

DKUUG-Nyt

Nr. 103 — maj 1998

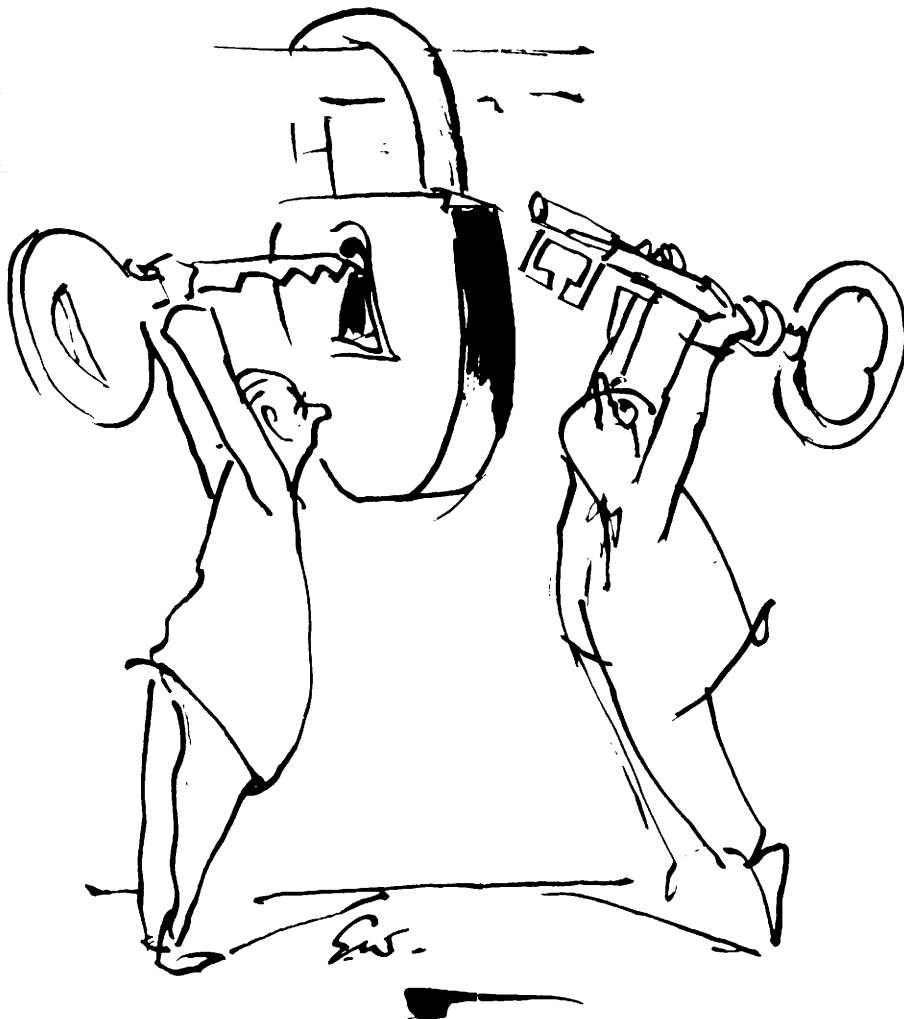
Kryptering

DKUUG-Nyt belyser emnet kryptering fra flere forskellige vinkler:

- Kryptering for dummies
- Implementation af kryptering i FreeBSD
- Hewlett-Packard's VerSecure
- Optakt til kursus med Bruce Schneier

Manden bag forsiden

Hvem er det egentlig der laver DKUUG-Nyts karakteristiske forsider? Vi bringer et portræt af Erik Werner



Indhold

Kryptografi for dummies

Sådan bruges kryptografi

Danmark importerer stærk kryptering fra USA

Historien om en password scrambler...

Lynindlæring med Intellix

Et par gode kursustilbud

Tegner fatter ikke en lyd af det hele

Tiden med rationeringsmærker kan komme tilbage

De ansvarlige vil ikke stille op til høring

Officielt referat

Linux 98

Tag dine forholdsregler

Per's hjørne

Etc.

Aktivitetskalender 1998

Nye medlemmer

Kryptering for fuld udblæsning

4 Når du sidder og læser disse
8 linier, sidder du med nøglen
til en masse viden om kryptering. Uden at DU behøver
10 en nøgle til at afkode denne viden. Vi har leveret denne
12 viden som "en åben bog", og du er mere end velkommen
16 til at lade andre læse indholdet, når du selv engang er
18 færdig.

Det er selvfølgelig med fuld overlæg.

20 Der er imidlertid situationer, hvor du ikke ønsker, at
23 andre end lige én bestemt modtager skal læse det, du
27 sender elektronisk til en anden. Derfor kommer kryptering
29 ind i billedet som en vigtig parameter. Lige som al
31 anden udvikling indenfor IT-verdenen, så går udviklingen
33 indenfor kryptering også meget stærk.

35 I dag tager det kun millisekunder at bryde en 40 bit
38 kryptering. Der skal mindst
39 en 128 bit kryptering til, før end det begynder at ligne noget.
39 Men der er jo lige et "men", hvis man ser det fra

myndighedernes side. I takt med at det bliver sværere at afkode en kryptering, så bliver det også sværere fra myndigheders side at kigge med over skulderen. Derfor er det forbudt i USA at eksportere en kryptering, der er længere end 40 bit lang. Men flere steder rundt om i verden arbejdes der med en nøgle på 1024 bit, som efter sigende skulle kræve 10296 gange så meget computerkraft for at blive afkodet.

En af de amerikanere, som har talt meget imod den amerikanske lovgivning på dette område er ekspertten Bruce Schneier. Det er lykkedes DKUUG i samarbejde med UniForum Association i USA at få Bruce Schneier til Danmark for at afholde et to-dages kursus om kryptering her i maj måned. En unik chance, da Bruce Schneier er meget efterspurgt i sit hjemland og derfor har måtte begrænse sin rejseaktivitet.

René Espersen

BEA Systems Nu 1 år i Danmark!

LOSNINGEKSEMPLER:

En bank ønskede at tilbyde sine kunder Internet-adgang til manitranche-baserede data uden onskrivning af applikationer. Samtidig udviklede man nye applikationer baseret på Web browser-NT, og disse applikationer skulle have adgang til eksisterende proprietære database-data.
Løsningen: BEA TUXEDO, Connect, Jolt.

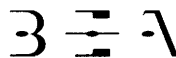
En europæisk offentlig administration havde over hundreder af forskellige UNIX-servere og adskillige manitranche-systemer, som var vanskeligt at integrere, for at give organisationens mere end 20.000 medarbejdere adgang til centrale applikationer og data.
Løsningen: BEA TUXEDO.

En førende bank har valgt et objektorienteret udviklingsværktøj som et middel til at reducere udviklingstiden for nye kundentjenestetekniker. Banken har behov for at sikre sammenhængende kommunikation og arkitektur.
Løsningen: BEA ObjectBroker.

BEA Systems Inc. er anerkendt som verdens førende leverandør af middleware til transaktionskritiske distribuerede applikationer. BEAs globale organisation består af 800 medarbejdere fordelt på 40 adresser i mere end 20 lande. I samarbejde med vore partnere yder vi support og rådgivning til mere end 1.000 kundevirksomheder med det formål at sikre kunderne maksimalt udbytte af deres investeringer i informationsteknologi.

Vi har nu virket i Danmark i 1 år og vores kundeliste omfatter blandt andet SAS Data, DSB Data, Post Danmark, Mærsk Data, Sonofon, Alta Copenhagen og DEFU Data.

Tak for opbakningen og interessen!



THE ENTERPRISE MIDDLEWARE SOLUTION



BEA Systems Danmark
Emdrupvej 28 C
2100 København Ø
Telefon 39270208
e-mail: info@beasys.dk



www.beasys.dk/www.beasys.com

Kryptografi for dummes

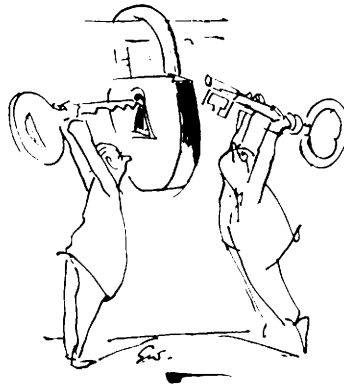
Af Flemming Jacobsen

Kryptografiske algoritmer findes i to hovedvarianter: symmetriske og asymmetriske, også kaldet private-key og public-key algoritmer.

Symmetriske algoritmer er de bedst kendte. Her benytter afsender og modtager den samme nøgle til at kode og afkode med. Den nok bedst kendte symmetriske algoritme er DES.

Asymmetriske algoritmer har to nøgler. Disse kaldes oftest den private og den offentlige nøgle. Hvad der er kodet med den privat nøgle, kan kun afkodes med den offentlige nøgle og omvendt. Den bedst kendte asymmetriske algoritme er RSA.

Den største forskel på symmetriske og asymmetriske algoritmer er den hastighed, hvormed de kan kode og afkode meddelelser og de muligheder, de giver udover kryptering.



Symmetriske algoritmer er langt de hurtigste (software implementeringer af DES er 100 gange hurtigere end RSA), tilgængæld giver de kun mulighed for, at afsender og modtager kan kommunikere uden, at andre kan læse indholdet af meddelelserne, samt at modtageren er sikker på, at meddelelsen er

afsendt af den, nøglen er aftalt med. Netop distribution af nøgler er et stort problem med symmetriske algoritmer. Hvis 10 personer skal kommunikere sikkert, så kræver det, at der på en sikker måde bliver aftalt 45 nøgler.

Asymmetriske algoritmer giver, ud over de samme muligheder som symmetriske algoritmer, mulighed for digitale signaturer og mulighed for væsentligt enklere nøgle distribution.

To parter, der ikke har haft mulighed for at udveksle nøgler i hemmelighed, kan kommunikere fortroligt. De to parter sender blot hinanden deres offentlige nøgle. Eftersom de offentlige nøgler er beregnet på at have bred distribution gør det ikke noget, at udvekslingen bliver aflyttet. Kun hvis andre har mulighed for at ændre de nøgler, der udveksles, er det muligt at kompromittere sik-

kerheden.

Brug af en asymmetrisk algoritme er meget lig brugen af en symmetrisk algoritme. Afsenderen (kaldet A) koder meddelelsen med modtagerens (kaldet M) offentlige nøgle. M afkoder meddelelsen med sin private nøgle (M afkoder altid med sin private nøgle, uanset hvem der modtages meddelelser fra).

I modsætning til når en symmetrisk algoritme benyttes, så har M ingen garanti for, at det nu også var A, der afsendte meddelelsen (i princippet har alle adgang til M's offentlige nøgle). Dette problem løses ved, at A laver en digital signatur på meddelelsen inden afsendelsen.

Digitale signaturer laves som regel ved, at der beregnes en checksum for den meddelelse, der skal signeres. Afsenderen koder checksummen med sin hemmelige nøgle. Modtageren verificerer, at checksummen kan afkodes med A's offentlige nøgle, og at den er den samme som

checksummen for den meddelelse, der blev modtaget. Er dette tilfældet, så ved M at checksummen er blevet kodet med A's hemmelige nøgle (der kun kendes af A), hvorfor det kun er A, der har kunnet signere meddelelsen.

Problemet med den meget langsomme kodning/afkodning, når asymmetriske algoritmer benyttes, løses som regel ved at kode meddelelsen med en symmetrisk algoritme og en (for hver meddelelse) tilfældigt valgt nøgle. Denne nøgle kodes så med den asymmetriske algoritme, og resultatet sendes med som en del af meddelelsen. På denne måde opnås hastighed svarende til en symmetrisk algoritme samtidigt med, at alle fordelene ved de asymmetriske algoritmer bevares.

Sikkerheden holder naturligvis kun, hvis algoritmen ikke er blevet brudt, og hvis nøglen ikke er blevet gættet. Hvordan sikrer man sig rimeligt mode dette?

For det første skal man sikre sig at der er brugt en

stærk/sikker algoritme. Dette er vanskeligere end man umiddelbart skulle tro. For den ikke professionelle ligner output fra en sikker algoritme til forveksling output fra en svag algoritme. Begge dele er en mængde tilfældigt/meningsløst udseende data. For den professionelle er der derimod stor forskel - også selvom det ikke vides, hvilken algoritme der er brugt. I den svage algoritme findes der utilsigtede genveje, der gør, at man ikke behøver at gætte nøglen for at afkode meddelelsen, eller også kan nøglen let bestemmes ud fra den kodede meddelelse. Den sikre algoritme er opbygget således, at den eneste mulighed, der er for at bryde krypteringen, er at gætte nøglen. Der er en glimrende diskussion af de forskellige algoritmer og deres styrker og svagheder i [1]. Programmer, der ikke benytter en algoritme, der gives god kritik i [1], bør ikke benyttes seriøst - specielt ikke hvis sælgeren nægter at oplyse om hvilken algoritme, der er be-

nyttet (se [2]).

Man kan kun undgå, at nøglen bliver gættet (dvs. fundet ved systematisk at prøve alle muligheder) ved at gøre antallet af mulige nøgler tilstrækkeligt stort. Det store spørgsmål er: Hvad er "tilstrækkeligt stort"? Dette afhænger af, hvad man ønsker beskyttet, og hvor længe man ønsker det beskyttet. Hvis vi antager, at meddelelsen ønskes beskyttet i min. 20 år, og at andre vil have stor økonomisk eller politisk gevinst af at afkode meddelelsen, kan vi se på hvor lang en nøgle minimum skal være. [1] diskuterer dette, og når frem til at for symmetriske algoritmer er 40 bit nærmest latterligt lidt mens 112-128 bit er rimeligt. For asymmetriske algoritmer er 1024 bit i underkanten, 2047 bit er et mere realistisk bud.

Konkurrencer på nettet har vist, at en lille gruppe kan gætte en 40 bit nøgle på en uges tid ved at benytte den overskydende CPU kraft i de computere, gruppen har adgang til. Mere dedikerede forsøg har fundet 40 bit nøg-

ler på nogle timer, blot ved at benytte et par hundrede workstations.

Forordet til [1] starter med: "There are two kinds of cryptography in this world: cryptography that will stop your kid sister from reading your files, and cryptography that will stop a major government from reading your files". 40 bit nøgler hører til den første type...

Desværre er det svært at finde kommercielle programmer, hvor nøglen i den symmetriske algoritme er tilstrækkelig lang. Dette skyldes, at USA stadig sidestiller eksport af kryptografisk software med eksport af våben. Det er så godt som umuligt at få en generel eksporttilladelse, hvis den effektive længde af nøglerne er over 40 bit.

Alle de kryptografiprogrammer og postsystemer med indbygget kryptering, der er udviklet i USA, og som kan købes af almindelige mennesker i resten af verden, benytter derfor 40 bit nøgler.

Det bedste kryptografi

program, der er alment benyttet, og som understøtter en fornuftig nøgle længde er PGP. PGP er free-ware og findes til stort set alle operativsystemer. PGP kan f.eks. hentes hos [3]. Mange programmer til elektronisk post har indbygget understøttelse af PGP, således at kodning, afkodning og digitale signaturer ikke kræver noget ekstra af brugeren.

Et andet problem i kommercielle programmer er, at den benyttede algoritme ikke er sikker. Mange tekstbehandlere og regneark kommer med en indbygget mulighed for at kryptere et dokument. Desværre gælder det for langt størsteparten af disse, at man kan finde andre programmer (enten free-ware eller kommercielle), der kan finde nøglen til dokumentet på et par timer. Brugeren er således værre stillet end hvis der ikke var benyttet kryptering, idet brugeren nu tror, at dokumentet er sikret, mens virkeligheden er, at alle, der har lyst, kan læse indholdet.

Netscapes browser er i

eksportversionen også begrænset til at benytte 40 bit nøgler. Hos [4] kan man dog hente et patch, der får den til at benytte 128 bit nøgler. Dette er endnu et eksempel på, hvor absurd USAs eksportlovgivning på kryptografi området er.

Selvom der benyttes en stærk algoritme med en tilstrækkelig lang nøgle er sikkerheden ikke nødvendigvis i orden.

Hvis nogen formår at stjæle en kopi af en hemmelig nøgle, så er vedkommen de i stand til at lytte med. Dette er især et problem, hvis tyveriet er foregået ubemærket. Skulle tyveriet være blevet bemærket, så vil et nøgleskift ikke forhindre tyven i at afkode tidligere meddelelser.

Selvom et dokument er sikkert krypteret, så kan det stadig slettes. Derfor er almindelige sikkerhedsprocedurer lige så vigtige som før.

Betroede personer kan stadig læse fortrolige dokumenter. Bestikkelse og afpresning er stadig en nem måde at få kopier af doku-

menter og nøgler.

Sløset omgang med dokumenter, og almindelig glemsomhed kan stadig føre til at udenforstående får adgang til hemmeligheder. Dette er især muligt, hvis ikke alle kender/anerkender firmaets politik om brug af kryptografi.

Selvom indholdet af en meddelelse er krypteret, så er det sommetider muligt for andre at bruge det, at der / er/ blevet sendt en meddelelse. F.eks. kunne krypterede meddelelser mellem to, der mistænkes for at have et forhold antyde, at der er hold i mistanken.

Hvis nogen ønsker at læse yderligere om teorier og principper bag den moderne anvendelse af kryptografi, kan [1] kun anbefales. Den fungerer både som en interessant introduktion til emnet samt som den for øjeblikket mest definitive reference på området. Bogen er både underholdende og (i betragtning af emnet) meget let læst. Indholdet i bogen kan opdeles i: Introduktion til kryptografi, krypto-

grafiske protokoller og hvad de kan bruges til, kryptografiske teknikker og metoder, diskussion og beskrivelse af forskellige algoritmer, brug af kryptografi i den virkelige verden.

Noter

- [1] Schneier, Bruce; Applied Cryptography, Second Edition; John Wiley & Sons. 1996; ISBN: 0-471-11709-9.
- [2] Curtin, Matt; Snake Oil Warning Signs: Encryption Software to Avoid; <http://www.interhack.net/people/cmcurtin/snake-oil-faq.html>
- [3] The International PGP Home Page
<http://www.pgpi.com/>
- [4] Farrell McKay, Wayfarer Systems Pty. Ltd. (Aust.)
<http://www.fortify.net/>



Sådan bruges kryptografi

Bruce Schneier står i spidsen for fortroppen, når det gælder cyber-sikkerhed. DKUUG har fået ham til København, hvor han vil holde et to-dages kursus om kryptering.

Kurset med titlen "Introduction and Advanced Cryptography" afholdes i Symbion den 25.-26. maj. Det henviser sig til dem, der vil forstå kryptografi: hvad det gør og hvordan det virker. Bruce Schneier vil fokusere på teknologien bag kryptering, hvorfor der ikke forudsættes nogen stærk baggrund i matematik hos deltagerne for at få et stort udbytte af kurset.

Fra omsætning af kode til digital signatur til elektronisk handle til sikker afstemning - kryptering er blevet den teknologi, der sætter os i stand til at tage de eksisterende forretninger og sociale interaktioner og flytte disse til computer netværket. Men meget af krypteringen er dårlig og problemet med dårlig kryptering er, at det ligner en god kryptering. De fleste kan

da heller ikke se forskel.

Sikkerheden er som en kæde - den er ikke stærkere end det svageste led.

Kurset vil omhandle kryptering som det bruges i hverdagen: algoritmerne, protokollerne og implementationerne. Bruce Schneier vil på kurset understrege "hvad" og "hvordan" mere end "hvorfor". Folk der opbygger - eller bruger - kryptering har ifølge Bruce Schneier brug for at forstå, hvad kryptering kan gøre og ikke kan gøre - kryptering er nemlig ikke altid det universalmiddel, som det oftest præsenteres som.

Følgende emner vil blive behandlet:

- Fundamentalt kryptografi
- Symmetrisk kryptografi: DES, triple-DES, IDEA, Blowfish, RC2, RC4, RC5 og AES

- Public-key kryptografi: Omsætning af kode og digital signaturer, RSA, Diffie-Hellman, ElGamal og DSA
- Hash funktioner og meddelsens ægtheds-koder: MD4, MD5, SHA, CBC-MAC, HMAC og NMAC
- Random Number Generation
- Protokoller: nøgle udveksling, ægthed, hemmelig deling, nøgle deponering, certifikater, digitale konstanter
- Hvad kryptografi kan gøre for dig
- Hvad kryptografi ikke kan gøre for dig
- Kryptografi i en verden af netværk
- Redskaber til Internet kryptografi
- Threat Modelling
- E-Mail sikkerhed: PGP, S/MIME

- Trust Management:
X.509, SDSI, SPKI
- IP Sikkerhed
- World Wide Web sikkerhed
- Elektronisk Handel::
Cybercash, Digidash,
First Virtual, SET

Bruce Schneier understreger, at han som "enlig" instruktør ikke kan lære deltagerne at blive kryptografer. Men efter at have gennemgået dette kursus, så vil deltagerne blive intelligente forbrugere af kryptografi, der vil forstå kryptografiens byggestene, hvordan disse byggestene sættes sammen for at danne et kryptografisk system, og endelig hvilke begrænsninger denne teknik har.

Lidt om

Bruce Schneier

Bruce Schneier er direktør for Counterpane Systems - et konsulentfirma med speciale i kryptografi- og computersikkerhed. Bruce Schneier er forfatter til en række bøger, hvor den bedst kendte nok er "Applied

Cryptography" (John Wiley & Sons, 1994 & 1996). Den anden udgave af denne bog er allerede blevet solgt i over 80.000 eksemplarer verden over. Den er oversat til fire forskellige sprog. Han har desuden skrevet dusinvis af artikler om kryptografi til de alle de store magasiner om IT-teknologi.

Bruce Schneier har desuden designet den populære "Blowfish encryption algorithm", som nu efter fire år stadig ikke er blevet brudt.

Praktiske oplysninger

Kurset afholdes som nævnt den 25.-26. maj i Symbion, Fruebjergvej 3, 2100 København Ø. Prisen er kr. 6.000 for medlemmer af DKUUG, mens ikke-medlemmer må betale kr. 8.500. Priserne er ekskl. moms.

Tilmelding skal ske til DKUUG's sekretariat, tlf. 39 17 99 44, fax 39 20 89 48 eller e-mail sek@dkuug.dk senest den 20 maj 1998.



Den Virkelige Verden

En tekniker hos Dell gav en kunde det råd at han skulle putte hans disketter tilbage ind i drevet og lukke døren. Kunden bad teknikeren at "blive i røret", hvorefter teknikeren kunne høre kunden lægge røret, rejse sig op og gå til den anden ende af værelset for at lukket døren til værelset.

En anden Dell-kunde ringede for at sige, at han ikke kunne få sin computer til at faxe noget som helt. Efter 40 minutter med fejl-finding uden held, opdagede teknikeren, at kunden forsøgte at faxe et stykke papir ved at holde det foran skærmen og trykke på "send"-tasten.

Danmark importerer stærk kryptering fra USA

Hewlett-Packard har fra den amerikanske regering opnået tilladelse til, at Danmark for første gang må importere produkter til stærk kryptering (128-bit) fra USA. Danmark er blandt de 5 første lande i verden, der opnår denne tilladelse.

HP's nye teknologi til kryptering, VerSecureTM, giver danske virksomheder og forbrugere nye unikke muligheder for at udveksle data sikkert på Internettet. Eksempelvis kan danske borgere nu kommunikere sikkert med det offentlige og sende personlige data over Internettet uden at bekymre sig om, at informationerne kan blive aflyttet eller opsnappet undervejs.

Den manglende sikkerhed på Internettet er hidtil blevet opfattet som den største barriere for en udbredt, kommerciel anvendelse af Internettet. Men HP's VerSecure teknologi giver mulighed for uhyre sikker kommuni-

kation og kan f.eks. anvendes til sikker elektronisk dataoverførsel, overenskomst- og politiske forhandlinger via Internettet, militære oplysninger, finansielle transaktioner, udveksling af sensitive sociale oplysninger, EDI, digitale signature, medicinske- og lovmæssige informationer samt afsendelse af private beskeder via e-mail.

- Tilladelsen til at importere VerSecure teknologien betyder, at den elektroniske verdens muligheder nu kan udnyttes fuldt ud også i Danmark, siger administrerende direktør, Jørgen Bardenfleth, Hewlett-Packard Danmark.

HP's VerSecure krypteringsteknologi har allerede fået tilslutning fra HP's internationale forretningspartnere inklusive IBM, Microsoft, Motorola, SAP, CertCo, RSA og Trusted Information Systems.

Danmark på forkant med Internetsikkerhed

Danske virksomheders muligheder for at kommunikere sikkert på Internettet har i lang tid været begrænset af amerikanernes forbud mod at eksportere produkter, der inkluderer stærk kryptering. Det er ændret med godkendelsen af HP's VerSecure.

Danmark er sammen med Tyskland, Frankrig, England og Australien de første lande, der har fået mulighed for at importere VerSecure baserede produkter.

- HP's danske kunder har længe udtrykt et stort behov for stærk kryptering så de bedre kunne udnytte mulighederne i E-business. Efter vi for første gang blev opmærksomme på VerSecure, har vi i HP Danmark presset hårdt på for at få VerSecure til Danmark hurtigst muligt. Da Danmark samtidigt betragtes som et IT-foregangsland, kom vi med i første bølge, siger Internet programchef Henrik Hvid Jensen, Hewlett-Packard Danmark.

- Det er glædeligt, at de amerikanske myndigheder nu har erkendt, at man også udenfor USA har brug for stærk kryptering i forbindelse med brug af amerikanske IT-produkter i overensstemmelse med en national politik og ikke kun en amerikansk. Det er en fjer i hatten til både Hewlett-Packard og Danmark, at vi



Internet programchef Henrik Hvid Jensen, Hewlett-Packard Danmark.

er med blandt de allerførste lande, som får adgang til dette, siger professor Peter Landrock, Ph.D. og administrerende direktør i Cryptomathic.

VerSecure er designet til at give den fleksibilitet, som adresserer disse bekymringer, idet teknologien tilbyder en arkitektur, som kan tilpasses ændringer i en nations krypteringspolitik. Hvis man i Danmark på et tidspunkt vælger at indføre restriktioner omkring brug af kryptering, kan disse ændringer aktiveres ved blot

at kopiere ny software ud til VerSecure komponenterne via Internettet. Tidligere måtte man foretage en omfattende re-programmering af software samt distribuere denne eller ligefrem udskifte hardware.

Detaljeret information om HP's VerSecure teknologi findes på HP's specielle VerSecure hjemmeside på adressen: www.hp.com/go/versecure



Historien om en password scrambler...

Af Poul-Henning Kamp
<phk@FreeBSD.org>,
The FreeBSD Core team.

Poul-Henning har hærget den danske UNIX branche i mere end elleve år. Han arbejder som freelance konsulent med eget firma og har slet ikke tid nok til FreeBSD nu om dage.

Egentlig skylder jeg læserne en fortsættelse af "FreeBSD, The Inside Story X/N" men jeg kan faktisk ikke huske, hvad nummer vi er kommet til...

Denne klumme er foranlediget af temaet for dette nummer: Kryptering.

Gode dyr var rådne

For nogle år siden, i 1994 faktisk, stod FreeBSD projektet med et problem: Vi kunne ikke distribuere den "sædvanlige" DES baserede password scrambler fordi sourcen naturligvis ville indeholde en fuld DES implementering, og sådan noget

må man jo ikke eksportere fra USA. "Almindelige" UNIX leverandører havde det nemmere, de distribuerede ikke sourcen og derfor kunne de få en ITAR licens idet man ikke kunne få fingre i den indlejrede DES rutine.

Gode dyr var rådne, som man siger, vi havde en rudimentær scramble routine, men den var klappet sammen i hast, for i det mindste at undgå at skrive password i klartekst i /etc/passwd, men den var utroligt dårlig, og havde hvis jeg husker ret det meste af en invers algoritme.

Vi havde ganske vist en fuldt funktionsdygtig og kompatibel implementering liggende klar til download fra Sydafrika, men det ville jo ikke hjælpe dem, der ikke havde InterNet adgang, og slet ikke dem der købte en CDROM.

Nød lærer nøgen...

Således frustreret satte jeg mig ned og begyndte at rode med det, og resultatet forelå

den 7. november 1994: En ny password scrambler baseret på MD5.

Forud for det var der gået mange timer. Jeg kunne selvfølgelig have klappet noget kode sammen efter "The International Obfuscated C Code Contest" princippet, men det ville ikke rigtig hjælpe os. Sikkerhed er ikke noget man fuser sig til, det kræver omhu. Jeg var, og er, udemærket klar over, at jeg ikke har hverken baggrunden eller erfaringen til at bide skeer med de professionelle på dette område, men der var jo heller ikke grund til at opfinde det dybe vand og den varme tallerken en gang mere.

Algoritmer

I stedet besluttede jeg mig for at basere koden på en allerede eksisterende algoritme, MD5. MD5 er ikke en krypterings algoritme som DES, det er en "hash" algoritme, det vil sige, at man føder et antal bytes ind i MD5 og får

en "signatur" ud. Der er ingen kendt metode til at komme fra signaturen til input andet end at prøve sig frem fra ende til anden.

Det er omtrent perfekt til password beskyttelse. Man gemmer signaturen, hvis det password som brugeren taster ind giver samme signatur, som den man har gemt, kendte hun det rigtige password.

Dette var også principet i den traditionelle DES baserede passwordsrambler, men der brugte man en DES som hash algoritme ved bl.a. at køre de samme data igennem mange gange. For at gøre det lidt sværere har man tilføjet et "salt" på 12 bit, som modificerer nogle parametre i algoritmen, det øger med en faktor 4096, den tid et brute-force angreb vil tage.

Desværre er de 12 + 56 bits ikke ret meget med moderne cpu-kraft. (<http://www.distributed.net>) og hvad der er endnu værre, det er så lille et udfaldsrum, at man kan forudberegne en ordbog.

FreeBSD

Tag f.eks. et moderne DLT bånd. Der kan ligge 20 GB ukomprimeret på det, det modsvarer 2^{30} password+salt=hash kombinationer, og man kan læse og sammenligne ca. 190 tusinde per sekund. Begge tal bliver noget større, hvis man anvender data komprimering.

Til sammenligning er der kun 2^{26} forskellige nummerplader mulige med det normale "\$\$ ## ###" format.

Det var ved at blive et seriøst problem i 1994 at crackere, hvis de fik adgang til de scramblede passwords, ville downloade dem og forsøge sådanne brute-force eller dictionary angreb. Cliff Stoll beretter f.eks. om et sådant angreb i "The Cuckoos egg".

Valget af MD5 var baseret på mange faktorer, heriblandt copyright, ITAR/eksport lovgivning osv., men der var nogle fundamentale egenskaber som skulle være opfyldt også: Udfaldsrummet skulle være af en væsentlig størrelse og det skul-

le være svært eller umuligt at optimere algoritmen både i HW og SW. Alle disse ting pegede på MD5, se f.eks. RFC1810 vedr. hastigheden.

Antallet af "salt" bits blev øget til 48 og selve det scrambled hash fra MD5 er på 128 bits. På den måde blev udfaldsrummet 2^{108} gange større end for den traditionelle DES metode. Selve rutinen jeg skrev, blev også skrevet på en sådan måde, at man ikke kunne forkorte, parallelisere eller optimere den. Den tog dengang 34msec på en P5/60 maskine, hvilket var et par størrelsesordener mere end den DES baserede kode tog.

Det er altid en tvivlsom affære at iterere en krypto algoritme, idet man nemt kan komme til at forstørre eventuelle svagheder i den grundlæggende algoritme, men jeg vurderede, at det var værd at tage chancen for forlænge den tid, det tager at gennemføre algoritmen.

For det første bedømte jeg det som meget tvivlsomt om nogen ville bruge den fornødne tid og energi på at finde

"THE BEER-WARE LICENSE" (Revision 42):

<phk@FreeBSD.org> wrote this file.

As long as you retain this notice you can do whatever you want with this stuff. If we meet some day, and you think this stuff is worth it, you can buy me a beer in return.

Poul-Henning Kamp

en sådan systematisk svaghed, men sekundært, når/hvis vi får nys om noget sådant, så kan vi jo bare lave en ny algoritme, det såkaldte "Krypto-Kleenex" princip.

Passwords bør jo principielt ikke leve lang tid (Hvornår skiftede DU dit password sidst ???), så der er ikke nogen stor katastrofe i at introducere en ny algoritme hvert andet eller tredje år, sålænge den nye kode kan genkende de gamle passwords også.

Den sidste hurdle der var at passere, var at repræsentere de 176 bits som ascii, så de kunne gemmes i /etc/{passwd|shadow} filerne. Der valgte jeg at anvende samme base-64 encodning som den traditionelle DES algoritme, men satte "\$1\$" foran til at markere at det var en anden algoritme og et "\$" mellem

salt og hash. Dette betyder, at man også nemt kan introducere nye algoritmer i fremtiden.

Resultatet

Et færdighash'et password kan dermed f.eks. se således ud:

\$1\$IREjh4B5\$VhEYXAJGSG/VMx8eTlZTZ.

Det var noget længere end traditionelle DES passwords, men forbavsende nok er det kun ganske få programmer, der havde problemer med dette, og de fleste af dem kunne fixes ved at gøre nogle char arrays lidt længere.

Koden kan findes på <http://www.freebsd.org/cgi/cvsweb.cgi/src/lib/libcrypt/crypt.c>

og er beskyttet af min "beerware" licens

Dermed var historien egentlig forbi for FreeBSDs vedkommende. Siden FreeBSD 2.0 har vi brugt denne algoritme som default, hvis ikke folk valgte at installere den separate "DES" distribution fra Sydafrika.

Jeg har naturligvis holdt antennerne ude for at høre om min kode holdt vand, og forskellige kontakter ude omkring har forwardet mig godbidder. Der er selvfølgelig blevet knækket passwords med bruteforce og dictionary attacks. Hvis folks password er tåbelige, kan ingen hash-algoritme beskytte dem. Men jeg har ikke hørt om nogen angreb baseret på forudberegne dictionary filer. Det er et stort fremskridt, fordi de betyder, at angriberen hver gang skal starte forfra med at tygge sin ordliste igen, det forsinker tingene en hel del.

Jeg har også modtaget nogle snippets fra IRC sessioner, hvor nogle elendige småkriminelle eksistenser siger ting som "Don't waste your time on FreeBSD sy-

stems takes too bloody much time :-(" Vi takker for de gode anmeldelser :-)

Så en dejlig dag i starten af 1997 opdagede jeg i en cisco-konfiguration pludselig en linie, der sagde:

```
enable secret 5
$1$ay44$Gsx7oyYljJcPBZ
JqFHA0
```

JasåJaveljaMONikke...

En diskret email af sted til en FreeBSD gut der sidder med fingrene dybt nede i Ciscos kildetekst: "kan du ikke lige checke... ?" svaret var: "Jo, jo, den er god nok!"

Jeg er blevet lovet, at jeg vil få en bajer af cisco hvis jeg stikker hovedet forbi en dag...



Den Virkelige Verden

En forbitret kunde ringede til Dell Computers tekniske support, fordi hun ikke kunne få tændt hendes nye Dell computer. Efter at have forsikret sig, at computeren rent faktisk var tilsluttet til kontakten, spurgte teknikeren hvad der skete, når hun trykkede på "power"-knappen. Hendes svar var: "Jeg trykker og trykker på fodpedalen, men ingenting sker". Fodpedalen viste sig at være musen til computeren.

Compag overvejer at ændre kommandoen "Press any Key" til "Press Return Key" på grund af det stigende antal telefonopkald, hvor folk spørger, hvor "any"-tasten er.

Lynindlæring med Intellix

Alle sejl var sat til, da Intellix A/S præsenterede deres videnbaserede program, KnowMan ved et gå-hjem-møde i marts måned.

Af René Espersen

I over tre timer guidede direktør Christian Liisberg og stort opbud af ansatte fra Intellix de 18 deltagere, som alle havde taget deres bærbare PC'ere med. Så kunne de hele tiden selv "lege" med de mange facetter i KnowMan-programmet.

Allerede inden deltagerne mødte op, havde DKUUG-sekretariatet travlt med at finde forlængerledninger nok til at kunne levere strøm til de mange PC'ere. Selvom Sym-bion er et stort sted, så måtte hjælpen hentes mange steder fra, men til sidst lykkedes det, og det blev en aften udover det sædvanlige.

Deltagerne i gå-hjem-mødet lærte at bygge deres eget ekspertsystem i programmet, der kombinerer neurale netværk og avancerede statisti-



Christian Liisberg fra Intellix havde deltagerne i DKUUGs gå-hjem-møde i sin hule hånd.

ske metoder. Programmet "kortlægger" den menneskelige viden dvs. der puttes data ind, og via simple svar-funktioner bliver ens eget ekspertsystem bedre og bedre, jo

flere data der lægges ind. Når et ekspert-system er opbygget, så kan brugeren hurtig finde frem til de rigtige svar. Hvad der - ifølge Christian Liisberg - normalt tager et



Der blev arbejdet intenst under DKUUGs gå-hjem-møde med Intellix, og som det ses, så var der næsten en hjælpende konsulent til hver deltager.

menneske 2 1/2 år at lære kan nu læres på seks uger. Dermed er indlæringstiden faldet - der er tale om en lynindlæring.

Deltagerne på gå-hjem-mødet prøvede at kortlægge deres eget følelsesliv med programmet dvs. give pro-

grammet svar på, om de vil have det pragtfuldt eller rædselsfuldt i forskellige situationer. Det kom der mange sjove og fantasifulde løsningsmodeller ud af.

De mange konsulenter fra Intellix var hurtige på pletten til at hjælpe delta-

gerne i enhver henseende, når det gjaldt at udnytte finesserne i programmet. Det var lærerigt for både deltagerne og for Intellix-konsulenter, så alle parter havde et stort udbytte af aftenen.



Et par gode kursustilbud

DKUUG har fået et par stærke personligheder til at gæste Danmark her i maj måned for at dele ud af deres viden.

Som nævnt i sidste nummer af DKUUG-Nyt, så kommer Nordens førende CORBA-ekspert, Pekka Kähkipuro fra Finland den 19. maj for at afholde et én-dags kursus om CORBA programmering. Ugen efter handler det om kryptering, når specialisten i kryptografi, Bruce Schneier fra USA afholder et to-dages intensivt kursus med titlen "Introduction and Advanced Cryptography". Det sker den 25.-26. maj. Begge kurser afholdes på Symbion i København.

Sidstnævnte kursus henvender sig til dem, der vil forstå kryptografi: hvad det går ud på, og hvordan det virker. Bruce Schneier vil koncentrere kurset om teknikken bag kryptografering, men der forudsættes ikke nogen stærk baggrund i matematik for at få et stort udbytte af

kurset. Faktisk kan både begyndere og erfarne få et stort udbytte af dette kursus.

Fra omsætning af kode til digital signatur over elektronisk handel til sikker afstemning - kryptering er blevet den teknologi, der sætter os i stand til at tage de eksisterende forretninger og sociale konstruktioner og flytte disse til det globale netværk. Men meget af krypteringen er dårlig, og problemet med dårlig kryptering er, at det ligner en god kryptering. De fleste kan da heller ikke se forskel. Sikkerheden er som en kæde - den er ikke stærkere end det svageste led.

Kurset vil omhandle kryptering, som det bruges i virkelighedens verden: algoritmerne, protokollerne og implementationerne. Bruce Schneier vil på kurset understrege "hvad" og "hvordan"

mere end "hvorfor". Folk der opbygger - eller bruger - kryptering har ifølge Bruce Schneier brug for at forstå, hvad kryptering kan gøre og ikke kan gøre - kryptering er nemlig ikke altid det universalmiddel, som det oftest præsenteres som.

Bruce Schneier understreger, at en enkelt instruktør ikke kan lære nogle at blive en kryptograf. Men efter at have gennemgået dette kursus, så vil deltagerne blive intelligente forbrugere af kryptografi, som vil forstå kryptografiens byggestene; hvordan disse byggestene sættes sammen for at danne et kryptografisk system, og endelig hvilke begrænsninger denne teknik har.

Lidt om Bruce Schneier

Bruce Schneier er direktør for Counterpane Systems - et

konsulentfirma med speciale i kryptografi- og computersikkerhed. Bruce Schneier er forfatter til en række bøger, hvor den bedst kendte nok er "Applied Cryptography". Allerede er den anden udgave af denne bog blevet solgt i over 80.000 eksemplarer over hele verden. Den er oversat til fire forskellige sprog. Han har desuden skrevet dusinvis af artikler om kryptografi til de alle de store magasiner om IT-teknologi.

Bruce Schneier har desuden designet den populære Blowfish encryption algorithm, som nu efter fire år stadig ikke er blevet brudt.

Pris og tilmelding

Prisen for medlemmer af DKUUG er 6.000 kr. ekskl. moms. For ikke-medlemmer er prisen 8.500 ekskl. moms. Yderligere oplysninger og tilmelding skal ske til DKUUG's sekretariat, tlf. 39 17 99 44, fax 39 20 89 48 eller email: sek@dkuug.dk.

CORBA 2

I samarbejde med BEA Sy-

stems Danmark og Tieturi Oy fra Finland tilbydes DKUUG's medlemmer et én-dags kursus med Nordens førende CORBA-ekspert, Pekka Kähkipuro fra Finland, som vil give en introduktion til CORBA 2 programmering.

Kurset afholdes tirsdag den 19. maj i Symbion i København.

Efter endt kursus vil deltagerne have en god, grundlæggende viden om, hvorledes man anvender en objektbroker fra C og C++. Herudover får man en god forståelse for CORBA-arkitekturen og de funktioner, som de forskellige dele af arkitekturen tilbyder.

Målgruppen for dette kursus er systemudviklere og projektledere med forståelse for objektorienterede teknikker og programmering i C og C++. Kurset afholdes på engelsk.

Pris og tilmelding

Prisen er 2.500 kr. for medlemmer af DKUUG - mens prisen er 3.500 kr. for alle ikke-medlemmer. Tilmelding og yderligere oplysninger kan fås hos DKUUGs sekretariat på tlf. 39 17 99 44, fax 39 20 89 48 eller email: sek@dkuug.dk



Tegner fatter ikke en lyd af det hele

Igennem en lang årrække har en flot tegning prydet forsiden af DKUUG-Nyt. Tegneren bag hedder Erik Werner, men hvem er manden bag navnet?

Af René Espersen

Han har ingen teknisk sans overhovedet; er formentlig den dansker, der går oftest i teatret, og når han skal lave noget for DKUUG, så må han have "førerhund" med! For han fatter ikke en lyd af det hele.

Det lyder umiddelbart ikke som den perfekte medarbejder i DKUUG, men faktisk er han én af nøglepersonerne. For hvem ville undvære de oftest meget humoristiske tegninger, som har præget forsiderne af nærværende blad igennem en længere årrække.

Navnet er Erik Werner, og han er - som man nu nok har regnet ud - bladtegner. Egentlig vil han helst have, at titlen er "Teatertegner", for det er faktisk i det virke, som han bruger langt det meste af sin tid. Faktisk gik Erik

Werner på pension lige før jul, men det stopper ham ikke fra at sætte streger på et stykke papir - til stor glæde for læsere af både Berlingske Tidende og DKUUG-Nyt.

Hvordan og hvorledes det lige blev Erik Werner, der skulle leverer alskens sjove tegninger til en forening, hvis emneområder han ikke fatter en meter af, kan han faktisk ikke huske.

- Der var nogle, der sagde, at det vil være en fordel, at jeg ikke ved noget om det. Jeg er således nødt til at have en "førerhund" med hver gang. Men det har været meget hyggeligt, understreger Erik Werner.

Førerhunden er bladets redaktør, der med nogle ganske få ord beskriver for Erik Werner, hvad bladets tema er - og få dage efter dumper så tegningen ind af døren.

Blæksprutten

Hans karriere startede som 20-årig, hvor den daværende redaktør af "Blæksprutten" så nogle af Erik Werner's tegninger. Der blev udvalgt to, som kom med i den næste udgave. Dette er en stor ære, da det som regel kun er ældre og mangeårige tegnere, som får lov til at være med i dette "pæne" selskab.

Men det blev startskuddet for en mangeårig karriere som bladtegner - oprindeligt ville han have været skovridder, men det blev altså ikke til noget. Det skulle i hvert fald være noget med mennesker, og det var nok også baggrunden for, at han valgte at blive teatertegner.

- Det er nok den frieste form for tegning - man slipper for at blive rutinerede, lyder det fra Erik Werner.

Der ligger således et "lille"



DKUUG-Nyt's tegner, Erik Werner, i et selvportræt.

udvalg af hans tegninger på Teatermuseet - cirka 4.000 tegninger ligger dér, men selvom Erik Werner nu er gået ind i pensionsalderen, så er han langt fra færdig med at sidde i teatrenes halvmørke og tegne.

- Jeg har to pladser på første række, hvor jeg så sidder og laver små "notater". Der er ikke lys nok til at lave en færdig tegning, så

det er vigtigt at finde sjælen hos skuespillerne, siger Erik Werner, hvis tegninger alene skal kunne være en slags minianmeldelse. Han understreger, at han tegner sådan, som han nu engang oplever skuespillerne på scenen.

Han mener, at der er to former for at tegne; enten som en billedhugger (hvor tegneren kigger på former-

ne) eller som maler (hvor tegneren mere koncentrerer sig om lys og skygger).

- Det gælder om at finde det karakteristiske ved personen - uden at det bliver til en karikatur.

Samtidig er det vigtigt for Erik Werner, at han er velopløst, koncentreret og en lille smule overtræt, når han skal i gang med en opgave. Det lyder måske lidt selv-

modsigende, men det gælder også om ikke at falde ind i en rutine, hvor der bare slås nogle streger "lige som sidste gang".

Ved siden af tegneriet, så modellerer Erik Werner også - således kan man bl.a. se tre bronzeskulpturer på det Kgl. Teater, som han har udført. Han er medlem af Kunstnersammenslutningen Grønnin-gen, så det bliver også til udstillinger i mere gængs for-stand.

DKUUG's tegner erkender, at han har været heldig, idet han allerede to år efter han fik et par af sine tegninger i "Blæksprutten" blev fastansat på Weekendavisen, men arbejdet bredte sig hurtigt til både Berlingske Tidende og B.T.

Verdensmester

Det blev dog til et år i ufrivillig "frihed", men efter en snak med daværende chefredaktør Niels Nørlund blev Erik Werner fastansat endnu engang. Faktisk er teatertegneren noget helt enestående. Det findes stort set ikke i nogle andre lande end i

Danmark. Traditionen er dog lang, idet teatertegninger netop i år har 100 års jubilæum.

Hvert år afholdes der "verdensmesterskab" i tegning, hvor der er forskellige kategorier. Ikke mindre end tre gange er Erik Werner blevet verdensmester - men i dag er den pågældende kategori røget helt ud af konkurrencen.

Tegningerne har næsten som alt andet her i livet haft sine bølgedale, og i denne tid vinder de igen større indpas. Efter Erik Werner's mening måske i lige rigelig målestok, idet mange tegninger blæses op i kæmpeformater - mere for at fylde siden ud end hensynten til, at det er en illustration.

Selvom Erik Werner ikke har nogen teknisk sans overhovedet, så var han faktisk den første, der tegnede med "mus" i TV. Egentlig var det med en pind, hvor fjernsynsskiggen så kunne følge tegningen tilblivelse samtidig med en transmission fra Folketinget. Anden gang det med en rigtig - elektronisk - mus.

- Man kan godt se, hvem der har lavet tegningen, men der mangler lige som noget. Det er svært at få sindet med. Det er svært at forklare, men kan ikke rigtig få den sidste ting med, når man tegner på en skærm, mener Erik Werner.

På redaktionen kunne vi ikke dy os for at se, om Erik Werner ville være at finde på Internettet! Og minsandten - han har lavet flere tegninger til Kulturministeriets hjemmeside "Kultur-profilen" - se selv bl.a. på <http://www.kum.dk/publ/jubi/kap09.html>, hvor både tidligere kulturminister Jytte Hilden, den endnu tidligere kulturminister Niels Matthiesen, og departementschef Henning Rohde er portrætteret.

Forhåbentlig vil DKUUG-Nyt's læsere mange år fremover kunne glæde sig over Erik Werners tegninger både her og i den daglige Berliner...

□

Tiden med rationeringsmærker kan komme tilbage

De værste forudsigelser kommer frem, når der tales om år 2000 problemet. Således også da IDG afholdt to-dages konferencen "Fokus på Y2K" i for en måneds tid siden.

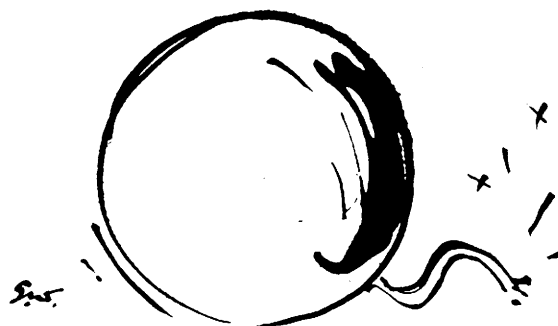
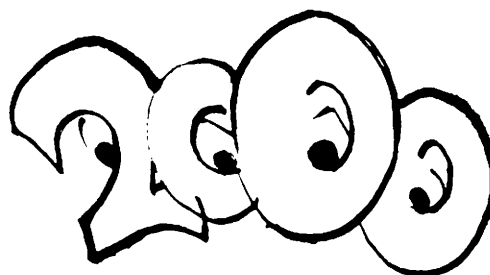
Af René Espersen

Ingen strøm, intet vand, ingen telefon, ingen varme - og hvad der så deraf følger, er nogle af de skræk-scenarier, som trækkes frem. Alle er dog enige om, at så slemt bliver det ikke, men ingen vil på den anden side garantere, at det ikke bliver sådan.

Hvad skal man så tro? Den, der ligger inde med det rigtige svar, vil kunne tjene en formue ved at gå til bookmakerne og satse sine sparepenge - hvis da ikke bookmakeren noterer kundernes indsatser på sin ikke-år 2000 sikrede computer eller han har sat pengene ind i en mindre bank,

der havde overset en eller flere dato-fejl, som lagde hele deres system ned ved overgangen til det nye århundrede. Det kan selvfølgelig også gå galt hos det of-

fentlige, hvorfor folk, der får en eller anden form for ydelse herfra, muligvis vil få "udbetalinger" i form af rationeringsmærker, da computersystemer er gået i sort



det ene eller andet sted i systemet.

Det er ikke for sjovt, at Claus Toftlund, projektleder for År 2000 fra medicinalvirksomheden H. Lundbeck afslørede, at de her i januar måned 1998 havde købt en splinterny PC'er hos Compaq/Digital, som ikke var År 2000 Parat. Og som han selv sagde, så er det mærker, hvor man ellers forventer tingene er i orden.

Problemerne er over alt, og det er umuligt for en virksomhed af en vis størrelse at tjekke alt, specielt hvis man har produktion af den ene eller anden art. Specielt svært kan det være at tjekke de indlejrede systemer. Og flere virksomheder lagde da heller ikke skjul på under ovennævnte konference, at de var nødt til at stole på de garantier, som leverandørerne gav dem. Dog gælder en mundtlig garanti ikke. Få garantien på skrift, så har du dit på det tørre - forhåbentligt.

Som det også blev nævnt af Jens Kolind i sidste nummer af DKUUG-Nyt, så gælder det under alle omstæn-

digheder at udarbejde en beredskabsplan i tilfælde af, at noget går galt. De større virksomheder vil have nogle på vagt nytårsaften næste år. At det bliver dyrt for virksomheden lægger ingen skjul på, men hellere det, end at det hele eventuelt bryder sammen. For Lundbeck er det således vigtigt, at deres mange forsøgsdyr ikke kommer til at lide overlast, hvis der eventuelt opstår strømsvigt. Og her hjælper det jo f.eks. ikke, at man opretter en telefonkæde, hvis telefonerne nu ikke virker. Der skal tænkes utraditionelt for at kunne tage højde for det, der kan ske.

En anden god idé, der kom frem på konferencen var, at man nedsatte erfaringsgrupper, hvor virksomhederne så kunne diskutere, hvad de gjorde for at imødekomme År 2000 problemet. Det behøver nødvendigvis ikke være branchebestemt, men kan lige så godt være for virksomheder, der ligger i det samme område. For hvis strømmen og telefonien forsvinder, så gør den det højst sandsyn-

ligt også hos naboen.

En hudløs ærlig Henrik M. Mogensen fra Grundfos A/S fortalte om, hvordan År 2000 bliver tacklet i virksomheden. Hos Grundfos startede man først i efteråret 1997, hvor et indlæg i en avis gjorde, at der for alvor blev sat fokus på problemet. Det var først på det tidspunkt, at man i Grundfos mente, at der kunne være grund til bekymring.

Der blev afsat økonomiske ressourcer til området, men samtidig har man i virksomheden erkendt, at man er nødt til at nedprioritere ny systemudvikling.

Grundfos regner med at skulle bruge mellem 10 og 20 mandeår på at finde, rette og teste for År 2000-problemer, men erkendte fra starten, at de ikke kunne frigøre en enkelt gruppe medarbejdere til udelukkende at beskæftige sig med dette. Derfor er så at sige alle ansatte involveret i arbejdet, dog med en 7 mand projektgruppe i spidsen, der står for den overordnede styring.

En ting havde man på

Grundfos dog ikke forudset, nemlig at nøglepersonen eller -personerne ville forlade Grundfos, inden alt var klappet og klart.

Der var hidtil ikke givet År 2000-medarbejderne nogle specielle fordele - eller stillet sådanne i udsigt. Men da nøglepersonen så sagde sit job op, erkendte man hos Grundfos, at de nu stod med et konkret problem - og at det godt kunne være, at man var nødt til at etablere en beredskabsplan, hvis andre skulle finde på det samme.

Fra Bankdata fortalte Lars Olsen, at de har givet deres medarbejdere en År2000-"gulerod" - 180 medarbejdere har fået en komplet multimedie PC'er, scanner m.v. leveret til privaten. Og har de pågældende haft et vist antal overarbejdstimer samt stadig er i virksomheden den 1. januar 1999, så PC'eren deres egen.

Klistermærker

Både hos Lundbeck og Bankdata har de mærket alt

deres udstyr, så de på en meget synlig måde kan se, om det pågældende udstyr er blevet testet igennem og fundet År 2000 Parat.

Hos Lundbeck er der tre kategorier: "Ja - År2000 Parat", "Nej - År2000 Parat" og "Undersøges År2000 Parat", mens de hos Bankdata kun opererer med "Virker" eller "Virker ikke"-mærkater. Begge anbefalede varmt denne måde at synliggøre løsningen af problemet på.

Er problemerne så så store, som det lyder til? Hos Bankdata regnede man med at skulle igennem 18-20.000 stykker kildekode, men efter en gennemgang steg tallet til 39.000! De har afsat 50 mandeår til opgaven, beregnet ud fra, at det i snit tager 45 minutter at kigge ét program igennem, fem timer at rette ét program med fejl, og at det tager en time og 45 minutter at teste programmet. Alt sammen ud fra en antagelse af, at fejlprocenten ligger mellem 15 og 20!

Hos Grundfos har man allerede testet et helt fa-

briksanlæg fra A-Z. Intet sted gik systemerne i sort, og det eneste problem, man fandt, var fejl i statistikkerne. De store CNC-maskiner blev ikke testet, da man ikke umiddelbart kan finde de enkelte chip og stille tiden frem på disse.

Dirigenten under konferencen var Arne R. Steinmark, journalist på ComputerWorld, og han fortalte bl.a., at han havde fået en email fra ét af Europas største stålværker, der kunne fortælle om én af deres egne oplevelser under testning af År 2000-problemer: Noget så enkelt som en pH-måler viste sig at indeholde en datofunktion. Udvikleren af måleren havde indsat en dato-funktion for at forsinke aflæsningen på displayet - ellers ville det ikke være muligt at aflæse måleren. Da virksomheden satte uret frem til efter år 2000, " fungerede" pH-måleren stadig dvs. i displayet vistes kun den seneste måling i år 1999! Et skræmmende eksempel på, hvad de indlejrede systemer kan få af betyde-

ning.

- Vi går ud til leverandørerne for at få en garanti. Vi har således måtte antage en holdning: Hvis vi får en garanti fra store soft-/hardware firmer, vil vi heller ikke teste standardløsninger, sagde Henrik M. Mogensen fra Grundfos.

Da man i Grundfos havde uddelegeret arbejdet, så var man i starten ude for, at den samme leverandør blev kontaktet af 6-7 forskellige fra virksomheden. Henrik Mogensen erkendte, at det selvfølgelig er kritisabelt, hvorfor det i dag kun er projektgruppen, der kontakter eventuelle leverandører.

Ingen forsikring

Er det muligt at forsikre sig imod en erstatningspligt forårsaget af År 2000? Det var ét af spørgsmålene, som direktør Claus Jakobsen fra Codan A/S skulle svare på i sit indlæg.

Svaret er kort og kontant et "Nej" - i hvert fald når det gælder erhvervskunder. Og i forsikringsverdenen kigger man ikke alene på den 1. ja-

nuar 2000 som den eneste kritiske dato. Ifølge Claus Jakobsen er der ikke én men hele 24 kritiske datoer i løbet af de kommende hundrede år bl.a. den 9.9.1999, 28.-29. februar 2000 og 1. marts 2000 - de sidste 2-3 datoer handler om, at det i år 2000 er skudår!

Forsikringsbranchen har indført undtagelsesbestemmelser for alle de 24 kritiske datoer. I USA, der jo som bekendt er advokaternes paradis, forventes det, at de rets-sager, som vil opstå i kølvandet på år 2000 problemet, vil komme til at koste tre gange så meget som at få løst selve År 2000-problemet.

Er der så hjælp at hente hos ens leverandør? Advokat Karin Absalonsen understregede, at det er en god idé at kigge ens kontrakter igennem - ifølge standardkontrakterne K18 og K33 skal leverandøren opfylde alle kontraktens krav dvs. ét års garanti og 7 år vedligeholdelsesgaranti. Spørgsmålet er samtidig, om man har lovlig adgang til kildekoden til de programmer, man har og

dermed lovlig kan gå ind og rette i programmerne. Når talen faldt på "gratis opgradering til ny version", så kan leverandøren kun tage sig betaling, hvis der er tale om ny funktioner i programmet - men År 2000 er ikke en ny funktionalitet.

Karin Absalonsen konkluderede, at ansvaret for løsning af År 2000 problemet ligger hos virksomhedens ledelse, at muligheden for at gøre leverandøren ansvarlig beror på konkret vurdering og endelig, at der ingen grund er til panik, men at der skal handles NU!

□

De ansvarlige vil ikke stille op til høring

År 2000 Forum afholder den første af tre konferencer om År 2000 problemerne i det offentlige. Der skulle have været tale om høringer, men de ansvarlige ville ikke stille op!

Af René Espersen

Mai Buch, formand for År 2000 Forum, er dybt foruro-
liget over, hvor lidt tjek der i
det offentlige er på eventuel-
le År 2000 problemer. Tre
planlagte høringer er æn-
dret til konferencer, idet de
ansvarlige indenfor de på-
gældende områder ikke vil-
le deltage, hvis der skulle gi-
ves nogle garantier.

Den 4. maj afholdes den
første konference i Lands-
tingssalen på Christians-
borg, hvor det er sundheds-
sektoren, der sættes fokus
på. Situationen på netop
dette område er så grave-
rende ifølge Mai Buch, idet
Forum ikke har kunnet få
nogle konkrete svar fra de
ansvarlige, om man vil nå at
teste alt udstyr i sundheds-
sektoren. Mai Buch har nu
bedt sundhedsministeren

tage affære.

I juni måned bliver der
en konference om den trafi-
kale infrastruktur; tog, fly,
veje m.v., mens der i august
måned vil blive sat fokus på

forsyningsområder såsom
el, gas og vand.

År 2000 Forum var én af
daværende Forskningsmini-
ster Jytte Hildens forslag, og
i dag sidder der 70 menne-



sker i det - uden penge og kompetence, men med det mål at sætte fokus på År 2000 problemerne, koordinere de forskellige initiativer på området samt vurdere de samfundsøkonomiske konsekvenser af problemet.

I spidsen for År 2000 Forum sidder som nævnt økonomidirektør Mai Buch fra Det Kongelige Teater. Forum er bredt sammensat af organisationer og brancheforeninger. Det bakkes op af År 2000 sekretariatet, der har fået 12 millioner kroner over tre år til at skabe opmærksomhed om År 2000-problemet og opbygge viden om problemerne i forbindelse hermed.

År 2000 Forum lavede i starten en undersøgelse hos danske virksomheder for at få et indblik i, hvor stor bevidstheden var om problemet. 81 pct. havde hørt om det, og kun 6 pct. svarede, at de ikke havde hørt om det. Men nok så vigtigt - 84 pct. havde ikke afsat én eneste krone til finde, rette og teste for År 2000 problemer.

Mai Buch fortalte på

IDG's konference i sidste måned om, hvor langt man er nået på Det Kongelige Teater. Her har man bl.a. også rettet henvendelse til Københavns Elforsyning og Tele Danmark, men ingen af de to har hidtil kunnet give et ordentlig svar, hvilket selvfølgelig er dybt bekymrende. Ikke alene for Det Kongelige Teater, men alle i der er afhængige af el og telefoni.

Endvidere har halvdelen af Det Kongelige Teaters leverandører kun ville give en mundtlig garanti for, at deres produkter er år 2000 sikker. Hvilket jo heller ikke er særlig betryggende. På teatret opererer man selvfølgelig med forskellige nødplaner, så der i det mindste vil kunne spilles forestillinger de første par uger i år 2000, hvis ellers er der strøm, varme, transportmidler osv. til rådighed.



Den Virkelige Verden

En kunde hos Dell ringede for at klage over, at hans tastatur ikke længere virkede. Han havde gjort tastaturet rent ved at fylde badekarret med vand og sæbe for derefter at lade tastaturen ligge i vandet i en dags tid. Derefter havde han fjernet alle tasterne og vasket dem individuelt.

En forvirret kunde ringede til IBM, da han havde problemer med at udskrive sine dokumenter. Han fortalte teknikeren, at computeren havde fortalt ham "couldn't find the printer". Kunden havde forsøgt at dreje skærmen til computeren, så den kunne se printeren, men computeren kunne stadig ikke "se" printeren.

Officielt referat

- fra den ordinære generalforsamling i DKUUG, torsdag den 27. november 1997 i Symbion.

Af advokat

Michael H. Svendsen

Quist • Stanbrook:

Til dirigent blev valgt advokat Michael H. Svendsen, der konstaterede, at generalforsamlingen var indvarslet og indkaldt med det i vedtægterne fastsatte varsel, men at de forslag, der skulle behandles på generalforsamlingen, ikke var udsendt med det i vedtægterne fastsatte varsel på mindst 2 uger. Samtlige de mødende accepterede dog, at generalforsamlingen var lovligt indvarslet og dermed beslutningsdygtig.

Bestyrelsen og de enkelte udvalgsformænd aflagde beretning om aktiviteterne i det forløbne år. Særligt blev de nye medarbejdere præsenteret, direktør Bo Folkmann, bogholder og sekretær Hanne Schmidt samt

den nye redaktør for DKUUG-Nyt René Espersen, som tiltræder pr. 1. januar 1998. Foreningen har planer om yderligere at ansætte en netpasser. Ansættelse vil formentlig finde sted pr. 1. januar eller straks i begyndelsen af det nye år.

Endvidere blev det nye sekretariat særligt omtalt og den opstramning i forretningsgangen, som nu er foretaget.

Bestyrelsen kunne berette, at der efter langvarige forhandlinger er skabt ro om foreningens skatteforhold.

Der blev afgivet særlige indlæg for de enkelte udvalg, Kim Biel-Nielsen, Myanne Olesen, Kristen Nielsen, Sven Thygesen og Gitte D'Arcy.

Beretningerne blev taget til efterretning.

Årsregnskab 1996

Benny Michelsen gennemgik regnskabet i hovedtræk, og der var lejlighed til at udveksle spørgsmål og svar.

Regnskabet for 1996, der udviser et underskud på kr. 967.955, blev énstemmigt godkendt.

Valg af bestyrelsesformand

Efter præsentation af kandidaterne blev Kim Biel-Nielsen valgt som formand.

Valg af medlemmer til bestyrelsen

Der skulle til bestyrelsen vælges 7 nye medlemmer. Efter præsentation af kandidaterne blev følgende valgt som nye medlemmer af bestyrelsen:

Sven Thygesen, Kristen

Nielsen, Myanne Olesen, Gitte D'Arcy, Jacob Bække, Bjørn Johannesen og Peter Holm.

Bestyrelsen har herefter følgende sammensætning:

Kim Biel-Nielsen, formand
Peter Lange
Benny Michelsen
Sven Thygesen
Kristen Nielsen
Myanne Olesen
Gitte D'Arcy
Jacob Bække
Bjørn Johannesen
Peter Holm

Valg af revisor

Som foreningsvalgt revisor blev genvalgt Bo Holst-Christensen.

Som revisorsuppleant blev genvalgt Lene Abild.

Indkomne forslag

Hr. Keld Jørn Simonsen har i overensstemmelse med vedtægterne fremsendt forslag til behandling på generalforsamlingen. De to forslag vedrører refusion af visse udgifter i forbindelse med en tidligere generalforsamling samt visse udlæg i forbindelse med hr. Simonsens rejse-

aktiviteter.

Generalforsamlingen udtrykte almindelige forståelse for, at bestyrelsen ikke havde bevilget disse udbetalinger til hr. Keld Simonsen, men besluttede desuagtet at honorere de af Keld Simonsen fremsatte krav om refusion, idet Keld Simonsen samtidig tilkendegav, at han herefter ikke har yderligere krav over for foreningen.

Budget og kontingent for 1998

Hr. Benny Michelsen gennemgik hovedpunkterne i foreningens budget for 1998. Med en enkelt korrektion, nemlig en forhøjelse af udgiftsbudgettet med kr. 10.000 for klubudvalg, blev budgettet godkendt af generalforsamlingen. Budgettet indebærer, at stormedlemmer for 1998 betaler kontingent på kr. 9.000 med tillæg af moms, organisationsmedlemmer betaler kr. 3.250 med tillæg af moms, mens individuelle medlemmer betaler kr. 560 med tillæg af moms.

Eventuelt

Et enkelt medlem henstillede til bestyrelsen, at man gjorde sig mere umage med at afgive en bred orientering på den ordinære generalforsamling, hvor en stor del af medlemmerne trods alt er samlet.

Hr. Benny Michelsen forelagde til drøftelse muligheden for at lade DKUUG stå som ansvarlig bag etableringen af et udviklingsselskab, som på joint venture basis skulle kunne stille risikovillig kapital til rådighed for mindre og mellemstore IT-virksomheder. Et enkelt medlem udtrykte sig kritisk over for tanken om, at foreningen skulle bruge sine midler som risiko-venture kapital frem for at bruge formuen som indtægtsgrundlag til at opfylde foreningens primære formålsparagraf.

Generalforsamlingen hæv-
vet.

Som dirigent
Michael H. Svendsen



Linux 98

- Konference om Linux på hjemmefronten

DKUUG afholder i samarbejde med SSLUG - Skåne/Sjælland Linux User Group - en konference om Linux. Konferencen afholdes lørdag den 16. maj 1998 kl 10-18 på Symbion, Fruebjergvej 3, 2100 København Ø.

Linux stormer frem som operativsystem, især på netværksområdet som web-server og firewall, men også som arbejdsstation og til hjemmebrug. Denne konference vil sætte fokus på, hvordan man får Linux til at fungere godt på hjemme-PC'en. Konferencen kommer ind på mange aspekter af Linux, såsom:

- Den bagved liggende filosofi med gratisprogrammel og fri kildetekst
- Hvordan man får fat på det og installerer det
- Hvordan laver man sin egen system-kerne
- Hvordan man nemt administrerer det med dotfile

Linux

generator

- Brug af systemet med komandofortolkeren bash
- Programmering i perl, med tråde, og kildetekstadministration
- Hvordan man sætter det op på Internet med web-server, posthus og firewall
- Hvordan man laver sit eget netværk derhjemme med win95 og mac klienter
- Nogle omfattende office-pakker der er tilgængelige
- Grafiske brugerinterfaces, window managers
- Ting man skal gøre for at bedre at køre med dansk og svensk
- Hjemmecomputeren som tal-knuser: Hvordan bygger man en billig super-computer

I forbindelse med konferencen laves en CDROM med et Linux-system, som udleveres gratis til alle deltagere, og der vil være mulighed for

at installere forskellige Linux-distributioner, samt få hjælp til Linux-problemer.

Aktiviteter

Udover det tekniske program vil der være en del andre aktiviteter om eftermiddagen:

- Installation af Linux - på din medbragte computer. Der planlægges at være en række forskellige distributioner tilgængelige, bl.a. RedHat, S.u.S.E, Debian og Slackware.
- Praktisk Perl programmering tutorial ved Ole P. Tange
- Planche om CVS - til administration af kildetekst ved Peter Toft
- Planche om programmering med tråde (threads) ved Ole Vilmann
- Planche om firewall ved Kristian Vilmann
- Planche om MPI ved Jacob Østergaard

Der vil også være mulighed for hjælp med praktiske Linux problemer. Se endvidere det detaljerede program på <http://www.dkuug.dk/keld/>

konf2.htm

Målgruppe

Konferencen henvender sig til hjemmebrugere af Linux, både avancerede brugere og også brugere der lige er begyndt med Linux. Andre teknisk interesserede i Linux som folk der påtænker at bruge Linux kan også få et godt udbytte af dagen.

Pris og tilmelding

I sædvanlig Linuxånd er der mange som giver en hånd med gratis, og derfor er det gratis at deltage. Af hensyn til plads og mad er tilmelding dog nødvendig. Der kan bestilles snitter/smørrebrød til kostpris, ca. 12 kr. stykket, og vand til ca. 4 kr. pr flaske. Tilmelding og bestilling skal ske til DKUUGs sekretariat, email sek@dkuug.dk. Der vil være mulighed for at få installeret Linux på din egen maskine på konferencedagen.

Hvis du medbringer en maskine, se så venligst tilmeldingsblanketten på DKUUGs websider

<http://www.dkuug.dk>.

Den Virkelige Verden

En IBM-kunde havde problemer med at installere noget software og ringede for at få hjælp. "Jeg satte den første diskette ind og det var OK", fortalte kunden og fortsatte:

"Da den fortalte, at den anden diskette skulle sættes ind, så havde jeg nogle problemer med den. Da den så sagde, at den tredje diskette skulle indsættes, så kunne jeg ikke få den ind".

Kunden vidste åbenbart ikke, at "Indsæt diskette nr. 2" betød, at man skulle fjerne diskette nr. 1 først.

Boganmeldelse:

Tag dine forholdsregler

*Time Bomb 2000**Edward Yourdon & Jennifer Yourdon*

ISBN 0-13-095284-2

Normalpris:

kr. 184,00 ekskl. moms

DKUUG-pris:

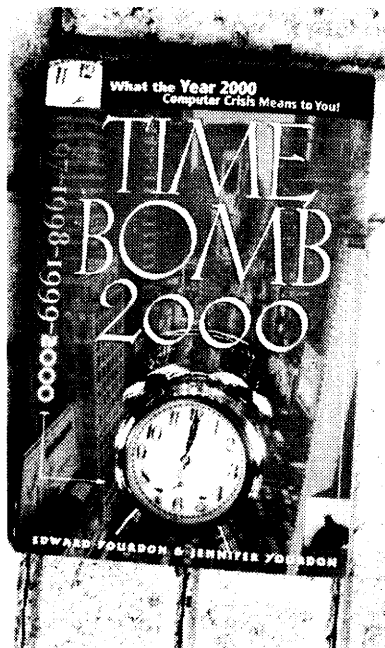
kr. 165,60 ekskl. moms

Af René Espersen

År 2000-problemet er uoverskueligt, men man kan tage nogle forholdsregler.

Det må være konklusionen på bogen "Time Bomb 2000", som er skrevet af Edward Yourdon og Jennifer Yourdon. Det er en amerikansk bog med stort A, som opstiller forskellige scenarier for, hvad der kan ske, når der på kalenderbladet står 1. januar 2000.

Det skal siges med det samme, at der her ikke er tale om nogen egentlig teknisk bog, hvor man får løs-



ningen på, hvordan man løser dato-problemet i alverdens programmer. Dette er mere en overlevelses håndbog, der giver nogle gode råd til, hvilke forholdsregler man skal (bør) tage. Alt efter, hvor mange nerver man nu engang har, og hvor me-

get tiltro man har til, at År 2000 problemet når at blive løst rundt omkring i samfundet.

Igennem 14 kapitler gennemgås, hvilken indflydelse År 2000-problemet vil få på finansverden, på dit job, din hjemme-PC'er, på transportsektoren, på fødevarer-situationen, sundhedssektoren, undervisningssektoren, de statslige institutioner, de indlejrede systemer m.v.

Samtidig giver forfatterne deres bud på, hvilke forholdsregler man skal (bør) tage, hvis de ovennævnte områder bryder helt sammen i henholdsvis to dage, én måned, ét år eller i 10 år.

I de fleste sammenhænge vil et nedbrud i et par dage nok kunne klares af de fleste, mens det straks ser værre ud, hvis nedbruddet varer en måned, især hvis der bliver problemer med at få fat i fødevarer og medicin.

Derfor opfordres læseren til at hamstre forskellige mere eller mindre livsnødvendige ting såsom fødevarer, vand, medicin, kontanter m.v. - i hvert fald så man kan klare sig en måned.

Et andet råd er, at man skal undgå at blive indlagt i dagene omkring nytåret 1999/2000. Det kan jo unægtelig svært at styre selv - men det var måske værd at overveje ikke at blive gravid i foråret 1999!

Nogle af læserne vil være klar over, at der kan blive problemer allerede før nytåret. Således skal man nok tænke en ekstra gang om, inden man begiver sig ud på en rejse den 22. august 1999.

Netop denne dag vil GPS satellitternes "tidsmåler" nå et vendepunkt. Tiden bliver her målt i sekunder, timer, dage og uger. Da hukommelsen kun er på 12 bit, så vil denne blive fyldt netop den 22. august næste år og skifte til 0! Spørgsmålet er, hvad det kommer til at betyde, men i værste fald vil de cirka 10 millioner skibe og fly, der navigerer efter disse satellit-

ter få udregnet forkerte positioner, hvilket kan få katastrofale følger.

I USA sørger den offentlige myndighed (SSA) for at udbetale folkepension til millioner af amerikanere hver eneste måned. SSA regnede med, at de skulle igennem og rette 30 millioner liner af kode. Et arbejde der forventes at være afsluttet i slutningen af 1999. Det er jo meget godt, men SSA startede altså også i 1991. Og det er unægtelig mange år før andre overhovedet vidste, at der kunne være problemer.

I bogen kan man også læse om en anden "pudsighed" (der er rent faktisk flere af den slags, end man går og tror!). Hos mange banker åbner døren til bankboksen kun på bestemte tidspunkter, naturligt nok på hverdage på et bestemt klokkeslæt. I de fleste tilfælde er den pågældende chip med datofunktionen indlejret godt og grundigt af sikkerhedsmæssige hensyn, og for at komme til denne skal halvdelen af banken rives ned. Det, der kan ske, er, at chip'en den 1.

januar tror, at det er den 1. januar 1900. Da dette var en mandag, vil døren til bankboksen åbne sig. Og det er jo ret uheldigt, idet 1. januar 2000 jo er en lørdag!

Forfatterne indrømmer, at skulle nedbruddet vare et år eller mere - hvilket er usandsynligt - så vil man nok i mellemtiden finde andre veje til at få fat i eller få udført de pågældende ting. Men meget kan også bryde sammen, hvis det går galt i én eller flere måneder.

De to amerikanske forfattere indrømmer også, at nogle af scenarierne kan virke noget dommedagsagtige, men at man selvfølgelig selv må vurdere, hvor galt man selv tror det går, og hvorledes det vil komme til at påvirke ens dagligdag.

Bogen skal man ikke læse, hvis man ønsker at komme i godt humør, men på den anden side er den god, hvis man ønsker at forberede sig godt, hvis det skulle gå galt i år 2000.

□

Per's hjørne

Kryptering - barnedrømmen levet ud

Af Per Andersen

De fleste af os - i hvert fald den halvdel af racen, jeg tilhører - kan huske, hvordan vi som børn var fascinerede af kode-skrift, så vi hemmeligt kunne kommunikere med hinanden. Man oversatte fx bogstaverne til tal og udførte en bestemt funktion på disse, som kun modtageren kendte. Bagefter var vi lige så tændte på at bryde de andres hemmelige kode, og vi anvendte mere eller mindre logiske måder at gøre dette på (jeg fandt det nu nemmere at banke oplysningerne ud af de andre snotunger).

Visse ingeniører har ikke helt kunne lægge denne idé fra barndommen fra sig, og de får derfor meget tid til at gå med at udtænke avancerede måder at kryptere data på, så ingen kan læse dem. Særlig avanceret er DES, der har en 56-bit kodelængde,



hvilket skulle betyde, at det ville tage 1.000 år for en PC at finde den korrekte kode.

Andre ingeniører så selvfølgelig dette som en udfordring, og de skulle straks udtænke en metode at bryde koden på. De lavede derfor et netværk af 20.000 arbejdsstationer (ja, du læste rigtigt!) over hele verden, der hver arbejdede i 150 dage for at bryde koden. Det lykkedes, og disse ingeniører følte det sikkert som en stor sejr (det skal her indskydes, at jeg ikke specielt har noget imod ingeniører, for man kan sagtens finde højteknologiske nørdere andre steder også, fx øhhhh ...).

Det fik fluks sikkerhedseksperter til at udtale, at så måtte man hellere anvende koder med 80 eller 90 bits længde. Så skulle man nemlig ikke kunne bryde koden før de 20.000 arbejdsstationer havde arbejdet i omkring

10.000 år. Jamen, siger du nu, arbejdsstationernes kapacitet vokser jo kraftigt! Jo, er det ikke noget med en fordobling ca. hvert år (nu er det faktisk kun for hver 18 måneder, men lad os bare overdrive). Det vil sige, at om 5 år vil de 20.000 arbejdsstationer "kun" skulle arbejde i 300 år for at bryde koden (og til den tid, vil de jo nok være forældede, ikke sandt!).

Nu håber jeg sandelig, at der lå noget meget værdifuldt bag ved denne 56-bit DES kode, for værdien af 20.000 arbejdsstationer i 150 dage er rundt regnet 300 mio. kr. plus mandtid. Så med mindre kriminalitet pludselig er blevet en velgørenhedsforretning, så vil det ikke rigtigt være attraktivt at ofre 300 mio. kr. for at få adgang til fx en stribe dankortnumre.

Det kan chefer og andre så tænke over, når de beder sekretæren kode indholdet på deres disk, så medarbejderne fx ikke kan snige sig til at finde ud af, hvad kollegerne tjener i løn. Og sekretæren så finder ud af, at det er en oplagt mulighed for hende

til at få mere i løn: Hun beder diskret chefen om mere i løn, eller også kommer hun "desværre" til at glemme hvilken kode, der er anvendt for at kode alle virksomhedens livsvigtige oplysninger!

Gennem en virtuel markedsanalyse (også kaldet et gæt) har jeg fundet ud af, at der mistes langt flere penge på ovenstående "anvendelse af kryptering" end gennem kriminel "brydning af kryptering". Så måske var det en idé at tænke sig lidt om, inden man kaster sig ud i det helt store krypterings-orgie.

Der er nu mange, der går amok med sikkerhed. Det har udbyderne af sikkerheds-software også fundet ud af, og der er ombrydninger i denne industri som sjældent set før. Alle ruster sig til, at hr. Jensen skal have indført sikkerhed over hele linien. Amerikanske virksomheder inden for edb-sikkerhed opkøber hinanden for et godt ord - eller rettere sagt dollars. Der er handlet sikkerhedsfirmaer for 12 mia. kr. på bare 6 måneder! McAfee har slået sig sammen

med Network General, Security Dynamics har købt DynaSoft og Cylink har købt Algorithmic for bare at nævne nogle få.

Men misforstå mig nu ikke, der er selvfølgelig brug for kryptering af meget høj standard. Jeg kan endda komme i tanke om flere eksempler, såsom når Bill Clinton skal udveksle oplysninger med sin advokat i sex-sagerne eller når Mette Lisby skal forberede sine jokes uden at Glintborg og Casper kikker hende over skulderen (ingen sex-vitser her).

For nu at vende tilbage til de 20.000 arbejdsstationer, som jeg helt ærligt har lidt svært ved at komme over, så er det hele jo faktisk meget enkelt: Et spørgsmål om sikkerhed er et spørgsmål om, hvor meget værdi informationer vil have for andre. Man investerer jo heller ikke for 100.000 kr. sikkerhed i sit hjem for at beskytte et stereoanlæg til kr. 20.000. Eller sagt på en anden måde: Det skal jo være umagen værd for tyven at bruge ressourcer på at bryde ind.

Det er altså ikke et spørgsmål om, hvorvidt koden kan brydes eller ej (det kan den altid). Det er derimod et spørgsmål om værdien af det, man ønsker at beskytte kontra, hvor besværligt det vil være at bryde koden. Men længe leve ingeniørerne, der både har opfundet arbejdsstationerne, og bagefter har kunnet finde på noget at holde jordens bestand af arbejdsstationer beskæftigede med.



Den Virkelige Verden

Fra formanden har redaktionen modtaget følgende lille historie, som kan give stof til eftertanke, når emnet falder på kommunikation:

Har du nogensinde undret sig over, hvordan front-ruden på flyvemaskiner testes mod sammenstød med flyvende fugle. Ifølge "California Poultry Industry Federation", så afskydes døde kyllinger mod ruden.

Åbenbart har det amerikanske luftfartsvæsen en speciel "kyllinge-kanon", som skyder med kyllinger som ammunition. Tanken er, at hvis frontruden ikke går i stykker, når den døde kylling rammer denne, så vil ruden sikkert også holde til en kollision med en levende fugl.

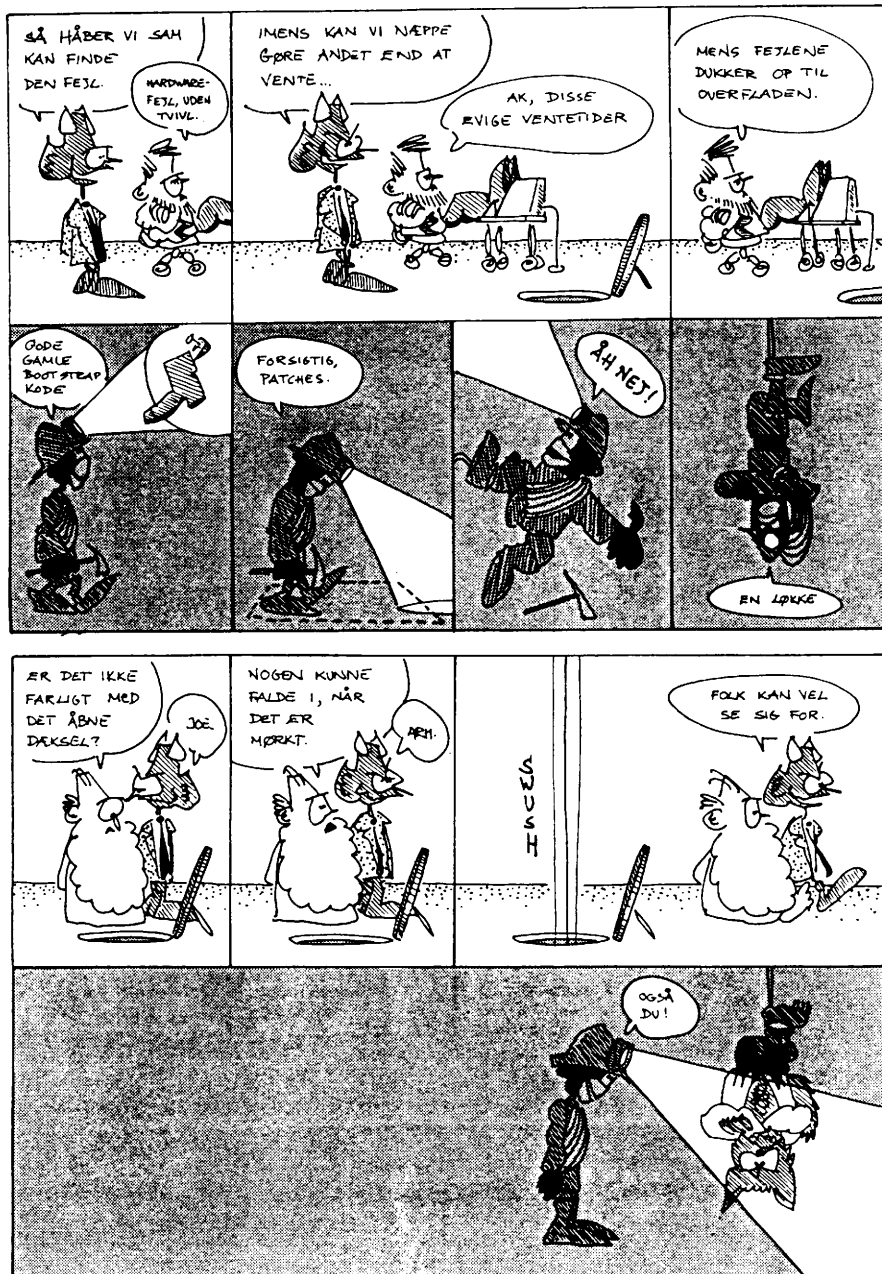
Da eksperterne fra British Rail hørte om "kyllinge-kanonen" spurgte de, om de ikke kunne teste frontruden på de nye høj hastigheds tog på ovennævnte måde. Som sagt så gjort, men da de ladede kanonen med en kylling

og afskød denne mod ruden, knustes ruden, og kyllingen røg lige igennem togførerens stol, ødelagde instrumentpanelet og hamrede sig fast i kabinens endevæg som et rigtigt projektil.

Englænderne var meget forbavset og spurgte det amerikanske luftfartsvæsen, hvad de havde gjort galt. Luftfartsvæsenet svarede med følgende korte sætning: "Husk næste gang at bruge optøede kyllinger".

ETC.

KYNDE & FREY 87



Aktivitetskalender 1998

Maj

06. Seminar

- Handel på Internettet

16. Konference

- Linux

19. Gå-hjem-møde

- Unicenter TNG

19. Kursus

- CORBA programmering

- Pekka Kähköpuro

25.-26. Kursus

- "Introduction and Advanced Cryptography"

- Bruce Schneier

25. Klub Århus

26. Klub København

28. Klub Sønderborg

Juni

02. Gå-hjem-møde

- WinFrame

10. Seminar IT

- Perspektiver og muligheder

17.-18. Kursus

- Advance C++

- Rex Jaeschke

19. Kursus

- Java

- Rex Jaeschke

22. Klub Århus

25. Klub Sønderborg

26. Klub København

Juli

Ingen planlagte aktiviteter

Nye medlemmer

Følgende er nye medlemmer i DKUUG:

Østbirk Bygningsindustri er blevet nyt organisationsmedlem.

Tele2 A/S er blevet nyt stormedlem.

Thomas Jørgensen, Annette Ibsen fra Netch, Poul Henning Kamp, Theis Passer fra TC Computing og Peter Jøvel fra Tempest er nye individuelle medlemmer.

Alle bydes hjertelig velkommen i DKUUG.

DKUUG-Nyt er medlemsbladet for DKUUG

Udgiver:

Dansk UNIX-system Bruger Gruppe

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:

René Espersen (ansvarshavende)

Gitte D'Arcy

Søren Oskar Jensen

Bjørn Johannesen

Jacob Bække

Keld Simonsen

Kim Biel-Nielsen

Peter Holm

Bo Folkmann

Tryk:

Palino Print

Papir: Cyclus

Annoncer:

DKUUG Sekretariatet

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

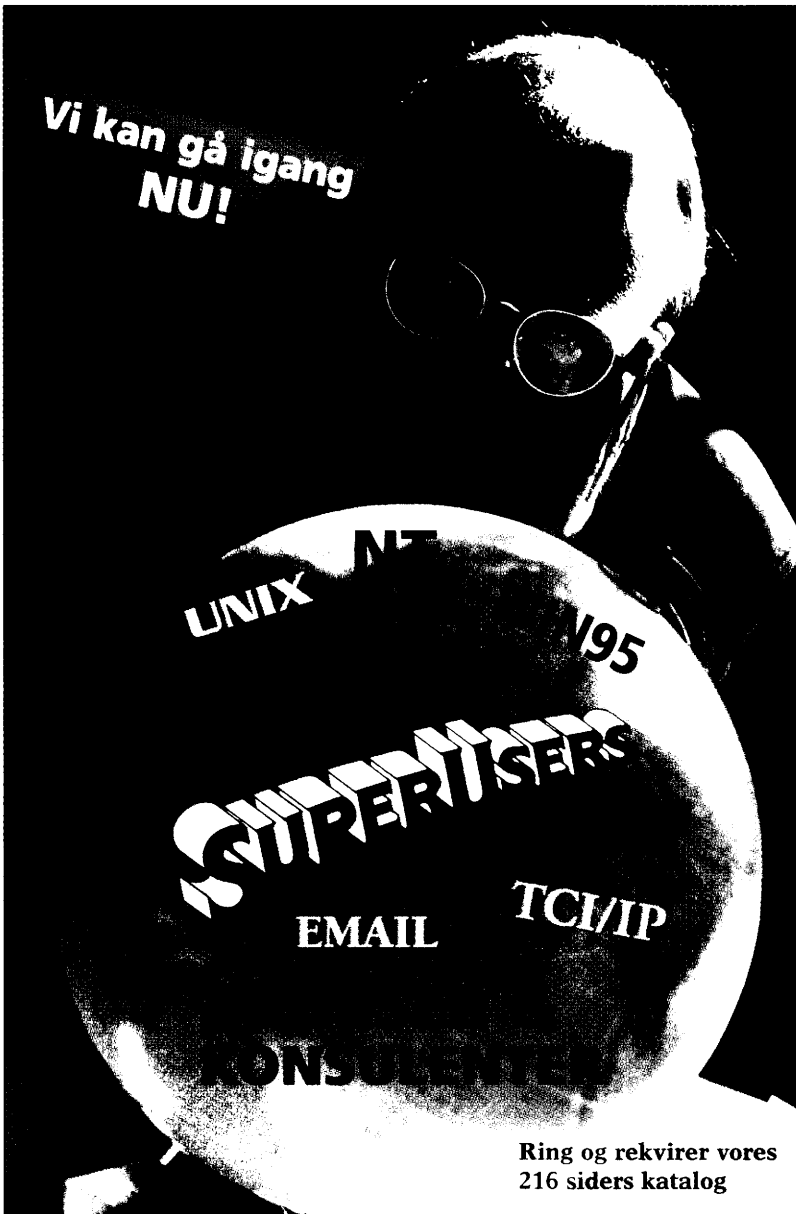
Deadline:

Deadline for næste nummer, nr. 104, er fredag den 15. maj 1998.

Medlem af Dansk Fagpresse

DKUUG-Nyt

ISSN 1395-1440



**Vi kan gå igang
NU!**

UNIX NT 1995

SUPERUSERS

EMAIL

TCP/IP

KONSULENTER

Ring og rekvirer vores
216 siders katalog

UNIX

20 UNIX-kurser med mulighed for afvikling på over 25 forskellige UNIX-versioner, samt konsulentopgaver indenfor drift og udvikling.

NT

Microsoft Authorized Technical Education Center (ATEC) med 22 kurser samt konsulentopgaver indenfor Windows 95 og NT samt MS BackOffice.

Internet

Vi var med da Internettet startede i Danmark tilbage i 80'erne. Stor erfaring med internet applikationer, teknologier og værktøjer.

C/C++, HTML/JAVA

Sprog som alle stammer fra UNIX-verdenen. 9 kurser og millioner af programliniers erfaring.

SuperUsers a/s
Karlebogaard
Karlebovej 91
3400 Hillerød
Tlf: 48 28 07 06

E-Mail: super@superusers.dk
URL: <http://www.superusers.dk>