

DKUUG

*Vejen til viden om
Åbne Systemer og Internet*

nytt

121/marts 2000

EnGNU kom forbi

Richard Stallman
i Danmark

LinuxForum 2000

Beretning fra
konferencen

Bjarne Stroustrup i Danmark

C++ opfinderen kiggede
forbi igen

En cyborg kom (også) forbi

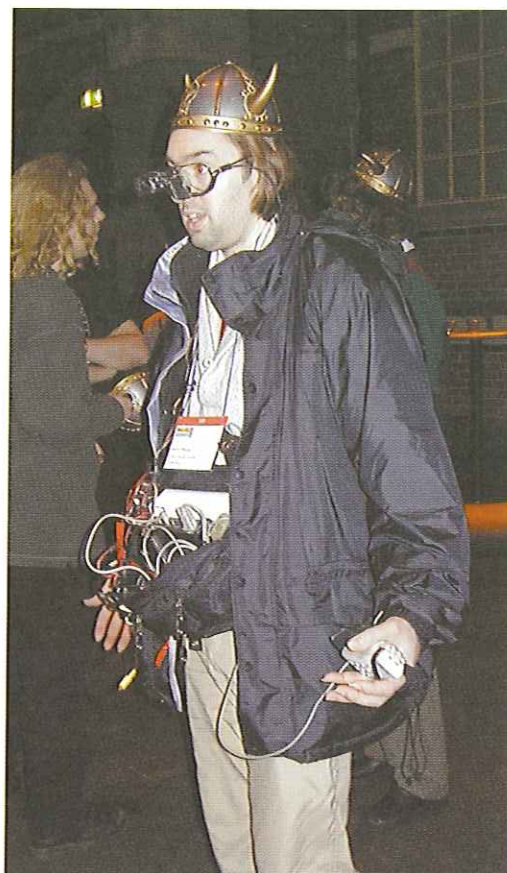
Steve Mann i Malmø

Bruce Schneier skriver om Open Source



INDHOLD

Bjarne Stroustrup hjemme på besøg	3
Danmark handler på Internettet	4
Richard Stallman og Free Software	6
En gnugurukom til byen	8
En cyborg til (også) til byen	10
Siden sidst	12
Tour de CeBIT 2K	14
Med AaLUG til Linux Forum 2000	16
Open Source og sikkerhed	19
Remote login og netværksaflytning	22
Etc.	27
FLUGs historie	28
Aktivitetskalender	30
Pers hjørne	31



Fortid møder fremtid: Cyborgen Steve Mann til vikingegilde - læs mere om ham på side 10.

LEDER

Farvel og tak for denne gang

Dette er min sidste leder som redaktør af DKUUG-Nyt: Jeg har fået et tilbud, jeg ikke kunne sige nej til, og har derfor overladt roret til en anden redaktør, der nok vil præsentere sig selv i næste nummer.

Det er rart at kunne forlade en arbejdsplads gennem næsten to år uden nogen former for sure miner. Jeg synes, DKUUG har udviklet sig gevaldigt i den tid, jeg har været med, og det er heldigvis mere end en arbejdsplads; det er et sted, hvor folk kan finde på at dukke op, fordi det er sjovt, man møder søde mennesker og der sker interessante ting. Derfor fortsætter jeg da også med at arbejde frivilligt i foreningen og har meldt mig ind i bladudvalget. Jeg vil gerne sige tak til mine gode kolleger gennem to år, Bo Folkmann og Hanne Schmidt, og jeg kan sige, at det i høj grad er p.g.a. de tos engagement, at DKUUG har flyttet sig i de senere år. Man kan i

denne måned f.eks. læse, at DKUUG har været medarrangør af to store konferencer, NordU2000 i Malmø og LinuxForum 2000 i Symbion, som efter de flestes mening var store succeser - den eneste svips er vist, da der manglede Boeuf Stroganoff til tre deltagere ved LinuxForum; desværre var jeg en af dem. Men spøg til side; det er da meget godt gået, at foreningen er i stand til at arrangere en hel-dags konference med 500 deltagere og internationale talere - og alt klapper. Det lover godt for fremtiden, og efter min mening har foreningen en enestående chance for at stille sig i spidsen for udviklingen indenfor Åbne Systemer - og det vil jeg gerne fortsat være med til. Så vi ses nok en gang i fremtiden - om ikke andet til den DKUUG-fest, jeg har hørt så meget om, men altså ikke har oplevet endnu (hint, hint)

Hilsen Hans Arne Niclasen

Bjarne Stroustrup hjemme på besøg

Af Hans Arne Niclasen

Opfinderen af C++ var i Danmark igen i forbindelse med NordU2000 – og han havde et hårdt program.

Det var første gang, Bjarne Stroustrup var i Danmark siden sidste gang, han holdt foredrag i DKUUG. Til oplysning for de uindviede udviklede århusianske Bjarne midt i 80'erne programmeringssproget C++, der stadig bruges af millioner af programmører verden over.

Bjarne Stroustrup har siden 1979 boet i New Jersey og er chef for afdelingen for Large-Scale Programming hos telegiganten AT&T. Han udviklede midt i 80'erne programmeringssproget C++, der stadig bruges verden over. I de sidste par år har afdelingen arbejdet på en software-båd, komplet med vandkanon til at skræmme gæs væk.

Bjarne forklarer: - "Min „software båd“ (som vi endnu ikke har fået navngivet) er et distribueret programmerings projekt. Vi havde brug for et miljø, hvor vi kunne eksperimentere med software arkitekturer. Et par computere i et wired network var for let og for uinteressant, så jeg fik ideen om båden og forskellige „gadgets“ som vi kan montere på den (f.eks. en vejrstation - men folk er jo altid mere interesserede i vandkanonen). " Ikke så underligt, at der øverst på Bjarne's opslagstavle står "It's a software project, goddammit!"

Bjarne på tur

Bjarne Stroustrup kom til København søndag aften d. 6. februar. Mandag holdt han velbesøgte foredrag henholdsvis på DTU og i Gimle på Amager, hvor det lykkedes for arrangørerne, FORA-medlemmet KLID, at trække 210 tilhørere. Om tirsdagen gik turen til Malmø, hvor Bjarne holdt en tutorial "Highlights of the C++ Standard Library", og om aftenen gik turen tilbage over Sundet, hvor talerne ved NordU2000 var på rundtur i København – ifølge pålidelige kilder var især besøget på Christania en stor succes. Onsdag var rolig, men torsdag holdt Bjarne foredraget "New about C++" på NordU. Efter at have holdt hundredevis af foredrag om C++ havde Bjarne denne gang valgt at tale om, hvordan man lærer C++ fra sig og den øgede



Bjarne Stroustrup (t.h.) beundrer en 10.000 hestes motor hos MAN B&W.

indsigt, det kan give. Foredraget faldt i megen god jord hos de talrige tilhørere – og så var det tid for Viking-fest på "Slagthuset" i Malmø.

Bjarne på B&W

Om fredagen var Bjarne inviteret på besøg hos MAN B&W i Sydhavnen, der gerne ville vise, hvordan de brugte C++ i styringen af deres store maskiner, bl.a. til skibe. Bjarne var imponeret, især da han fik forevist en 10.000 hestes motor (se billederne). Virksomhedsbesøget gav også DKUUG-Nyt lejlighed til at få afleveret de flasker snaps, der har stået i sekretariatet siden sidste gang Bjarne var på besøg. Bjarne elsker nemlig intet mere end at arrangere en dansk frokost med sild og snaps hjemme i USA, så der bliver tanket op, hver gang han er i landet. Desværre kunne Bjarne kun tage den ene flaske med p.g.a. tolden, men hvad – så er der da en flaske, til næste gang Bjarne er i landet.

Du kan finde Bjarne Strostrups hjemmeside på <http://www.research.att.com/~bs/homepage.html>

Danmark handler på Internettet

af Per Andersen,
Direktør, IDC Nordic

Der bliver skrevet og talt meget om mangel på Web-handel i Danmark. Statistikker fra PBS viser et meget lavt niveau af transaktioner med Dankort og kreditkort, og mange danske virksomheder slutter trop i klagesangen: Hvor bliver kunderne af, spørger de.

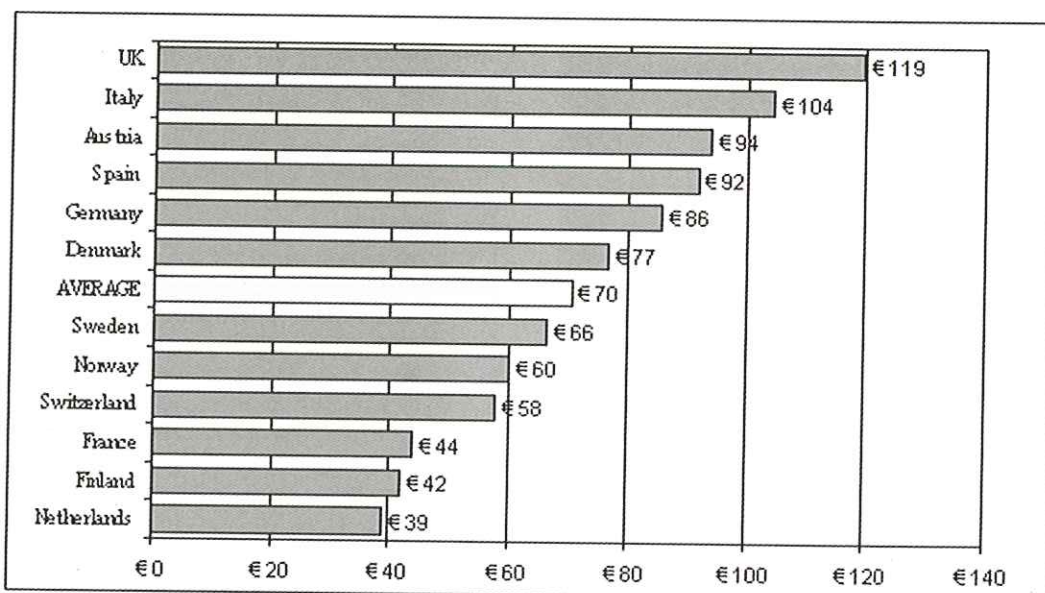
Men er dette den rigtige kilde til information om Web-handel i Danmark? Nej! I en storstilet undersøgelse af de faktiske Internet-brugere har IDC netop placeret Danmark på landkortet. Og undersøgelsen viser, at det ikke går helt galt i Danmark i forhold til de øvrige Europa – faktisk ligger Danmark nogenlunde på gennemsnittet.

Den nye analyse fra IDC indeholder en række interessante nyheder om anvendelsen af Internet i Europa og de forskellige lande. Blandt andet begynder der nu at være ligevægt mellem mænd og kvinder, unge og gamle på Internettet. Internettet er langt mindre forbeholdt visse befolkningsgrupper i forhold til tidligere. Samtidig er der et stort antal brugere af Internettet. Lige omkring halvdelen af den danske befolkning har anvendt Internettet inden for de seneste 3 måneder, og andelen fortsætter med at stige. Af resten udtrykker omkring 1/3 interesse i at komme i gang med at bruge Internettet.

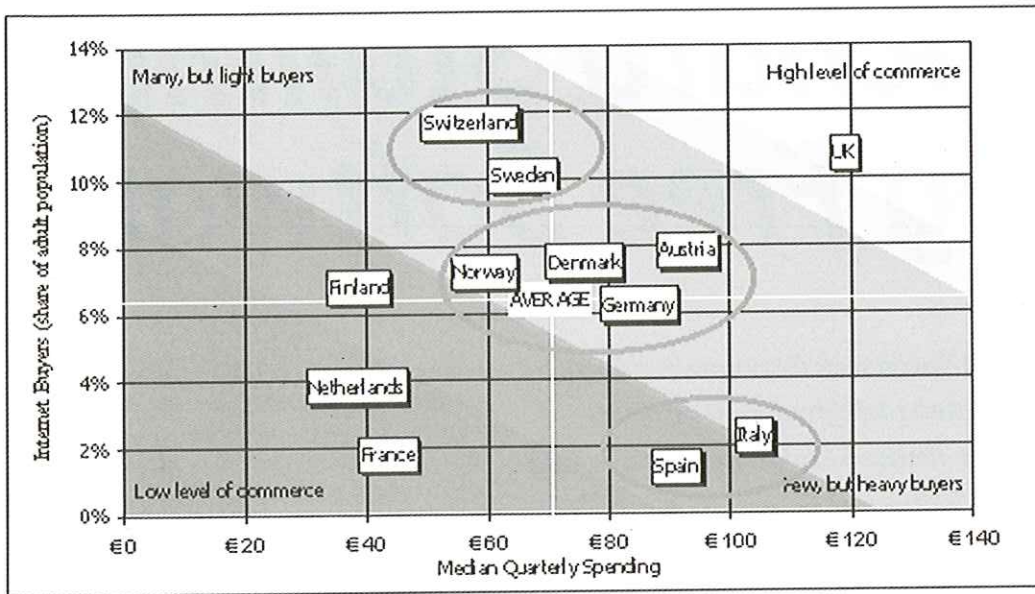
Det er derfor forkert at tale om, at Danmark er ved at blive opdelt i et A-hold og et B-hold – sådan som den nye IT højskole i Snoghøj gjorde det for nylig. Tendensen er tværtimod modsat: Anvendelsen bliver mere og mere gennemgribende i alle grupper, og Internetteknologien slår langt hurtigere igennem end nogen anden teknologi, vi har set (TV, mikrobølgeovn mv.).

Handel på Internettet er en kombination af to faktorer: Hvor mange, der handler, og hvor meget de handler for.

- **Antal handlende:** Hvad angår antallet af Web-handlende følger Danmark ganske godt med. Omkring 7% af danskerne siger, at de har handlet på Internettet, og det er på niveau med Norge og Finland, men dog lavere end i England og Sverige. Til gengæld er der relativt flere end i lande som Tyskland og Holland.
- **Køb pr. bruger på Internettet:** Her ligger Danmark stort set på gennemsnittet for Europa. Det fremgår af figur 1, hvor Danmark er sammenlignet med de øvrige lande i Europa. De angivne beløb er gennemsnitlig forbrug de seneste 3 måneder, og det udgør



Figur 1
Gennemsnitlig anvendt
beløb på Internet-handel
de seneste tre måneder –
kun blandt købere



Figur 2
Placering af Danmark i
blandt Europæiske lande
hvad angår Internet-

altså Euro 70 i gennemsnit for de danskere, der har handlet på Internettet de seneste 3 måneder.

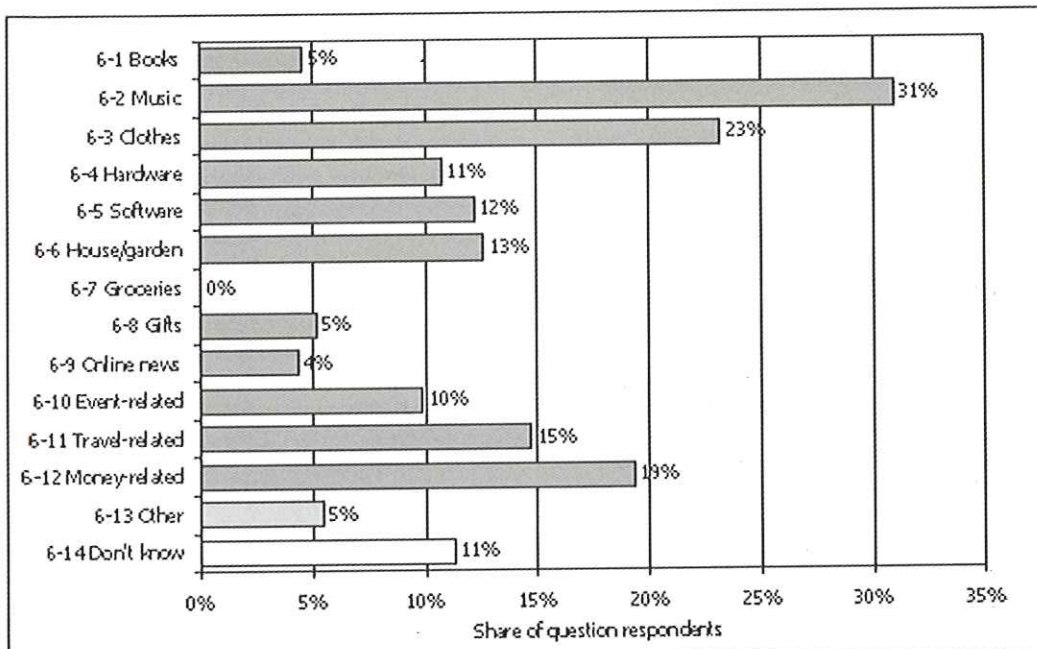
Som det ses af figur 2 ligger Danmark i samme gruppe som Norge og Tyskland hvad angår Internet-handel, og placerer sig i øvrige ganske godt i forhold til de fleste andre europæiske lande. Forklaringen er nemlig, at danskerne ikke handler særligt meget hos danske virksomheder – og det er dét branchen hæfter sig ved – men det meste af handlen lægges uden for landets grænser.

Danskerne handler først og fremmest standardvarer på Internettet. Det er musik, der placerer sig på førstepladsen, mens bøger kommer meget langt nede på listen. Man må konstatere at det stive danske bogsystem kombineret med mindre heldige sites fra boghandlernes side ikke har kunne gøre køb af bøger særlig attraktivt. Derefter følger tøj og som noget meget interessant og nyt: penge-

transaktioner. Dette dækker blandt andet over køb/salg af værdipapirer, som også forventes at slå igennem i Danmark, som vi har set det i andre lande – først og fremmest USA.

Mønsteret for handel har klart ændret sig. Tidligere var de edb-relaterede områder højt på listen (hardware og software), men nu er det mere de områder, der tiltaler konsumenter i bred forstand. Igen et klart tegn på, at Internethandel er på vej fra en niche til en generel ting.

Vi må håbe og ønske, at danske virksomheder kommer op på tærerne og forbedre deres positioner på det virtuelle Internet-marked. Hvis dette ikke sker, vil danskernes lyst til at købe fortsat blive dækket af først og fremmest udenlandske virksomheder. Fortsætter denne tendens, kommer der et tidspunkt, hvor Danmarks import/eksport forhold vil forværres væsentligt, og de burde vække bekymring hos både danske virksomheder og erhvervene.



Figur 3
Hvad danskere køber via
Internettet

Richard Stallman og Free Software

DKUUG-Nyts korrespondent på Fyn benyttede lejligheden til at interviewe Richard Stallman, manden bag Free Software.

Af Jesper "Blackie" Pedersen

Tirsdag d. 8. februar 2000 var en stor dag i FLUG's historie: Selveste Richard Stallman gav et foredrag om Free Software. Foredraget blev overværet af godt 210 mennesker, og bagefter var der stor enighed om, at hans foredrag var spændende og inspirerende. I denne artikel vil jeg fortælle lidt om hvem Richard Stallman er, samt hvad han snakkede om i hans foredrag.

Er du interesseret i at se foredraget, må det glæde dig at høre at foredraget er blevet optaget på video af en lokal tv-station i Odense. Lige i øjeblikket arbejder vi i FLUG på at få dette foredrag konverteret til elektronisk form. Er du interesseret i at se foredraget, send en email til mig (blackie@ifad.dk), så skal jeg give dig besked når jeg har det på elektronisk form, og jeg kan til den tid da sende det til dig på en cd.

Free Software's fader

Tilbage i 1984 arbejdede Richard Stallman på MIT og der havde han en oplevelse, som skulle ændre hans syn på software. Hele historien udspringer i et behov for at skrive ud til en printer. Richard Stallman fortæller:

- Printerne dengang var ikke særlig hurtige, hvilket betød, at når man havde sendt et udskrifts-job til printeren, så ventede man en halv times tid inden man gik hen til printeren for at hente udskriften.

- Desværre var printerne heller ikke særligt stabile, så når man kom derhen, var situationen ofte den, at printeren var brudt sammen, og det krævede manuel indgriben for at få den til at skrive videre. Efter at have fået printeren til at skrive igen, kunne man så gå tilbage på sit kontor og vente endnu en halv time.

- Dette betød at printeren det meste af tiden stod og ventede på manuelt indgriben, og at vi spildte masser af tid på at løbe frem og tilbage til printeren.

- Heldigvis havde vi kildeteksten til det program der styrede printeren, så vi rettede det til, således at når programmet opdagede at

printeren krævede manuelt indgriben, så sendte det en email til de mennesker der havde et printjob i kø. Disse mennesker kunne således straks få løst problemet, så printeren kunne komme igang med at skrive igen. Denne løsning virkede ganske udmærket, men med tiden skulle printeren dog udskiftes, og vi fik en ny meget hurtigere printer, som dog desværre af og til stadig krævede manuelt indgriben.

- Til den nye printer hørte et nyt printerstyringsprogram, hvor vi ikke havde kildeteksten, og leverandøren nægtede at give os den, så vi var nu tilbage ved den gamle situation, hvor printeren det meste af tiden stod stille, og folk spildte en masse tid med at løbe frem og tilbage til den.

- Denne problemstilling blev i mine øjne forværet, da jeg en dag opdagede at en kollega ved et andet universitet havde kildeteksten til printer programmet. Jeg tog kontakt til ham og bad om kildeteksten, men han ville ikke udlevere den, da han havde lovet printer producenten ikke at videregive den.

Richard Stallman siger sit job op

Det var på det tidspunkt Richard Stallman besluttede sig for at han ikke ville leje sin software, og som programmør ikke blot være slave. Han sagde sit job på MIT op, og besluttede sig for at han ville lave et frit operativ system, med dertil hørende frie programmer. Dette system døbte han GNU, og skulle du undre dig over hvad GNU betyder, så er det altså: Gnu's Not Unix.

Med frit mener Richard Stallman: frihed til at give kildeteksten videre, frihed til at rette kildeteksten til efter eget ønske, og endda videregive den tilrettede kildetekst.

Som en del af hans arbejde lavede han en slags inverse copyright, en copyright, som fraskriver folk retten til at forhindre andre i at udøve de ovenstående friheder. Hans skræk eksempel var X11, som var ganske frit i ovenstående betydning. Kommercielle UNIX producenter bundtledte X11 sammen med deres eget arbejde, og solgte dette med en copyright der fratog køberen at videregive endelige tilrette den X11 der kom med UNIXen. Licensen som han lavede, er den vi alle i dag kender som „The Gnu General Public License“ eller blot „GPL“.

Efter at have sagt sit job på MIT op, skulle

Richard Stallman's
GNU Foundation har
hjemmesiden
www.gnu.org

RMS nu finde noget at leve af. Han tog derfor kontakt til en række store firmaer, og bad om et sponsorat med følgende begrundelse:

Når jeg engang er blevet færdig med at lave et frit alternativ, vil I kunne bruge dette istedet for de UNIX versioner I bruger i dag. Derved vil I spare masser af penge.

Det gav dog ikke bid nogen steder, men det slog ham ikke ud af kurs. Han arbejdede ufortrødent videre på en nyudvikling af et program han tidligere havde lavet, nemlig Emacs. Et halvt års tid senere havde han den første version af dette program færdigt. Han gjorde straks programmet frit tilgængeligt på Internettet.

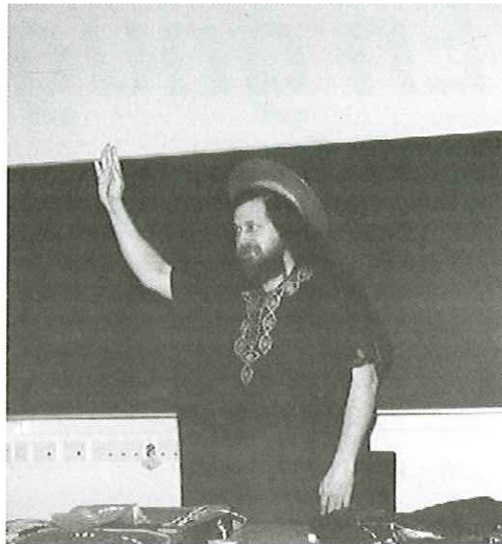
Her bør det nok indskydes at vi snakker om 1985, altså for 15 år siden, og dengang var internettet ikke noget hr og fru hvemsomhelst havde hjemme i stuen, nej, tværtimod var det kun de færreste der havde adgang til internettet. Derfor fik Richard Stallman mange henvendelser, der gik på om det var muligt at få fat i Emacs på anden måde end ved at downloade den fra nettet. I starten svarede han, at folk skulle prøve at se om de ikke kunne finde en eller anden med adgang til nettet som

kunne downloade det for dem, men snart fik han den ide at tilbyde at sende et bånd med Emacs på, mod betaling. På denne måde tjente han til dagen og vejen ved at distribuere Emacs, vel og mærke i kildetekst form, så folk stadig havde friheden til at gøre hvad de ville med Emacs.

Mange kritikere af Richard Stallmans ideer har gennem tiden sagt til ham at han aldrig ville kunne leve af at lave frit software, for når han havde solgt et eksemplar, så ville køberen straks dumpe prisen, og sælge en kopi videre (en gerning som GPL tillader, ja endog opfordre til), hvorved Richard Stallman aldrig ville få solgt mere end det ene eksemplar. Dette viste sig dog heldigvis (for Richard Stallman) ikke at være tilfældet.

Gennem 80'erne arbejdede Richard Stallman på denne måde med at udvikle frit software til GNU systemet, og med at overtale andre til også at gøre det. Han oprettede som en del af dette arbejde „The Free Software Foundation“, forkortet FSF. Han var faktisk ganske succesfuld med GNU projektet, og i starten af 90'erne var man næsten færdig med grundstenene, dvs. en editor, en C compiler, en linker, osv. (Grafiske desktops og lignende højniveau-applikationer var han selvfølgelig ikke kommet til endnu.) Han manglede dog en grundsten for at få hele fundamentet til at hænge sammen, nemlig kernen.

Kernen er den del af systemet, som tager sig af de eksterne enheder, såsom hard disk, tastatur, skærm o.l. samt tager sig af at håndtere og schedulere processerne. FSF arbejdede hårdt på at udvikle en sådan kerne, under navnet „The Gnu Hurd“. Grundet de strategier der var lagt



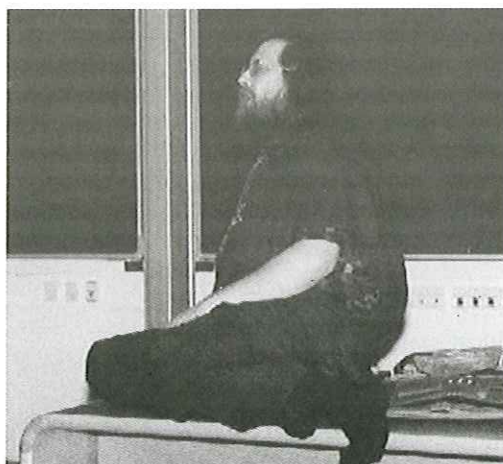
„Overbevis alle de vantrø om, at free software er vejen frem, amen!“

bag, var det dog en del sværere end de først havde antaget, og det trak derfor ud med at få den færdig - den dag i dag er de stadig ikke færdige med den!.

GNU/Linux

Og så skete det, at en finne ved navn Linus Thorvalds lavede en UNIX kerne, med langt mindre ambitiøse krav end dem, som Hurd skulle designes efter. Da det var lykkedes ham at få denne kerne til at køre bare nogenlunde, kiggede han sig om efter nogle UNIX programmer han kunne bruge sammen med sin kerne, og der fandt han heldigt nok næsten et helt færdigt system, nemlig GNU- systemet. Ifølge Richard Stallman var det ikke blot held at Linus Thorvalds fandt sådan et helt system. Det var jo præcis det FSF havde sigtet mod gennem mere end 7 år.

I modsætning til hvad man umiddelbart ville forvente, glæder Richard Stallman sig væsentligt mindre over det vi i daglig tale kalder Linux's succes. Han argumenterer nemlig for, at kun få af os i dag kender til GNU og FSF's filosofi om frit software, og at Linux' succes gør det sværere for ham at komme igennem med hans budskab. Derfor næsten tigger Richard Stallman os om at kalde tingene ved deres rette navn, og ifølge ham bør navnet være: GNU/Linux.



„May the source be with you!“

En gnuguru kom til byen

Forfatteren har haft den store ære at have Richard Stallman på besøg i to dage. Det har gjort uudsletteligt indtryk.

af Anne Helene Kahr
Thomsen

"Vi skal have besøg af en rigtig guru" meddelte min kæreste begejstret en mørk januaraften. „Vægtig, ærværdig: Indisk betegnelse for åndlig leder", forklarede Nudansk Ordbog. „Hm?" tænkte jeg. „Det er da okay med mig" Jeg har aldrig været specielt religiøs. Ugen gik og min kæreste blev mere og mere eksalteret ved tanken om guruens ankomst.

"Jeg har flere ting, jeg lige skal tale med ham om, henådede han, mens han pudsede sine Emacs-macroer af en sidste gang.

Hvorfor nu denne gurusnak? Vi bygger store dele af vores livsopfattelse/livssyn på myter, helte, martyrer, mystiske personer og historiske figurer. Visse ting kan vi bare godt lide at få af og bekræftet. Vi forventer vel lidt skuespil fra mennesker, vi selv udnævner til at være guruer. Hvor ville hele medieindustrien være henne uden hjælp fra disse guruer? (Idoler, når man er lidt yngre) Men min kære halvdel så i hvert fald stærkt frem til mødet med denne guru og havde omhyggeligt gjort rent og trimmet bulen til noget, der efterhånden i hysteritermer mindede mest om Jesu genkomst. Herudover havde han omhyggeligt instrueret mig i ALDRIG at sige OPEN SOURCE, men ALTID sige FREE SOFTWARE!!!! (Ordene på den til lejligheden producerede plakat lød nemlig „Free Software - i daglig tale bedre kendt som Open Source")

RMS kommer til middag

Op af trappens stejle trin kom Stallman så. Med et fjernt blik kiggede han ud gennem det lange hår og lige forbi mig. Min hånd flagrede lidt nervøst i luften, men guruen stavrede forbi mig ind til min bogreol, hvor han flåede alt engelsk-sproget litteratur ud. „It's british literature most of it", bemærkede jeg klogt. „And what is wrong about that?!" knurrede guruen. Guruer skal vel dybest set opføre sig anderledes. Det kan også betragtes som en art markedsføring, argumenterede min indre teoretiker. „You are right about that" sagde jeg høfligt.

Aftenens næste punkt var spisningen på en af

byens studentervenlige restauranter. En lille flok fra FLUUG var opsat på at møde Mr. Stallman inden næste dags foredrag på UNI. Vi fik bestilt. Uheldigvis havde restauranten pyntet risene med chilisauce, hvilket på ingen måde tiltalte Stallman. „The rice is infected with the stuff" gjorde han personalet opmærksom på. Nå ja - man kommer langt med rigelige drikkepenge.

Efter at have tilbragt efterhånden noget tid under det samme tag, fandt guruen, at det var tid til at henvende sig til mig for 2. gang. Efter at have konstateret, at substansen på brøddet om leverpostej, kiggede han næsten venligt på mig og bemærkede „Liver makes me wanna puke". „Oh I see" sagde jeg velopdraget og kiggede modvilligt på min halve med nævnte danske specialitet.

I forbindelse med DVD-sagen i Norge ville Stallman skrive et brev til den norske regering. Han skrev selv den engelske version, men havde efterfølgende brug for en oversætter. Her henvendte han sig for 3. gang til mig (i 3. person til min kæreste godt nok), idet han spurgte om ikke *hun* kunne skrive den oversættelse. Det kunne *hun* jo godt. Uheldigvis ringede telefonen og jeg måtte jo nødvendigvis tage den. 2 minutter efter afbrød Stallman samtalen, mens han lettere irettesættende gjorde mig opmærksom på, at vi havde noget, der skulle være færdigt!! No problem! Et kvarter til at oversætte et brev til den norske statsminister - nå, hvis der er for mange stavfejl - må jeg jo påstå, at det er et forsøg på at skrive ny-norsk!

RMS og kommunikation

I visse Linux kredse findes en kultomgivet t-shirt med Allan Cox som Prinsess Lea, Linus Torvalds som Luke Skywalker og Stallman som R2 D2. Måske passer det meget godt. R2 D2 er en lille lidt gnaven og lettere forældet robot, der ikke kan kommunikere ved tale. Den kan som bekendt kommunikere med en ligesindet robot, men har ikke evnen til at kommunikere med „almindelige" mennesker. Jeg laver naturligvis ingen direkte sammenligning, men konstaterer blot, at Stallmans mest brugte sætninger på Fyn var: „I don't know what you are saying" „You're statement is ambiguous", „I simply don't understand what you're trying to say!"



Leverspostej!!

RMS som guru

Nu er der gået noget tid. Stallman lavede et vældig godt foredrag på Odense Universitet. Han præsterede at fængsle sine godt 200 tilhørere i 2 timer.

Alligevel sidder jeg tilbage og tænker på, hvor aktuel Stallmans stil egentlig er udenfor denne endnu forholdsvis snævre kreds. Bliver Stallmans missionerende selvdyrkede gurustil for meget i det lange løb? Vel drages vi vel alle af det anderledes og vel fascineres vi af eksentriske personer, men open source/free software kan godt forekomme alle os udenforstående noget fjernt, hvis det kun repræsenteres af folk, der (i hvert fald for det utrænede øje) „mytificerer“ det som Stallman kan forekomme en at gøre. Jeg ved det på ingen måde er meningen, men hvad hvis mennesketyperne, der repræsenterer Open Source/free software ligger for tæt på den store gruppes opfattelse af noget, der er fjernt og skræmmende? Kan det evt. resultere i afstandstagen? Det burde ikke betyde noget, men man kan i DR1's program "Pengemagasinet" stadig kan høre begrebet NØRDER. Udtrykker dette måske en form for leflen for den målgruppe, der

sidder og ser programmerne og som man regner med har dette billede af Linux-folket? Og burde disse stereotyper ikke udrydes hen af vejen?

Tak for besøget Guru Stallman - det gav mig fornøjelsen at skrive denne artikel. Og ja - helt ærligt så var det heller ikke værre!!

Næste gang vil vi gerne have besøg af Linus Torvalds. Foruden at udfylde den folkekære myte om "The American Dream" ligner han en, der både har bordskik, almindelig pli - og så ser han altid så.....venlig ud. (apropos stereotyper!!)

Til orientering vil Anne Helene gerne have besøg af en guru en anden gang - men nok ikke af Richard Stallman. Det skal iøvrigt nævnes, at RMS til daglig bor på sit kontor på Massachusets Institute of Technology, hvor han engang har arbejdet, så det er måske ikke så mærkeligt, at hans sociale evner er begrænsede.

En cyborg kom (også) til byen

Steve Mann har eksperimentet med "wearable computing" siden 1970'erne, og han er ikke bare en nørd, der går rundt med en masse udstyr på hovedet - han har en mission.



Af Hans Arne Niclasen

En af de foredrag, der blev imødeset med størst spænding ved NordU2000 var Steve Manns. Til daglig er Mann professor ved universitetet i Toronto indenfor det felt, han selv har opfundet, nemlig wearable computing eller Wearcomp. De bærbare computere dækker altså i denne sammenhæng ikke over laptops, men over computere, man kan gå med på kroppen - på hovedet, foran øjet, på hænderne, indsyet i tøjet o.s.v. Som det fremgår af billederne, er disse wearable computere heldigvis blevet mindre med årene og kan nu bestå af et par normalt-udseende briller forbundet med en modtager indsyet i undertøjet (jo, jo - bl.a. 6 Gigabyte harddisk indsyet i underbukserne, sådan). Steve Mann holder masser af foredrag, men rejser sjældent nogen steder, fordi han på et tidspunkt fandt ud af, at han altid viste, hvad der foregik på hans øjekamera, og det kunne tilhørerne jo se lige godt, om han sad i samme rum som dem eller hjemme i Toronto. Men det lykkedes altså at få lokket Steve Mann til Malmø.

En kunstner og idealist

Som sagt er Steve Mann ikke bare en nørd, der vil lege med noget teknik, han er en mand med en mission. Siden sine high-school dage i 70'erne har han eksperimentet med Wearable Computers - Wearcomps. Han har to mål med sine Wearcomps: (1) At udforske fordelene i, at mennesket bliver til en cyborg, en sammen-smeltning af menneske og maskine og (2) at give det enkelte menneske kontrol over sine egne data, dvs. lægejournaler, offentlig registrering, skat, bank, forsikring o.s.v. Steve Mann gør oprør mod den overvågning, den enkelte borger er udsat for i dagligdagen, og han gør det på en meget kontant måde: Hvis han f.eks. bliver filmet af et overvågningskamera i en bank, filmer han

tilbage og offentliggør billederne på Internettet. Det er ifølge Steve den eneste måde at imødegå den stigende overvågning på; for når billeder kan lyve, og det kun er den ene side, der kontrollerer billederne, kan borgeren blive udsat for uretfærdige overgreb. Samtidig ser Steve Mann sine billeder som kunstværker og har haft billeder fra sit øjekamera udstillede på gallerier flere gange. Han har foreslået, at man kalder hans kunstretning "Refleksionisme", en videreudvikling af kunstarbejdsformen "Situationisme" fra 60'erne - kendteste danske udøvere er Jørgen Nash, Jens Jørgen Thorsen og Christiania-kollektivet Solvoggen. Situationisme går ud på at konfrontere systemet, offentligheden, med sig selv - at gøre mod det, som det gør mod os.

En cyborg er altid beredt

En hel afgørende forudsætning for Steve Manns cyborg-vision er, at man ALTID har udstyret på. På hans hjemmeside kan man finde en lang række instruktioner i, hvorledes det kan undgås at tage udstyret af og ja - Steve Mann sover ofte med udstyret på. De fleste steder i USA og Canada er det efterhånden tilladt at tage Wearcomp på til eksamen, fordi Steve har argumenteret kraftigt for, at den bærbare computer er en del af studenten - en "hjerne nummer to" som studenten skal lære at udnytte ligeså godt som sin egen hjerne. Med udviklingen af stadig mindre devices kan wearcomp bæres under de fleste sportsaktiviteter, men svømning er stadig et problem - og det samme gælder at bade. Men det er også de eneste steder, hvor Steve Mann medgiver, at det kan være nødvendigt at afføre sig computeren - man kan f.eks. sagtens jogge, mens man via sit display foran øjet (som f.eks. kan være søgeren fra et kasseret videokamera) surfer på Internettet eller

Steve Mann's "wearable computer" and "reality mediator" inventions of the 1970s have evolved into what looks like ordinary eyeglasses.



svarer på sin e-mail via sit en-håndsbetjente tastatur.

På hjemmesiden kan man også finde eksempler på de talrige ulemper, udstyret udsætter en for og de forandringer, der sker med kroppen. F.eks. har Steve observeret, at kroppen efter års tilvænning vænner sig til varmen fra udstyret og at cyborgen ligefrem fryser, hvis han/hun/den ikke har udstyret på - selv om sommeren. Der er også problemer med at udsætte øjet for skarp lys gennem længere tid, og cyborgen har forståeligt nok store problemer i lufthavne, hvor den altid står på kropsvisitering og nærkontakt med sniffende hunde. Og så er der toilet-problemet: Der er som regel ikke plads på offentlige toiletter til at få udstyret ordentligt af og på.

Det tekniske

Steve Mann har mange forskellige apparater på kroppen. Mest iøjnefaldende er øjendisdisplay'et, der både fungerer som kamera, der transmitterer til Internettet og som skærm, når man læser beskeder, surfer på Nettet eller åbner sin kalender. Signalerne sendes via ledere på tøjet til indmaden af en laptop-computer, som kan være distribueret på to måder - som en box, man har i bæltet eller gemt forskellige steder i tøjet. En trådløs radiosender forbinder apparatet med Internettet. Senderen er baseret på TCP/IP og fungerer begge veje, så ikke alene kan andre se, hvad bæreren kigger på, man kan sende beskeder til bæreren. Radio design'et er langsommeligt, men hurtigere radioer skulle være undervejs. Steve Mann benytter for det meste GNU/Linux Freeware som billed-manipulatoren GIMP (Gnu Image Manipulation Program), XV, emacs o.s.v. og forskellige kalender-

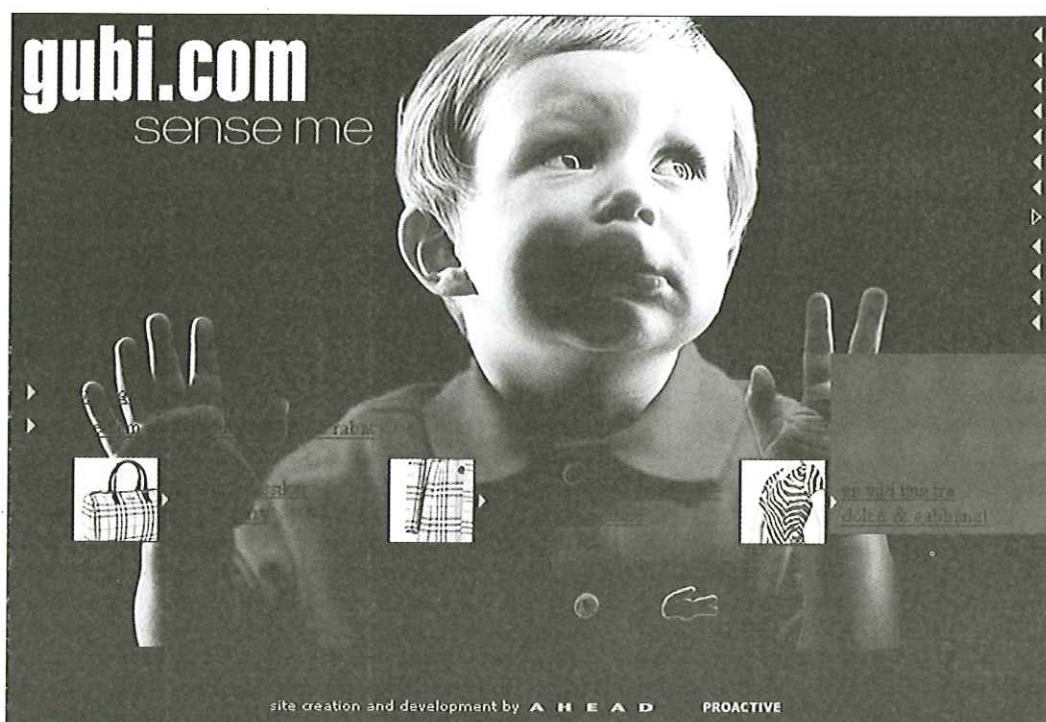
og planlægningsprogrammer. Skulle nogen være interesseret, er det muligt at købe færdige wearcomp-systemer, men de er meget dyre, og det anbefales at bygge dem selv. Med en kasseret lap-top og et kasseret video-kamera er man godt på vej. På Steve Manns hjemmeside kan man finde instruktioner til hjemmebyg af Wearcomp.

Er cyborgen fremtiden?

Det er nemt at grine af Steve Mann og det gjorde undertegnede da også, da han så Steve forsøge at drikke en øl under Viking-festen i Malmø - det var ikke nemt at få et ølglas ind under de store briller, der skjulte kameranøgleren og plastic-vikingshjelmen gjorde ikke synet mindre morsomt. Men Steve er en dybt seriøs forsker - og frihedskæmper - der altså har opnået en professorstol indenfor et område, han selv har opfundet. Han får flere og flere tilhængere verden over og måske får han i sidste ende ret: Mange af os kan efterhånden ikke forestille os en hverdag uden en mobiltelefon (WAP eller ikke), en Palm Pilot og en lap-top, og Steve Manns arbejde er vel bare en videreudførelse af denne udvikling til dens yderste konsekvens. Måske smelter vi alle mere eller mindre sammen med maskiner i fremtiden.

Læs mere om Steve Mann og hans Wearable Computers på www.wearcomp.org.

Siden sidst



Månedens hjemmesidebøf

Denne gang går månedens bøf til en eksklusiv kandidat: Gubi.com hedder den Internet-portal, der markedsfører sig med store annoncer på busser o.s.v. Gubi sælger eksklusivt modetøj, parfume, interiør og vine som f.eks. Dolce og Gabbana cowboybukser til over 2000 kr. og D & G luffer (!) til kr. 1750- (!!). Med de millioner, der er lagt i markedsføringen af Gubi, kan det undre, at der ikke har været råd til en designer, der kan gøre opmærksom på, at det ikke er særligt smart at skrive med SORT på SORT baggrund. Se Gubi's forside ovenover: På barnets højre hånd kan man ane noget skrift, men hvad der mere kritisk er måske, at de små pile i højre side af billedet er menupunkter – men man må altså gætte sig til, hvad det er, man vælger.

Ny opfindelse på LinuxForum

På LinuxForum 2000 præsenteredes den lille dansk-udviklede PC, der går under navnet Linux In A Box (LIAB). Udvikleren hedder Mikael Dich, tidligere lektor på DTU og nuværende udviklingsingeniør hos Simrad Shipmate.

„Vi regner med at kunne starte med at sælge vores Linux-pc om cirka en månedstid. Prisen bliver omkring 4000 kroner med mulighed for lavere priser til uddannelsesinstitutioner“, siger Mikael Dich til Ingeniøren. Det tog seks måneder for Mikael Dich at udvikle en fuldt køreklar mini-pc med indbygget Linux og webserver. Det lille pc-print rummer en 386-processor fra Intel, PROM til at gemme en komplet 2.036-linuxkerne med TCP/IP-stak, ramdisk og applikationer, som eksempelvis en Apache 1.2.6 web-server, som kan bruges til at kontrollere pc'en via et Ethernet-interface. - LIAB er designet til industriel styring og datalogging. Flere firmaer har vist interesse for produktet, og vi er i gang med konkrete forhandlinger med firmaet Jutlandia Døre, som vil bruge LIAB til styring af sine trævaremaskiner, siger Mikael Dich. Men med montering af et lille ekstramodul kan Linux-pc'en omdannes til en komplet MP3-afspiller. Mikael Dich peger på en række områder, hvor den lille pc kan anvendes. Primært inden for produktionsstyring.

Mikael Dich vurderer, at interessen for



prisbillige løsninger som Linux er stigende, når det drejer sig om markedet til produktionsstyring. Dette marked er i øjeblikket domineret af proprietære, licenskrævende styresystemer.

Linux In A Box er Open Source (Open Hardware?), og printudlæg og konstruktionsdetaljer kan frit downloades fra Internettet. Hjemmekonstruktører kan dermed selv bygge deres Linux In A Box. Udgifterne til hardware'n beløber sig til godt 1500 kroner.



WAP (Wireless Application Protocol) er fremtiden – måske

Ericsson vil have gang i det mobile Internet og har derfor taget initiativet til et dansk WAP partnerskab - WAPplayground - hvor udvalgte virksomheder samler kompetencer for at skabe nye WAP-baserede tjenester og forretningskoncepter til det mobile Internet. Målet er samtidig at give WAP-rådgivning til danske virksomheder. Foruden Ericsson, der stiller massive kompetencer, viden samt WAP-udstyr til rådighed, inkluderer partnerskabet en række tunge drenge med

udspring i web- og IT-verdenen, nemlig Datakomm, eHuset DDE (rygter vil i øvrigt vide, at gode gamle Dansk Data Elektronik er ved at skifte navn til eHuset), Bording Data, MÆRSKIT, Icon Medialab og Wireless Workers World Wide.

„Danmark er et af de få lande, som nu er modne til at udnytte mulighederne inden for mobilt Internet baseret på høje brugertal for både Internet og mobiltelefoni. Det er derfor naturligt, at vi sætter ekstra fokus på udviklingen af WAP markedet her i Danmark“, siger Bent Andersen, Director, Market Development, WAPplayground. Læs mere på www.wapplayground.dk

Annonceringen af WAPplayground falder sammen med meddelelsen fra CeBit om, at Siemens satser kraftigt på at øge deres markedsandel på det danske mobiltelefonmarked og i den nærmeste tid vil tilbyde WAP-telefoner til under 1000 kroner. Branchen forudser mindst 500.000 WAP-brugere indenfor det næste år.

Microsoft overfor Tux



Tour de CeBIT 2K

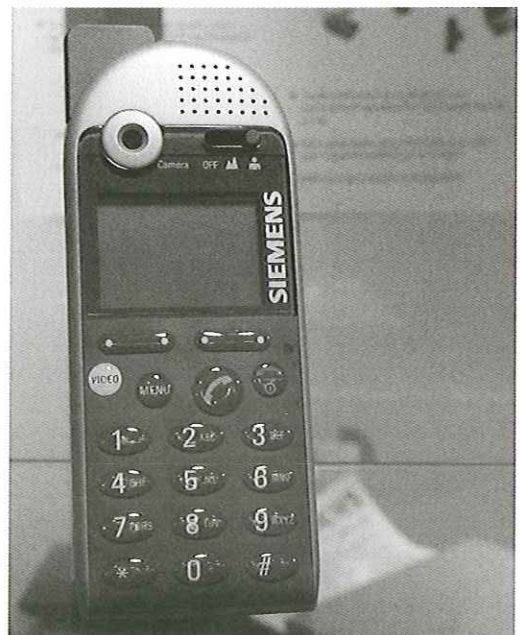
Af Kristen Nielsen

Årets tur til CeBIT er nu overstået. Facts og stats er følgende: I år var der igen besøgs rekord, godt 700.000 besøgende, 7000 udstillere fra næsten 70 forskellige lande, fordelt på 35 haller og paviljoner, udgjorde CeBIT eventet i år. Samtidig var der i år oven i dette godt gang i opbygningen af den kommende verdensudstilling EXPO 2000, som foregår i messeområdet, med et areal dækkende ca. 5 gange det areal, som Hannover messerne normalt dækker. EXPO 2000 foregår fra 1 maj til 31 oktober 2000.

Efter at have været på messen i 4 dage – er det overordnede indtryk at året ikke bringer store nye paradigmeskift, men der var en del trends som tydeligt viste sig – i det følgende vil jeg fortælle om de vigtigste.

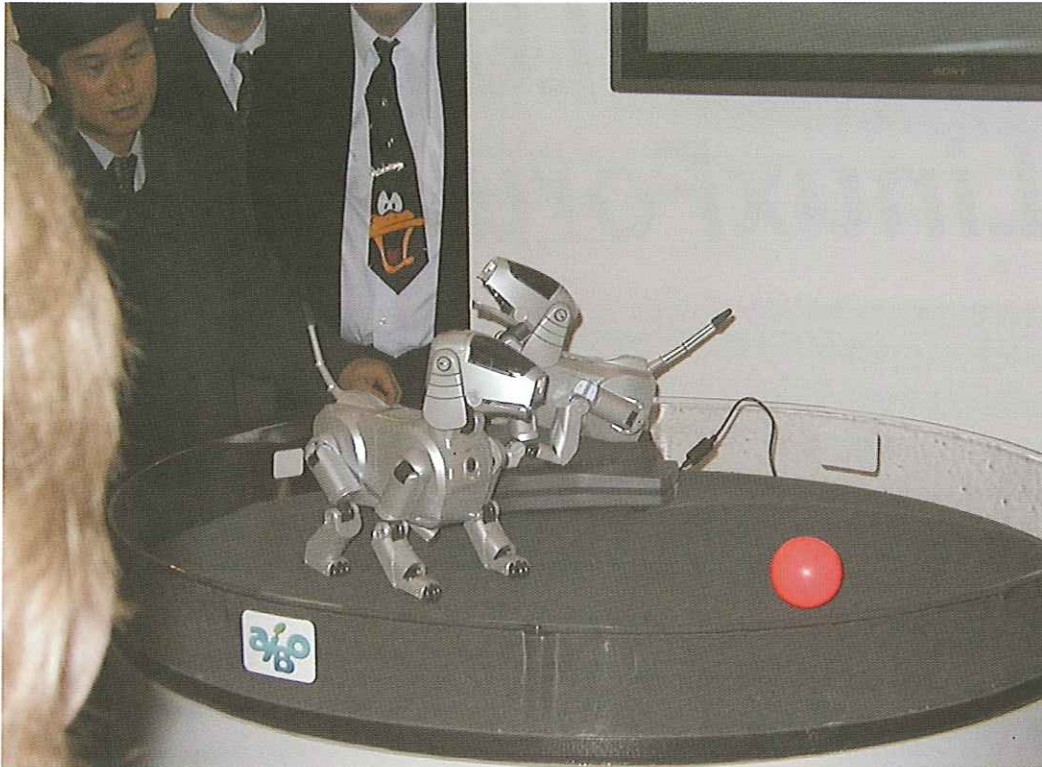
Der var mange bud på en fremtid med et bredt udbud af bærbare digitale dimser, som ingenting fylder og som stort set kan "det hele". Fotografiapparater/Videokameraer i en nøgle skilts størrelse, bærbare personlige kommunikationsterminaler med stemmestyring af de fleste funktioner, kalender, telefon (selvfølgelig) og videotelefon, osv. Der blev givet flere bud på en nær fremtid med meget lovende digitale mobile kommunikationsmuligheder.

Af eksperimentielle ting som blev vist, fandt jeg en 3D skærm som ikke kræver specielle farve eller polarisations briller, men som virker med



Siemens WAP-telefon kommer i Danmark til at koste mellem 700 og 1.000 kr.

det blotte øje – interessant, samt en demonstration af robotter som spiller fodbold, med holdorienteret og fælles strategisk angrebs taktik spændende.



Sony's robohund IAIBO

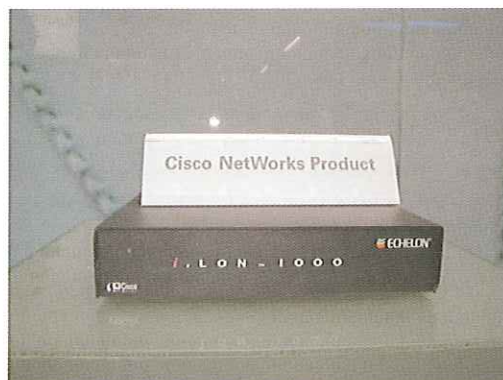
Tux (linuxpingvinen) befandt sig i Maxi plys udgave på alle relevante hardwareudbyders stande, med passende skiltning. Det virkede næsten helt forkert at se Tux på IBMs stand på toppen af en S/390 maskine, Compaqs stand på toppen af et serverrack, hos Oracle, Silicon Graphics, og naturligvis hos Corell, Linux International, Lotus og mange mange andre af de store dominerende firmaer. Det er klart at FreeUNIX verdenen er blevet en betydelig faktor i branchen, som man gerne vil skabe og oprettholde positive relationer til. Og det er tydeligt at de store leverandører har fået øjnene op for den betydning som den kult ånd, grænsende til religiøse ånd der er i brugerrækkerne af FreeUNIX systemer, og den PR goodwill her giver. Man er klart opmærksom på at goodwill i FreeUNIX verdenen har kort pay back time. Hvilket aldrig har været så tydeligt på CeBIT som det var i år. Personligt syntes jeg at det er svært at forestille sig et bedre signal for græsrodderne her på kanten til det kommende årtusinde.

En anden trend som tegner sig er at den fremtidsvision som jeg så gode bud på, allerede er godt på vej til at blive en realitet. På terminal-siden er man langt – men netdelen er klart the missing link. Både hvad angår GSM/UMTS (Universal Mobile Telecommunication System) / HSMD (High Speed Mobile Data) / GPRS (General Packet Radio Service) og Blue Tooth, er det tydeligt at dette er de manglende services som producenterne står og sukker efter.

Derimod offline terminalerne er helt med fremme. Videokamera indbygget i låget på en ultratyke midi laptop, drejbart og med fuld videomøde sw leveret med som standard men

pt kun til lokalnetsbrug, kan leveres nu. Mobiltelefoner med Wap bliver kraftigt markedsført som den hotte uundværlige forbrugergimmick, der leveres nu, integrationen er GPS (Global Positioning System) modtagere i bla. Mobiltelefoner og personlige kommunikatorer er få måneder fra at være på markedet. En robot hund (AIBO fra Sony) blev vist frem til den nette pris af 14000 DKr, har været på markedet i ca. 6 måneder. Den helt umiddelbare fordel som jeg selv ser, er at den kan slukkes, og ikke tisser bag potteplanterne.

Jeg havde forventet nogle nyheder på Storage løsninger, specielt indenfor SAN (Storage Area Network), men dem så jeg ikke. Cisco havde sjovt nok lavet en boks som de kalder Echelon, men der var ikke nogen på standen som kunne forklare hvad boksen kunne, eller hvorfor den netop havde fået dette navn. Det er mange år siden jeg ved at stille et så simpelt spørgsmål er blevet sendt videre til så mange forskellige personer på samme stand. Men det kan jo være at de kommer i tanke om det senere på året.



Sådan ser Echelon ud.

Med AaLUG til LinuxForum 2000

Publikum til LinuxForum



Et par håndfulde af medlemmerne i Århus Linux User Group trodsede deres normale døgnrytme for at deltage ved DKUUG's og SSLUG's konference LinuxForum 2000.

Afgang fra Århus

Med søvn i øjnene og jakken trukket godt op om ørerne lister en flok AaLUG'ianere ind i det ventende tog. Klokken er 5:53 og toget sætter i gang fra perronen på Århus banegård. Stemningen er alt andet end høj denne råkolde marts-morgen. Det skyldes sikkert at der ikke rigtigt nogle af os der er vågne endnu, og at DSB på stokastisk vis har spredt os rundt i alle 4 hjørner af hvilekupeen.

Efter hånden som vi vågner op og får lidt kaffe inden for vesten stiger stemningen. Den stiger så meget, at konduktøren er nødt til at bede os dæmpe os eller finde pladser et andet sted end i hvilekupeen, men med tanke på Claus' taske fuld af dåseøl som skal konsumeres på vej hjem, skal der mere til at ødelægge den gode stemning.

20 minutter over ni ankommer vi til Københavns Hovedbanegård. Tasken med øl placeres i en boks på banegården, og vi går os til at vente på S-toget. Mens vi venter dukker et par

stykker fra FLUG op. De skal også til LinuxForum, så vi følges resten af vejen. Vi ankommer til Symbion netop som Bo Folkmann og Peter Toft byder velkommen og præsenterer Matt Welsh - hvilken timing!

En spændende dag venter

For mange vedkommende er Matt Welsh fyren der „tog dig ved hånden og førte dig gennem den første svære tid med Linux“, og det er med store forventninger vi tager plads foran scenen i centerhallen. Foredraget indfrier til fulde vores forventninger og fuldt fortjent er køen for at få signeret "Running Linux" næsten længere end køen i kantinen.

Mens frokosten indtages lægges slagplanen for eftermiddagen. Det er svært at blive enige, da der er mange spændende arrangementer at vælge imellem, så det ender med at vi spredes for at pleje vores forskellige interesser.

Et program for alle

Mens nogle bruger tid i spillehulen, forsøger andre sig med FreeBSD eller besøger de mange forskellige udstillere, der er til stede. Eftermiddagen byder desuden på adskillige spændende foredrag og BOF (Bird Of a Feather) sessions man kan deltage i.

Derudover bliver der tid til lidt social networking med de andre LUG'er og med vores serverdonor Liga. Midt i det hele får Bjarke Johannesen overtalt Preben Bille Brahe (SSLUG) til at lege chauffør. Et par stykker af os kører ind

af Claus Glavind og
Jesper Meyer



Yngste deltager på
LinuxForum

til Lindesgade for at „redde“ AaLUG's server ud fra Kybers flytterod og få den med hjem til Århus.

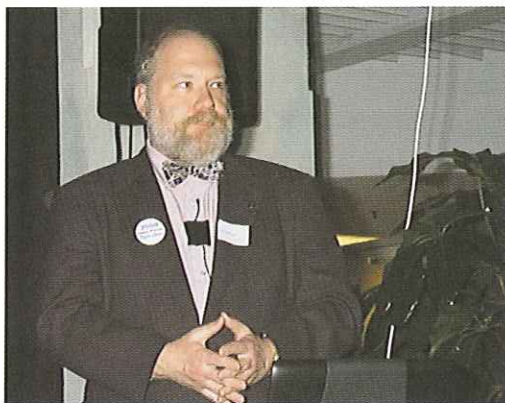
Endnu engang er det blevet spisetid, og vi samles atter i kantine for at sætte en velsma-

gende portion Boeuf Stroganoff til livs, mens vi diskuterer nogle af de ting, vi har deltaget i i løbet af eftermiddagen.



Hanne Schmidt tæller
dagens omsætning

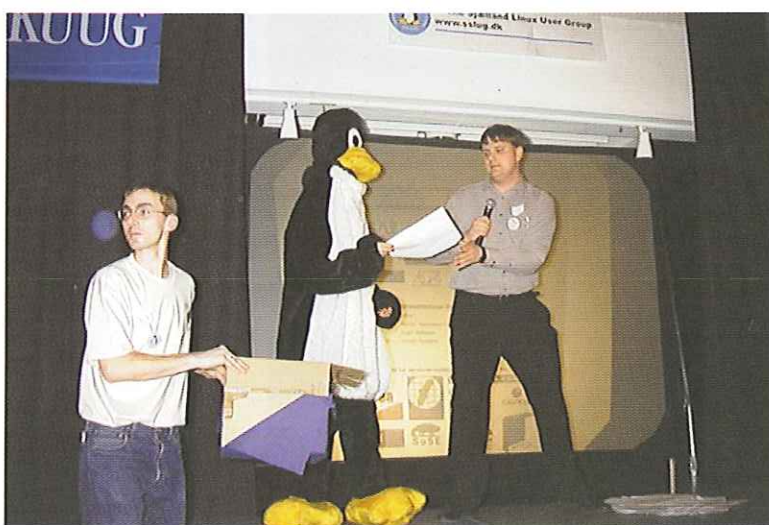
Gene Spafford udfordrede Linux-fanatikerne



Aftenens arrangement

Dagens anden hovedtaler, Eugene Spafford, indtager scenen i centerhallen med et foredrag om sikkerheden ved Open Source software. En del af deltagerne har valgt kun at købe billet til dagsarrangementet, så Symbion er ikke helt så fyldt som tidligere på dagen. Flere af de tilbageværende deltagere ser efterhånden lidt trætte ud, men Spaf's lidt kontroversielle men spændende foredrag sørger dog for, at ingen falder i søvn.

Efter foredraget er det muligt at køre et eksemplar af Spaf's bog "Practical Unix & Internet Security", som Spaf naturligvis signerer. Ligesom ved Matt Welsh's og Kalle Dalheimer's bog-signering tidligere på dagen, er dette et stort tilbudsstykke. Herefter er det muligt at stille spørgsmål og foredraget har åbenbart sat tankerne i gang og spørgelysten er derfor stor.



Peter Toft, Tux og Jesper Pedersen udfører en lille ballet under præmieudtrækningen

Høj stemning på hjemturen

Spaf's spørgerunde er knap overstået før det er blevet tid til at vende næsen mod Jylland. På hovedbanegården henter vi tasken med dåseøl og gør klar til at fordøje dagens indtryk. På trods af at dagen allerede har været lang fejler humøret intet, og da vi har fundet vores pladser bliver dagens konkurrencevindere overfaldet. Mikkels pakke med Applixware studeres nøje, mens Svends S.u.S.E.-kasket trækker knap så mange misundelige blikke. Corel-skumterningerne flyver hastigt gennem kupeen mens den ene øl efter den anden pumper liv i de trætte „pingviner“.

Ti minutter over et ruller toget ind på Århus H. og vi gør klar til at forlade de magelige pladser. På banegårdspladsen skilles vi - de fleste for at få et par timers søvn inden en ny dag truer, enkelte fortsætter dog ud i det århusianske natteliv.

Vi tror vi taler for alle, når vi siger det har været en god tur - vi er i hvert fald et par stykker der glæder os til næste år.

Facts om AALUG/Klub Århus:

Webside: www.aalug.dk

Startet: Sensommeren 1998.

Organisering:

En bestyrelse (kernen) bestående af 5 medlemmer samt en suppleant.

Fem arbejdsgrupper (arrangement, cdrom, møde, pr og web) hvor alle frit kan deltage og hjælpe.

Aktiviteter:

Møde/foredrag hver ca. 14. dag (pt. hver anden tirsdag) et centralt sted i Århus (oftest på universitetet).

Installfester.

Udflugter til arrangementer hos andre LUG'er ol.

FORA-medlem af DKUUG, Klub Århus.

Antal medlemmer: 442 pr. 1. marts 2000.

Open Source og sikkerhed

Amerikanske Bruce Schneier er en af verdens førende eksperter indenfor kryptografi og computersikkerhed. Bruce Schneier er forfatter til en række bøger, deriblandt den definitive bog om kryptering „Applied Cryptography“, der er solgt i over 120.000 eksemplarer over hele verden. Derudover er Bruce forfatter til talrige artikler og udgiver af månedsbrevet Cryptogram. Bruce Schneier har designet den populære "Blowfish encryption algorithm", som efter seks år stadig ikke er blevet brudt. I bedste Bill Gates-stil er Bruce netop stoppet for direktør for det firma, han har startet, Counterpane Internet Security, for istedet at koncentrere sig om jobbet som teknisk chef. I denne artikel, der er oversat til dansk af SSLUG, fortæller Bruce, hvorfor Open Source er den bedste måde at udvikle krypteringsprogrammer på.

Som kryptografi- og computersikkerhedseksperter har jeg aldrig forstået al den snak der foregår om Open Source-bevægelsen. I krypteringsverdenen betragter vi Open Source som en nødvendighed for god sikkerhed; og det har vi gjort i årtier. Offentlig kendt sikkerhed er altid mere sikker end proprietær sikkerhed. Dette gælder for krypteringsalgoritmer, sikkerhedsprotokoller og programtekst til sikkerhed. For os er Open Source ikke blot en forretningsmodel, det er en intelligent udviklingspraksis.

Open Source kryptering

Kryptering har levet op til Open Source-idealene i årtier, selvom vi kalder det „at bruge offentlige algoritmer og protokoller“. Ideen er simpel: Kryptering er svært at gøre fejlfrit, og den eneste måde at vide om noget er gjort fejlfrit er at være i stand til at undersøge det.

Det er vitalt i kryptering fordi sikkerhed intet har at gøre med funktionalitet. Du kan have to algoritmer, én sikker og én usikker, og de virker begge perfekt. De kan kryptere og dekryptere, de kan være effektive og have en pæn brugergrænseflade, og måske går de aldrig ned. Den eneste måde at kende forskel på god og dårlig kryptering er ved at få krypteringen undersøgt.

Værre endnu: Det hjælper ikke at få tilfældige folk til at undersøge programteksten; den eneste måde at kende forskel på god og dårlig kryptering er at have programteksten undersøgt af eksperter. At analysere kryptografi er svært, og

der er kun få mennesker i verden, der er kompetente til at gøre det. Før en algoritme kan blive betragtet som virkelig sikker må den undersøges af flere eksperter over en årrække.

Dette taler meget stærkt for krypteringsalgoritmer i Open Source. Da den eneste måde at have tillid til en algoritmes sikkerhed er at få eksperter til at undersøge den, og den eneste grund til eksperter gider bruge den nødvendige tid på at undersøge den er for at offentliggøre videnskabelige artikler om algoritmen, derfor må algoritmen nødvendigvis være offentlig. En proprietær og hemmelig algoritme er, ligemeget hvem, der har designet den og hvem der blevet betalt for at undersøge den, meget mere risikabel at benytte end en offentlig kendt algoritme.

Du hører nogle gange modargumentet, at kryptering med en hemmelig algoritme er meget sikrere netop fordi algoritmen er hemmelig, og at offentlige algoritmer er mere usikre fordi de er offentlige. Umiddelbart lyder det fornuftigt, men prøv at tænke nærmere efter. Offentlige algoritmer er designet så de er sikre selvom de er blevet offentliggjorte; de er netop lavet til dette. Så der er ingen risiko ved at offentliggøre dem. Hvis en algoritme kun er sikker hvis den forbliver hemmelig, så vil den kun være sikker indtil nogen efterligner algoritmen og publicerer efterligningen. Der har været en mængde hemmelige algoritmer til mobiltelefoner på markedet, men disse er kort efter blevet brudt, hvilket netop illustrerer pointen.

I stedet for at benytte offentlige algoritmer besluttede de amerikanske mobiltelefonselskaber at lave deres egen proprietære kryptering. Gennem de seneste år er forskellige algoritmer blevet offentliggjorte. (Og nej; det var ikke mobiltelefoniindustrien, der ønskede dem offentliggjort. Det der generelt sker er, at en kryptografiekspert modtager en fortrolig specifikation i en brun konvolut.) Og efter de er blevet offentliggjorte, er de blevet brudt. Nu overvejer mobiltelefoniindustrien at benytte offentlige algoritmer i stedet for deres brudte proprietære.

På den anden side har det populære emailkrypteringsprogram PGP altid brugt offentlige algoritmer. Og ingen af disse algoritmer er nogensinde blevet brudt. Det samme gælder for en række krypteringsprotokoller på Internettet: SSL, S/MIME, IPSec, SSH og så videre.

af Bruce Schneier
<schneier@counterpane.com>

Den bedste undersøgelse, der ikke kan købes for penge

Netop nu er den amerikanske regering ved at vælge en krypteringsalgoritme der skal erstatte DES, kaldet AES (Advanced Encryption Standard). Der er fem kandidater til standarden og før den endelige er valgt vil verdens bedste kryptografeksperter bruge tunsindvis af timer på at undersøge dem. Intet firma, hvor rigt det end måtte være, har råd til den slags undersøgelse. Og siden AES frit kan bruges til alt, er der ingen grund til, at noget firma skulle spille tid på at lave deres egen standard. Offentlig kryptografi er ikke blot bedre - det er også billigere.

Den samme grund, der får intelligente virksomheder til at bruge offentliggjort kryptering, for dem også til at bruge offentliggjorte sikkerhedsprotokoller: Alle, der laver deres egen sikkerhedsprotokol, er enten et geni eller en nar. Da der er flere af sidstnævnte end af førstnævnte, er det simpelthen blot mere intelligent at bruge offentliggjorte protokoller.

Tag for eksempel IPsec, internetprotokollen for kryptering over IP. Fra starten i 1992 var den designet i fuld offentlighed af en komite og blev udsat for en grundig, offentlig gennemgang. Alle vidste, det var en vigtig protokol og folk brugte meget tid på at gøre den fejlfri. Forskellige sikkerhedsteknologier blev foreslået, brudt og efterfølgende ændret. Versioner blev implementerede og analyserede. Det første udkast til en standard blev offentliggjort i 1995. Man debatterede de forskellige aspekter ved IPsecs sikkerhedsniveau, effektivitet, om hvor nemt det var at indføre og opgradere samt brugen.

I november 1998 offentliggjorte komiteen en række RFC'er - et af de skridt, der skal til for at gøre IPsec til en standard på Internettet. Og IPsec bliver stadig studeret. Kryptoeksperter ved Naval Research Laboratory opdagede for nyligt en mindre implementeringsfejl. Arbejdet fortsætter i fuld offentlighed af alle, der er interesserede. Resultatet baseret på flere års offentlig analyse er en stærk protokol, som mange stoler på.

På den anden side udviklede Microsoft sit eget alternativ Point-to-Point Tunneling Protocol (PPTP). De opfandt deres egen autentificeringsprotokol, deres egne hash-funktioner, og deres egne nøglegenererings-funktioner. Hver eneste én af disse havde store fejl. De brugte en kendt krypteringsalgoritme, men de brugte den på en sådan måde, så den ikke gav yderligere sikkerhed. De lavede implementations fejl som svækkede systemet endnu mere. Men da de lavede alt arbejdet internt, var ingen klar over, at PPTP var svag.

Microsoft gik på markedet med PPTP i Windows NT og 95 og brugte det i deres VPN-produkter (Virtual Private Network). De offentliggjorde til sidst deres protokoller. I sommeren 1998 publicerede mit firma (Counterpane) en rapport, der beskrev de fejl, vi havde fundet. Igen

betalte offentlig undersøgelse sig. Microsoft udsendte hurtigt en række fejlrettelser, som vi undersøgte i sommers. Rettelserne var bedre, men stadig behæftede med fejl.

Ligesom med algoritmer er den eneste måde at kende en god sikkerhedsprotokol fra en dårlig på ved at have eksperter til at undersøge den. Så hvis du har brug for en sikkerhedsprotokol, er det klogeste at tage én, der allerede har været undersøgt. Du kan lave din egen, men hvad er chancen for at den skulle være lige så sikker som én der har været undersøgt af eksperter gennem flere år?

Sikring af din programtekst

Det er præcis den samme begrundelse som får enhver intelligent udvikler til at kræve Open Source programmer til alt relateret til sikkerhed. Lad os lige opsummere: Sikkerhed har intet at gøre med funktionalitet. Derfor kan testning af programmet aldrig vise en brist i sikkerheden. Den eneste måde man kan finde sikkerhedsfejl i en programtekst - så som en kryptografisk algoritme eller sikkerhedsprotokol - er derfor at undersøge den. Dette gælder for alle programmer, hvadenten de er Open Source eller proprietære. Og det er ikke ligemeget hvem du får til at undersøge programteksten: Det skal være eksperter i sikkerhedssoftware. De skal undersøge programmet flere gange og fra forskellige vinkler gennem flere år. Det er muligt at hyre den slags ekspertise, men det er meget billigere og mere effektivt at lade samfundet som sådant gøre dette. Og den bedste måde at gøre det på er at offentliggøre programteksten.

Men hvis du virkelig ønsker din programtekst skal være sikker, kræver det mere end blot at offentliggøre den under Open Source. Det er to åbenlyse fælder, som du skal være klar over.

For det første: bare fordi du offentliggør programteksten betyder det ikke automatisk, at folk vil undersøge den for sikkerhedsfejl. Sikkerhedsfolk er travle. De har ikke tiden til at undersøge enhver programkode, der er offentliggjort. Så selvom offentliggørelsen er en god ting, så garanterer det ikke sikkerhed. Jeg kunne nævne et dusin sikkerhedsbiblioteker under Open Source, som ingen nogensinde har hørt om, og som ingen nogensinde har undersøgt. På den anden side er sikkerhedssoftwaren i Linux blevet undersøgt på kryds og tværs af mange dygtige sikkerhedsfolk.

For det andet: Du skal være sikker på, at sikkerhedsfejl bliver rettet så snart de er fundet. Folk finder sikkerhedsfejl i Open Source programtekster og det er en god ting. Der er ingen grund til at tro, at Open Source programmer på det tidspunkt de først er skrevet skulle være mere sikre end proprietære programmer. Pointen i at gøre programmet Open Source er, at så utroligt mange folk gennemgår programteksten for sikkerhedsfejl og finder dem. Hurtigt. Disse fejl skal så rettes. Så et to-år gammelt Open Source

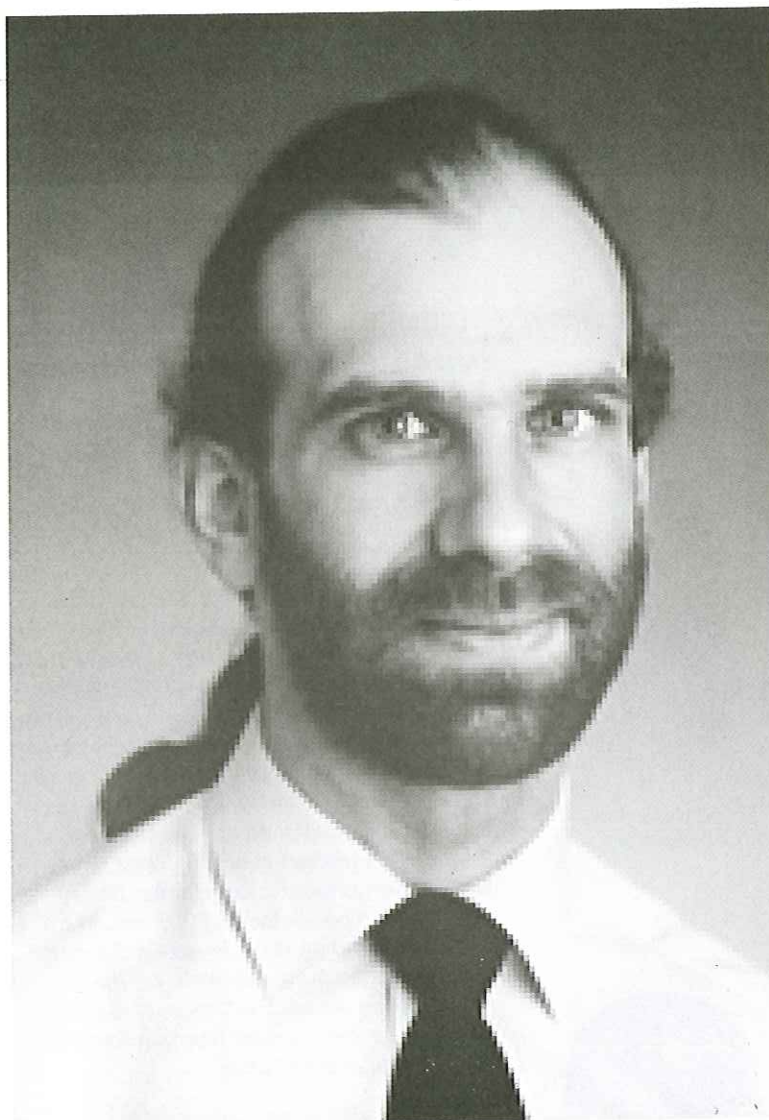
program har sandsynligvis færre sikkerhedsfejl end et proprietært program - simpelthen fordi så mange af fejlene er fundet gennem tiden. Sikkerhedsfejl bliver også fundet i proprietært software, men meget langsommere.

At sammenligne sikkerheden i Linux med sikkerheden i Microsoft Windows er ikke noget godt eksempel. Microsoft har gjort et utroligt dårligt stykke arbejde på sikkerhedssiden og det er derfor ikke en rimelig sammenligning. Men at sammenligne Linux med Solaris er et meget bedre eksempel. Folk finder sikkerhedsfejl i Linux hurtigere og de bliver samtidigt rettet hurtigere. Resultatet er et operativsystem der - selvom det endnu kun er få år gammelt - allerede er meget bedre end Solaris var i samme alder.

Sikker PR

En af de store fordele ved Open Source-bevægelsen er den positive feedback man får ved offentliggørelse. Gå ind i en vilkårlig større computerforretning og du vil se en hel hylde med Linux-baserede produkter. Folk køber dem fordi Linux' appeal ikke længere er begrænset til nørder; det er et brugbart værktøj til visse opgaver. Den samme feedback gælder inden for sikkerhed: offentlige algoritmer og protokoller vinder troværdighed fordi mange folk kender og bruger dem og de bliver et buzzword. Marketingsfolk kalder dette „mindshare“. Det er ikke en perfekt model, men hey, det er bedre end alternativet.

Bruce Schneier har flere gange besøgt DKUUG, sidst i maj 1998. Originalversionen af denne artikel kan findes på <http://www.counterpane.com/crypto-gram-9909.html>.



Remote login og netværksaflytning

Dette er første del af den fjerde artikel i serien om netværks-sikkerhed på Linux. Næste del følger i næste nummer af DKUUG-Nyt.



af Hanne Munkholm
<hanne@aub.dk>

En af de store styrker ved en Linux (UNIX) maskine er, at man kan administrere den fra en anden maskine via netværk. For at være kompatibel med alle andre UNIX varianter følger de gode gamle værktøjer telnet og ftp med i Linux distributionerne, og de er meget anvendte til fjernadministration. Vi vil i denne artikel se på, hvorfor værktøjer som telnet og ftp ikke bør anvendes, hvis maskinen er koblet til Internet eller et andet usikkert netværk. Vi skal se på, hvordan netværkstrafik kan aflyttes. Derefter skal vi se nærmere på alternativer til telnet og ftp, hvor datastrømmen bliver krypteret. Specielt fokuserer vi på ssh (secure shell) og viser installation og anvendelse. Meget af det, der beskrives i artiklen, gælder ikke blot for Linux, men også for andre UNIX'er.

Nem men usikker netværkstrafik

Fra en Linux maskine kan man nemt logge ind på en anden Linux maskine og køre programmer, endog grafiske programmer. Dermed kan man køre tunge programmer på en stærk server og få vist resultater på en anden (måske langsommere) maskine.

Antag, at vi har et lokalnet bestående af tre maskiner. Vi anvender maskinen „sherwood“ (IP adresse 192.168.0.1) med brugernavnet robin, men vi vil køre programmer fra maskinen „locksley“ (192.168.0.2). I netværket finder vi desuden maskinen „nottingham“ (192.168.0.3), som vi leger er en ondsindet maskine, der ønsker at bryde vores sikkerhed. I praksis kunne det være tre maskiner på Internet, hvor netværkstrafik mellem „sherwood“ og „locksley“ tilfældigvis også kommer forbi „nottingham“.

Resten af artiklen vil handle om programmer til remote login, som telnet, rlogin og ssh, samt programmer til filoverførsel (ftp og scp). Men hvad bruges det til? Med remote login kan man udføre tekstkommandoer på den maskine, man er logget ind på, men man kan også køre X-programmer over nettet.

telnet og xhost

Hvis du på sherwood kører en X-baseret grafisk brugergrænseflade, og du vil køre X-programmer (grafiske programmer) fra maskinen locksley, skal du starte med at fortælle sherwood, at det er i orden, at locksley benytter dens display. Dette gøres ved at føje locksley til listen over godkendte hosts med kommandoen xhost:

```
[robin@sherwood robin]$ xhost +
locksley
locksley being added to access
control list
```

Dermed vil grafiske programmer fra locksley vil blive accepteret af sherwood. Udelades maskinnavnet, betyder det, at alle maskiner kan vise grafik på din skærm. Lad være med det, da det sikkerhedsmæssigt er en dårlig ide.

Lad os nu logge ind på locksley med telnet,

```
[robin@sherwood robin]$ telnet
locksley
Trying 192.168.0.2...
Connected to locksley.herne.dk.
Escape character is '^]'.
Debian GNU/Linux 2.1
locksley.herne.dk
```

```
locksley login: robin
Password:
```

Efter at have skrevet loginnavn og password på locksley maskinen får du en kommandolinie, og du kan udføre programmer på maskinen, som om du var logget ind lokalt.

For at kunne få de grafiske programmer, du starter på locksley, til at vise sig på sherwoods skærm er det nødvendigt at sætte DISPLAY environment variabelen:

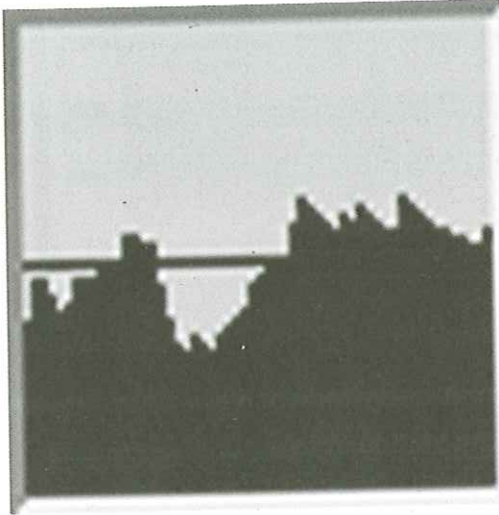
```
[robin@sherwood robin]$ export
DISPLAY=sherwood:0.0
```

Mange X-programmer kan dog også kaldes med „-display“ som option.

Nu kan du køre dit X-program, f.eks. „xload“, som om du sad på locksley. Programmet kører på locksley, men alt grafik vises på sherwood, og programmet styres fra sherwood.



og Peter Toft
<pto@sslug.dk>



```
[robin@locksley robin]$ xload -
display sherwood:0.0 -geometry
60x60 -nolabel &
```

Det er nemt, og allerede ved disse enkle operationer kan du have mistet hele din password-sikkerhed. Sagen er, at da man i sin tid designede telnet tænkte man ikke så meget på sikkerhed, men mere på driftstabilitet. Når man laver telnet fra en maskine til en anden, sender man først sit brugernavn og derefter password. Begge sendes klar tekst. Det kan selvfølgelig udnyttes til at stjæle passwords på Internet - og det gøres!

Pas på passwords sendt over netværk

For at aflytte netværkstrafikken kan man downloade programmet sniffit til Linux. Når det startes op vises alle kommunikationslinier, såsom telnet- og ftp-forbindelser, mellem maskinerne på netværket. Det kommer an på konfiguration af routere, firewalls, switcher og hubs, hvor meget man reelt får at se. Sniffit kan downloades fra <http://reptile.rug.ac.be/~coder/sniffit/sniffit.html>. Sniffit skal køres som root.

Lad os antage, at den ondsindede „nottingham“ (192.168.0.3) lytter med på, hvad vi laver mellem „sherwood“ (192.168.0.1) og „locksley“ (192.168.0.2). Programmet sniffit startes i interactive mode med angivelse af hvilket netværks-interface, der skal lyttes på:

```
[root@nottingham root]# sniffit -F
eth0 -i
```

hvor eth0 betyder første ethernet kort i maskinen, og i betyder interactive mode. Ud kommer nedenstående billede, hvor man ser, at maskinen med netværksadresse 192.168.0.1 (sherwood) har oprettet en forbindelse til port 23 på maskinen med netværksadresse 192.168.0.2 (locksley). Port 23 er den port, telnet lytter på. Port 3211, som man sender fra, er valgt blandt maskinens ledige porte, dvs. de porte, der

ikke er nogen service, der lytter på. Der er valgt et portnummer, som er større end 1024, dvs. en ikke privilegeret port.

Trykkes return på en linie vil den blive markeret med „*LOGGED*“, og det mindre vindue mod højre vil vise trafikken på den forbindelse. Først kommer login navn: „robin“, og efter to punkummer kommer passwordet i klar tekst: „qwe123“. Der skal ikke stor fantasi til at forestille sig, at dette program nemt kan sættes til at dumpe samhørende loginnavne og passwords ned i en fil over en periode, indtil der er gevinst.

Vi har vist, at man ikke skal bruge telnet til at kommunikere mellem to maskiner, hvis der er risiko for, at nogen lytter med, og slet ikke hvis man skal logge ind som root på maskinen. Det er simpelthen for nemt at lede efter loginnavn root og derefter få passwordet. Derfor har mange Linux distributioner per default forhindret, at root logger ind via netværket. Red Hat 6.0, Debian 1.3 og SuSE 6.2 har filen „/etc/securetty“, der indeholder de konsoller, hvor root må logge ind. Dette kan være „tty1“ til „tty6“, som er de tekst login konsoller, der normalt er på selve Linux maskinen - dvs. ikke via netværket. Hvis man absolut vil tillade root login via netværk, kan man tilføje „0“, „1“ og opefter (for Linux kerne 2.2.X) svarende til hvor mange logins, du forventer på maskinen fra netværket. Normalt er det ikke klogt at tillade direkte root login via netværk.

ftp

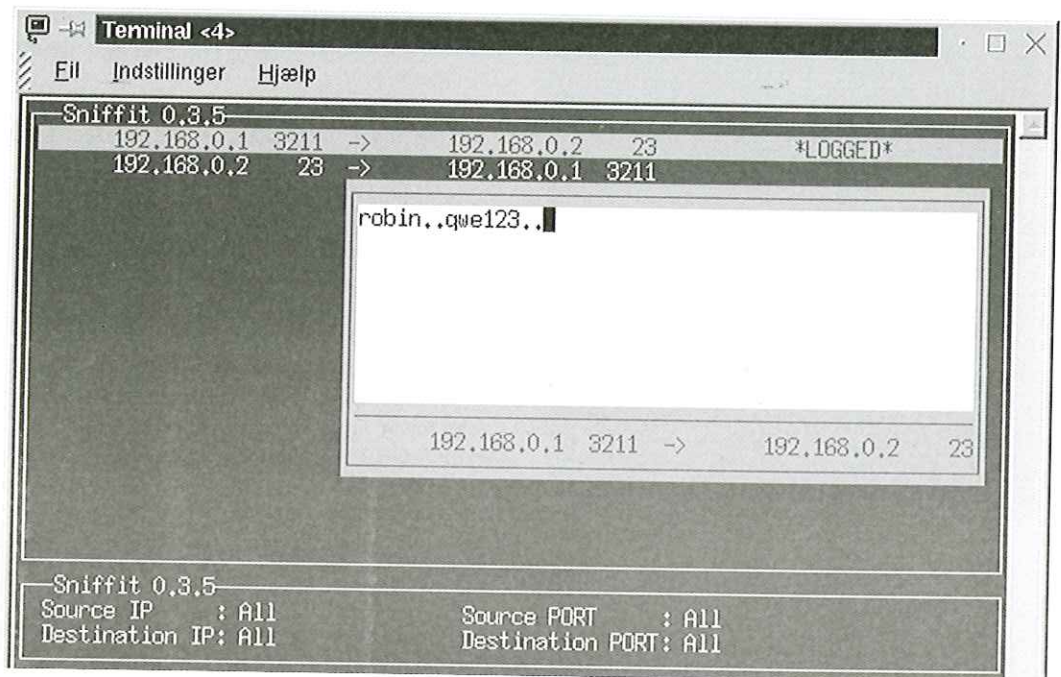
Hvis vi vil overføre filer fra „sherwood“ (192.168.0.1) til „locksley“ (192.168.0.2), er ftp et af de gennemprøvede og gamle værktøjer. Også her er der sikkerhedsproblemer. Vi sætter igen „nottingham“ (192.168.0.3) til at køre sniffit som vist nedenfor. Denne gang sætter vi sniffit op til at vise alle pakker som ankommer til „locksley“ (192.168.0.2), og man kan nemt se, hvad der sker.

```
[root@nottingham root]# sniffit -
t192.168.0.2 -a -F eth0
```

```
Packet ID (from_IP.port-to_IP.port):
192.168.0.1.1299-192.168.0.2.21
E . . 4 . . @ . @ . . . . . . . . . .
. . . . . . . . . . b . . . . . P . . } x
i !
. . U S E R   r o b i n . .
```

```
Packet ID (from_IP.port-to_IP.port):
192.168.0.1.1299-192.168.0.2.21
E . . ( . . @ . @ . . . . . . . . . .
. . . . . . . . . . b ( . . . . . P . . } x
. .
. .
```

```
Packet ID (from_IP.port-to_IP.port):
192.168.0.1.1299-192.168.0.2.21
E . . 5 . . @ . @ . . . . . . . . . .
. . . . . . . . . . b ( . . . . . P . . } x
N D
. . P A S S   q w e 1 2 3 . .
```



På den første af de tre data-linier kan man se login navn, og som vist på den sidste data-linie, vil man direkte kunne læse passwordet. Ser man lidt nøjere efter, vises også ftp-porten, port 21. Port 1299 er ligesom ved telnet en ledig port, der vælges til denne session.

Som vi ser, er ftp også et meget usikkert program, hvor andre kan lytte med. Så brug det med omtanke. For en systemadministrator er paranoia ikke en sygdom, men en kvalifikation...

Det skal nævnes, at også resten af den nettrafik, du laver med telnet og ftp, kan læses i klar tekst via f.eks. sniffit. Starter du andre programmer, kan man se det.

Laver du „su - root“ og skriver root-passwordet, er sikkerheden på den maskine væk, for root passwordet er ude, hvis du bliver aflyttet.

Remote login, remote shell og remote copy

To andre velkendte programmer i samme kategori er „rlogin“ og „rsh“. Programmerne virker næsten ens. Begge giver interaktivt login på maskinen, men rsh kan udføre en kommando samtidig med, at man logger ind. F.eks. vil den følgende kommando logge ind direkte fra sherwood til locksley og køre kommandoen „df“ (som viser hvor fyldte dine diske er).

```
[robin@sherwood robin]$ rsh locksley
df
```

Nu prøver vi at køre sniffit på en rlogin session for at se, hvad man kan se. På maskinen „nottingham“ kører vi sniffit:

```
[root@nottingham root]# sniffit -x -s192.168.0.1 -a -F eth0
```

Vi logger ind fra sherwood til locksley med kommandoen:

```
[robin@sherwood robin]$ rlogin
locksley
Password:qwe123
$
```

hvor password'et naturligvis ikke kan ses på skærmen, når man taster det ind. Udklip fra sniffit's output:

```
TCP Packet ID (from_IP.port-to_IP.port): 192.168.0.1.1023-192.168.0.2.513
SEQ (hex): C2D0BA41 ACK (hex): 105DA03F
FLAGS: -AP- Window: 7D78
Packet ID (from_IP.port-to_IP.port): 192.168.0.1.1023-192.168.0.2.513
E . . ? s . @ . @ . F Q . . . . .
. . . . . A . ] . ? P . } x
C .
. . r o b i n . r o b i n . x t e r
m / 9 6 0 0 .
```

```
TCP Packet ID (from_IP.port-to_IP.port): 192.168.0.1.1023-192.168.0.2.513
SEQ (hex): C2D0BA58 ACK (hex): 105DA040
FLAGS: -A- Window: 7D78
Packet ID (from_IP.port-to_IP.port): 192.168.0.1.1023-192.168.0.2.513
E . . ( s . @ . @ . F g . . . . .
```



```

. . . . . X . ] . @ P . } x
} A
. .
TCP Packet ID (from_IP.port-
to_IP.port): 192.168.0.1.1023-
192.168.0.2.513
SEQ (hex): C2D0BA58 ACK (hex):
105DA041
FLAGS: -AP- Window: 7D78
Packet ID (from_IP.port-to_IP.port):
192.168.0.1.1023-192.168.0.2.513
E . . 4 s . @ . @ . F J . . . . .
. . . . . X . ] . A P . } x
. .
. . . . . s s . . . . P . . . . 1
TCP Packet ID (from_IP.port-
to_IP.port): 192.168.0.1.1023-
192.168.0.2.513
SEQ (hex): C2D0BA64 ACK (hex):
105DA04B
FLAGS: -A- Window: 7D78
Packet ID (from_IP.port-to_IP.port):
192.168.0.1.1023-192.168.0.2.513
E . . ( s . @ . @ . F U . . . . .
. . . . . d . ] . K P . } x
} *
. .

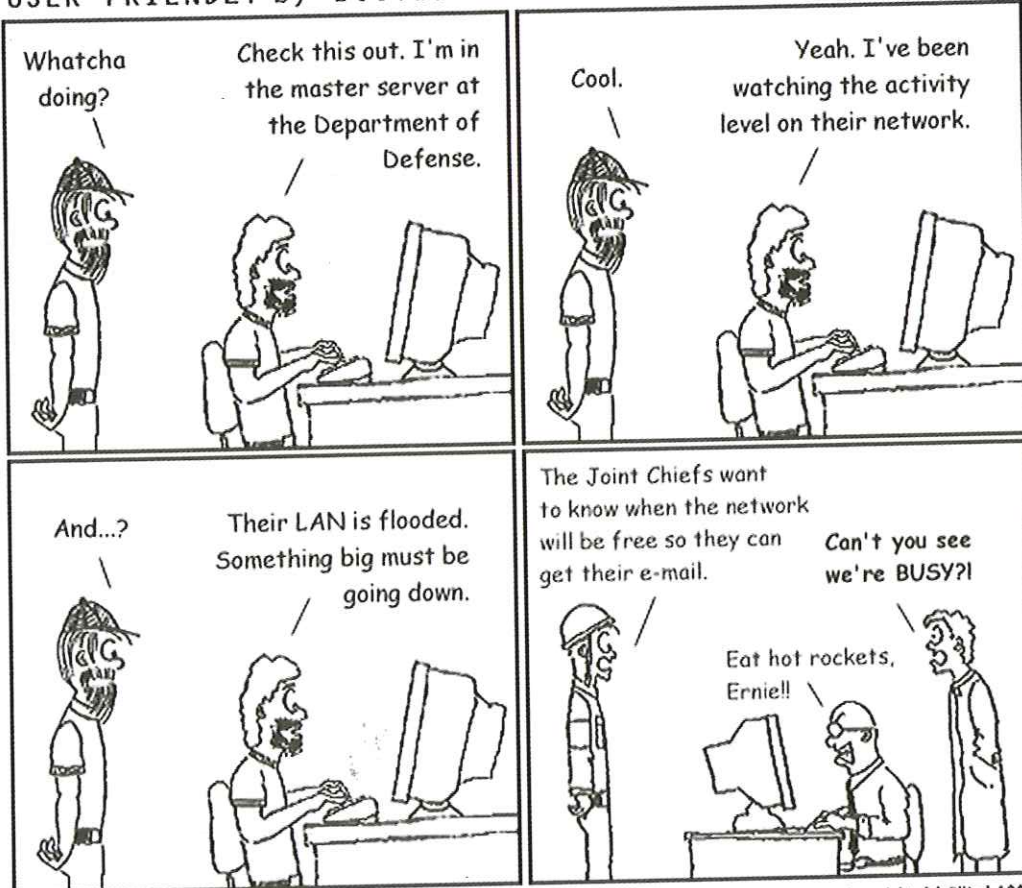
```

```

TCP Packet ID (from_IP.port-
to_IP.port): 192.168.0.1.1023-
192.168.0.2.513
SEQ (hex): C2D0BA64 ACK (hex):
105DA04B
FLAGS: -AP- Window: 7D78
Packet ID (from_IP.port-to_IP.port):
192.168.0.1.1023-192.168.0.2.513
E . . ) s . @ . @ . F S . . . . .
. . . . . d . ] . K P . } x
. !
. . q
TCP Packet ID (from_IP.port-
to_IP.port): 192.168.0.1.1023-
192.168.0.2.513
SEQ (hex): C2D0BA65 ACK (hex):
105DA04B
FLAGS: -AP- Window: 7D78
Packet ID (from_IP.port-to_IP.port):
192.168.0.1.1023-192.168.0.2.513
E . . ) s . @ . @ . F R . . . . .
. . . . . e . ] . K P . } x
.
. . w
TCP Packet ID (from_IP.port-

```

USER FRIENDLY by Illiad



```

to_IP.port): 192.168.0.1.1023-
192.168.0.2.513
  SEQ (hex): C2D0BA66  ACK (hex):
105DA04B
  FLAGS: -AP-  Window: 7D78
Packet ID (from_IP.port-to_IP.port):
192.168.0.1.1023-192.168.0.2.513
  E . . ) s . @ . @ . F Q . . . . .
. . . . . f . ] . K P . } x
. .
. . e

```

```

TCP Packet ID (from_IP.port-
to_IP.port): 192.168.0.1.1023-
192.168.0.2.513
  SEQ (hex): C2D0BA67  ACK (hex):
105DA04B
  FLAGS: -AP-  Window: 7D78
Packet ID (from_IP.port-to_IP.port):
192.168.0.1.1023-192.168.0.2.513
  E . . ) s . @ . @ . F P . . . . .
. . . . . g . ] . K P . } x
L .
. . 1

```

```

TCP Packet ID (from_IP.port-
to_IP.port): 192.168.0.1.1023-
192.168.0.2.513
  SEQ (hex): C2D0BA68  ACK (hex):
105DA04B
  FLAGS: -AP-  Window: 7D78
Packet ID (from_IP.port-to_IP.port):
192.168.0.1.1023-192.168.0.2.513
  E . . ) s . @ . @ . F O . . . . .
. . . . . h . ] . K P . } x
K .
. . 2

```

```

TCP Packet ID (from_IP.port-
to_IP.port): 192.168.0.1.1023-
192.168.0.2.513
  SEQ (hex): C2D0BA69  ACK (hex):
105DA04B
  FLAGS: -AP-  Window: 7D78
Packet ID (from_IP.port-to_IP.port):
192.168.0.1.1023-192.168.0.2.513
  E . . ) s . @ . @ . F N . . . . .
. . . . . i . ] . K P . } x
J .
. . 3

```

Igen ser man tydeligt brugernavn og password blive sendt ukrypteret over nettet. Man kan se, at rlogin på locksley bruger port 513, og at der på sherwood sendes fra port 1023.

Skal du kopiere filer mellem to maskiner, så er ftp som tidligere skrevet meget anvendt. Alternativt kan remote copy „rcp“ anvendes. Skal du kopiere filen „emacs“ fra sherwood til locksley, sker dette med

```
[robin@sherwood robin]$ rcp .emacs
locksley:
```

Sikkerhedsmæssigt er rcp på linie med rlogin og rsh. Vi skal senere i artiklen vende tilbage til et fuldt krypteret alternativ til rcp.

Med rlogin, rsh og rcp kan man vælge, at login kan ske uden password. Dette gøres ved at sætte sit hostnavn og evt. brugernavn ind i filen „~/rhosts“ i sit hjemmekatalog på den maskine, der skal logges ind på. Hvis du gerne vil kunne logge ind fra sherwood til locksley uden password, som brugeren robin, kan „rhosts“-filen i dit hjemmekatalog på locksley se sådan ud:

```
sherwood robin
```

Der kan godt stå mange flere linier med andre hostnavne. Brugernavnet kan udelades, idet brugeren sættes til den, hvis hjemmekatalog filen ligger i. Hvis filen er læsbar for alle, er det kun en bruger med samme brugernavn som sit eget, der kan logge ind fra en anden maskine. Er filen ikke læsbar for andre, kan man anføre linier i „rhosts“-filen med først maskinnavn og dernæst det brugernavn, som anvendes på den anden maskine. For at „marian“ skal logge på ind på „sherwood“ som „robin“, kan man således bruge „rlogin sherwood -l robin“.

Den viste „rhosts“-fil vil betyde, at du fra maskinen sherwood som brugeren robin, godt må komme ind på locksley som robin, uden password. Det kræver, at brugeren findes på begge maskiner, og „rhosts“ filen skal ligge i brugerens hjemmekatalog på den maskine, man prøver at logge ind på. Det er nemt og giver lynhurtig adgang til, at man hopper fra maskine til maskine og laver meget effektive arbejds-gange. Det lyder smart, men medaljen har en bagside. En med root-adgang på maskinen „nottingham“ (eller andre maskiner i netværket) kan aflytte rsh/rlogin netværkstrafik et stykke tid, og derved finde ud af fra hvilken maskine og med hvilket bruger navn, man kan logge ind direkte. Derefter kan man med lidt snilde sætte maskinen „nottingham“ lidt anderledes op, så „locksley“ tror, at den er „sherwood“.

Der kan imidlertid være situationer, hvor det kan virke mere sikkert at lade en bruger logge ind uden password fra en kendt host end at lade brugeren have et password. Har man tillid til sit interne netværk, og er det nødvendigt, at nogle brugere kan logge på en udsat maskine, kan man vælge, at disse brugere ikke har noget password på den udsatte maskine. I stedet får de en stjerne („*“) i „etc/passwd“, der hvor passwordet normalt ville stå. Dette vil forhindre dem i at logge ind fra andre maskiner end dem, der er angivet i deres „~/rhosts“ fil i deres hjemmekatalog på den udsatte maskine. Når en bruger ikke har et password, kan man ikke bryde ind på den udefra ved at gætte eller knække passwordet. Men kan kun logge ind som denne bruger, hvis man kan overbevise maskinen om, at man logger ind fra en betroet maskine. Der kan i

øvrigt læses mere om passwords beskyttelse og håndtering i Artikel 3 - Root access - hvem, hvordan og hvorfor ikke?.

Hvis man ikke tillader „rhosts“-filer, vil der ved hver login sendes passwords i klar tekst over nettet. Hvis der er „rhosts“-filer, bliver der slet ikke sendt passwords over nettet - i stedet for at give sit password skal man logge ind fra en betroet host. Ingen kan nu opsnappe passwords - til gengæld kan de udgive sig for at være den betroede host. Stoler man ikke på sit interne netværk, eller er nogen „sluppet ind“, er begge dele nok lige dårligt.

Vi vil anbefale, at man i stedet for rlogin bruger et program, der krypterer login såvel som selve dataoverførslen, som f.eks. ssh giver mulighed for.

Som systemadministrator kan du se om dine brugere har „rhosts“ filer, og hvis det ikke er ønsket, kan du slette dem (og skælde brugeren ud). Hvis brugerne har hjemmekataloger under „/home/“, så kan dette gøres med

```
[root@sherwood root]# find /home/* -
maxdepth 1 -name „.rhosts“ -print;
```

Hvis man samtidigt vil slette de fundne .rhosts filer kan man anvende

```
[root@sherwood root]# find /home/* -
maxdepth 1 -name „.rhosts“ -print -
exec rm {} \;
```

Det er enklere at disable brugernes egne „rhosts“-filer ved, at man tilføjer parameteren „-l“ efter „in.rshd“ i filen „/etc/inetd.conf“ og genstarter inetd-dæmonen. Læs mere om inetd i Artikel 2 - Services.

Et andet argument imod at tillade „rhosts“-filer er, at brugeren kan komme til at køre et program, som skriver til en fil uden hans viden. Filen kunne „~/rhosts“ og dermed give adgang til en ekstern bruger, som ikke behøver at have en konto på maskinen.

Et alternativ til „~/rhosts“ metoden er „hosts level equivalence“ via filen „/etc/hosts.equiv“. Dine brugere har ikke adgang til denne fil, og kun root kan rette i den. Root kan vælge at sætte en række hostnavne ind i denne fil eller evt. bare et plus. Det betyder, at disse hosts (+ betyder alle maskiner) har adgang til at udføre rlogin og rsh kommandoer uden password. Dette gælder alle brugere (dog ikke root) - brugeren skal dog findes på begge maskiner. Filen „/etc/hosts.equiv“ kan være en bekvem løsning, men den er en bombe under systemsikkerheden - find en anden løsning, hvis du har et åbent eller halvåbent netværk.

User Friendly fra den 12. december 1997 kan Greg fra Columbia Internet aflytte netværkstrafikken i forsvarsministeriet...

Fortsættelsen kan findes på <http://www.userfriendly.org/cartoons/archives/97dec/19971216.html> :-)

Forfatterne har copyright på artiklen, men udgiver den under OpenContent License. Alle kan trykke artiklen så længe OPL licensen overholdes, men vi vil gerne vide hvor den bringes.

Licensen, der skal overholdes, kan findes på <http://www.opencontent.org/opl.shtml>. Alle artikler i denne serie kan findes på http://www.sslug.dk/artikler/Linux_sikkerhed.



FLUGs historie



Af Jesper "Blackie" Pedersen

Som et led i vores præsentation af DKUUGs klubber er vi nået til FLUG, som formanden præsenterer således:

FLUG - Fyns GNU/Linux User Group er FORA-medlem af DKUUG, hvilket vi har været i ca. et år nu. Vi er, som navnet næsten siger, bosat på Fyn, og vores foredrag finder sted på Odense Universitet. I det følgende vil jeg opsummere hvad der er sket i FLUGs 1-årige historie, og især hvad vi har lavet de sidste par måneder.

Lad mig starte med at præsentere mig selv, jeg hedder Jesper Pedersen, og er formand for FLUG.

FLUG er på samme tid både en af Danmarks ældste LUG'er og en af de yngste, afhængig af hvad der skal til for at være en LUG. Det hele startede helt tilbage i 95, hvor en række systemadministratorer og ex-systemadministratorer på Odense Universitet indkaldte til et møde, hvor emnet var Linux. Til dette møde var vi godt og vel 15 mennesker, og vi blev enige om at mødes en gang om måneden til erfaringsudveksling. Det gjorde vi så, men desværre ikke mere end to gange eller så, så gik det lidt i sig selv igen.

3 år senere tog jeg atter tråden op, og vi begyndte at mødes - og denne gang var det faktisk regelmæssigt. Vi gik endda så langt som at reklamere for os selv på Universitetet og nogle få kollegier. På dette tidspunkt var vi nu godt 20 medlemmer, hvoraf der var ca. 5-8 til hver møde.

23 december 1998 fik jeg så et brev fra Peter Toft (formand for SSLUG), som skulle ændre tingene i FLUG drastisk. I dette brev stod der, at

Eric Raymond kom på besøg i Danmark, og hvis vi var interesseret, så kunne han komme forbi FLUG og give et foredrag. JO! vi var interesseret!

Et møde med 20 FLUG medlemmer havde sikkert været hyggeligt for Eric Raymond, men han ville nok også have følt at vi spildte hans tid lidt. Så vi måtte lige finde et par hundrede flere medlemmer. Dette lykkedes os faktisk. På blot en måned lykkedes det os at få lavet en meget flot plakat, og få denne plakat hængt op en masse steder (dvs. alle computerforretninger, mange kollegier og mange videregående uddannelser!)

Til foredraget kom der godt 180 mennesker, og til det efterfølgende møde i FLUG var der 65 mennesker. Desværre er det ikke lykkedes os at vedholde dette fremmøde-tal til alle vores møder, men vi er dog flere end de 5-8 stykker vi var blot 2 måneder tidligere.

FLUG det sidste år

Efter Eric Raymonds foredrag har vi haft en lang række meget spændende foredrag. Følgende er en liste over højdepunkterne:

Miguel de Icaza talte om Gnome.

Kalle Dalheimer talte om KDE.

Jon „maddog“ Hall talte om „Linux in the enterprise“.

Marcus Meissner talte om WINE (Windows emulator).

Oracle var på besøg, gav øl og talte om deres database produkter.

Henrik Størner talte om Firewalls.

Richard Stallman talte om Free Software.

Ud over denne stjerneregning af foredrag udefra, så har vi også haft et utal af foredrag som medlemmer af FLUG selv stod for, herunder kan nævnes „C++ Programmering og debugning“, „Perl“, „Python“, „Star Office“, „CVS“, „The Dotfile Generator“, „Emacs“, og The Gimp.

Siden Eric Raymonds besøg har vi mødes cirka hver fjortende dag (og her betyder „cirka“ faktisk ikke at der en gang imellem gik lidt længere imellem vores møder, men tværtimod at vi i perioder havde så meget stof til vores foredrag, at vi afholdt foredrag hver uge). Til disse møder er der normalt mellem 15 og 50 fremmødte.

I Juni måned 1999 blev FLUG så endelig en forening med en demokratisk valgt bestyrelse og formand (før det var jeg diktator ;-)

Da FLUG blev til FLUG

Bag den noget kryptiske overskrift gemmer sig en sønderrivende magtkamp, som var meget tæt på at splitte FLUG til atomer.

Historien udspringer af, at jeg arbejdede på en Emacs pakke kaldet power-macros. Dette gav mig kontakt til Richards Stallman, som jeg efter et stykke tids samarbejde inviterede på besøg i FLUG. Til min overraskelse sagde han ja, men gav dog en betingelse, vi skulle omdøbe FLUG til at hedde „Fyns GNU/Linux User Group“.

Da jeg som en meget lykkelig og stolt mand skrev til FLUG listerne og fortalte at jeg havde fået Richard Stallman overtalt til at komme på besøg hos os, havde jeg aldrig nogensinde forestillet mig at det ville være andet end en form sag at få det lille ubetydelige GNU ind i vores navn.

Sådan skulle det desværre ikke være, og den efterfølgende måned var der en lang og opslidende diskussion på en af vores postlister, om hvorvidt dette navneskifte var „røvslikkeri“ eller „blot at give ham den ære han havde fortjent“.

Diskussionen blev endnu mere trættende, da jeg foreslog at vi stemte om denne ændring per email istedet for ved en generalforsamling (ideen var, at email trods alt var vores primære kommunikationskanal). Det var der nogle der var imod, da dette ikke var i overensstemmelse med vedtægterne.

Resultatet blev, at vi afholdt ekstraordinær generalforsamling, hvor vi vedtog at alle afstemninger kunne foretages per email, og derefter stemte vi per email om vi skulle omdøbe foreningen fra at hedde „FLUG - Fyns Linux User Group“ til „FLUG - Fyns GNU/Linux User Group“.

Den opmærksomme læser vil have opdaget at det ikke var til afstemning om vi skulle ændre forkortelse til FGLUG. Der var bred enighed om, at 1) dette lød meget grimt 2) alle kendte os nu som FLUG, en omdøbning til FGLUG ville betyde at meget PR ville være tabt, 3) at det teknisk ville betyde at vi skulle til at ændre domaine (flug.dk), hvilket ville være besværligt.

Ved denne afstemning blev det et ja, og jeg tror jeg taler for alle når jeg siger at vi var glade for at denne diskussion nu endelig var tilendebragt.

Og så begyndte arbejdet

Da vi nu endelig var blevet enige om at skifte navn, skulle vi igang med forberedelserne, hvilket indebar at vi skulle have lavet en plakat, få den hængt op, taget kontakt til pressen m.m.

Designet af plakaten stod Per Zachø endnu en gang for (som de fire forrige plakater vi har fået lavet). Vores tidligere plakater kan ses på www.flug.dk, og de er virkelig et kik værd!

Til ophængningen måtte vi atter en gang have fat i Tordensskjold soldater. Desværre er FLUG's medlemmer ikke særlige villige til at hænge plakater op (endsige til at lave noget andet aktivt arbejde). Som en sidebemærkning kan det nævnes at vi maksimalt er 10-15 aktive medlemmer i FLUG, men det er vel vilkårene for

foreninger i Danmark.

Plakaten blev ophængt i alle computer forretninger i Odense, på mange af de vidregående uddannelsesinstitutioner, og på mange af gymnasieskolerne. Udover dette blev en række af kollegierne tapetsret.

Gennem DKUUG blev der sendt en pressemeddelelse til alle computerbladene og alle de større dagblade og derudover tog jeg kontakt til lokalpressen i Odense og forsøgte at få dem i tale. Dette resulterede i en notits i den lokale ugeavis om arrangementets komme, samt at foredraget blev optaget af UTV.

UTV er en lokal tv station, der sender indslag med interesse for studerende i Odense. De sender på Tv-Danmarks frekvenser om formiddagen og sent om aftenen.

UTV optog hele foredraget, og så vidt jeg er orienteret vil det blive sendt i sin fulde længe. Ud over dette blev vi enige om at FLUG måtte konvertere deres optagelser til et elektronisk format, og lægge dette på nettet. Om hele foredraget kommer på nettet afhænger af hvorvidt vi kan finde et sted med båndbredde nok, hvor det kan ligge. Desuden har jeg talt med et par stykker andre om muligheden for en service, hvor folk kan få tilsendt foredraget på cd. Vi skal dog have diskuteret hvorledes dette skal foregå i praksis. Afslutningsvis kan jeg da oplyse at foredraget var en kæmpe succes, godt 210 mennesker kom til foredraget, og det var utroligt spændende og inspirerende.

FLUG holder som nævnt møde hver 14. dag. Hold øje med de spændende arrangementer på www.flug.dk, og www.dkuug.dk, hvor du også får at vide, hvordan du kan tilmelde dig til FLUGs mailinglister.

DKUUG-Nyter
medlemsbladet for
DKUUG, foreningen for
Åbne Systemer og
Internet

Udgiver:

DKUUG

Fruebjergvej 3,

2100 København Ø.

Tlf: 39 17 99 44

Fax: 39 20 89 48

email: sek@dkuug.dk

Sekretariatet er åbent:

Mandag-fredag

kl. 9.00-17.00

Direktør:

Bo Folkmann

Redaktion:

Hans Arne Niclasen

(ansvarshavende)

Gitte D'Arcy

Søren Oskar Jensen

Jacob Bække

Peter Holm

Bo Folkmann

Tryk:

Palino Print

Annoncer:

Kontakt DKUUGs

sekretariat

Oplag:

1500 eksemplarer

Artikler m.v. i DKUUG-Nyt
er ikke nødvendigvis i
overensstemmelse med
redaktionens eller
DKUUGs bestyrelses
synspunkter. Eftertryk i
uddrag med
kildeangivelse er tilladt.

Deadline:

Deadline for næste

nummer nr. 122 er

fredag d. 31. marts 2000

Medlem af Dansk

Fagpresse

DKUUG-Nyt

ISSN 1395-1440

Aktivitetskalender

Maj:

2 Internationale SANE-konference

23.-24.: Seminar:
Komponentbaseret systemudviklingSe www.dkuug.dk for nærmere oplysninger**Afholdte arrangementer i 2000****Januar:**

11. Hyggemøde på Niels Bohr Institutet

11. Møde i Klub Odense:
Oracle giver øl17. Klub København:
GnuPG med Werner Koch18. NBD:
Netware 5.1 lancering Århus19. SILD:
E-commerce m. BEA

20. NBD: Netware 5.1 lancering Kbh.

25. Klub København:
FreeBSD m. Klub København25. Klub Århus:
Hyggemøde**Februar:**7. KLID Gå-Hjem-Møde
m. Bjarne Stroustrup

8-11: NordU2000

8.: Klub Odense:
Richard M. Stallman20. Klub Odense:
Linux Installfest

Pers hjørne

Danmark verdens 5. bedste informationsamfund

IDC måler hvert år sammen med World Times et indeks for mere end 50 lande i hele verden. Indekset kaldes for "Information Society Index" og er et mål for, hvor langt de enkelte lande er i udviklingen mod et informationsamfund i bredeste forstand.

Jeg skal spare den tålmodige læser for alle detaljerne omkring de 25 parametre, som anvendes til denne benchmarking – som det vist hedder på godt dansk. Men de fire overordnede grupper er:

- IT infrastruktur (udbredelsen af PCere mv.)
- Internet infrastruktur (udbredelsen af Internettet)
- Informations-infrastruktur (tele, mobiltelefoner mv.)
- Social infrastruktur (uddannelsesniveau mv.)

I den nyeste undersøgelse, der netop er udgivet, ses de nordiske lande helt at dominere toppen af listen. Svenskerne er nu kåret til verdens bedste informationsamfund foran USA (der var nummer 1 sidste år). I Sverige har de vist ikke helt fået armene ned endnu!

Men også Danmark er rykket frem på listen fra at være nummer 6 sidste år til nu at være nummer 5. Finland er nummer 3 og Norge nummer 4, så de nordiske lande sidder solidt på 4 af de 5 øverste pladser på listen.

Hvad er det så, som Danmark kan? Vi har et godt uddannelsessystem (også selv om det siges, at børn ikke lærer grammatik eller at stave, hvilket man blot skal tage et kikk på deres skoleopgaver for at konstatere rigtigheden af). Samtidig har vi en god informationsinfrastruktur. Der er med andre ord en god adgang til og distribution af information i vores samfund.

Men samtidig peger analysen også på nogle svagheder for Danmark som informationsamfund. Det er – heldigvis – nogle af de områder, som jeg har rejst debat om tidligere, og som det stadig er utrolig vigtigt at adressere:

Hjemme-PC ordning: Udbredelsen af hjemme-PCere er gået noget i dvale efter den store bølge de sidste par år. Og det på trods af, at en nylig analyse fra IDC har vist, at der stadig er over 600.000 hjem i Danmark der faktisk godt kunne tænke sig en hjemme-PC via hjemme-PC ordninger der giver skattebegunstigelse eller tilsvarende. Udvalget omkring "Det Digitale Danmark" havde mange gode forslag (ja, det mener jeg faktisk!), men hjemme-PC ordninger glimrede ved deres totale fravær i forslagslisten,



og emnet har ganske enkelte ikke nok bevågenhed.

Internet: På mange måder er Danmark godt med i Internet-kapløbet. Men vi er stadig efter på nogle områder. Blandt andet ville en styrkelse af hjemme-PC ordninger som nævnt ovenfor ikke alene give et IT-løft, men vi ved også, at disse PCere i høj grad bliver anvendt til Internet-adgang. Så man kunne faktisk slå to fluer med ét smæk ved en større udbredelse af PCere, idet man også ville give Internet-anvendelsen et løft.

Samtidig kunne man godt ønske sig lidt mere udvikling på mulighederne for tilslutning til Internettet. I andre lande er man godt igang med debatten om kabel-tilslutning til Internettet og nye teknologier såsom ADSL. Hvor er denne debat i Danmark? Ja, den er druknet i TeleDanmarks usympatiske forsøg på at få alle over på ISDN inden man går videre. Dette er reaktionær tænkning – ikke progressiv tænkning!

Så der er stadig områder, hvor Danmark med en målrettet indsats kunne forbedre vores position som informationsamfund. Og det er i høj grad det, vi skal leve af de næste 20 år!

IDC's indeks for Informationsamfund, 2000

1. Sverige
2. USA
3. Finland
4. Norge
5. Danmark

Kilde: IDC, 2000

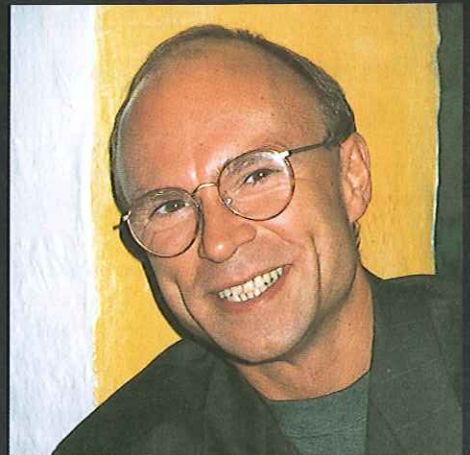
SUPERUSERS



**BESTIL VORT NYE 272-SIDERS
KURSUSKATALOG!**

SuperUsers a/s

Karlebogaard · Karlebovej 91 · DK-3400 Hillerød
Tel.: +45 48 28 07 06 · Fax: +45 48 28 07 05
Giro 458-2764 · E-mail: super@superusers.dk
URL <http://www.superusers.dk>



Brian Eberhardt, Direktør

SuperUsers a/s

SuperUsers a/s, en 100% dansk virksomhed med ca. 35 medarbejdere, har mange års erfaring inden for åbne netværk, operativsystemer og programmeringssprog:

- UNIX, Windows NT/ 98/CE, NetWare
- Internet/Intranet baseret på TCP/IP
- C/C++ /Java/Perl/ActiveX/HTML/CGI
- ORACLE og andre åbne databaser
- System Drift
- System Support
- System Management
- System Integration
- System Udvikling

SuperUsers a/s leverer viden og løsningsmuligheder i form af undervisning og konsulentytelser inden for systemnære områder:

Her ses SuperUsers anno 1999 i rokokostemning på gamle Karlebogaard.



Kurser

Åbne kurser: SuperUsers a/s afholder løbende ca. 115 forskellige kurser inden for internet, åbne netværk, operativsystemer og programmeringssprog.

Specialkurser: Derudover tilbyder vi at afholde kurser tilpasset efter kundens individuelle ønsker. Ved at plukke dele af eksisterende kurser og sammensætte disse, kan næsten ethvert behov opfyldes.

Kursusforløb: Vi hjælper gerne med at vurdere og sammensætte flere kurser, således at der opnås et sammenhængende forløb.

SuperUsers a/s er:

- Sylvan Prometric Testcenter og tilbyder/afholder tests, som fører frem til følgende certificeringer:
Microsoft: MCP, MCSE og MSCD
Novell: CNA, CNE og Master CNE.
- Microsoft Certified Technical Education Center (CTEC)
- Novell Authorized Education Center (NAEC).

Konsulentytelser

SuperUsers a/s har konsulenter indenfor:

- Drift: Support og konfiguration
- Udvikling: Analyse, design, programmering og test

Faste opgaver: Konsulenter til udførelse og styring af drift i større installationer.

Tilkald: Et af specialerne er udrykning med sekunders varsel til hasteopgaver - ofte opgaver, hvor andre har givet op.

Telefontilbud: Endelig tilbyder vi pakkeløsninger inden for "online support".