Institutionen för Data- och Systemvetenskap

STOCKHOLMS UNIVERSITET

KUNGLIGA TEKNISKA HÖGSKOLAN

Bidrag till IT-kommissionens hörning om
”Etik på nätet”
från Jacob Palme
Senast ändrat: 98-05-23 17.22
Detta dokument finns på URL
http://www.dsv.su.se/~jpalme/society/etikteknik.html

Etik på nätet

Tekniska åtgärder

1.1 Motverka anonymitet

Om man vet vem som gjort något, kan man försöka påverka denna person att ändra sitt beteende. Den som är anonym, gör ibland under skydd av anonymiteten saker som han/hon inte skulle göra annars. Men möjligheten till anonymitet på nätet kan också ha fördelar: Det kan leda till större öppenhet vid diskussion t.ex. om personligt känsliga saker eller om missförhållanden, som man inte vågar berätta om annars.

Anonymitet motverkar man genom att kräva att folk identifierar sig. Tre viktiga tekniker är:

Elektronisk identifiering	Datorn kontrollerar vem en person är.
Behörighets-kontroll	Bara personer med behörighet får vidta vissa åtgärder. Elektronisk identifiering används för att kontrollera behörigheten.
Elektroniskt sigill	Ger möjlighet kontrollera att ett dokument inte blivit förvanskat på vägen, utan ser ut som det gjorde när det skrevs.
Elektronisk signatur	Garanti att ett dokument skrivits av den uppgivna författaren.
Elektronisk försegling	Ger skydd mot att ett dokument läses av andra än de som får läsa det.

Det finns olika varianter av teknikerna. En vanlig metod för identifiering är t.ex. lösenord. Den metoden ger dålig säkerhet och brukar kallas för ”svag identifiering”. Med kryptografiska metoder baserade på tillräckligt långa krypteringsnycklar (64/120 symmetriska eller 1024/2048 assymetriska) kan man åstadkomma hög säkerhet. Identiferingsmetoder, baserade på långa nycklar kallas t.ex. för stark identifiering.

Dessa tekniker har varit kända länge. Trots det används de för det mesta inte. E-post är t.ex. mycket lätt att förfalska. Varför används inte dessa tekniker?

1. Kanske är behovet inte så stort? E-post brukar ju fungera bra ändå.
2. Bäst är att lagra krypteringsnycklarna på så kallade smarta kort. Men det kräver att de datorer man använder har läsare för smarta kort, och folk är inte beredda att betala kostnaden för detta.
3. Säkerhetsmetoderna fungerar bäst om det finns ett system av s.k. certifikatservrar. Att bygga upp sådana system är komplicerat, och kräver centraliserade lösningar, som användarna inte är beredda att betala för.
4. Man har haft svårt att ena sig om standarder. Just nu konkurrerar två standarder, S/MIME och PGP. Ingen av dem är ännu allmänt accepterad. Säkerhetsåtgärderna fungerar bara om alla parter använder samma standard.
5. De är inte 100 % säkra: Snabbare datorer i framtiden kan komma att bryta krypton som idag är säkra, certifikatservrar kan korrumperas, en person kan göra sina egna signaturer och sigill ogiltiga genom att publicera sin hemliga nyckel.

1.2 Identifiera aktören

Kan man söka reda på och identifiera en person som begått en brottslig handling via Internet? Svaret på den frågan beror både på hur mycket och skickligt den sökte ansträngt sig att hindra identifiering och på om handlingen utförs mer än en gång. En skicklig och förslagen person kan koppla sig från dator till dator i flera steg i olika länder. För att spåra den skyldige, kan man behöva koppla på nya loggningar i de missbrukade datorerna. Detta är givetvis lättare att göra om missbruket upprepas.

Ett annat problem kan vara behovet av samverkan mellan flera olika länder och att lagen kan tänkas hindra spårande. Det har t.ex. hävdats att spårande av aktören skulle vara fråga om hemlig teleavlyssning eller hemlig teleövervakning.

De flesta som missbrukar nätet är dock inte särskilt smarta och är lätta att spåra.

1.3 Filtrering

Med filtrering menas att datorn granskar dokument och sorterar eller väljer dokument åt användaren. Resultatet av filtrering kan vara:

1. Personlig filtrering för en enda person, eller filtrering för en grupp av personer, t.ex. alla vid ett företag eller i ett land.
2. Att hindra vissa personer att ta emot vissa dokument (censur), t.ex. ett land som vill hindra folk att läsa ”statsfientliga” dokument (Kina, Iran, Irak), föräldrar och skolor som vill hindra barn att ta emot ”olämplig”

information, arbetsgivare som vill hindra anställda från att ägna arbetstid åt nätsurfning, internetföretag som vill undvika åtal enligt BBS-lagen och andra liknande lagar.

3. Att hjälpa personer att hitta det mest värdefulla och mest intressanta för just dem.
4. Bortfiltrerade meddelanden kan tas bort.
5. Avsändaren kan få ett meddelande att dokumentet har sorterats bort.
6. Meddelanden kan sorteras i olika fack eller efter prioritet.

Filtrering kan utföras både i e-post och diskussionsgrupper och vid sökning av dokument på webben.

Men datorer är inte bra på att göra nyanserade omdömen om vad som är lämpligt, önskvärt, etiskt, intressant, ointressant.

1.1.1 Exempel på filtrering som kan fungera:

1. Sortera meddelanden från viss avsändare.
2. Sortera meddelanden som kommer via en viss e-post-lista.
3. Sortera meddelande, för vilka avsändarnamnet inte svarar mot någon existerande e-post-brevlåda.
4. Sortera meddelanden som är märkta med en markering av typen ”direktreklam” eller ”direktreklam: spädbarnsvård” eller ”sex- och nakenhet-snivå: 5” eller ”olämplig för barn under 12 år”.
5. Sortera bort meddelande som sänds till många olika mottagare utan logiskt samband med varandra.
6. Sortera bort meddelanden med viss ärendemening i e-post eller liknande.

1.1.2 Exempel på filtrering som kan vara svår att få att fungera:

1. Att datorn automatiskt analyserar text för att avgöra om den är pornografisk eller olämplig för barn eller strider mot någon etikregel. Erfarenhetsmässigt är detta inte särskilt effektivt och kan detta ge oönskade effekter, t.ex. pornografifilter som felaktigt filtrerar bort information om bröstcancer, därför att de detekterat ordet ”bröst”.
2. Att datorn automatiskt analyserar en bild och detekterar om den är pornografisk, t.ex. genom att mäta hur stor andel av bildytan som är hudfärgad. Erfarenhetsmässigt är detta inte särskilt effektivt och kan detta ge oönskade effekter, t.ex. pornografifilter som felaktigt filtrerar bort bilder av grisar eller av ansikten.

Som framgår av exemplen ovan fungerar filtrering bäst, om den görs på attribut som har ett standardiserat utseende, som datorn lätt kan känna igen. Filtrering för att bli av med meddelande som avsändaren vill tvinga igenom är speciellt svårt, eftersom sådana avsändare snabbt lär sig att kringgå filtreringsmetoderna. T.ex. har de flesta e-post-sorteringsprogram på nätet under våren 1998 ändrats så att de vägrar ta emot e-post med vissa karaktäristiska, som ofta utmärkte oönskad direktreklam. Detta gav en tillfällig reducering av spamming (oönskad direktreklam) men sändarna av reklamen lärde sig snabbt att ändra sina meddelanden så att de inte kändes igen av filtren.

I e-post och diskussionsgrupper är det relativt lätt att filtrera bort meddelanden från vissa avsändare, men det är svårare att bli av med andras svar på dessa meddelanden.

1.1.3 Social filtrering

En viktig variant av filtrering är s.k. ”social” eller ”kollaborativ” filtrering. Den bygger på att människor har värderat meddelanden och lagrat sin värdering i datorn. Detta liknar alltså den filtrering av information som görs av redaktörer på tidningar, bokförlag, redaktionskommittéer och andra mediaföretag. Lagringen av omdömen kan göras av medlemmar i en förening som hjälper varandra, av redaktörer vid företag som utför sådan värdering. Mest kända verksamhet av social filtrering är företag som Yahoo. Dessa väljer dock ut bara en liten delmängd av all information på nätet.

Ett annat exempel på sådan filtrering är företag i USA som erbjuder olika typer av program för att föräldrar skall kunna hindra barn från att få tag i viss information (t.ex. pornografi, våldsskildringar, bombrecept). Dessa företag bygger upp databaser, åtkomliga via nätet, över olämpliga dokument och dokumentsamlingar.

En vanlig variant av social filtrering är s.k. modererade diskussionsgrupper, där en eller flera redaktörer granskar och godkänner meddelanden innan de sänds ut. Fördel är att kvalitén på det som släpps igenom blir högre, nackdel är att tiden från det ett inlägg skrivs, tills det det blir läst, ökar från mindre än ett dygn till flera dagar, vilket hämmar interaktiviteten i diskussioner.

1.1.4 Lagstiftning och filtrering

Filtrering underlättas starkt om de som producerar dokument lagstiftningsmässigt tvingas märka vissa dokument på ett visst sätt. T.ex. finns i vissa delstater i USA lagar mot att sända pornografi till den som inte begärt det. För att undvika åtal väljer därför porr-producenterna att tydligt märka sina sidor. (Denna märkning kan göras så att den syns för filtreringsprogrammen, men inte när man läser dokumenten). Dessa märkningar kan då användas för filtrering. Se vidare avsnitt 1.1.12 nedan.

1.1.5 PICS – Platform for Internet Content Selection

PICS är en standard för utformning av omdömen på dokument för att underlätta filtrering. PICS-märken kan sättas av den som producerar ett dokument eller av andra som gör värderingar av dokument. Fördelen med PICS är att olika programvaror lätt kan samverka i filtreringen: E-post-program kan t.ex. filtrera på PICS-märken även om avsändare och mottagare använder olika programvara.

PICS tillåter olika slag av skalor för att märka dokument. T.ex. finns en skala, som graderar dokument i en skala för sex och nakenhet, en för våld och en för ovårdat språk. En annan skala graderar dokument efter vid vilken ålder de anses lämpliga för barn.

PICS har mest använts för att hindra barn läsa det som anses olämpligt för dem, men kan mycket väl användas för andra former av filtrering.

1.4 Innehåll i etikregler

Olika etikregler som utfärdats av olika organisationer har ibland varit mycket olika. Det har t.ex. funnits etikregler för datornät som förbjudit politisk diskussion i nätet! Man kan skilja på:

Etikregler	Regler för vad som bör tillåtas för att undvika skador
Etikettregler	Konventioner för hur man skall bete sig, som lika väl kunde se olika ut, men är praktiska därför att om många använder samma konventioner, begriper man varandra bättre.

Typiskt exempel på en etikregel kan vara: Om du blir arg över något som någon skrivit på nätet, vänta i så fall till nästa dag innan du svarar. Typiskt exempel på etikettregel är att man skall använda en speciell märkning ":-)", när man skriver något som är avsett att vara skämtsamt eller ironiskt.

Ibland har etikregler tillkommit för att komma tillrätta med begränsningar i nätets funktion. En etikregel att man inte skall sända samma meddelande till flera distributionslistor, hade t.ex. inte varit nödvändig om programvarorna för e-post bättre kunde samordna, hos mottagarna, flera kopior av samma meddelanden som anlänt olika vägar. Man kan här fråga sig om man inte borde förbättra tekniken istället för att reglera den med etikregler.

1.5 Metoder för självreglering

Självreglering kan ske genom information och frivillig påverkan, eller genom andra slag av tvångsåtgärder än via polis och domstol.

Frivillig påverkan kan ske genom utbildning, utfärdande av etikregler, föreskrifter till nya Internet-användare, speciell information till speciella grupper. Ett problem med denna frivilliga påverkan är att det kan vara svårt att få folk att läsa den. De innehållsrikaste och mest genomtänkte etikreglerna, t.ex. de som IETF (Internet Engineering Task Force) har utarbetat i RFC 1855 "Netiquette Guidelines"[1] tenderar att bli långa och utförliga, svåra att lära sig och komma ihåg.

Andra tvångsåtgärder än via polis och domstol kan vara att en Internet-leverantörer stänger av, eller hotar med att stänga av, ett konto. Det kan vara att den som ansvarar för en server raderar dokument i servern, den som driver ett web-hotell kan t.ex. radera sina kunders dokument, om de strider mot web-hotellets regler, eller den som driver en newsserver kan radera artiklar i servern.

1.1.6 Rough Justice

Med orden "Rough Justice", som kanske kan översättas som "vildavästernrättvisa", menas åtgärder för att utan stöd av polis och domstol bekämpa missbruk av näten. Den kan innefatta sådant som "mail bombing" (att man bombarderar den man vill straffa med e-post så att hans/hennes e-postbrevlåda blir överfull). Det är för att skydda sig mot mail bombing, som spammare (sändare av direktreklam via e-post) oftast anger förfalskade avsändaradresser. Det har förekommit att spammare som avsändare angivit personer de ogillat, och dessa har då oskyldigt drabbats av mail bombing.

1.1.7 Cancelbots i Usenet News

I Usenet News har det utvecklats en serie av samverkande åtgärder för att motverka missbruk av nätet utan inblandning av rättsliga myndigheter. Historien om detta kan ge ett exempel på hur man kunnat utveckla ett system av åtgärder mot missbruk.[2]

Det hela började med att Usenet News sedan länge haft ett kommando (*Cancel-kommandot*), med vars hjälp en författare kan radera sina egna meddelanden. Detta kommando är märkt med författarens namn och verkställs bara om detta är samma namn som författaren av det meddelande som skall raderas.

När Usenet News växte och Internet spreds utanför forsknings- och universitetsvärlden, började nätet missbrukas, bl.a. för oönskad direktreklam. Någon person satte då upp ett program (*the Cancelmoose*) som detekterade oönskad direktreklam genom att samma meddelande sänts till många olika nyhetsgrupper. Programmet sänder ut Cancel-kommandon, som felaktigt uppges vara skrivna av författaren till det meddelande som skall raderas. Att göra så blev allmänt accepterat. Men andra upptäckte möjligheten att radera andras meddelanden, och upprättade verksamheter för att radera sådant de ogillade. Ett välkänt exempel är den s.k. scientologykyrkan, som raderade kritik mot sig själva.

För att skydda sig mot detta började de som driver newsservar att ställa nya krav på vilka Cancel-kommandon som skulle utföras. Dessutom upprättades en tjänst av s.k. re-mailers, program som åter la in meddelanden som raderats med förfalskade Cancel-kommandon.

1.1.8 Usenet Death Penalty

De som driver Newsservrar samarbetar kring åtgärder för att förebygga missbruk[3]. Om en newsserver vägrar att medverka i detta samarbete, riskerar denna server att kopplas bort från Usenet News[4]. En sådan uppkoppling kallas Usenet Death Penalty. Det har visat sig att den mycket snabbt (inom några dagar) får den skyldige att hålla sig till reglerna, för att åter få komma med i gemenskapen. Detta är alltså en rättsutövning som utförs internationellt och utan medverkan av rättsväsendet. Reglerna för vad man vill reglera utvecklas successivt, men de är mycket snäva. Av hänsyn till yttrandefriheten ingriper man bara mot mycket uppenbara och flagranta missbruk.

1.1.9 Vem har rätt vidta tvångsåtgärder i Sverige?

Man måste skilja på den som tillhandahåller nättjänster, och den som tillhandahåller lagring av data, t.ex. i form av webhotell (även om samma företag givetvis kan erbjuda båda tjänsterna). T.ex. gäller *BBS-lagen*[5] bara den som lagrar data.

Det är tveksamt om en Internetleverantör i Sverige har rätt att vidta sådana tvångsåtgärder annat än om de stöds av särskild lag, t.ex. BBS-lagen. Och BBS-lagen gäller bara för vissa i lagen uppräknade brott (uppvigling, hets mot folkgrupp, barnpornografibrott, olaga våldsskildring och intrång

i upphovsrätt). Den gäller *inte* för någon allmän etiköver-vakning, och *inte* för t.ex. förtal, bedrägeri, stämpling eller kränkning. *Telelagen*[6] **§** 16 förbjuder troligen teleoperatör att vidta sådana åtgärder gentemot sina kunder. Inte heller BBS-lagen torde kunna åberopas av en Internetleverantör gentemot den som har en egen webserver kopplad till leverantörens nät. Och detta kommer inom något eller några år att vara mer än hundratusen olika webservrar, många ägda av privatpersoner eller småföretag.

Om Internetleverantörer skulle ha rätt att vidta tvångs-åtgärder mot verksamhet de anser vara etiskt klandervärt, kan det bli svåra avvägningar mellan skyddet av yttrande-friheten och sådan etikhöjande verksamhet. Man kan fråga sig om det är Internetleverantörerna som bör göra sådana avvägningar, och inte åklagare och domstol.

1.6 Vad är bäst, självreglering eller lagstiftning?

1.1.10 Problem med lagstiftning

Erfarenheterna av lagstiftning för att bekämpa missbruk av Internet är dålig. Lagarna har baserats på dålig förståelse för hur nätet fungerar, och de tillämpas i stor utsträckning inte. *Datalagen*[7] och dess ersättare *Personuppgiftslagen*[8] är t.ex. så skriven att praktiskt taget hela Internet skulle vara förbjudet om lagen tillämpades bokstavligt. Men så har inte skett annat än sporadiskt när datainspektionen velat komma åt någon som de ogillar. Jag hör själv till en av de drabbade, vårt KOM-system förbjöds 1978 av datainspektionen[9], och förbudet upphävdes 1979 om vi lovade att inte diskutera bl.a. politik och religion. Vi fortsatte dock att diskutera politik och religion i strid med datainspektionens föreskrifter, och inget gjordes för att beivra detta. Datainspektionens agerande i detta och andra liknande fall är märkligt med tanke på att *grundlagen*[10] speciellt föreskriver skydd just för rätten att diskutera politik och religion.

När BBS-lagen skrevs sökte utredarna kontakt med Internetanvändare. Trots detta innehåller lagen en del underligheter och motsägelser och kan bli svår att tillämpa i praktiken.

Ett problem med lagstiftning är också att den ofta inte hinner följa med i den tekniska utvecklingen, och att den inte smidigt kan anpassas efter nya förhållanden på nätet.

Ännu en svårighet med lagstiftning är Internets internationella karaktär där olika lagar i olika länder kan bli inblandade.

1.1.11 Problem med självreglering

Självreglering utan tvångsmedel kan fungera i en verksamhet med ett fåtal stora aktörer. Det blir svårare att genomföra med miljontals aktörer, som vi har i Internet. Den väsentliga sanktionen är att en internetleverantör kan stänga av anslutningen för den som missbrukar nätet. Men det är tveksamt om detta är tillåtet enligt svensk lag. Under alla omständigheter måste stor hänsyn tas till yttrandefriheten om man vill bedriva en sådan verksamhet.

I USA har denna metod för självreglering (avstängning från Internetanslutning) använts för att bekämpa spamming, men det har bara varit begränsat framgångsrikt.

1.1.12 Samarbete mellan lagstiftning och självreglering

Man kan tänka sig ett samarbete mellan lagstiftning och självreglering. Detta kanske är den bästa lösningen. Lagen kunde klargöra vilka rättigheter en Internetleverantör har att stänga av den som missbrukar nätet.

Ett annat bra exempel är bekämpande av spamming (oönskad direktreklam i bl.a. e-post). Om man lagstiftar om att all direktreklam skall vara märkt med speciell ”reklam”-märkning, eller ännu hellre reklam-märkning som även anger bransch, t.ex. ”Reklam: Bilar”, skulle det bli mycket enklare att filtrera bort oönskad direktreklam automatiskt. Det är viktigt att reklammärket och branschbeteckningen har ett standardiserat utformande, så att filterprogram lätt kan känna igen det. Sådan reklammärkning vore önskvärd även i andra Internettjänster, t.ex. Usenet News och World Wide Web.

1.1.13 Internationellt samarbete

För att bli verkningsfull måste självreglering ha stöd av användare i olika länder. Internationellt samarbete är därför nödvändigt. Med tanke på den bristande kompetens, som lagstiftare ofta haft för nätets funktion, är det viktigt att sådant internationellt samarbete sker i samverkan med personer med kompetens om hur tekniken fungerar och används. Jag tycker att den bästa organisationen för att hantera sådant internationellt samarbete vore IETF[11] (Internet Engineering Task Force), på grund av organisationens höga kompetens, men det är inte säkert att IETF är villigt att medverka.

Referenser

HTML-versionen av detta dokument på URL http://www.dsv.su.se/~jpalme/society/etikteknik.html har utförligare länkar till andra dokument av intresse.

---

1 RFC 1855 ”Netiquette Guidelines” (http://ftp.sunet.se/pub/Internet-documents/rfc/rfc1855.txt)

2 http://www.ews.uiuc.edu/~tskirvin/faqs/cancel.html

3 http://www.cybernothing.org/faqs/net-abuse-faq.html

4 http://www.stopspam.org/usenet/faqs/udp.html

5 BBS-lagen, 1998:12, http://www.notisum.se/rnp/sls/lag/19980112.HTM

6 Telelagen, 1993:597, http://www.notisum.se/rnp/sls/lag/19930597.HTM, § 16.

7 Datalagen, 1973:289, http://www.notisum.se/rnp/sls/lag/19730289.HTM

8 http://rixlex.riksdagen.se

9 http://www.dsv.su.se/~jpalme/s1/history-of-KOM.html

10 Regeringsformen, 1974:152, http://www.notisum.se/rnp/sls/lag/19740152.HTM, 2 kap. § 12.

11 IETF, Internet Engineering Task Force, http://www.ietf.cnri.reston.va.us/.