the system will use this if another one fails). While we are on security, it is common to use Raid 1 for mirroring a database-disc, for example. Once it is time for a back-up, you can disconnect one of the mirrored discs, using this for a nice and easy back-up. However, this does reduce security during back-up. To counter this, you use a 3-step mirroring, that is, disc one is mirrored onto two others. Using this method, you can disconnect a disc for back-up without compromising security. With SCO´s new disc management this is no problem.

Power Management

With APM (Advanced Power Management) becoming more common, systems are made more power efficient as any part of the system not operating is shut down ("Green PCs"). Normally, this does not go well with Unix systems being made for continual running. Still, SCO has built in APM support in SCO Unix, bettering the potential for running SCO Unix on mobile computers, as this saves power when working in the field. It also includes built-in support for UPS-systems in the kernel, making it possible for suppliers of UPS-systems to create drivers for their UPS-systems. Via the new API you can manage Power Fail, Battery drained and Power restored. It also has built-in management to prevent starting up on a rundown battery (risking stops the UPS-system cannot handle), as well as signals occuring if the system fails, making it possible to shut down the UPS. Everest includes support for American Power Corporation´s UPS.

Adminstration

Another major new feature is SCO´s new administrative tool, SCOadmin, in itself interesting enough to justify the investment. In principle, the entire systems administration has been rewritten in a new language, Visual TCL (Tool Command Language). VTCL is an expansion of TLC creating a common user interface in both x-environments and characterbased environments. Several of the new administrative tools are network compatible; if I am working on my portable unit and wish to add a user on my main server, I simply choose Host>Open Host on the menu, choosing my main server, making me able to work on this directly. This simplifies the administration considerably when working on network-linked systems with several host-systems or many work-stations. The installation has been changed for installment through networks or even from the CD or tape of some other machine, or from a package already installed on some other machine.

Windows Integration

SCO realized years back that Microsoft Windows are to be taken seriously and consequently created the "Windows Friendly" strategy. This has been expanded in Everest, which includes a netware client making it possible to log in, store, and read files on a Netware server. You can also print out on printers connected to the Netware server. This gateway is the same one included in Unixware 2.0. This, however, was the only feature I had no possibility of testing, not having access to a Novell-net.

Conclusion

It would seem that SCO has hit the bull´s-eye with Everest. The new administrative user interface is very easy to work with, and with the new features and file systems, a very pleasant and modern system has been created.

❑

PGP, the Book and more

Andrew Macpherson

In previous issues we have had much publicity for Phil Zimmerman, his program PGP and his current problems with the US Authorities. He is accused of exporting munitions by allowing the program to be posted to the net. In late January Simson Garfinkel´s book ,"PGP Pretty Good Privacy" from O´Reilly, became available through their European distributors, International Thompson Publications. The book looks at the background to the program as well as how the program works.

PGP The Book

PGP: Pretty Good Privacy
Simson Garfinkel
O´Reilly & Associates, Inc.
ISBN 1-56592-098-8
393 pages 178 x 235 mm
European Distributor ITP.

O´Reilly used to publish books that were 153 mm wide. They were good and easily readable. They also fitted my shelves. Fortunately the publisher has resisted the temptation to put an excessive print line length in this wider volume. PGP the book is readable, if unwieldy. Some other recent books from O´Reilly (e.g. "Managing INTERNET Information Servers") are simply a strain to read.

Layout

The book has four major sections. if you are interested in diving straight in to using PGP the program then you may be tempted to go directly to the third section. I would recommend "passing GO" and reading the first as well, it has many of the ideas about how cryptography is used which make the other parts clearer.

As with other books in the series, there is a quick-reference card for one to tear from the back of the book.

PGP Overview

As well as the outline overview promised, this is "Cryptography 101" with a quick overview of ciphers, codes and digital signatures. Most interesting is also a (US) description of the legal situation in which all discussion is framed. In general the USA does not permit the export of cryptographic technology, classing it as munitions. Then there is Lotus Notes

Lotus Notes

Lotus Notes is a US exported product. It uses cryptographic techniques to ensure integrity and privacy of messages, and builds on the integrity feature for workflow automation. The cryptography export restriction is avoided by restricting the key-length in the exported versions to 40 bits (5 octets).

"Notes" uses the RC2 block cipher, and the RC4 stream cipher. Both are inventions of Prof. Rivest, and trade secrets. Unfortunately RC4 was posted to the Internet some years back, so the secret has been revealed, and can now be found on various servers. The comments in the book on the strength of the algorithm imply that finding the algorithm is still part of the problem for any attacker.(

Cryptography History and Policy

For me this section was the most interesting. Much of the material has been rehashed to death in "alt.security" and similar fora; here it is presented in a cogent, coordinated structure. At the end of the section one can expect to understand the difference between symmetric and asymmetric ciphers, know about one time pads and be comfortable with the ideas of key-escrow as applied to "clipper".

Key distribution

I found the discussion of the "mesh of trust" inadequate. This area is PGP´s unique selling point when compared with schemes such as PEM. Whether the "web of trust" is indeed an appropriate method for establishing a framework for mutual authentication is open to attack. Commercial users will probably prefer an institutional third party scheme, while the individual may well prefer the free and informal scheme developed by Zimmerman.

Using PGP

The tutorial section of the book does what is needed. There are the usual problems of having to avoid subissues in one area until the major topic is covered later. There is nothing of special note otherwise.

Appendices

Installing on various platforms

The first and obvious question of "where to get PGP" is covered for US citizens only. Other nationals should get the "UI" version (see below Fast facts for Europe) Otherwise the installation instructions can be followed as presented.

Mathematics of Cryptography

This is the only part of the book where the reader is exposed to anything that looks even remotely mathematical. Even here the descriptions are constrained to nice short bits, and easy numbers. Even so, part of reviewing a book is finding the deliberate error, just to prove you´ve been paying attention. The worked example of Diffie Hellman on page 356 gets seriously lost, and will be corrected for the second edition. The RSA description is clear.

I found the included analysis of the difficulty of factorisation fascinating.

Who should buy this book?

If you are at all interested in "What is cryptography, and what can it do for me?" but do not want to be swamped with mathematics, this is the book for you. The topics are well covered, clear, and the anecdotes clarify the points.

The section on the program itself will lead you into using it in a friendly step-by-step manner.

If you think that Phil Zimmerman is a hero / thief, and want the view reinforced, avoid chapter 4 "A Pretty Good History of PGP.".

Fast facts for Europe

Where to get PGP

In the USA it is possible to obtain patents on algorithms, and to apply for them for up to a year after first publication. Neither is the case throughout most of the rest of the civilised world. It would none the less be polite to avoid embarrassing the owners of US based ftp servers by picking up one´s copy of PGP from outside North America.

For the Web Connected, please start with the page maintained by Ståle Schumacher <staalesc@ifi.uio.no>, as this will give one a good background.

http://www.ifi.uio.no/~staalesc/PGP/home.html

The software one requires is the 2.6.2i release. In fact the "unencumbered international" software is to be found on

ftp://sable.ox.ac.uk/pub/crypto/pgp/(

for both unix and dos

What to do next

There are a few things that people usually forget when they start with PGP. The main one being how to revoke a public key whose private key you can no longer access, or which has become compromised.

After you have installed your copy of PGP, and made the various tests suggested in the documentation, you should make a key pair for yourself. Before you start to use the key, or to add other people´s public keys to your keyring, you need to finish making it useful. Attach all the many names to your new key that you might ever use (e.g. your multiple mail accounts) with the pgp -ke command. Then sign the key yourself (pgp -ks) Signing the key prevents the names you have attached being changed when the key leaves your control. You then wind up with something like figure 1.

Now make a copy of your public-keyring file (e.g. to copy.pgp), and revoke your newly created public key in the copy file:

```
pgp -kd andrew copy.pgp
```

```
(pgp -kvv)
Key ring: 'c:\pgp\pubring.pgp'
Type bits/keyID  Date       User ID
pub  768/A8336D 1995/03/13 Andrew Macpherson
<A.Macpherson@bnr.co.uk>
sig     A8336D
Andrew Macpherson <A.Macpherson@bnr.co.uk>
Andrew Macpherson <andrew@bnr.ca>
Andrew Macpherson <andrew@nt.com>
1 key(s) examined.
```

Figure 1

```
Key ring: 'copy.pgp'
Type bits/keyID  Date     User ID
pub  768/A8336D 1995/03/13 *** KEY REVOKED ***
Andrew Macpherson <A.Macpherson@bnr.co.uk>
Andrew Macpherson <andrew@bnr.ca>
Andrew Macpherson <andrew@nt.com>
                1 key(s) examined.
```

Figure 2

When you check this with "pgp -kv copy.pgp" you get the result in Figure 2 — you have a revocation certificate. Put this file on a floppy disk and lock the floppy away. Delete the file from your computer. This is your ultimate backout (you can use the revoked key to tell the world that the key is no longer valid).

The other thing you ought to do is to put the key to your secret keyring in a secure deposit somewhere (home safe, with your will, in a bank deposit.) This is for that time when you have the apocryphal meeting with a moving bus (There are better ways of doing this described in Chapter 13 of the book.)

Registering Keys

The key servers act as a repository for public keys. They make no warranty on the validity of the names associated with the keys (you have to validate them yourself on the basis of the "web of trust" or by some other means, such as a business card with the key signature on it.) The servers are a good starting point for finding if your correspondent has a public key.

Signatures

Before you deposit your key on the server, it might be a good idea to get some of your friends to "sign" your key. This means that they are prepared to warrant that you own the key, nothing more. Equally you might sign their keys.

Registering / Retrieving Public Keys.

As is becoming common, there are two classes of citizen. The WEB connected and the mail user. The web connected may pull up:
`http://wwwswiss.ai.mit.edu/~bal/pkscommands.html`
and follow the instructions. Mail users should send mail to pgppublickeys@pgp.-ox.ac.uk with a subject of "help".

Legal Status

The patent issue is of course a non-issue outside the USA as far as RSA goes. The other code used heavily by PGP is IDEA, which certainly is protected in Europe, though I understand from the net it is available for personal, non-commercial use. More interesting are our governments´ attitudes to cryptography. It´s probably illegal to import good cryptography into most states of the EU (definitely France), and there are re-export restrictions in many countries as well.

❑

This article was originally published in News@UK

Calendar of Open Systems Events

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

This calendar is made from different sources (newgroups, Usenix papers, etc.). Last update: 09 Nov 1995 22:46.

Date	Title	Location	Organizer
December			
2-7	UNIX Security	San Francisco, CA, USA	DECUS
3-6	Symposium on Operating Systems principles	Copper Mountain, CO, USA	ACM
3-7	SGML ´95 A technical conference on SGML implementation and application issues.	Boston, MA, USA	GCA
3-8	Supercomputing ´95 http://sc95.sdsc.edu/	San Diego, CA, USA	ACM/IEEE
4-8	34th IETF	Dallas, TX, USA	
4-8	DB/Expo Conference and exposition on database, client/server, and information technology.	New York, NY, USA	
5-7	Database & Client/Server World http://www.dciexpo.com/	Chicago, IL, USA	Digital Consulting, Inc.
8-10	DECUS - West http://www.decus.com	San Francisco, CA, USA	DECUS
11-14	4th World Wide Web Conference http://www.w3.org/hypertext/Conferences/WWW4/	Boston, MA, USA	W3C
11-15	ULPAA (upper layers)	Sydney, Australia	
11-15	ProjectWorld ´95	Santa Clara, CA, USA	

Date	Title	Location	Organizer
11-15	11th Computer Sec Applications	New Orleans, LA, USA	
14-15	MVS & UNIX Security	Washington, DC, USA	
19-20	Location Independent Computing http://www.northern.co.uk/~andrew/ukuug/wincon95.html	York, UK	UKUUG

January ´96

8-10	International Workshop on Artificial Intelligence in Economics and Management	Tel-Aviv, Israel	ACM
8-10	International symposium on software testing and analysis. http://www.cs.ucsb.edu/Conferences/ISSTA96/	San Diego, CA, USA	ACM SIGSOFT
9-12	MacWorld Expo	San Francisco, CA, USA	
9-12	Internet World ´96 Canada	Toronto, Ontario, Canada	
10-12	Rik Farrow's "Advanced UNIX and Internet Security" http://web.dcs.bbk.ac.uk/ukuug/wshop/farrow/rik.html	London, UK	UKUUG
15-17	Rik Farrow's "Advanced UNIX and Internet Security"	Copenhagen, Denmark	DKUUG
22-26	USENIX 1996 Technical Conference	San Diego, CA, USA	USENIX
29-30	Publishing on the Internet	Zurich, Switzerland	EurOpen
29-1	ComNet Conference & Expo	Washington, DC, USA	
30-1	Publishing on the Internet	Stockholm, Sweden	EurOpen

February

5-7	Workshop on Network Security, Firewalls and Internet Services http://www.iwi.com/mjr/mjr-top.htm	San Jose, CA, USA	
6-8	Data Warehousing Conference http://www.dciexpo.com/	Orlando, FL, USA	Digital Consulting, Inc.

Date	Title	Location	Organizer
12-16	UniForum ´96 http://www.uniforum.org	San Francisco, CA, USA	UniForum

March

Date	Title	Location	Organizer
11-13	Workshop on Network Security, Firewalls and Internet Services http://www.iwi.com/mjr/mjr-top.htm	New York, NY, USA	
11-13	7th Annual International Help Desk Conference	Reno, NV, USA	
14-20	CeBIT Hannover ´96	Hannover, Germany	

EurOpen on WWW

Thanks to Simon Kenyon the EurOpen WWW home page is now a fact.

The URL is:

www.europen.org

EurOpen Quarterly

EurOpen Quarterly is published by EurOpen

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

Staff

Editor
Søren Oskar Jensen
Translators
Anja Hitz
Berit Nyholm

Address

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

❑