DKUUG-Nyt

Nr. 91 — Marts 1997

Kryptografi

Hvordan skal staten og borgerne forholde sig til kryptering af data - hvad skal veje tungest: borgernes frihed eller statens sikkerhed? Danmarks førende autoritet, juraprofessoren Mads Bryde Andersen, beskriver problemerne og de mulige løsninger.

Domæner

Slaget om domænerne blev blodigt - Søren Hornstrup fra DKnet forklarer hvad det hele egentlig drejede sig om.

Per mener

Vi har fået Per Andersen fra IDC som fast skribent - han giver sin mening om NC'ere (network computer).

Indhold

Stort og småt...

Sä er vinteren endelig ved at slippe sit sidste krampagtige tag i lille Danmark, og foråret presser sig på. Alt i medens den sidste af de store kinesiske ledere trækker vejret for sidste gang. Bekymringerne dukker straks op til overfladen i dagspressen. Og spørger man manden på gaden er kommentaren blot "Kunne han dog ikke have ventet til efter den 1. Juli, til Hong Kong er blevet genforenet med Kina."

I Danmark annoncerer Præsident Bill Clinton sin ankomst den 12. marts, hvor han gælder sig til at hilse på vores Dronning. Og for at det ikke skal være løgn, så kører Hans Engell galt i en "herre" brandert. Hvad tænker du dog på Engell? En mand i din position! Vi er så tæt på igen at komme til magten, og så begår du årets brøler. What is the world comming to? "And you can ask yourself - Do I feel lucky? Well do you punk?" Som en kendt skuespiller en gang sagde. Jeg tror nok han hedder Dirty Harry alias Clint Eastwood.

I vores egen lille andedam går det jo godt. Vores søgen efter en ny direktør ser nu ud til snart at bære frugt. Hvis alt går efter planen kan vi byde DKUUG´s nye direktør velkommen til juni. Redaktionen vil naturligvis i den forbindelse bringe et portræt af direktøren. Næste skridt på vejen i bemanding af DKUUG´s sekretariat er en administrativ medarbejder. Denne stilling er netop blevet annonceret i Berlingske Tidende.

I bladet denne gang kan du læse lidt om DKUUG´s bestyrelse. Vi har valgt at profilere bestyrelsen ved et mindre portræt af det enkelte medlem, og hvad de har bedrevet gennem tiden. Vi har også billeder på, for på den måde at synliggøre (den var god?), om ikke foreningen så i det mindste DKUUG´s bestyrelse. Vi skal jo starte et sted.

DKUUG's blå bog

Et nogenlunde retfærdigt portræt af bestyrelsesmedlemmerne

Ole Farbøl

Den sovjettiske avis Pravda (Sandhed) bestod af 98 % løgn, ligegyldigheder og bortforklaringer samt 2 % sandhed. De sidste procent stod ofte mellem linierne og krævede stor opmærksomhed hos læserne.

Også her i vesten består enhver publikation af både skidt og kanel. Det gælder ikke kun den mest oplagsliderlige boulevardpresse, men også i den seriøse ende - omend i varierende mixninger. Selv når journalistik er allerbedst (hvilket pr. definition er en sjælden foreteelse) så er det journalistiske produkt altid en forkortet udgave af virkeligheden, der er baseret på en research, som altid kunne være endnu bedre. I worst case udgaven hører det journalistiske produkt hjemme i eventyr- eller horrorgenren.

Man burde derfor forsyne enhver avis med en klar advarsel: »Stol ikke 100 % på os«.

Efterfølgende kommer en stribe portrætter af DKUUG's bestyrelsesmedlemmer efter det seneste kampvalg, som jeg har begået, og som jeg for en gangs skyld vil forsyne med en varedeklaration:

De er ikke sande!

Jeg har prøvet at gøre dem sande og fair ved at tale med de pågældende selv samt en stribe personer rundt om dem. Det resulterede i bunker af fakta, skidt og skamros, som jeg har siet og vægtet for sandsynlighed og relevans, hvorefter det er groft beskåret til at fylde et manuskriptark pr. bestyrelsesmedlem.

Resultatet er, at portrætterne (efter min egen mening) gengiver rimelige billeder af personerne, men de er ikke sande i den klassiske mur- og nagelfaste forstand. Så læs dem med et gran salt. De gutter og den kvinde, det handler om, rummer mere end, der står her.

Kim Biel-Nielsen

Udvalg:
Næstformand samt med i: Medlemsmødeudvalget (fmd.), Administrationsudvalget, Eksternt udvalg.

Formand for EurOpen

Job:
Adm. dir. for Uniware danmark aps

Den 47-årige Kim Biel-Nielsen er en af DKUUG's grundlæggere og ankermænd. Helt tilbage i 1982 solgte han den første Zilog Unix-boks til Fiskernes Bank i Tromsø, ved stiftelsen af DKUUG året efter var han derfor en af 'de kommercielle', som foruroligede teknikerne med de rene hjerter dengang.

Men den kommercielle Kim Biel-Nielsen så snart, at nøglen til merkantil succes lå i software og med et stort talent for at overbevise skaffede han imponerende agenturer, som Informix og Uniplex, hjem. For knap et halvt år siden købte han sammen med en partner flere attraktive softwareagenturer (bl.a. Frame og EBT) fra sin tidligere arbejdsplads og stiftede det nye Uniware danmark.

I DKUUG og i bestyrelsen, hvor han har siddet i mange år, er han da også den professionelle forretningsmand, men også teknologi-entusiasten. Giv Kim Biel-Nielsen en ny dims, og han elsker den ubetinget. Derfor brænder han også for Unix, men ikke Unix-only.

I kraft af det årelange, vedholdende arbejde i foreningen er han i høj grad medansvarlig for drejningen væk fra ren bit-vending til 'syndig' business og professionalisering - uden at have droppet begejstringen for hard core teknologi undervejs.

Det præg, han har sat på DKUUG, mærkes også på foreningens kagetradition, hvor feinschmeckere i nærende former for livsnydelse idag har kronede dage

Myanne Olesen

Udvalg:
Kasserer, Administrationsudvalget (fmd.), Medlemsmødeudvalget, Klubudvalget, Netforum, Eksternt udvalg, Marketingudvalget, Fora.

Job:
Selvstændig, Myanne Olesen Consulting

Den 32-årige Myanne Olesen er en af de hårdeste arbejdsheste i DKUUG, hvilket listen over hendes deltagelse i udvalg afspejler. Hun mener da også, at nogen burde tage sig sammen til at få rettet den fundamentale fejl, at der ikke er 80 minutter i timen.

Hun har en sjældent stor vennekreds, der skal plejes samtidig med alle de arbejdsmæssige projekter. Derfor er aftener og weekender tæt belagt, og godt styrket af kaffe tager B-mennesket også morgener til hjælp.

My var hendes ingeniørfaders kælenavn til hende allerede fra før hendes fødsel, idag er det både kalde- og emailnavn, og måske er hendes store tekniske interesse ballast medbragt hjemmefra.

Hun fik som ganske ung arbejde hos IBM, læste parallelt datalogi, stiftede nærmere bekendtskab med Unix hos først Pro Informatic, senere Uniware. Idag hedder levevejen rådgivning om rapid application development, hvor hun nu driver sin egen forretning.

Myanne Olesen har været med i DKUUG i cirka otte år og har næsten fra starten siddet i bestyrelsen, hvor hun er en bærende kraft. Engagementet er meget stort, og hun påtager sig gerne stort ansvar. Mys svaghed er, at hun ikke helt forstår, hvis andre ikke har helt samme engagement, og parret med hendes temperament betyder det lejlighedsvis udslip af stort damptryk.

Derimod er hun ikke indpisker på kagesiden, men helt i DKUUG's ånd har hun en veludviklet sans for bedre restauranter og ædel rødvin

Benny Michelsen

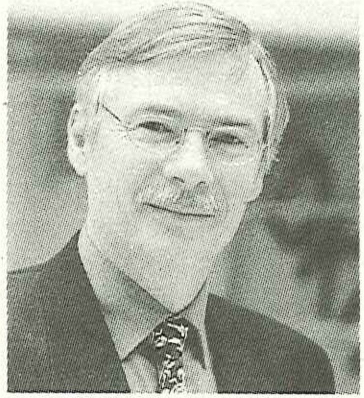
Udvalg:

Marketingudvalget (fmd.), Administrationsudvalget

Job:

Direktør for DKnet A/S

Den 49-årige Benny Michelsen er ny i DKUUG's bestyrelse, men en af veteranerne i den danske IT-verden. Unix har spillet en stor rolle i hans liv dels hos NCR, dels i hans mangeårige regeringstid som administrerende direktør for Control Data, der tidligt erkendte de proprietære systemers bortgang. Han er idag direktør for DKnet, hvor Unix' rolle blot er en underliggende teknologi.



Benny Michelsen er bredt anerkendt som fuldtids og fuldblods professionel. Diskussioner er en demokratisk nødvendighed, men på et tidspunkt må der trækkes en streg i sandet og træffes en beslutning som alle følger. Ellers bliver diskussionerne både ørkesløse og en parodi på den demokratiske beslutningsproces.

Denne evne til at trække streger i sandet har han. Uden at slå i bordet, men med en stor gennemslagskraft i kraft af en professionel distance. En distance, der til gengæld gør det svært for andre at finde personen inde bag jakkesættet.

Han er stærk som troubleshooter, men det er naturligvis også svagheden, at hans interesse falder, når først skuden er i smult vande og bare skal sejle ligeud.

Selv synes han, at det er svært at finde rette balance mellem det professionelle liv og privatlivet. Han tenderer mod at involvere sig i for mange projekter ad gangen.

Brian Eberhardt

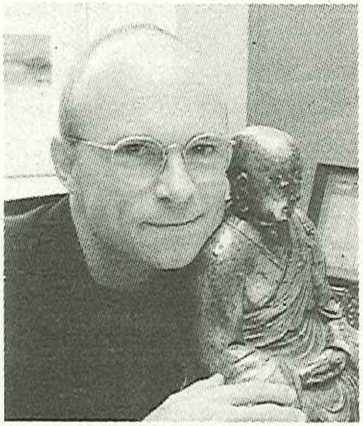
Udvalg:

Klubudvalget (fmd.), Medlemsmødeudvalget, Festudvalget

Job:

Adm. dir. SuperUsers a/s

For den 38-årige Brian Eberhardt vil den planlagte professionalisering af foreningen være en kærkommen udvikling, fordi dermed vil bestyrelsen kunne komme til at beskæftige sig med dét, der er bestyrelsers opgave: Strategi, de store linier.



Som det har været hidtil har bestyrelsesmedlemmerne af gode grunde brugt det meste af krudtet på at være praktiske grise, på foreningens daglige drift. Brian Eberhardt har siddet i bestyrelsen i en håndfuld år.

En af hans egenskaber er at kunne dykke ned i et stof og blive fuldstændigt opslugt af det - således mangler han et par år i 80'erne, mens han levede og åndede Unix på Regnecentralen - for så bagefter at vende tilbage til verden og konstatere, at andre har beskæftiget sig med alt muligt andet i mellemtiden.

Denne forsvinden fra omverden skyldes en grundmuret indstilling til, at opgaver ikke bare skal løses godt nok. Kunder og brugere kan med rette forvente noget mere end godt nok.

Han bruger meget tid på at vedligeholde sit tekniske fundament, men man stifter selvfølgelig ikke et firma som SuperUsers uden at være forretningsorienteret.

Her har hans stil som administrerende direktør forbløffet flere. At han kører Porsche er bare ikke udtryk for, at biler betyder særligt meget i hans tilværelse. Han er heller ikke buddhist, selvom man finder buddhaer både på hans kontor og i SuperUsers brochurer, men han værdsætter ro og omtanke, før han går ombord i projekter. Derfor indgår meditativ musik også i hans foretrukne fritidsbeskæftigelser som musiker.

Bjørn Johannesen

Udvalg:

Bladudvalget (fmd.), Medlemsmødeudvalget, Fora

Job:

Salgschef Vision International A/S

Den 46-årige Bjørn Johannesen er oprindeligt bankuddannet, men blev i sin tid som den ottende dansker også uddannet datanom, så han er en af veteranerne (det er stort set kun som soldat, man kan blive veteran tidligere) i branchen.

Idag er han sælger af ledelsesinformationssystemer, som han hævder faktisk kan bruges af ledere, der ikke tilfældigvis også er programmører, men tilbage i 1985 var han hos NCR, der med stor dygtighed angreb Unixmarkedet.

Gennem medlemsmøder og seminarer øjnede han i DKUUG mulighed for at møde ligesindede og en genvej til den nyeste viden om Unix, hvilket førte til både medlemsskab og bestyrelsespost.

De to elementer er den dag idag efter Bjørn Johannesens overbevisning DKUUG's eksistensberettigelse. Foreningen er »Vejen til viden om åbne systemer«, og den skal være et mødested for professionelle, hvor de kan pleje deres netværk af hensyn til sunde egeninteresser og af hensyn til deres job.

Et eksempel er WWW, som fagblade og aviser idag bruger spaltekilometer på, men for forbavsende få år siden var webben et spritnyt og ukendt begreb, der på dansk grund blev introduceret i DKUUG.

Bjørn Johannesen er en teamplayer. Bannerførere for 'sager' finder ham for udglattende, når han med sit altid positive væsen prøver at løsne op og kompromisse i en diskussion, der i hans øjne ikke rigtigt fører nogen vegne eller er ligegyldig i den store sammanhæng.

Bjørn Jørnvig

Udvalg:
Marketingudvalget, Fora

Job:
International technical manager, Unidata Inc.

Den 46-årige Bjørn Jørnvig har af gode grunde endnu ikke sat det store præg på foreningen gennem sine snart to år i bestyrelsen. Viljen er god nok, men han er sædvanligvis ude at rejse.

Bjørn Jørnvig er gammel databasemand uddannet hos Nixdorf i Tyskland. Efter en længere årrække som selvstændig har han de sidste fire år virket for det amerikanske databasefirma Unidata.

Her har han Europa, Afrika, Mellemøsten og Indien som jagtrevir, hvilket afspejler sig i 200 rejsedøgn årligt. Ringer man til ham, er der rimeligt god sandsynlighed for at fange ham med 180 i timen på en tysk Autobahn.

Også som person kører Bjørn Jørnvig i femte gear. Han er en mand med store armbevægelser og meget talende, men også teknisk velfunderet. Han har haft fingrene ned i materien og kan stadig programmere i en hastighed, hvor 10-fingerskrift er en nødvendighed.

Men han er ikke manden, der fuldfører alle sine ideer - det ville han heller ikke være uden de mange rejsedage - for han er altid på vej til næste projekt, som begejstrer ham, fordi nu er det dét, der er nyt.

Bjørn Jørnvigs bevæggrund til at gå ind i DKUUG var ret kontant: Den nyvundne formue skulle sikres mod et kup. Nu, hvor dette er overstået, er hans agenda at få realiseret Fora-ideen, at få NT endnu mere ind på banen og at gøre foreningen mere slagkraftig.

Kristen Nielsen

Udvalg:
Netforum (fmd.), Festudvalget (fmd.), Klubudvalget, Eksternt udvalg, Standardiseringsudvalget

Job:
Systemkonsulent, TeleDanmark Udvikling

Den 34-årige Kristen Nielsen er det næsten arketypiske DKUUG-medlem, teknikeren med fingrene helt nede i Unix og netværk hver eneste dag. Selv beskriver han sig som 'ikke nær så meget nørd, som jeg var engang'.

Men det er en dybtgående teknisk interesse, der sidste år fik ham til at gå ind i foreningens bestyrelse. Han vil sikre et fortsat levende miljø for hard core teknikerne i DKUUG.

Han er uddannet elektroniktekniker og har arbejdet gennem ni år på Sønderborg Teknisk Skole, der er et af DKUUG's mangeårige medlemmer. Her underviste han i blandt andet Pascal, C, Unix og hardware.

DKUUG's aktivitetsniveau i det sønderjyske er med en eufemisme ikke stort. Der skulle køres langt for at deltage i klubaftener, men det blev noget lettere for to år siden, da han kom til TeleDanmark i Høje Tåstrup, hvor han arbejder med intern edb. Parallelt med arbejdet læser han datalogi på universitetet som fritidsstudie.

Med studiet og med især klubben og Netforum plus naturligvis arbejdet går en ganske pæn del af hans vågne tid med IT, men hans interesser er blevet bredere. Blandt andet med regnskab og arrangement af ø-lejr på Skarø.

Som de øvrige bestyrelsesmedlemmer ser han lyst på tilværelsen med en kniv og gaffel i hånden, men har ikke udviklet samme søde tand. Endnu ihvertfald.

Peter Holm

Udvalg:
Medlemsmødeudvalget, Bladudvalget

Job:
Projektleder fra 1. april, Hewlett-Packard A/S

Det siges om den 41-årige Peter L. Holm, at han altid kommer for sent til møderne, og at møderne altid varer længere, når han er til stede, fordi han har en hel masse at sige og iøvrigt er en god taler.

Men det siges også, at han er god til at skære igennem med de mange ord. At han ofte siger tingene åbent på trods af eventuelle tabuer. Da det så samtidig sker med smittende humør og uden fordømmelse, er han bramfri uden at såre.

Selv betragter han ikke denne evne som en ubetinget stærk side, fordi det også er et udtryk for lovlig megen stædighed. Men somme tider skal der træffes hårde beslutninger i stedet for at køre rundt i en evindelig diskussion.

Peter Holm er civilingeniør af uddannelse, han har arbejdet på Uni•C, hos Danosi, ICL, SimCorp og er nu på vej til en stilling hos HP som projektleder indenfor netværks- og systemadminidtration.

Han har været medlem af DKUUG siden midten af 80´erne. Oprindeligt med en meget teknisk fokus, idag mest markedsrettet. Gennem en del år har han siddet i bestyrelsen, hvor han er en af de mere aktive.

For nogle år siden brugte han to kalendre. En til arbejde, en til fritid. Men istedet for at få mere struktur på den sparsomme tid bibragte det forvirring på et højere niveau, hvorfor han pensionerede systemet, som ingen siden har glemt

Peter Lange

Udvalg:
Medlemsmødeudvalget, Marketingudvalget

Job:
Markedschef, Sun Microsystems AB

Den 43-årige Peter Lange har været med i DKUUG fra den første spæde start, men er først gået ind i foreningsbestyrelsen for et par år siden.

Gennem de sidste 10 år har han arbejdet med Sun, idag som markedschef for Sun, og inden da hos ICL, der var distributør. Nogen betragter ham da også som Mr. Sun-DK. Længere tilbage i hans fortid finder man en periode hos Chr. Rovsing og en uddannelse som civilingeniør.

For Peter Lange er Unix en markedsplatform, men også en sag, og DKUUG et forum, hvor der både kan hentes og formidles information og budskaber til nøglepersoner i markedet. Det er også stedet, hvor netværket og de personlige interesser kan plejes.

I bestyrelsen står han sædvanligvis for bløde synspunkter uden at være synderligt kompromissøgende. Når andre svæver lovlig højt over jorden, disker han op med stille snusfornuft. Fagligt er han velfunderet, men teknik i sig selv interesserer ham ikke, teknik er et middel til at nå mål.

Herudover råder han over klassiske svagheder, der kvalificerer ham til DKUUG. Han siger aldrig nej til en god kage og er en kompetent deltager i studier af Medoc-vin, hvor han gerne forøger videnniveauet på ferierne i Frankrig. Bortset fra DKUUG bruger han fritiden på basketball samt familie og hus.

Keld Jørn Simonsen

Udvalg:
Formand, Eksternt udvalg (fmd.), Standardiseringsudvalget (fmd.), Medlemsmødeudvalget, Klubudvalget, Netforum, Bladudvalget, Administrationsudvalget, Marketingudvalget, Fora

Job:
Direktør, Rationel Almen Planlægning

For DKUUG's formand siden foreningens start, den 44-årige Keld Jørn Simonsen, er det nemmere at fortælle, hvilket af foreningens udvalg han ikke er medlem af: Festudvalget. Ellers har han smidt slæberne ind overalt.

På uddannelsesområdet har det også skortet med mådehold. Keld Jørn Simonsen er jurist, men han har også bachelorgrader i datalogi og økonomi.

Keld Simonsen er næsten vokset sammen med rollen som formand for DKUUG, en i princippet farlig cocktail, men engagementet og den arbejdspræstation, han lægger i foreningen, er næsten frygtindgydende. At DKUUG er, hvad DKUUG er idag, er i høj grad et produkt af hans indsats.

Han er særdeles kompleks som person. Han er en rigtig Unix-hacker med en formidabel teknisk indsigt, fundamentalist, fantast, vedholdende, men også en livsnyder med stor sans for livets mere behagelige sider og et hyggeligt og lunt rodehoved. Og dette udvalg af ord dækker kun en del af personen.

I kraft af denne mangefarvethed, men også i kraft af sin høje grad af synlighed i foreningen har han formentlig også lokal rekord i øge- og kælenavne.

❑

NC, din næste PC?

Per Andersen
IDC Scandinavia

Debatten bliver hedere og hedere omkring Netværkscomputeren (NC). Meget af debatten er forvirrende, idet det endnu ikke er klart defineret, hvad en NC egentligt er for et dyr. Og begrebet vil sandsynligvis fortsat udvikle sig over de næste 5-10 år.

I denne sammenhæng vil jeg definere en NC som en enhed uden disk, der ikke kører et traditionelt Windows operativsystem og som kan anvendes til Internet-opkobling. Således dækker begrebet over både traditionelle Internet-terminaler (fx Wyse WinTerm), Internet PCere med Intel-teknologi (fx Net-PC) og Internet PCere med andre processorer (fx Java-Station).

Tilbageblik

Det er interessant at se, hvordan debatten omkring PC contra NC har udviklet sig over det seneste års tid. Diskussionerne begyndte i september 1995 ved IDC's europæiske IT konference. Larry Ellison fra Oracle gjorde sig til talsmand for en billig, nem at anvende og nem at administrere ikke-PC enhed til brugerne, og gjorde i den forbindelse helt op med Wintel arkitekturen. Ved den samme konference gjorde Bill Gates nar af enhver tanke om at tilbyde noget mindre end en PC med komplet Windows funktionalitet.

Et år senere ved den tilsvarende konference fik Ellison selskab af Scott McNealy fra Sun, mens Gates fik selskab af Eckhard Pfeiffer fra Compaq. Men det overraskende var, at krigen syntes at gå i stå. Begge sider fastholdt selvfølgelig deres synspunkter, men var derudover enige om, at fremtiden vil have brug for både PCere og NCere - omend i konkurrence på nogle områder. Begge sider indrømmede, at hverken PC eller NC visionen kunne stå alene.

Jeg kan derfor allerede nu besvare spørgsmålet: Er NCen den næste generation PC? Svaret er nej. Der er ikke tale om den ene eller den anden teknologi, men snarere tale om to teknologier, der kommer til at supplere hinanden. NCen er ikke PCens afløser, men adresserer nye markeder, som PCen ville være dårligt egnet til.

Overraskende udtalelser

Ved 1996-konferencen kom der visse overraskende udtalelser fra både NC- og PC-siden. Gates og Pfeiffer indrømmede begge, at kompleksiteten af den traditionelle Wintel PC gør anvendelsen og administrationen forholdsvis dyr. Begge var enige om, at der er behov for en desktop enhed, der er nemmere at administrere og mere enkel i brug. De var også enige om, at fremtidens desktop marked sikkert ville have et betydeligt bredere udbud af forskellige enheder i forhold til i dag. Dette har så senere ledt til specifikationen af en Intel-baseret NetPC.

Fra NC-siden kom den mest overraskende udtalelse fra Scott McNealy på spørgsmålet om, hvornår der vil være Java-applikationer i samme omfang som til PC-applikationer. McNealy svarede, at der ville gå mindst 5 år inden der vil være Java-applikationer i noget betydeligt omfang.

En anden overraskelse kom fra Larry Ellison, der tidligere fokuserede på ikke-Intel processorer som drivkraft i NC markedet. Nu forudsiger Ellison, at langt den største volumen af NCere vil komme til at køre Intel processorer.

Dermed oplevede man næsten enighed om, at der i fremtiden kommer til at være et vist marked for NCere baseret på Intel-processorer. Spørgsmålene er så, hvor stort dette marked vil blive og hvad NCere først og fremmest vil blive anvendt til.

Salget af Internet-enheder i år 2000 (værdi worldwide)

PCere	850 mia. kr.
Internet PCere	7 mia. kr.
Internet terminaler	25 mia. kr.
Set-top bokse etc	20 mia. kr.
Total	902 mia. kr.

Figur 1.

Niche-marked

Det første marked for NCere vil først og fremmest være i virksomhederne. De fleste steder opererer man allerede med forskellige former af client/server applikationer, og vi begynder at se større og større interesse for anvendelsen af Intranet. Samtidig tilbyder flere og flere applikationer såsom SAP en HTML grænseflade til deres løsninger.

Dermed kommer der et marked for simple enheder, der ved hjælp af en browser udnytter applikationer og data i virksomheden. Områder, hvor denne anvendelse først bliver set, er hvor der er tale om en enkelt applikation såsom kundeservice. Det er steder, hvor der i dag anvendes en PC eller terminal, der stort set altid kører den ene, samme applikation.

På denne måde bliver NCen først og fremmest en erstatning for terminaler og PCere anvendt som terminaler. Idet der går lang tid inden der er NC software tilgængeligt i stort omfang, vil NCen ikke foreløbig blive en konkurrent for den traditionelle kontor-PC.

Omvendt tror vi ikke på en massiv udskiftning af terminaler med NCere. Langt de fleste terminaler fungerer i dag i et forholdsvis stabilt applikations-miljø, hvor der ikke er planer om drastiske ændringer i løsningerne.

Konsekvenserne er, at i hvert fald til den anden side af år 2000 vil NCere kun udgøre et lille niche-marked på linie med, hvad vi tidligere har set med X-terminalen. Dette fremgår også af IDC's forudsigelse af salget af Internet-enheder i år 2000 (figur 1).

God idé - også til PCere

Det er vigtigt at skelne imellem netværks-orienteret software og NCere. Netværks-orienteret software er designet til at minimere mængden af kode på skrivebordet, mens NCere er designet til udelukkende at køre netværks-orienteret software. Det er sandsynligt, at netværks-orienteret software, såsom programmer baseret på Java, vil vokse langt hurtigere end NCerne.

Årsagen til dette er ganske simpel: Mens NCen forudsætter netværks-orienteret software, kræver dette software ikke NCere! Netværks-orienteret software kan også køre på en almindelig PC.

Mange virksomheder vil bevæge sig hen imod brugen af mere og mere netværks-orienteret software, blandt andet for at opnå de økonomiske fordele ved lavere administrationsudgifter. Men dette vil ikke ske på én gang. Der vil i mange år være brug for at kombinere traditionelle programmer og de nye programmer, og den eneste mulighed er derfor fortsat at anvende PCerne.

PCen i ny forklædning

Der har været fremhævet to fordele ved NCen. Dels at den er lettere at administrere (contra en PC) og dels at den vil blive billigere. Sidstnævnte argument har været fremført, idet NCen ikke vil have disk eller hukommelse i samme omfang som en PC.

Dette førte i første omgang til ideen om en helt ny type enhed med en speciel processor og speciel design og arkitektur. Men når man ser på salgstallene vil en sådan forretningsmodel slet ikke hænge sammen. Udgifterne er nemlig først og fremmest til udvikling (fx af nye processor-generationer) og disse kolossale udgifter skal fordeles på det antal enheder, der bliver solgt.

Det er derfor en stor misforståelse at tro, at man kan producere en NC baseret på alternative teknologier langt billigere end en PC! Det kan man ikke.

Hvis NCen overhovedet skal have en chance, skal den være billig. Den eneste model for dette er at anvende så meget teknologi som overhovedet muligt fra PCerne. De succesrige NCere vil derfor være baseret på Intel-processorer og standard teknologierne omkring disse. Det er ikke utænkeligt at forestille sig, at Intel om kort tid vil starte en produktion af en "NC på et kort" lige som de i dag fremstiller SMP kort til servere.

Dermed vil Intel også ride på flest mulige heste: Hvad enten NCen eller PCen bliver dominerende vinder Intel!

Efter år 2000

Traditionelt forudsiger IDC kun markedet 5 år frem og med god grund. Når vi bevæger os ud til en tidshorisont på 5-10 år bliver det meget vanskeligt at spå om udviklingen. Ikke desto mindre vil netop denne periode 5-10 fra nu blive afgørende for NCens succes på lang sigt.

Årsagen til dette er, at hvis NCen skal blive en "rigtig succes" skal den vokse sig stærk på forbrugersiden - altså den private brug af Internet-enheder. Eftersom samfundet bevæger sig mod det "elektronisk integrerede samfund", hvor alle hjem naturligt bruger Internettet som en ny infrastruktur på linie med telefonen i dag, så kunne NCere i forskellige former bliver solgt til dette marked. Og dette marked er en størrelsesorden større end det traditionelle forretningsmarked.

Det kan derfor ikke udelukkes, at markedet i år 2010 ser helt anderledes ud, og at NCen bliver en succes i hjemmene. Hvis dette sker, vil der på dette tidspunkt være sket et dramatisk skift fra PCere til NCere som den mest anvendte konsumentenhed.

Et sådant gennembrud vil dog også være afhængigt af lokale forhold og den eksisterende brug af teknologier. Tager man et meget udviklet marked som det danske, vil penetrationen af traditionelle PCere i hjemmene i år 2000 være mindst 50%. Det er derfor vanskeligt at forestille sig, at PCere generelt vil blive afløst af NCere.

Anderledes forholder det sig i lande som Kina, hvor penetrationen af PCere i hjemmene er ganske lav. Her vil der ikke være nogen barriere fra eksisterende teknologier ved indførelse af NC-brug. Det vil derfor først og fremmest være i sådanne lande, at NCen har mulighed for at få succes i hjemmene.

❑

Det store Domæneslag

Søren Hornstrup
Product Marketing
DKnet A/S

Det er nok de færreste med interesse for Internet, der ikke har opdaget, at der er sket "noget" med domænenavnene på den "danske del" af Internettet: DK-zonen. Hvis man har fulgt lidt med i pressen den sidste måned, ja, bare læst lidt overskrifter, så virker det jo nærmest som om, at Internettets berømte kaos nu for alvor er sluppet løs. Og at ikke alene Internettet, men hele den danske handelsstruktur er brudt sammen, og de danske borgeres retssikkerhed er truet. Enhver ærlig dansk borger risikerer at blive overfaldet og plyndret af Domæne-pirater.

Jeg vil her forklare lidt om baggrunden for de nye regler for DK-domæner. Men først en kort introduktion til domænenavne og DK-zonens historie.

Domænenavne

Internettet er jo opbygget af en række selvstændige netværk. Der findes ingen central myndighed, der bestemmer over disse selvstændige netværk, men man er blevet enige om at benytte samme sprog til kommunikationen. Dette "lingua franca" er selvfølgeligt TCP/IP, og hvad deraf følger. En af forudsætningerne for TCP/IPs funktion er, at alle maskiner tilsluttet nettet har et helt unikt nummer, nemlig et IP-nummer. Ved at benytte disse IP-numre kan man kommunikere med alle maskiner på nettet. For ikke at løbe sur i IP-numrene opfandt man symbolske domænenavne og Internettets "telefonbog" DNS. Domænenavne er simple mnemotekniske navne på servere ("www.DKnet.dk"), der v.h.a. DNS (Domain Name System) kan oversættes til IP-numre (193.88.44.22). Et domænenavn er opdelt i delnavne adskilt af punktum: www.DKnet.dk. Hver af disse delnavne indikerer en såkaldt zone, hvori en række navne kan optræde (dk-zonen kunne indeholde f.eks. DKnet.dk, danfoss.dk, fls.dk osv. DKnet.dk-zonen kunne indeholde f.eks. serverne: www.DKnet.dk, mail.DKnet.dk, adm.DKnet.dk etc.). Ligesom IP-numre skal domænenavne også være unikke. Dette opnås ved, at der for hver zone udpeges en ansvarlig, der bl.a. skal sikre dette, den såkaldte hostmaster for zonen. Det sidste led i domænenavnet (her f.eks. dk) kaldes TLD (Top Level Domain), og bruges bl.a. til opdeling af serverne i tilhørsforhold til lande. F.eks. DK-zonen til danske servere. Denne lande-tilknytning er kun en ren konvention. DKnet i Danmark administrerer bl.a. servere, der hører under se-zonen (Sverige). Den ansvarlige hostmaster for hver TLD er udpeget af organisationen IANA (Internet Assigned Numbers Authority). TCP/IP applikationerne finder IP-nummeret, der svarer til et domænenavn ved at foretage en forespørgsel til nærmeste/lokale DNS. Denne kender egen zone og evt. nærmeste omgivelser. Hvis den ikke kender det søgte domænenavn, vil den videresende forespørgslen til en DNS, der tager sig af et højere niveau af domænenavne (www.DKnet.dk -> DKnet.dk -> dk), og finder derved præcist hvilket IP-nummer, den søgte server har. Normalt vil der højest skulle foretages 2-3 opslag, før IP-nummeret er fundet. Oplysningerne om IP-nummeret bringes derefter tilbage til de DNSere, der er spurgt, og her vil de blive gemt i en periode, så næste forespørgsel vil gå hurtigere, idet allerede første DNS giver svar på hvad IP-nummeret er.

DK-zonen

Siden etableringen af DK-zonen i 1988 har DKnet været ansvarlig DK-hostmaster, og har udført opgaven vederlagsfrit indtil 1996. Regler for og brugen af domænenavne i DK-zonen har DKnet traditionelt udfærdiget i samarbejde med andre Internet-brugere/udbydere. De først mange år blev reglerne aftalt i samarbejdsorganisationen Netsam (bl.a. DKnet, Uni-C og universiteter) og siden etableringen af Foreningen af InternetLeverandører i vinteren/foråret 1996, er det FIL, der har fastsat reglerne for domænenavne i DK-zonen. Det er i FIL aftalt, at DKnet skal fortsætte som DK-hostmaster indtil foråret ´98. DKnets varetagelse af DK-hostmaster funktionen overvåges og kontrolleres af FIL.

En hostmasters (herunder DK-hostmasters) opgaver er bl.a. at sikre, at strukturen og reglerne for zonen overholdes, at domænenavne er unikke, at DNS for zonen fungerer, og at registrerer brugerne af navnene i zonen.

Gamle regler

De regler, DK-hostmaster hidtil har skullet administrere efter, kan vel nærmest karakteriseres som værende fastsat af Internetildsjæle, der i regelsættet forsøgte at indbygge en retfærdighed for alle. Nogle af elementerne i regelsættene var:

1 Ikke sted- og personnavne (man forestillede sig, at man på et tidspunkt ville benytte disse til en adressestruktur for alle personer og byer i Danmark).

2 Et domænenavn pr. organisation (hvad skulle man bruge flere til, og så var der jo bedre plads).

3 Dokumentation af at man havde adkomst til navnet (så man ikke "hamstrede" navne, man ikke selv skulle bruge).

Disse regler blev så administreret af DK-hostmasters personale, og afgørelser blev kontrolleret af og anket til et udvalg nedsat af Netsam/FIL. Igennem en lang årrække har sådanne regler og en sådan administration fungeret tilfredsstillende. Men med Internettets voldsomme vækst og med den øgede kommercielle interesse blev det sværere og sværere for DK-hostmaster at undgå konflikter omkring, hvilke navne der var tilladt, og hvem der havde mest ret til navnene. Allerede i ´95 var der en del problemer, og gennem hele ´96 har DK-hostmaster haft klagesager dagligt, og ankeinstansen er blevet voldsomt belastet. Mange klager drejede sig om, at virksomheder ikke havde mulighed for at sikre sig anvendelsen af f.eks. varemærker som domænenavne.

Det var tydeligt, at reglerne måtte revideres, dels for at tilpasse sig de øgede krav, men også for at sikre, at DK-hostmaster og FIL ikke pådrog sig ansvar og e.v.t. erstatningspligt. DK-hostmasters/FILs afgørelser kunne f.eks. risikere at blive omstødt af en domstol. Nogle typiske sager kunne være:

1 En virksomhed havde fået godkendt et domænenavn og haft det i brug igennem en periode. En anden virksomhed ønsker senere samme domænenavn, og har f.eks. registreret navnet som varemærke. Kan /skal DK-hostmaster fratage den oprindelige domænebruger navnet?

2 To forskellige virksomheder kan have registreret samme navn som varemærke i forskellige grupper. Hvem af dem skal så have ret til navnet? Den største? Den ældste? Den kendteste? Den første? Den med flest varegrupper?

3 Repræsenterer en organisation f.eks. en branche tilstrækkeligt bredt til, at de skal have dispensation til at få branchenavnet som domænenavn. Eller vil en anden organisation/virksomhed kunne føle sig forfordelt?

4 Er et varemærke mere eller mindre end et virksomhedsnavn? Dette er bare nogle få af de sager, DK-hostmaster og ankeinstansen måtte tage stilling til. Som det kan ses, var en ændring og tilpasning nødvendig.

Nyt regelsæt pr. 15. januar 1997

Hverken FIL eller DK-hostmaster har grundlag for at påtage sig at udøve en kontrolfunktion og et evt. erstatningsansvar i relation til, om et ønsket domænenavn kunne krænke tredjemands rettigheder. Præcis som det er tilfældet ved registrering af selskabsnavne, er der med de nye regler lagt op til at eventuelle krænkede rettigheder henvises til retssystemet. Dette er i overensstemmelse med, at INTA (The International Trademark Association) i en udtalelse anbefaler, at Internetleverandørene begrænser sig til at registrere domænenavne, og overlader løsningen af tvister til domstolene.

Der har været forslag fremme, om at lade eksisterende regler for varemærker, selskabsnavne m.m. gælde for domænenavne. En sådan løsning kan ikke benyttes. Dette skyldes blandt andet den manglende entydighed i varemærker sammen med, at domænenavne kun kan indeholde bestemte tegn og har en maksimal længde, ligesom der ikke skelnes mellem store og små bogstaver.

For at imødegå piratopkøb af domænenavne i DK-zonen, det vil sige domæneoprettelser alene foretaget for senere at blive videresolgt til selskabs- eller varemærkeindehaver, har FIL i de nye regler indføjet et krav om en erklæring på, at tredjemands-rettigheder ikke krænkes. Kontrollen af dette er dog alene domstolenes.

FIL har også overvejet men afvist, at der blev etableret et nævn eller ankenævn til behandling af tvister. Enhver tvist kan føres igennem til domstolene, og kan derfor efter en ankeafgørelse inddrage FIL eller DK-hostmaster som part i sagen.

Overvejelser omkring at lade en offentlig instans stå for hostmaster funktionen har også været inddraget, men er blevet afvist som upraktisk og fordyrende. DK-hostmasterfunktionen er, udover selve navneregistreringen, også en teknisk funktion, der står for driften af en primær DNS og mindst en sekundær DNS som backup for DK-zonen. En sådan drift kræver teknisk kompetence, døgnovervågning og gode, sikre Internet-forbindelser. Dette betyder, at Internet-leverandører er de nærmeste til at udføre denne opgave. Samtidig er det et krav, at domænenavne tildeles entydigt, hvorfor DK-hostmasterfunktionen nødvendigvis må placeres hos én og kun én Internet-udbyder. Og da kontrollen og overvågningen af hostmasterfunktionen foretages af konkurrerende Internet-udbydere, er der en garanti for fri konkurrence, idet disse vil være de mest kritiske og have mest indsigt.

Hvad gør jeg for at registrere et domænenavn?

Gennemlæs regler og vejledning f.eks. på siderne:

- http://www.nic.dk/regler.html
- http://www.nic.dk/dkvejl.html

Undersøg om domænenavnet er optaget vha.:

- http://www.DK.net/nic/resIPno.html
- http://www.ripe.net/db/whois.html

Henvend dig til en Internetleverandør f.eks. DKnet, og forhør dig om, hvordan deres procedurer for domæneoprettelser er. Hos DKnet kan man enten rekvirere en formular pr. telefon, eller man kan hente den på:

- http://www.DK.net/dknet/registrering.html

og skrive den ud.

Formularen udfyldes, underskrives og faxes eller indsendes pr. brev. Vær opmærksom på, at reglerne siger, at domænenavnet skal tages i brug. Dette betyder, at der skal konfigureres en fungerende DNS server. Hvis ikke du selv kan eller vil opsætte en sådan DNS, har DKnet et tilbud, hvor vi vederlagsfrit indtil 1.7.97 opsætter og driver DNS for et sådan domæne.

DK-hostmaster fremsender derefter et registreringsbevis til Internet-leverandøren (DKnet), der så videregiver den til dig som bevis på, at domænenavnet er registreret med dig som bruger. Prisen for oprettelse af domæne varierer fra udbyder til udbyder, og kan være en del af den samlede Internet-ydelse. FIL har på nuværende tidspunkt fastsat følgende gebyrer:

- Vejledende gebyr for anmeldelse:
  Kr. 995,-
- Vejledende gebyr for rettelser og overdragelser:
  Kr. 600,-
- Årlig afgift for domænenavn:
  Kr. 0,-

DKnet følger de vejledende priser

Jeg håber, at ovennævnte har sat nogle af problemstillingerne omkring domænenavne og DK-hostmasterfunktionen i relief og gjort dem forståelige således, at det røre, der er i medierne, kan ses i rette perspektiv.

❑

Klubaften i København

DSDM — en nyhed på metodesiden

Myanne Olesen
DSDM Consortium Denmark

Tirsdag den 25. marts
kl. 19:00
Datalogisk Institut (DIKU)
Universitetsparken 1

Administrative såvel som teknisk tunge applikationer har som regel en identificerbar grænseflade ud mod forretningen og brugerne, og kontakten hertil forløber sjældent smertefrit. Fortvivl dog ikke, selvom du hører til den udskældte race af software-udviklere, der angribes for at være ude af trit med forretningen og for ikke at levere det, der ønskes, indenfor de udstukne rammer (tid/bemanding).

Svaret er hastig udvikling, Rapid Application Development (RAD), hvor processen forløber som beskrevet i Dynamic System Development Method (DSDM). DSDM er en ikke-proprietær metode, der på mindre end et år har fjernet det dårlige ry omkring RAD og er blevet-defakto-standard for forretningsorienteret udvikling.

Kort fortalt fordobler DSDM produktiviteten ved udvikling af nye systemer, muliggør levering af projekter til tiden, eliminerer unødvendigt bureaukrati og giver den løsning, som brugerne ønsker - hver gang.

Kom og check min troværdighed :-)

Vel mødt!
Myanne

Encryption and interception

Mads Bryde Andersen
University of Copenhagen
and
Peter Landrock
University of Aarhus & Cambridge University

The problem

The need for data security

Electronic data interchange has become an integral part of life in the information society. A substantial part of business and personal data is transmitted in open networks - either cabled or airborne (for example via satellites, microwave connections or in digital mobile telephone networks). In these networks the information can often be accessed easily by physical means. While interference via cable connections normally leaves a trace (for example by logging of calls), tapping of unprotected data- or fax-communication via modem is in principle simple to carry out, and leaves no trace.

As businesses increasingly depend on digital information, they become proportionally vulnerable to disclosure of trade secrets. In electronic commerce (contract formation by EDI and electronic payment), the consequences of a security flaw may be fatal, their damages often measured as the costs of the transactions in question.

Although in most countries interference or tapping of telecommunications is a violation of criminal law, it has become a regular sport in certain circles to engage in hacking activities. Some courts have taken a quite tolerant view of such crime forms by rendering suspended sentences for hacking. For these and other reasons, there is a profound need to secure data against theft and manipulation.

Integrity of data

Data communication must be secured against outside manipulation of transferred messages. Communicating parties who engage in business transactions may as well need to secure the authentication of their communication; that is parties should be able to establish the identity of the sender at the receiver's end in a secure manner. Even stronger is the need for non-repudiation; that is certainty that a communicating party can not deny having sent a message with a specific content. It must also be possible to produce evidence in court as to who sent the message. And last but not least, the confidentiality of communication must sometimes be secured.

Encryption as a tool

The only way to protect the integrity, authenticity, nonrepudiation or confidentiality of data communication, is by using cryptographic functions. The object of protection is a bit-string which is sent through an unprotected network, typically without guarantee of origin. However, when encryption is used for confidentiality purposes, problems of quite a different nature than those related to communication security arise. Whereas encryption may be used to conceal information, law enforcement and perhaps essential parts of government intelligence activities may be obstructed. Investigating authorities often face difficulties when suspects have locked written communication by encryption, as is already the common practice among hackers. Furthermore, it is also practice to keep lists of accomplices, essential to unravel criminal cases, in encrypted form on Personal Digital Assistants (PDA's).

Just as in the case of organised business, criminal and subversive activities also need effective and secure communication. A substantial part of investigation of drug related crimes is surveillance and ransacks. If encryption is allowed, criminals and criminal organisations deprive the investigation authorities of one of their most important tools.

Therefore, the need for businesses and individuals to secure communication by encryption and the need for governments to be able to intercept communication has created a confrontation between two valid interests. The balancing of these fundamental interests has already given rise to political discussions in various forums as well as to some legislative initiatives.

In this article, the following problems will be presented. For the benefit of readers not aware of the technical problems, we first present the fundamental principles of cryptographic techniques in part 2. We then focus in part 3 on the ruling view on public-key systems, which provides encryption facilities - and with that the possibility for concealment - in open networks. In part 4 - 5, we address the legal principles which have been applied until now and suggest some new possible paths for solving the problems outlined.

The technical aspects

The history of cryptography

The history of cryptography up until the second half of this century is a part of military history. Encryption (or enciphering) was a technique employed by masters of war and diplomats (not to mention lovers, of course). By enciphering, the sender could control with whom he would share a secret by giving only a specific number of recipients the key to decipher his information. Information and calculation power have always been vital for the security of encryption techniques. It is no coincidence that the digital computer was created in military research environments during World War II, and that even today some of the leading cryptologists in the world originate in countries which have often been at war.

Cryptography has been deployed in virtually all cultures and countries with a written language. The historical methods fall into two categories: encoding and encryption. By encoding, each word is typically replaced by another word which can be looked up in a code book shared by the transmitter and the recipient. In contrast, encryption requires a shared secret key that determines how a character is encrypted, by means of substitution and transposition.

Conventional crypto-systems

One of the classical examples of encryption is Caesar substitution: Every letter in the plaintext is replaced by the letter found a fixed numbers of steps forwards in the alphabet (repeating the alphabet after the last letter). The "key", being the number of steps required, also indicates the number of steps to go backwards in order to decrypt the information. This is the characteristic property of a conventional system: The same key is used for encryption and decryption. Such systems are also said to be symmetric.

The public key concept

With the introduction of data transmission, research and development of crypto-systems accelerated. At the end of the 1970's, a new concept was introduced, the public key concept, which formed the basis for so-called asymmetric systems. Here, two different yet matching keys are used. Given one of these keys, known as the public key, it is practically impossible to calculate the other key, known as the secret key. Every user may then generate his own key pair and publish his public key for use by his communicating parties, or communicate it to them in a secure manner, while at the same time keeping the other key secret. These systems have made it possible for parties to communicate together in a secure manner without ever before having met. Previously, they had to share a (one) secret key. Now, they only need to communicate their public keys, while the secret keys are kept secret and never communicated.

As an illustration of how this key-pair works, one may conceptually visualise the secret key as a means to translate the message from English into an artificial language only known by the key holder. The secret key is the dictionary by which the message is translated from English into the artificial language, while the public key is the adverse dictionary that translates the message back to English. Being the only holder of the dictionary into the artificial language (the secret key), the recipient of the encrypted information, who generates plain English text by using the "public" dictionary, is certain that the text was generated by the sender. Thereby, non-repudiation is provided. In principle, it may be possible to reverse engineer from one key (the public key) to the other (the secret key), namely by going through all the words of the "public" dictionary, one by one, but this method will be too time-consuming by selecting sufficiently large keys.

These crypto systems are of pure mathematical nature. Typically, they rely upon properties of prime numbers. The most widely used public key system is the RSA system, named by its inventors, Rivest, Shamir and Adleman. It was conceived at MIT in 1978. The underlying mathematical problem is that of factoring: Given two sufficiently large prime numbers, p and q, it is practically impossible with the methods known by mathematicians today, and the computational power available, from the product n of p and q to recover them, just given this product, in spite of the fact that they are uniquely determined from the product.

It is difficult to establish exactly where the borderline between secure and insecure is, but it seems to be approaching 250 bits. Factoring the product of two prime numbers of this bit-length today requires access to a large computer network of computers running in parallel. In contrast, prime numbers of this size can be generated on one computer, and even on a chipcard, in a matter of seconds.

Achieving confidentiality using cryptographic techniques

Public key schemes such as RSA are based on encryption-decryption methods and can therefore be used to obtain confidentiality: Encrypting under the public key will result in a ciphertext that can only be decrypted by means of the secret key, and vice versa. Since the processing of public key algorithms typically require substantial computer power, a combination of asymmetric and conventional crypto techniques is often applied. Rather than encrypting the whole message under the public key of the recipient, the message is encrypted using a fast, conventional system. The (conventional) key used for this is then encrypted under the public key of the recipient and forwarded with the ciphertext. The recipient first recovers the conventional key and then decrypts the message using this key. Confidentiality is achieved, but the recipient does not know the transmitter, or rather cannot prove anything about his identity.

Non-repudiation by cryptographic techniques

Public key techniques may also be used to achieve non-repudiation, as explained in the example above. By use of the secret key, the transmitter creates an encrypted text which can only be translated into something meaningful by means of the corresponding public key. When the public key translates the encrypted text into plain text, it is certain that it was created by means of the secret key, and if only one person in the whole world has access to that particular key, it is certain that he has created the encrypted text. He cannot thus successfully repudiate that the corresponding plaintext message originates from him.

The process of encrypting plaintext by use of the secret key is often referred to as digitally signing. It is important to note that digital signatures depend on and vary with the secret key and the plaintext. The process of applying the public key of the originator to recover the plaintext is called verification.

A technically different type of public key schemes can also be applied to generate digital signatures (signing) and verification without encryption and decryption. Again, a pair of keys is used: The secret key generates digital signatures, while the public key verifies them. But the difference is that the secret key and the plaintext are used to generate input for a mathematical equation, while the public key and the plaintext are used to verify this mathematical equation. Verification can thus only occur if the input was generated using the corresponding secret key. The original plaintext must be forwarded together with the digital signature, since it cannot be determined from the digital signature.

Hash values

To make the picture reasonably complete, we have yet to describe the technique of hashing. As already mentioned, public key schemes are very slow because they demand substantial computer resources. In public key encryption, this impediment can be overcome by generating a fingerprint, called a hash value. Hash values are used as input for the generation of the signature, rather than the message itself. The verifier, receiving the signature as well as the message, may also generate the hash value and then verify the signature by that.

A hash value is calculated by use of an agreed, publicly known mathematical algorithm. By use of that function, a bit-string with a certain, fixed length, typically somewhere between 64 and 160 bits (as short as possible to avoid overhead), is created so that it is practically impossible to find two different messages with the same hash value. Furthermore, given a hash value, it is practically impossible to recover any message with that hash value. For this reason, the hash value must be of some considerable length to prevent any attack since the number of possibilities amounts to 2 multiplied by itself as many times as the bit-length.

RSA vs. DSA

As explained above, we distinguish between (at least) two different public key schemes, depending on whether the public key can be used for verification and encryption, or for verification only. In the former situation, the system will allow for confidentiality, as is the case with RSA. In contrast, an algorithm as DSA (Digital Signature Algorithm, see vol. 56 FIPS, NIST Notices, 1991) can only be used for signing (i.e. generating a value using the secret key of the originator). The latter type of system is freely exportable from traditionally restrictive countries such as USA, UK and France, the former typically only for financial institutions. More on this later.

One more remark: By using tamper-resistant hardware which does not allow users to alter the functionality, one may use RSA as the underlying algorithm, yet ensure that the system cannot be used for encryption. This is the situation e.g. with IBM's realisation of RSA in their TSS PKA solution, where by using the digital signature standard ISO IS 9796, the result of the verification process using a public key is communicated as the values yes or no. In other words, there are no functions available in the system, directly or indirectly, which allow the user to encrypt "an arbitrary message" under a public key.

The way to the political agenda

As difficult as the schism between data protection and criminal investigation is, it has been similarly intricate to place the topic on the political agenda. With the widespread public awareness of privacy considerations (the ghost of "Big Brother" etc.) hardly any Secretary of Justice in a civilized country will find it easy to submit a proposal to ensure interception of citizens by prohibiting safe communication. As for intelligence interests, it is easy to understand the hesitation to disclose "working problems" in public.

The GSM net

With the GSM digital mobile telephone net, now in widespread use for microwave telephony as well as for data transmission, the schism between confidentiality and data security on one hand, and the interests of investigation authorities on the other, moved to the political arena for the first time. Airborne GSM data are automatically encrypted. Furthermore, interception of the communication between the cellular phone and the base transmitting station (BTS) requires certain steps in regard to each base station with which the cellular phone communicates. At that point, data are decrypted and transferred to the cable-based telephone network. Since the user will always communicate with the closest available BTS, conventional means to intercept cable-based telephone lines are not applicable. Furthermore, GSM telephony rises some practical legal problems. Criminal laws are only applicable within each jurisdiction - a problem which is increasingly urgent in relation to the enforcement of crimes committed via the Internet.

At a meeting in London, December 1992, within the EU police co-operation (formerly known as TREVI), European Secretaries of Justice decided to appoint a committee to investigate problems related to encryption on the GSM net - apparently with the purpose to develop general guidelines within the EU. Specifically, the interest focused on the possibility of identifying where in Europe a person is when he uses his GSM telephone. To the best of our knowledge, none of the results of the committee work has been published yet.

NSA develops DSA

As mentioned above, the public key system RSA enables users to provide confidentiality by encrypting information transmitted in open nets. This possibility has raised concern within the special investigation unit under the White House, the National Security Agency (NSA). The RSA algorithm, was patented in 1980 in USA, and the patent was until recently controlled by PKP Inc. Due to a dispute among the shareholders (MIT, Stanford, RSA Inc. and Cylink), PKP Inc. has now been dissolved.

In the late 1980's, NSA developed a new algorithm, called DSA, which has the property that it cannot be used for encryption. The algorithm is based on a variant of the so-called El Gamal algorithm from 1982 which applies the technique of so-called discrete logarithms. NSA has applied for a worldwide patent on DSA, a patent later accused of colliding with other patents (a patent on another variation taken out by Professor C. Schnorr from the University of Frankfurt and a fourth patent, which is also owned by PKP Inc.).

INFOSEC's Green Paper

In 1992 INFOSEC, the EU Commission's security program took up the task of working out a Green Paper on security needs in Europe. The Green Paper was published in the spring of 1994 as a draft to SOGIS (Senior Officials Group in Information Security), which has the formal responsibilities for INFOSEC program. The main purpose was to make a new action plan for security projects within INFOSEC. SOGIS is made up of officials from different countries, with only a few security experts. During the work on the Green Paper, it proved difficult to reach political consensus on the program. Some observers have indicated that the program is being controlled by representatives from the intelligence communities.

The Green Paper can be criticized for the lack of coordination between the different kinds of expertise represented in the working groups. At the outset, the goal was to cover the areas of digital signatures, encryption and the use of Trusted Third Parties. But the end result identified many more areas. The Green Paper (version 4.2) suggests that an algorithm with the characteristics of DSA be adopted or developed in Europe. Nonetheless, these drafts and contributions have not been well received and at the moment it still seems complicated to agree on a new INFOSEC action plan. As of January 1996, it is still not settled as how the INFOSEC program will be continued, although it looks as if the emphasis will be on trusted third party services in relation to Escrow-solutions (see below).

The inquiry from NSA and NIST

In the summer of 1993, SOGIS was contacted by NSA and NIST (National Institute for Standards and Technology) who wanted the DSA algorithm to become a standard for digital signatures in Europe and thereby an integral part of the European telecommunication architecture. The long-term goal seemed to be to ensure the development of common secure telecommunication networks - in the sense of applying digital signatures, but not addressing confidentiality - on both sides of the Atlantic. The additional benefit was that no royalties would be demanded from the patented DSA algorithm. At the same time, the use of DSA might restrict the European development of the much more "dangerous" (seen from an investigation point of view) RSA algorithm. The picture is much less clear now that DSA has been claimed to infringe on existing patents, and we have been told that the first case has been taken to court in USA against a non-government application in USA, although we have not been able to confirm the details.

The procedures in SOGIS bear worth a closer study. The EU involvement concerning data security is dominated by four members; the UK, France, Germany and the Netherlands. For many years, these countries have had vast intelligence interests and, as indicated below, two of them have introduced - or attempted to introduce - legislation prohibiting encryption. From an outsider's viewpoint it was not surprising that the US initiative was quite well received by SOGIS.

The negotiations with USA proved to be quite difficult because NSA decided to transfer its DSA patent to PKP Inc. at the same time. Being the holder of almost every patent on public key encryption, PKP Inc. claimed that the DSA patent violated some of these patents. As a result of the negotiations, NSA agreed to allow the US government and its communication partners to use the DSA on a license-free basis if PKP Inc. could hold the patent rights for DSA related to other applications. By this action PKP Inc. became the only DSA patent holder in Europe. SOGIS has temporarily given up the DSA. Rumours have it that the Clinton administration considers the deal with PKP Inc. a mistake, and now wants to renegotiate it.

The Clipper chip

Independently of the contact between NSA and NIST and SOGIS, the Clinton administration suggested on April 16, 1993, the confidential symmetrical Skipjack algorithm to be used for encryption. The algorithm has been implemented in a special chip, called the Clipper Chip, and has been developed for concealment in civil and commercial communication. The Clipper Chip is integrated into the terminals and is manufactured with an identification key, the master key, which is placed into escrow at two different public entities ("trusted third parties") in order to allow for lawful interception of communication. During a communication session, the chip first transmits the so-called law enforcement access field (LEAF). The LEAF is an encrypted version of the session key used for encryption of the message. The two escrow authorities now hold the escrow values which in combination with the LEAF segment, makes it possible to recover the session key, but not the masterkey itself. With a court order, it is then possible for authorities to intercept messages which are encrypted under the Skipjack algorithm (but not messages otherwise encrypted). If sufficient assurance can be given that this will only take place in the designed manner, one would think that opposite interests have been honoured in a fair manner. However, the practice for granting court orders seem to vary quite dramatically from country to country.

The US government has proclaimed that the Clipper Chip will not be the only legal means of encryption. Nevertheless, it is obvious that by introducing the Clipper solution to public administration, the Clipper Chip will have an excellent position against other encryption standards. The US Ministry of Justice has already ordered equipment worth of several millions of dollars. Other branches of the federal Administration are expected to follow. Export restrictions for encryption equipment based upon Clipper are also expected to loosen up. This official support to the Clipper project has not been well received by the computer vendors and users, who - probably rightfully - fear that the market will avoid encryption tools which make it possible for the governments to intercept communication.

Even though it is, in principle, easy to evade an enforced escrow solution by using a (self) chosen algorithm for encryption, one may ask if a solution la Skipjack/Clipper/escrow may not be acceptable in communication systems which are provided to the general public by government, and which automatically secures all communication by cryptographic techniques. In our opinion, there is a difference between on one hand - in the name of secrecy of mail - maintaining a right for any citizen to develop or buy tools for encrypting messages in a closed group of communicating partners, and, on the other hand in open communication nets to guarantee any citizen against interception according to court orders. We can therefore not join the highly emotional resistance against the Skipjack/Clipper/Escrow project which certainly does not - at present - imply any ban on or prohibition of private encryption.

The Council of Europe initiative

On September 11, 1995, the Committee of Ministers to Member States Concerning Problems of Criminal Procedure Law Connected with Information Technology under the Council of Europe issued Recommendation No R (95) 13. The Recommendation consists of three parts. Part one deals with search and seizure and establishes the principle that investigation authorities should be permitted to search computer systems and seize data under similar conditions as under traditional powers of search and seizure. The second part deals with Technical Surveillance. Paragraph 8 reads:

> "Criminal procedure laws should be reviewed with a view to making possible the interception of telecommunications and the collection of traffic data in the investigation of serious offenses against the confidentiality, integrity and availability of telecommunications or computer systems."

Furthermore, paragraph 10 on the "Obligations to cooperate with the investigating authorities", reads as follows:

> "Subject to legal privileges or protection, investigating authorities should have the power to order persons who have data in a computer system under their control to provide all necessary information to enable access to a computer system and the data therein. Criminal procedure law should ensure that a similar order can be given to other persons who have knowledge about the functioning of the computer system or measures applied to secure data therein."

Furthermore, section 11 reads:

> "Specific obligations should be imposed on operators of public and private networks that offer telecommunications services to the public to avail themselves of all necessary technical measures that enable the interception of telecommunications by the investigating authorities."

The provisions which has drawn most attention, at least in Denmark, is found within the fifth part of the document, entitled "The use of Encryption":

> 14. Measures should be considered to minimise the negative effects of the use of cryptography on the investigation of criminal offenses, without affecting its legitimate use more than is strictly necessary.

As it reads, the provision indicates that restrictions against the free use of encryption techniques may be introduced. The guidelines as such, however, neither force nor recommend member states to implement any specific encryption policy in national jurisdictions.

The SOGIS proposal

SOGIS is currently preparing of Proposal for a Council Decision in the field of security of information systems concerning the establishment of a Europe-wide network of Trust Third Party Services (ETS). The proposal will establish an action in the field of security of information systems with the aim to promote effective and practical security for information held, processed or transmitted in electronic form "without compromising the interests of the public at large or leading to the distortion of competition in the Community". Among the actions proposed is the development of a Europe-wide network of Trusted Third Party Services, accredited and/or licensed by the member states, with a view to offering the ability to use either digital signature and/ or message confidentiality in support of the full range of public information and telecommunications services and applications (including broadcasting services).

In the explanatory memorandum to the proposal, the role of encryption technologies is thoroughly discussed. It is stated that governments have a long tradition of controlling the availability of encryption technology for national security reasons in much the same way as other critical defence technologies, namely by export licensing regimes, but that controls of the use of such technologies are less common and, clearly, rather difficult to enforce in most western democracies.

The text, however, then goes on to say that the use of TTPs potentially solves the legal interception problem: In those cases where legal interception of the communications of a particular individual or telephone is authorised by an appropriate national legal process, the law enforcement authorities can then apply to the TTP for access to the targeted individual's private encryption key without his knowledge or cooperation, if necessary. The statement presupposes that users forward their private keys to TTPs, or that the key-pairs are generated within the TTPs. In many cases, this may not be so. Users may wish to generate their own key pairs (which is easily done by software products), and they may very well decide not to use TTPs to store and forward public keys. This is indeed the case in regard to encryption provided by use of the freeware encryption program called PGP. More on this later.

The OECD initiative

OECD has been one of the international bodies first to take up the problems of computer security and encryption. Reference to encryption as a tool for computer security is mentioned in the OECD Guidelines on information security. Upon the initiative of the United States, the organization summoned a meeting on global encryption policy in Paris, December 1995. Another meeting followed in May 1996, and a third one is scheduled to take place in Paris in June 1996. The works of these meetings are not public yet, but it is clear at this stage that there is a widespread understanding among many OECD member states that the problems facing investigation authorities due to encryption technology should be solved in cooperation between governments and the business community. It is also clear that the aim of the present consultations is to reach agreement on a set of non-binding principles on the use of encryption technologies.

Denmark's position

In the beginning of 1994, the Ministry of Justice set up an informal working group concerning interception of GSM communication. The working group is supposed to keep telecommunication agencies and legal authorities mutually informed about standing and future problems related to the interception of telecommunication due to the technical progress. In January 1995, the committee delivered its report to the Ministry of Justice. Based on its recommendations, certain initiatives have been considered at the national level.

In 1995, an IT Security Council was appointed by the Danish Minister of Research and Information Technology. One of its goals is to define a policy for the use of encryption and digital signatures. When this article goes into print (May 1996), the Council is in the process of adopting a policy on encryption.

PGP

Long before these projects were known there was a growing understanding among users that the freedom to encrypt information might soon be an option of the past. To ensure that encryption devices were widely available, the American citizen Phil Zimmerman in 1991 developed a software package known as PGP - Pretty Good Privacy. The package is based on the RSA algorithm and is intended for users of electronic mail on the Internet. Fearing restrictions in the free use of encryption tools, Zimmerman chose (or according to himself - somebody chose) to make the package available via the Internet as public domain. Today, PGP has become a de facto standard for encryption of electronic mail. PGP signed and encrypted files are often found with an accompanying message that the public key of the transmitter is available upon request.

Very quickly this de facto "export" of a strategic product put Zimmerman on collision course with another set of rules pertaining to public law that is the U.S. export control restrictions previously mentioned. According to press information, Zimmerman has been charged with violation of U.S. export control rules, and searches have been made against Zimmerman himself as well as Viacrypt and Austin Code Works - two companies working closely with Zimmerman on PGP. In the spring of 1996, however, all charges against Zimmerman were dropped. Zimmerman has now established a private company, PGP Inc., that will market encryption technology.

Conventional legal models

Having outlined the problem, its technical nature, and its political handling we will now discuss the ways that have thus been considered to solve the schism between encryption rights and interception possibilities.

Provisional restrictions

One solution may be to oblige providers of telecommunication services to maintain the technical capability to intercept communication. The need for this has grown with the distribution of digital telecommunication. In the days of analog telephones, this was not a serious problem. Anybody with a computer and appropriate software and with knowledge of what cables to tap could, by simple wiring, tap the communication in these cables. But with digital communication it is necessary to know the "language" (that is, standard or protocol) which, in different layers of the communication process, can translate digital bits into information. If tele-suppliers choose their own "language", this could make interception more difficult or even impossible. This is also so, if encryption is included. One may look upon the Clipper project as a first step in this direction. Although Clipper is a non-obligatory standard, its expected widespread use (at least from the outset) would give it considerable impact. But even if it will have such an impact, a sender could evade the "backdoor" of Clipper encryption by encrypting his information before it passes through the Clipper terminal.

Restrictions on use

From the outset, it may appear easy to prohibit the free use of encryption. But prohibitions of that kind may face political, technical and legal obstacles. Some commentators have claimed that a ban on encryption may violate principles of freedom of speech. It would be similar to prohibiting people to speak incomprehensibly or by means of "interpreters" from remote a location with a unique language. In any event, any proposal to ban encryption or to make it subject to licensing is likely to face substantial resistance among users.

In France, encryption for confidentiality purposes is only allowed by permission of the authorities, see Code of December 29th, 1990 (chapter III, article 28). Encryption tools can only be applied upon authorization by Service Central de la Security des Systmes d'Information (SCSSI). Similar legislation was proposed in the Netherlands in early 1994, but due to strong public pressure withdrawn. Lately the same discussion has arisen in Belgium. The latest development in France seems, however, to allow for encryption as long as the private key is made available to the law enforcement authorities.

In our opinion, problems experienced by the investigation authorities as a consequence of encryption techniques should not to be solved by banning. Firstly, a ban on encryption would be difficult to enforce because of the magnitude and complexity of modern digital communication. A user can hide his sensitive information as data which seemingly holds different information. Unlike a computer virus hidden in files, which can be detected by someone with sufficient insight, encrypted files cannot be detected definitely. It is relatively simple to camouflage an encrypted file in another digital material, apparently perfectly innocent. A trivial solution would be to store some random data, which, if the encryption algorithm is sufficiently strong, cannot be distinguished from encrypted data. A DAT-tape with rock'n'roll music can hold a number of hidden tracks with encrypted files, which can not be seen or heard when playing the tape, and which would only be spotted using considerable resources. With these countless numbers of possibilities to send "junk mail", investigating authorities will have an overwhelming job examining tapped data.

Secondly, a ban on encryption is likely to hit targets which were not intended to be affected in the first place. To justify legislation which prohibits encryption because of the threat from communication related to illegal activities, which otherwise cannot be investigated, is comparable to banning certain locks, because they make it more difficult to carry out search warrants. If we give precedence to the interests of investigating, we would question one of the most effective methods to provide data security. Even an attempt to distinguish between cryptographic techniques used for confidentiality and those used for all others - typically authentication related services - would impose prohibitive restrictions on sound and reasonable intentions.

Thirdly, it is difficult to see how a ban on encryption could be enforced in practice. Envision this situation: The police is tracking down a drug lord and attempting - unsuccessfully - to tap his communication. What should authorities do when they realise that he uses encryption? Threatening with sanctions will immediately signal what means of communication the suspect should not use if he wants to remain at large! Moreover the - presumably lenient - punishment one will face for violating a ban against encryption probably will have a limited impact on the offender committing serious crimes.

For these reasons, we strongly advise not to introduce any bans on encryption. The results achieved are too moderate and the price too high.

Licence restrictions

A third angle could be to use Intellectual Property Rights (IPRs) like patents and copyrights to control the use of encryption. However, the U.S. experiences regarding the public key patents seem to indicate that this solution is not very easy to implement. Furthermore, in order to control encryption by intellectual property means, there have to be such protection for the encryption technology in question. This is far from so. Patents for algorithms are not available in all jurisdictions and if they are, they will expire sooner or later.

New approaches

The history of encryption policy teaches us that traditional legal and political measures tend to fail: An outright ban against encryption is difficult to enforce and has therefore only been attempted by very few jurisdictions. Export control schemes are only applicable in regard to international transactions, but will not apply to national applications. The same could be said of other means that eventually lead to enforcement of specific requirements against communicating parties. Consequently, interception of live communication between communicating parties who use their own encryption techniques is not a real option.

If one accepts this, the discussion for and against encryption legislation should be replaced by a discussion on the legislative problems regarding the role of tele-operators and other trusted third parties in relation to their use of encryption and of use of encryption technologies (key management etc.).

There is no doubt that the GSM problems have caused the present urge for a global encryption policy, as seen with the OECD initiatives and in other frameworks. But the GSM problems are only to a slight degree caused by encryption. Closer examination of the issue reveals that obstacles against interception of GSM communication have nothing to do with encryption but with the fact that GSM terminals (i.e. GSM phones) are connected to an unknown set of base transmitting stations, whereas traditional cable phones connect to a fixed terminal point. The only encryption technique in the GSM net takes place in the air segment between the terminal and the BTS. There is no encryption in the cable segment and the location of this segment is known "in real time", for control and billing purposes. Therefore, there are only technical obstacles against interception.

It is, therefore, more adequate to say that the problems facing the investigating authorities in the GSM net are technical and financial, due to the extra costs involved in building interception facilities upon telecommunications standards that were never aimed at such functions. The "shock effect" caused by the obstacles of intercepting GSM communication should not form the paradigm for a general encryption policy regarding internet applications.

To conclude, we will present some thoughts that might work as alternative means for investigating authorities to catch up with the problems caused by the widespread use of encryption techniques on the internet.

Telecom providers

As a first suggestion, one could consider a proposal whereby future digital communication standards should be designed to allow interception or that telecommunications providers should not be allowed to implement encryption of telecommunications traffic with the effect that interception be made impossible or excessively costly. Such a rule would not prevent communicating parties from encrypting their own traffic (since, as already mentioned, such a ban would be impossible to control), but it would solve the problems that we have seen in the GSM net and that we might face in future digital nets, such as DCS 1800 and others.

Reversal of proof

Another angle is to consider how encrypted information should be dealt with under rules of evidence. In an article in the Danish legal journal "Juristen" (vol. 1995, p. 306 and subseq.), we have suggested that Danish courts, when exercising their power to determine what is "proper evidence" (cf. section 896 of the Danish Court Procedures Act), should take into account whether a party has made offensive use of encryption techniques to conceal information that could otherwise prove him guilty of an offence. In the said article, we proposed that a principle of "reversal of proof" should apply in cases where three conditions were met: First, circumstantial evidence suggest that a person is guilty of an offence. Second, there is a substantial likelihood that the defendant has encrypted information that might provide evidence of guilt. And third, the defendant is in a position to decrypt that information and thereby free himself of any allegation, but decides not to.

It must be admitted that the said proposal may be difficult to accept within certain jurisdictions, among them those where the weight of evidence is determined by rules. Another argument against it may be that the proposal is in conflict with fundamental principles of fair trial, including the ban against self-incrimination in article 6, subsection 2, of the European Convention on Human Rights. Such objections are certainly reasonable to raise, but when considering their weight, it must be borne in mind that in regard to fundamental human rights principles, we are dealing with a delicate balance of interests.

To illustrate the flexibility by which Danish courts have modified the ban against self-incrimination, a 1990 decision by the Danish High Court of the Eastern Circuit may be considered (UfR 1990.866): A Danish taxpayer had moved all his assets to a tax haven where no accounting obligations applied. Being continuously taxable in Denmark, the Danish Tax authorities claimed that he had committed fraudulent tax evasion by not reporting the proceeds of these assets. Despite this claim, the tax-payer refused to give any accounting information regarding his foreign assets. Notwithstanding the self-incriminating principle ("the right to remain silent"), the High Court held that the tax payer was guilty of fraudulent tax evasion. Not only should he therefore had paid tax based on an estimated income figure, he was also punished (and that is the interesting part of the case) for not having reported that figure.

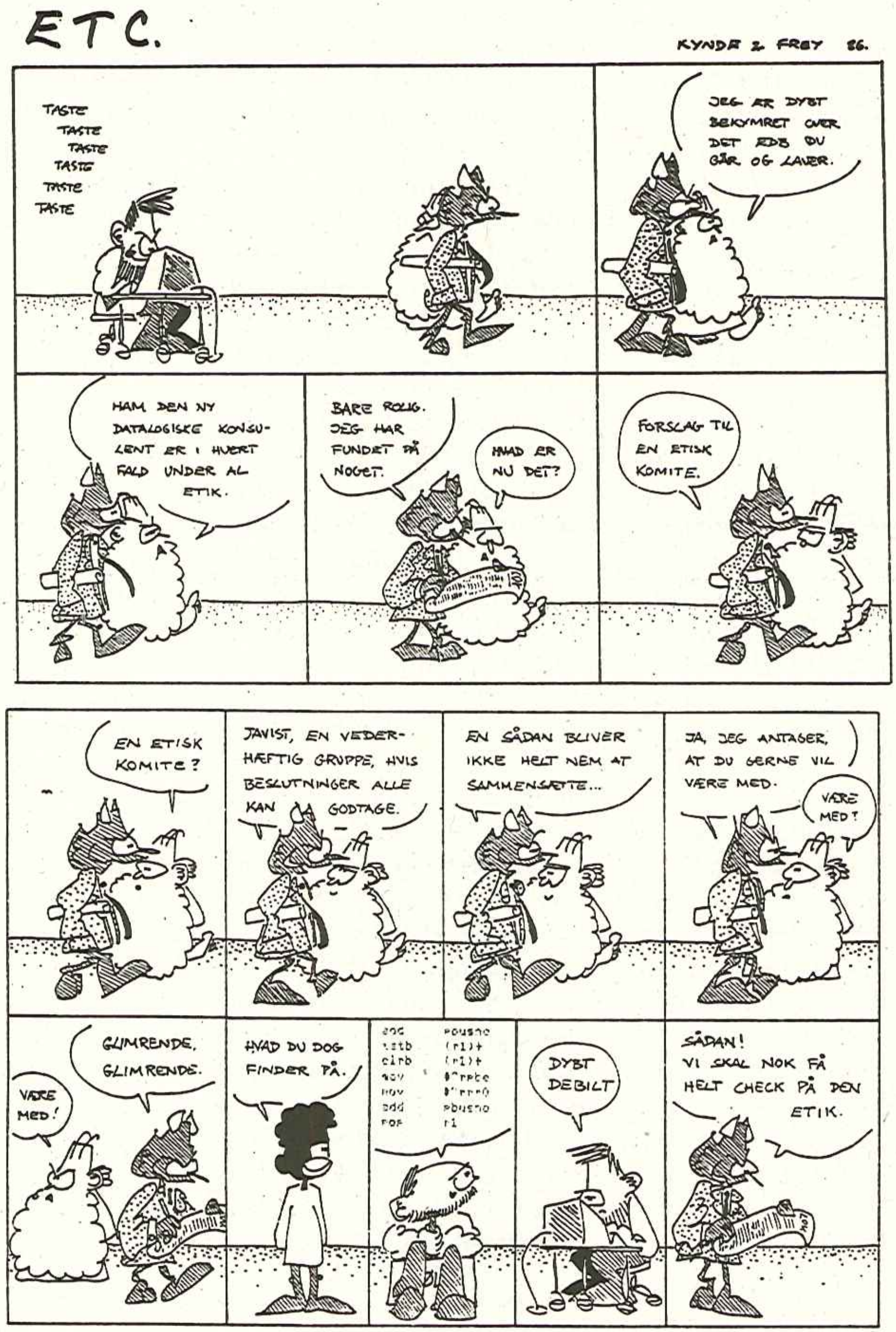
We find it adequate to draw a parallel between the tax haven case and the problems facing investigating authorities when crucial information is only available in encrypted form. A parallel case would be the following: In the unravelling of a drug cartel, police finds that all information communicated by a telephone line known to belong to one of the key figures are encrypted. It is known, however, that the telephone line has only been used to plan transactions to parties that are known to be in the business of purchasing and selling drugs. If the suspect is not willing to hand over encryption keys or otherwise make it plausible that the communication with the said parties had legitimate purposes, one might consider a reversal of proof.

An obligation to store communication

A third path, perhaps primarily for consideration in regard to administrative obligations within special legislation, would be to oblige communicating parties to store communications and encryption keys under certain conditions. Such obligations are commonplace within tax legislation and in regard to certain control schemes (among them regarding environmental legislation). But there is no absolute or relative limit as to what areas of legislation such rules might apply.

These three suggestions are not only meant for discussion. They are made here to indicate that the balancing of interests between the right to communicate by way of encryption and the possibilities of investigating authorities to carry out their work, is not a question of either or. Many other proposals should be taken into account. But one thing is certain: There are no easy answers. Neither seen from a political nor a legal perspective.

❑


ETC.
KYNDE & FREY 86.
TASTE TASTE TASTE TASTE TASTE TASTE
JEG ER DYBT BEKYMRET OVER DET EDB DU GÅR OG LAVER.
HAM DEN NY DATALOGISKE KONSULENT ER I HVERT FALD UNDER AL ETIK.
BARE ROLIG. JEG HAR FUNDET PÅ NOGET.
HVAD ER NU DET?
FORSLAG TIL EN ETISK KOMITE.
EN ETISK KOMITE?
JAVIST, EN VEDERHÆFTIG GRUPPE, HVIS BESLUTNINGER ALLE KAN GODTAGE.
EN SÅDAN BLIVER IKKE HELT NEM AT SAMMENSÆTTE...
JA, JEG ANTAGER, AT DU GERNE VIL VÆRE MED.
VÆRE MED?
VÆRE MED!
GLIMRENDE. GLIMRENDE.
HVAD DU DOG FINDER PÅ.
doc pousnc
tstb (r1)+
clrb (r1)+
mov $^rpte
mov $'rrr0
add pbusno
pop r1
DYBT DEBILT
SÅDAN! VI SKAL NOK FÅ HELT CHECK PÅ DEN ETIK.
MOT

Introduction and Advanced Cryptography

One-Day Technical Seminar

Symbion den 23. marts.
Bruce Schneier.
Forfatter til biblen indenfor kryptering:
Applied Cryptography.

Program udsendes særskilt, men sæt allerede nu kryds i kalenderen.

Kryptering er mere aktuelt end nogensinde, ikke mindst i forbindelse med betaling via Internet samt USA's holdning til området.

Seminaret er delt i to: Introduktion til kryptering efterfulgt af avanceret teknologi hvor også fremtiden indenfor krypteringsalgoritmer belyses.

Deltageren lærer krypteringens rolle i et totalt sikkerhedskoncept og henvender sig til personer med interesse for sikkerhed, system- og netadministration, udviklere og andre professionelle IT medarbejdere.

Emnet er mere aktuelt end nogensinde, ikke mindst i forbindelse med betaling via Internet.

Gå ikke glip af denne enestående chance for at møde Mr. Cryptography.

DKUUG-Nyt udgives af:
Dansk UNIX-system Bruger Gruppe
DKUUG, sekretariatet
Fruebjergvej 3
2100•København Ø
Tlf. 3917 9944
Fax 3120 8948
Email: sek@dkuug.dk
Man - fre kl. 9 - 16.00

Redaktion

Gitte D'Arcy (ansv.)

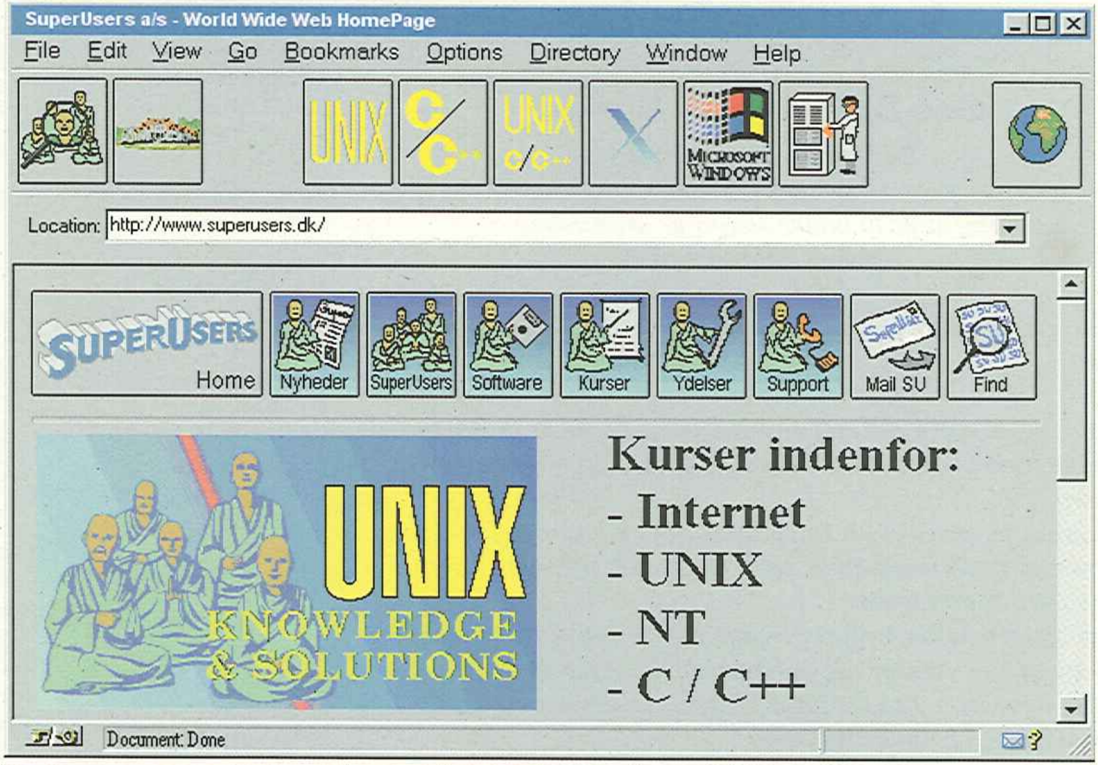
DKUUG-Nyt
Fruebjergvej 3
2100 København Ø
Tlf. 3917 9944
Fax 3120 8948
Email: dkuugnyt@dkuug.dk

Deadline

Deadline for næste nummer, nr. 92, er fredag d. 21.03.97

DKUUG-Nyt
ISSN 1395-1440

❑



SuperUsers a/s - World Wide Web HomePage

Location: http://www.superusers.dk/

Kurser indenfor:
- Internet
- UNIX
- NT
- C / C++

Document: Done

INTERNET	MAR.	APR.	MAJ	JUNI/JULI.	AUG.
SU-070 Internet Grundkursus	13-14/3		15-16/5		28-29/8
SU-075 Internet Systemadministration	20-21/3		22-23/5	3-4/7	
SU-071 Internet Videregående		17-18/4		19-20/6	
SU-086 WWW Java Basics		14-15/4		16-17/6	25-26/8
SU-087 WWW Java Advanced		16-17/4		18-19/6	27-28/8
UNIX / NT					
SU-100 UNIX Grundkursus	3-6/3	7-10/4	12-15/5	9-12/6	4-7/8
SU-110 UNIX Systemadministration Grund.	3-6/3	7-10/4	12-15/5	9-12/6	11-14/8
SU-500 NT Grundkursus	13-14/3	10-11/4	1-2/5	2-3/6	14-15/8
SU-510 Supporting Windows NT	10-13/3	14-17/4	20-23/5	9-12/6	4-7/8

Få den nye 1997 Kursuskalender

Samt SuperUsers a/s 244-siders hovedkatalog

EMAIL: katalog@superusers.dk
URL: http://www.superusers.dk

SuperUsers a/s
Karlebogaard
3400 Hillerød
TLF: 4218 0706
FAX: 4218 0705